Optimizing DSL Network Through New Architectures Level 2 Communication Networks

A. Boava and Y. Iano

Abstract— **The purpose of this paper is to propose a minor change in the conventional model to build VPN level 2.A new architecture for low cost using DSL technology in tanden with frame relay or ATM technologies aiming the formation of level 2 networks is presented in this document, in order to turn backbone feasible and optimize by making use of stablished DSL access which is operated by local telecom operators which provide applications through VPNs. The architectures of traditional VPNs level 2 will be then compared with the new proposed level 2 VPN by DSL access through OPNET simulator. Simulation shows us that by using the new proposed model along with DSL access, VPN´s provide an equivalent performance with Frame Relay or ATM access, assuring levels of service well defined, insurance and low cost.**

Keywords— **VPN, DSL, FRF-8, QoS e ATM.**

I. INTRODUÇÃO

INICIALMENTE, as redes de DSL foram desenvolvidas basicamente para o serviço de acesso à internet residencial em alta velocidade. Mas, no estágio atual dessa tecnologia, vários fatores estão levando as operadoras de telecomunicações a disponibilizar novos serviços sobre a tecnologia DSL. Entre alguns desses fatores podemos citar a migração dos usuários de internet que usa a tecnologia DSL para o acesso à internet sem fio e esse artigo irá propor uma nova arquitetura que pretende otimizar a planta de cabos DSL já instalados pelas operadoras há anos através de construção de VPNs de nível 2 sobre DSL.

A arquitetura convencional do ADSL com acesso a internet utiliza o protocolo PPPoE entre um roteador do usuário e o DSLAM que se conecta ao backbone internet. Nessa arquitetura todo o tráfego entre o roteador do usuário e a internet é do tipo best effort (melhor esforço). Nenhum trabalho ainda investigou as possibilidades de construir uma VPN de nível 2 equivalente ao ATM e frame relay com acesso ADSL de baixo custo e sem conectividade com a internet publica.Todas as propostas apresentadas até então baseiam-se nesse modelo sobre a internet diferentemente da proposta que será apresentada nesse artigo.

Até o final de 2007, aproximadamente todas as VPNs de nível 2 no Brasil utilizavam a tecnologia frame relay e ATM[3]. Nesse modelo, cada rede do ambiente do usuário tinha um roteador, que era conectado, através de enlaces ponto a ponto, a outro roteador remoto do usuário. As redes ATM e FR apresentam dois grandes problemas que limitam o desenvolvimento em larga escala do serviço de VPN que são: a complexidade e o alto custo dos acessos frame relay e ATM [6], mas apresentam como vantagens um elevado nível de QoS e Segurança.

Diferente das arquiteturas tradicionais de projeto de redes de comunicação de nível 2,a proposta apresentada nesse trabalho aproveita a rede DSL disponível das operadoras de telecomunicações aliado com o baixo custo dos modems DSL para então formar uma arquitetura completa de baixo custo, com QoS e segurança equivalente as redes de nível 2 tradicionais.

A motivação para a nova arquitetura aqui proposta é o alto custo para formar uma rede de nível 2 com QoS e segurança através da tecnologias tradicionais e a ociosidade da rede DSL em função da migração para outros serviços.

Em Davie, Bruce e Y.Rekhter [6,9], são avaliados os aspectos mais importantes da segurança em redes de comunicação que utilizam as tecnologias ATM e frame relay. São apresentados os mecanismos de segurança baseados em CVP (Circuitos Virtuais Permanentes) e DLCI (Data-Link Connection Identifier), esses mesmos mecanismos serão aplicados na nova proposta, mas com acesso DSL.

Na tentativa de oferecer níveis de QoS às redes IP próximos ao ATM e Frame Relay, foram propostas várias arquiteturas, sendo que as principais são IntServ [12] e DiffServ [12,13]. A arquitetura IntServ apresenta problemas de escalabilidade, limitando-se a redes de pequeno a médio porte. DiffServ, por outro lado, provou ser bastante escalável, pois a maior parte do trabalho é feita na borda e, consequentemente, não precisa manter qualquer estado de microfluxo no núcleo, como no caso da arquitetura IntServ.

Rong Ren, Deng-Guo Feng e Ke Ma [9] apresentam uma proposta de IPSec sobre MPLS para prover segurança contra o ataque de usuário da mesma VPN e, como MPLS não utiliza nenhum tipo de criptografia entre o CE e PE, os autores sugerem a utilização de IPSec em conjunto com MPLS para aumentar o nível de segurança com a implementação de criptografia. É importante dizer que o custo de solução aumenta significativamente com a implementação de IPSec. De acordo com os autores, há quatro formas de implementar segurança em uma VPN: Tunelamento, Criptografia, Gerenciamento de chaves e Autenticação. É importante destacar que a proposta dos autores é baseada em IPSec de CE a PE, enquanto este artigo sugere uma forma de construção de VPNs baseadas somente em túneis de nível 2 com acesso DSL.

Esse artigo faz uma revisão da arquitetura para prover serviço de VPNs e mostra o resultado de simulação de uma nova proposta de VPN nível 2 baseada em DSL . O artigo se propõe viabilizar uma nova arquitetura de VPNs de nível 2 de baixo custo através da utilização de acesso DSL e de desempenho e segurança equivalente ao ATM e Frame Relay

A. Boava, Universidade Federal de Santa Catarina, Florianópolis, Brasil, adao.boava@ufsc.br

Y. Iano, Universidade Estadual de Campinas, Campinas, Brasil, yuzo@decom.fee.unicamp.br

através da FRF-8 [5]. A Seção II contém uma breve descrição das principais arquiteturas das VPNs nível 2 e as motivações para construir de VPNs de nível 2 com acesso DSL. A Seção III acrescenta informações de QoS em VPNs. A Seção IV apresenta os novos cenários da arquitetura proposta. A Seção V apresenta os testes de desempenho realizados. A Seção VI explora os resultados obtidos e finalmente a Seção VII apresenta as conclusões.

II. Modelos de Arquiteturas das VPNs

As VPNs descrevem como construir uma rede fechada sobre uma infra-estrutura pública, normalmente a internet. Quando utiliza a internet essas VPNs são chamadas de nível 3, nesse caso garantir a segurança e a qualidade de serviço são os principais desafios da VPNs de nível 3. Quando a infra-estrutura utilizada para construir uma VPN fechada são as redes ATM e Frame Relay, essas são chamadas de VPNs de nível 2, essas VPNs apresentam um elevado nível de qualidade de serviço e segurança, mas um elevado custo. As VPNs e as tecnologias utilizadas para implementar se relacionam pela QoS (quality of Service) ofertada, segurança e o menor custo.

Para qualquer provedor de serviços de VPNs, existe sempre a necessidade de desenvolver VPNs que satisfaçam os requisitos da aplicação do usuário e um compromisso entre a QoS, segurança e os custos para implementar.

A. Arquiteturas tradicionais de VPNs de nível 2

Esse tipo de arquitetura apresenta alguns problemas que limitam o desenvolvimento em larga escala do serviço VPN que são a complexidade e principalmente o alto custo dos acessos frame relay e ATM [6,8].

A complexidade é devido a grande quantidade de CVPs para configurar uma rede ATM ou Frame Relay, essa complexidade é proporcional a quantidade de sites (n) ao quadrado da VPN ($n^2/2$) para configurações mesh, conforme a equação 1, onde n é o número de sites da VPN.

$$CVP = \frac{n!}{(n-2)!2!}$$

$$CVP = (\mathrm{n}^2 - n)/2$$

$$n \to \infty$$

$$CVP \cong \mathrm{n}^2 / 2 \qquad (1)$$

O alto custo das tecnologias ATM e Frame Relay também é um fator que inviabiliza a sua utilização em alta escalabilidade, principalmente em segmentos de pequenas e médias empresas.

Entretanto, as soluções de nível 2 construída através de frame relay e ATM apresentam duas grandes vantagens que são o alto nível de qualidade de serviço (QoS) e a segurança.

Nesse tipo de implementação, conforme a Fig. 1, todas as conexões são realizadas ponto a ponto através de CVPs. A rede frame relay ou ATM é totalmente transparente aos protocolos de roteamento, o que tem importante impacto se o usuário decidir mudar o protocolo de roteamento, pois a operadora não terá nenhum conhecimento da troca.

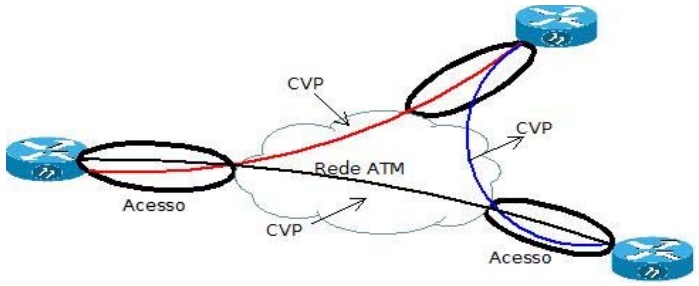

Figura 1. Topologias de VPNs com acesso frame relay e ATM.

B. Soluções de VPNs de nível 3

A primeira alternativa as VPNs ATM e frame relay de alto custo, foi a construção de VPNs com túneis IPSec sobre a rede pública internet. O usuário contratava um acesso ADSL de um provedor qualquer e configurava um túnel IPSec sobre a internet pública. Essa alternativa apresenta um baixo custo, pois utiliza um acesso ADSL, mas apresenta alguns problemas que são os mesmos problemas intrinsicos da internet pública que são a qualidade de serviço (QoS) e segurança.

C. O Fórum de Frame Relay (FRF)-8

Esse fórum publica acordos da execução ou padrões para que as redes frame relay promovam a interoperabilidade entre os protocolos frame relay e ATM. A proposta desse artigo utiliza a facilidade da FRF-8 para formar redes de comunicação de nível 2. Nessa nova proposta três elementos são utilizadas: Modem DSL, Roteador com protocolo ATM e Roteador com protocolo Frame Relay[5].

A entrega de serviços de VPNs através da rede de acesso DSL exige mais recursos de rede que a entrega dos serviços tradicionais de internet em alta velocidade, pois enquanto esta utiliza o protocolo PPPoE entre um roteador do usuário e o DSLAM que se conecta ao backbone internet, fazendo que todo o tráfego entre o roteador do usuário e a internet seja do tipo best effort (melhor esforço), aquela utiliza o protocolo PPPoA.

Em função de demandas por VPNs seguras com alto desempenho e baixo custo e objetivando ampliar suas opções de meios de acesso para formar VPN com baixo custo, os pesquisadores e as empresas de telecomunicações iniciaram um processo de investigação da possibilidade de desenvolvimento de um nova arquitetura que permita otimizar a utilização da planta de DSL já instalada. Essa nova proposta será baseado em acessos ADSL combinados com as outras tecnologias, tais como ATM e frame relay.

III. Arquiteturas de QoS das VPNs

Apesar deste trabalho focar em avaliações de uma proposta de construção de VPN nível 2, foi construído um perfil do

usuário que contém aplicações de voz (VoIP), e-mail e FTP. Essas aplicações devem ser atendidas pela rede de comunicação de acordo com a QoS. O objetivo de adicionar essas aplicações foi de tornar o cenário de simulação mais próximo de uma VPN real que transporte diversos tipos de tráfego. As VPN de nível 3 baseada em internet convencional oferece um serviço de melhor esforço a todas as suas aplicações, ou seja, ela não garante nenhum nível de qualidade de serviço (QoS) que uma aplicação receberá. A QoS (Quality of service) pode ser definida com parâmetros específicos necessários para uma determinada aplicação do usuário. Esses parâmetros de serviço podem ser definidos em termos de largura de banda, latência, jitter e perdas de pacotes, de forma que a aplicação possa obter uma melhor qualidade ao longo da rede. A tabela1 mostra os requisitos para algumas aplicações típicas e que serão simuladas sobre as redes convencionais e sobre a nova proposta para comparação e análise dos resultados.

TABELA I. REQUISITOS DE ***QOS*** PARA AS APLICAÇÕES.

Aplicações Típicas	Requerimentos de QoS			
	Bandwidth	Latência	Jitter	Perda de Pacote
e-mail	Baixo	-	-	-
FTP	Altas rajadas	-	-	-
VoIP	Moderada	Crítica	Crítica	Sensível

Para o tráfego de VoIP,no que diz respeito à aplicação de voz, escolhemos o modelo de telefonia sobre o protocolo IP (VoIP) que utiliza a qualidade de voz do PCM (PCM Quality Speech).

Para o tráfego de e-mail foi utilizado uma distribuição constante com o tamanho de e-mail (E-mail size) de 100 Kbytes.

Para o tráfego de FTP foi usado uma distribuição constante com média de 100 Kbytes

A seguir será apresentado uma pequena definição dos parâmetros de QoS [10]:

A. Jitter

De acordo com a RFC 3550, o jitter é definido como uma estimativa da variação estatística do tempo entre chegadas dos pacotes RTP (Real-Time Transport protocol). Este parâmetro é importante para as aplicações executadas em rede cuja operação adequada depende, de alguma forma, da garantia de que as informações (pacotes IPTV ou VoIP) sejam processadas em períodos de tempo bem definidos.

B. Dellay

De maneira geral, o atraso da rede pode ser entendido como o somatório dos atrasos impostos pela rede e pelos equipamentos utilizados na comunicação. Do ponto de vista da aplicação, o atraso resulta em um tempo de resposta (tempo de entrega da informação, ou pacotes) para aplicação.

C. Loss – Peda de Pacotes

As perdas de pacotes são normalmente ocasionadas por três fatores: o enlace físico, que pode não permitir a transmissão dos pacotes; congestionamento; e ruído, que pode corromper os pacotes. Os enlaces físicos dificilmente oferecem problemas, pois possuem um elevado índice de disponibilidade. Portanto, a causa principal das perdas de pacotes em rede é o congestionamento. Essas perdas de pacotes têm influencia na qualidade de serviço e pode causar o estouro de buffers em roteadores e switchs .

D. Vazão

A vazão (banda) é o parâmetro mais básico da QoS e é necessária para a operação adequada de qualquer aplicação. Em termos práticos, as aplicações geram vazões que devem ser atendidas pela rede.

IV. NOVA ARQUITETURA PROPOSTA

Através da combinação acima aproveita-se toda a capilaridade da malha de acesso banda larga ADSL instalada pelas operadoras, em conjunto com as redes ATM e frame relay, para prover conectividade entre vários sites da rede, similarmente a um serviço VPN de nível 2 baseado somente em tecnologia frame relay e ATM.

A principal aplicação da proposta desse artigo é a interligação das LANs (Local Area Network) das empresas de forma simplificada e de rápida implementação para tráfego multimidia. A topologia das propostas que utilizam a combinação dessas três tecnologias será sempre uma rede com topologia em estrela, com um site de concentração conectado através das tecnologias frame relay e ATM, podendo os outros sites ser ADSL, frame relay ou ATM.

A implementação dessa nova proposta consiste na instalação nos sites de um CPE com interface WAN que trabalhe com os protocolos ADSL, frame relay e ATM. Deste CPE é configurado um PVC (Permanent Virtual Circuit) para que este possa se comunicar com os demais dispositivos que compõem a VPN. Nesse PVC, é possível oferecer a algumas aplicações QoS (Quality of Service), de acordo com o perfil de tráfego do usuário. No caso da QoS, os mecanismos adotados devem ser de nível 3 e devem atuar sobre cada pacote IP em trânsito pelo CPE; portanto, devem suportar as características mais comuns. Normalmente, é configurado nesse PVC o parâmetro CIR, que se refere à velocidade garantida, e o parâmetro EIR, que especifica a velocidade máxima que o acesso suporta.

O CPE de cada site pertencente a uma VPN poderá ser gerenciado local ou remotamente. Para a gerência a distância, pelo menos um PVC deverá ser configurado entre os centros de gerência e um dos CPEs dos sites da VPN. Uma vez tendo conectividade com um dos elementos da VPN, todos os demais podem ser acessados. Como regra básica, o CPE a ser conectado ao centro de gerência deverá ser o do ponto de concentração[6].

A. Nova Arquitetura com concentrador ATM e acessos DSL

Em função de a própria tecnologia ADSL já fazer uso do ATM como protocolo de nível 2, foi observado através de simulações que sua integração com outros CPEs que possuam interface ATM ocorre naturalmente. Esse cenário é formado com vários sites remotos utilizando conexões físicas ADSL e uma localidade conectada à rede ATM através de um enlace ATM, como mostrado na Fig. 2 [1,2,6].

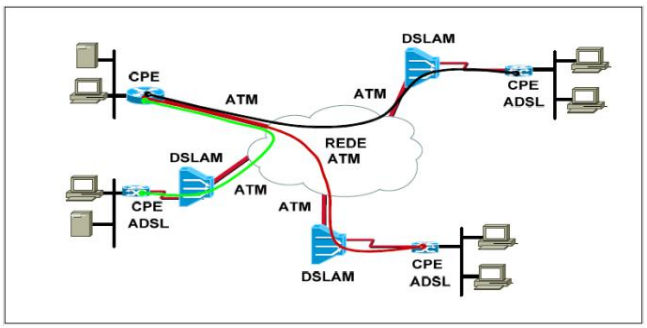

Figura 2. Topologia com concentrador ATM e acessos ADSL.

A conectividade entre os vários sites foi alcançada através da configuração de circuitos virtuais permanentes (PVC) ATM entre os sites com CPEs ADSL e o site concentrador com CPE ATM. Nesse cenário que foi simulado, o CPE ATM ficou como um site de concentração para as várias localidades remotas numa topologia em estrela e poderá usar qualquer tipo de interface ATM para conectar-se à rede, podendo ser E1, E3 e STM-1[6].

B. Nova Arquitetura com concentrador Frame Relay e acessos DSL

Em função da própria tecnologia ADSL já fazer uso do ATM como protocolo de nível 2, e da possibilidade de interoperabilidade entre o frame relay e o ATM através do padrão FRF.8 (ATM and frame relay Service Interworking), o artigo investigou a possibilidade do provisionamento de um PVC entre um CPE ADSL e um CPE frame relay.Através desse padrão, a rede ATM efetua um mapeamento entre os PVCs de uma interface ATM (VPI/VCI) e seus atributos para DLCIs e respectivos atributos em uma interface frame relay. Para os CPEs frame relay e ADSL, todo o processo de mapeamento descrito acima se passou de forma transparente, ou seja, não houve a necessidade de qualquer configuração especial para operação [1,2,6]. A Fig. 3 apresenta a topologia com o concentrador Frame Relay e os acessos ADSL.

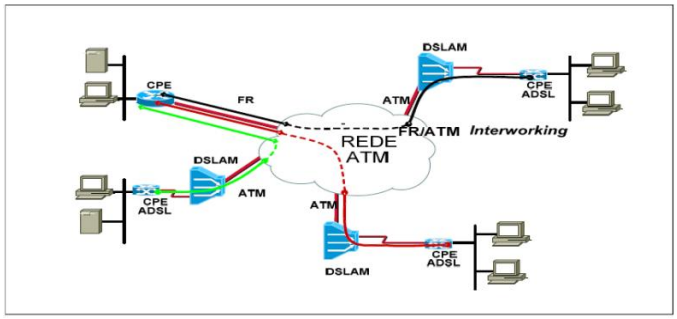

Figura 3. Topologia com concentrador Frame Relay e acessos ADSL.

A classe de serviço implementada em nível 2 consiste na configuração de parâmetros ATM associados aos PVCs da interface ADSL do CPE. Os parâmetros mais comuns medidos através do OPNET foram os relacionados a controle de banda, delay e variação de delay (jitter). Nesse tipo de controle, todo o tráfego pertencente a um dado PVC é tratado da mesma maneira, ou seja, o CPE não se preocupa efetivamente com fluxos de pacotes IP de diferentes aplicações. É importante salientar que, durante o provisionamento de uma determinada solução, os elementos da rede ATM deverão ser configurados de forma adequada para que não se tornem gargalos durante os períodos de pico de tráfego, afetando as aplicações dos usuários finais. Foi possível verificar durante a simulação que com o OPNET o desempenho da VPN com acesso ADSL para o tráfego de dados apresentou desempenho equivalente a frame relay e ATM, mas para o tráfego de vídeo sugerem-se alterações no DSLAM. Essas alterações podem ser a priorização dos pacotes de vídeo pelo DSLAM no instante em que esses pacotes forem processados.

Somente essas duas alternativas devem-se à impossibilidade constatada durante as simulações com o OPNET de um acesso ADSL se conectar com outro acesso ADSL.

V. SIMULAÇÃO COM O OPNET

Com base na arquitetura proposta para integração dos acessos DSL com os acessos ATM e Frame Relay, a Fig. 3 ilustra a topologia proposta para a prestação de serviço de VPNs de nível com acesso DSL baseados na FRF.8.

Nesse tópico serão apresentados os ambientes de simulação que foram desenvolvidos através do software de simulação computacional OPNET para que sejam coletados os principais parâmetros da QoS de cada topologia desenvolvida para posterior comparação no próximo tópico.

O software OPNET IT, em sua versão acadêmica, é uma ferramenta computacional utilizada para modelar redes em um ambiente virtual, analisar e predizer seu desempenho, incluindo aplicações, usuários e tecnologias de redes e protocolos. É usado por milhares de organizações comerciais, universidades e órgão do governo ao redor do mundo [1].

A. Simulação do Ambiente Internet

Esse ambiente foi montado para simular uma VPN convencional com acesso DSL sobre a internet publica. Para uma comparação justa com a nova proposta foi configurado a velocidade de UPLINK igual a de DOWNLIN, mas na prática sabemos que a velocidade de DOWN é sempre maior que a velocidade de UP. Para a simulação nesse cenário foram considerados acessos DSL de 2 Mbps simétricos conectados à internet convencional.

Esse ambiente (Fig. 4) representa uma VPN de nível 3 sobre a internet convencional. Os requisitos de segurança e a QoS são os problemas mais típicos de cenário. Mas, apresenta como grande vantagem o seu baixo custo.

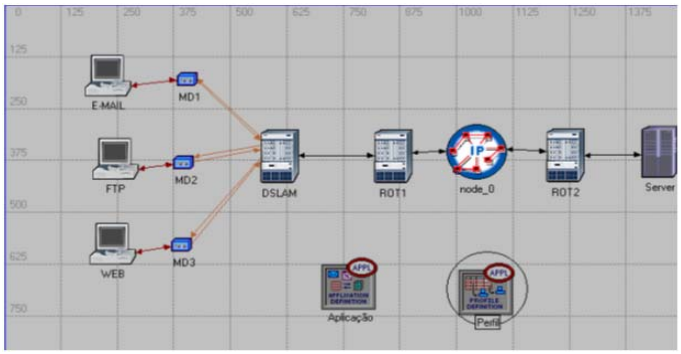

Figura 4. Simulação do ambiente Internet.

B. Simulação das topologias convencionais ATM e FR

Esse cenário representa a aplicação de voz, FTP e E-mail sobre uma VPN formada de acessos ATM e Frame Relay.

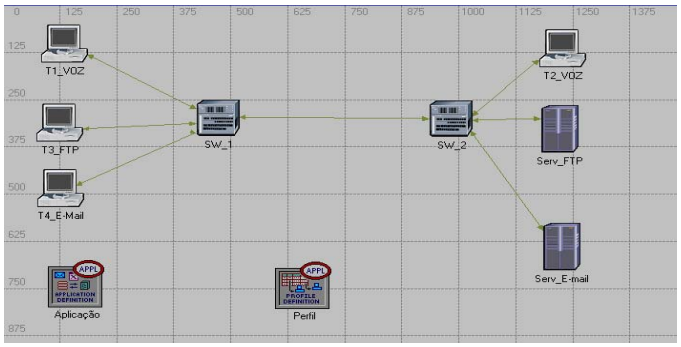

Figura 5. Topologias convencionais.

Esse cenário de simulação é constituido de roteadores ATM de 2 Mbps que conectam ao site principal/concentrador que está configurado em sua porta WAN como ATM e os sites remotos se conectam ao principal através do frame relay[11]. Esse cenário representa uma simulação típica das redes tradicionais de nível 2 que foram as mais utilizadas nas décadas de 80, 90 e em alguns paises até o final da década passada.

C. Simulação da Arquitetura proposta com acessos DSLs

Essa simulação foi desenvolvida no simulador OPNET e representa a nova arquitetura apresentada no item IV da Fig. 2. Os acessos DSL formam uma conexão virtual privada até o site concentrador ATM e com isso apresentam características semelhantes a uma conexão ATM-ATM, mas com um modem DSL [4,14].

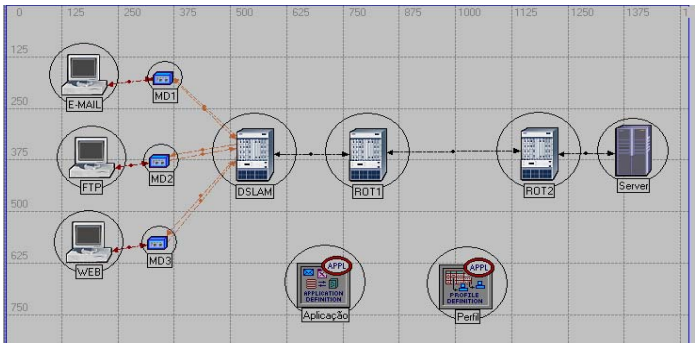

Figura 6. Simulação da nova Arquitetura proposta.

VI. COMPARAÇÃO DOS RESULTADOS

A Fig. 7 abaixo apresenta os resultados da simulação da transmissão de um mesmo arquivo sobre os três cenários anteriores. O ATM apresentou o melhor desempenho e a internet o pior desempenho. A nova solução proposta apresentou um desempenho intermediário entre as soluções ATM e Internet. A solução proposta apresenta um nível de segurança equivalente ao ATM com bom desempenho e um custo de implementação significativamente menor que o ATM. A variável medida e utilizada para análise foi o tempo de transmissão para os três cenários de um arquivo de 100kbyte.

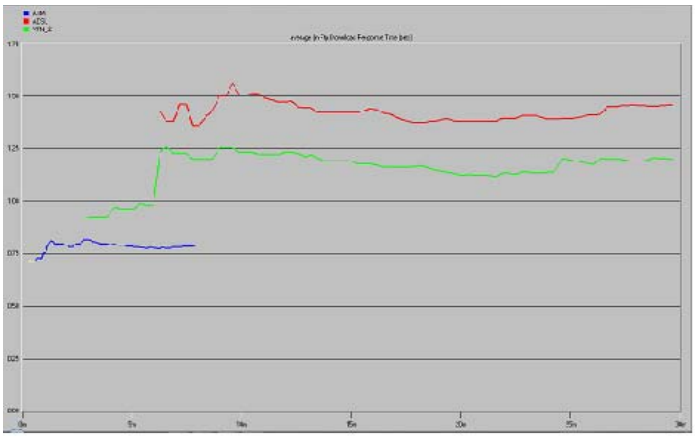

Figura 7. Resultados da simulação do tempo de transmissão para: A Nova Proposta X Internet X ATM.

VII. CONCLUSÕES

É possível para as operadoras de telecomunicações utilizar os acessos ADSL como forma de acessos de VPN nível 2 com desempenho equivalente às VPNs tradicionais Frame Relay e ATM, desde que as configurações nos acessos ADSL sejam alteradas para simétricas e com CIR igual ao EIR. Foi possível concluir que é requisito que a topologia seja em estrela, sendo que o site concentrador necessariamente precisa ser configurado como Frame Relay ou ATM. Para o tráfego de vídeo é recomendado alterações no DSLAM

VIII. REFERENCIAS

[1] Alecrim, Paulo Dias – Simulação Computacional para Redes de Computadores, 2009, Editora Ciência Moderna.

[2] Andrews S. Tanenbaum – Computer Networks, 5a Edição, 2011.

[3] Barometro Cisco/IDC de Banda larga –Dezembro de 2008, OCDE, Booz & Company e ITU/2009.

[4] Bin Ali, Z. ; Samad, M. ; Hashim, H." Performance comparison of video multicasting over Asynchronous Transfer Mode (ATM) & Multiprotocol Label Switching (MPLS) networks" – IEEE Conference Publications/2011

[5] Cisco[http://www.cisco.com/cisco/web/support/BR/104/1042/1042794_frf8modes.html] – acessado em 26/11/2014

[6] Davie, Bruce and Y.Rekhter "MPLS Technology and Applications" Morgan Kaufmann Publishers 2000

[7] I. Pepelnjak, J. Guichard, "MPLS and VPN Architectures – Volume I" Cisco Press 2002

[8] RFC - 4381 Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs) http://www.faqs.org/rfcs/rfc4381.html, /2010 – acessado em 26/11/2014

[9] Rong Ren , Deng-Guo Feng, KE MA, "A DETAILED IMPLEMENT AND ANALYSIS OF MPLS VPN BASED ON IPSEC" , IEEE 2004

[10] Ruela, J. Carlos, "Algumas análises sobre mecanismos para prover qualidade de serviço em redes multimídia", Dissertação de mestrado de 2006.

[11] Sarah Mustafa Eljack, Suhail Badawi Abdelkarim; Khartoum, Sudan; "Effect of the Interior Gateway Routing Protocols in the Multiprotocol Label Switching Networks" - 2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)

[12] Shioda, S. ; Mase, K, "Performance comparison between IntServ-based and DiffServ-based networks", Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE.

[13] S. Blake, D. Black, M. Carlson, E.Davies: "An Architecture for Differentiated Services", RFC 2475, December 1998.

[14] Yarali, A. ; Ahsant, B., Ethernet: The future network access technology; SoftCOM 2007. 15th International Conference on; IEEE Conference Publications/2007.

Adao Boava, received his B.S. degree in Electrical Engineering in 1991 from Federal University of Santa Catarina (UFSC), Florianopolis-SC, Brazil. He received his M.S. degree from the State University of Campinas (Unicamp), and M.B.A. from Foundation Getulio Vargas (FGV), São Paulo, Brazil. In 2011, he received his PhD in Telecommunication Engineering and Telematics from Unicamp, São Paulo, Brazil. Currently, he is a professor at Federal University of Santa Catarina (UFSC), Santa Catarina, Brazil. He has worked in Brasil Telecom and OI for 16 years with MPLS product development. In addition, he has worked as a consultant in different data communication projects for Monsanto, Santander, Itau, Visa, Redecard and others.

Yuzo Iano, received his PhD. in electrical engineering in 1986. Currently he is an Associate Professor in Electrical Engineering at Unicamp (State University of Campinas, Brazil). He also works at the Visual Communication Laboratory in the same University and is responsible for digital signal processing (sound and image) projects. His research interests include video and audio coding, digital video and audio compression and digital signal transmission. He is a member of IEEE.