Mapeamento dinâmico de prioridades para provimento de QoS em VPN MPLS

Marcel Cavalcanti de Castro e Walter da Cunha Borelli

***Abstract*— This work describes a proposal for the implementation of quality of service (QoS) in VPN MPLS architecture. A new system was developed based on the VPN MPLS architecture, in which an extension is being proposed to construct a dynamic mapping of VPN clients priorities into service provider network through the insertion of priority field at *vrf* table and MP-BGP protocol modifications to exchange such informations. The new proposal was specified using SDL(Specification and Description Language) through the SDL TAU Suite, and the performance analysis was realized through the Opnet Modeler simulator.**

***Resumo*— Este trabalho apresenta uma proposta de implementação de qualidade de serviço (QoS) na arquitetura *VPN MPLS*. Foi desenvolvido um novo sistema com base nessa arquitetura e sugerido uma proposta de expansão com a criação do conceito de mapeamento dinâmico de prioridades dos clientes *VPN* na rede do provedor de serviço, através da inserção dos valores de prioridade de rotas na tabela *vrf* e modificações realizadas no protocolo *MP-BGP* para troca destas novas informações. A proposta foi especificada em *SDL* (*Specification and Description Language*) utilizando o software *SDL TAU Suite*[1], e a análise de desempenho foi realizada com o uso do simulador *Opnet Modeler*[2].**

***Palavras-Chave*— VPN, MPLS, MP-BGP, Qualidade de Serviço, Sinalização, Provedor de Serviço, SDL - *Specification and Description Language*, Opnet Modeler, Análise de Desempenho.**

I. INTRODUÇÃO

Corporações e empresas estão se tornando cada vez mais dependentes de suas redes para comunicação de dados e serviços de telecomunicações. Atualmente a necessidade de interconectar redes corporativas em lugares geograficamente distribuídos tornou-se cada vez mais importante.

Com a iniciativa de alguns provedores de serviço, as organizações *itu-t* (*international telecommunications union - telecommunication standardization sector*) e *ietf* (*internet engineering task force*) reconheceram a importância de se iniciar um trabalho de padronização da tecnologia *vpn* (*rede privada virtual*). O grupo de estudo 13 do *itu-t* (*itu-t study group 13*) iniciou o processo de definição de requisitos para *vpn* [9] e a classificação das propostas técnicas de *vpn* para serviços de nível 3 sobre tecnologia *mpls* [8] em Maio de 2000. Alguns meses depois, o *ietf* iniciou a discussão que levou a criação do grupo de trabalho *ppvpn* (*provider provisioned VPN*)[16] [1] no início de 2001, incumbido de padronizar as propostas de *vpn* para serviços de nível 2 e 3. Baseado na classificação usada pelos órgãos padronizadores citados, as propostas de *vpn* são classificadas de acordo com a responsabilidade de gerenciamento; *vpn* gerenciada pelo cliente (*customer edge - ce based vpn*) ou *vpn* gerenciada pelo provedor (*provider edge - pe based vpn*).

Em 2003 o grupo de trabalho *ppvpn* do *ietf* foi dividido em dois grupos de trabalho, o *l3vpn* (*layer 3 vpn*) responsável por padronizar as propostas de *vpn* para serviços de nível 3 e o *l2vpn* (*layer 2 vpn*) responsável por padronizar as propostas de *vpn* para serviços de nível 2. A partir do grupo *l3vpn*, três propostas surgiram como padronização para *vpn*. São elas; *vpn ce-based ipsec* [10], *vpn virtual router ip* [15] e *vpn bgp/mpls ip* [4] [3].

Este trabalho está baseado na arquitetura *vpn bgp/mpls ip*, também denominada arquitetura *vpn-mpls*, onde o provedor de serviço usa o protocolo *mp-bgp* (*multiprotocol border gateway protocol*) padronizado pelo *ietf* [18] no *backbone* da rede. O protocolo *mp-bgp* troca informações de roteamento de cada *vpn* entre todos os *sites vpn* pertencentes à aquela *vpn*. A arquitetura também faz uso dos rótulos *mpls* para identificar e separar o tráfego de diferentes *vpns*, sendo possível a implementação de qualidade de serviço através do mapeamento das prioridades do cliente na rede do provedor de serviço. É importante ressaltar que este mapeamento é criado na contratação do serviço *vpn*, sendo possível alterá-lo apenas pelo provedor de serviços, ou seja um mapeamento estático do ponto de vista do cliente *vpn*.

Neste contexto, este trabalho desenvolve uma proposta em *SDL* de expansão da arquitetura *vpn-mpls* para criação de um mapeamento dinâmico das prioridades dos clientes *vpn* na rede do provedor de serviço. Logo, de acordo com as necessidades dos clientes, e levando-se em consideração os níveis de serviços contratados, o cliente *vpn* pode ao longo do tempo criar e/ou modificar prioridades de suas aplicações. Este mapeamento é implementado através da inserção de um novo parâmetro na tabela *vrf*, que representa a prioridade da rota do cliente *vpn*, e a modificação do protocolo *mp-bgp* para o transporte dos valores de prioridade de rota entre o cliente *vpn* e provedor de serviço, estabelecendo-se novos níveis de qualidade de serviço em tempo real. Baseado na proposta de expansão, foi realizado a análise de desempenho através de simulações do mapeamento de prioridades da arquitetura de serviços diferenciados implementada no cliente *VPN* na rede *mpls* do provedor de serviços.

II. ARQUITETURA VPN MPLS

A arquitetura *vpn-mpls*, também denominada arquitetura *vpn bgp/mpls ip*, define mecanismos que permitem o provedor

Marcel Cavalcanti de Castro , CPqD Telecom & IT Solutions, e Walter da Cunha Borelli, DT/FEEC/UNICAMP, Campinas, Brasil, E-mails: mcastro@cpqd.com.br, borelli@dt.feec.unicamp.br.

[1]Pacote Telelogic SDL TAU Suite 4.2 : adquirido pelo DT/FEEC/UNICAMP através do Projeto Temático - FAPESP (Proc. 91/3660-0)

[2]Pacote Opnet Modeler v9.1 : adquirido pelo *CPqD* através do Projeto de Pesquisa Redes de Próxima Geração(Projeto *NGN*)

de serviço utilizar seu *backbone IP* para prover serviços *VPN* à seus clientes. Nesta arquitetura, o protocolo *mp-bgp* (*multiprotocol bgp*) [18] é usado para distribuir informações de roteamento dos clientes *vpn*, e o *mpls* para envio do tráfego dos clientes através do *backbone* do provedor de serviço.

Nesta arquitetura, o IETF padronizou através da RFC 2858 [18] o *mp-bgp* como uma extensão do *bgp* [19] para transportar informações de roteamento de múltiplos protocolos de rede, como; IPv6 ou IPX.

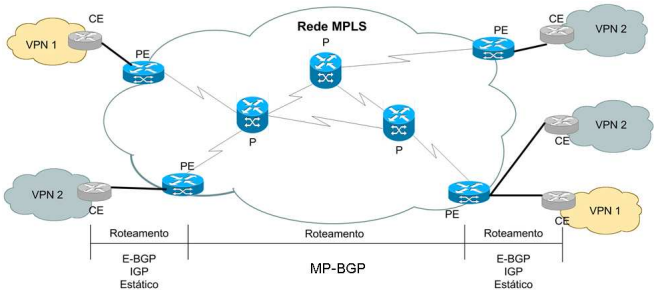

Fig. 1. Componentes da arquitetura *vpn-mpls* [14]

A figura 1 apresenta os componentes de uma arquitetura *vpn-mpls*. O equipamento de borda do cliente, também conhecido como roteador *ce* (*customer edge*) proporciona aos clientes acesso a rede do provedor de serviço. Através da conexão entre os roteadores *ce* e o provedor de serviço (Rede MPLS), o cliente *vpn* divulga suas informações de rotas à toda rede, e por onde é informado de novas rotas adicionadas à rede por outros *sites vpn*. O roteador *ce* não implementa a tecnologia *mpls*, e representa o ponto de conexão em que os pacotes entram e saem da rede do cliente *vpn*, atravessando a rede *mpls* do provedor.

O equipamento de borda do provedor, também conhecido como roteador *pe* (*provider edge*), troca informações de roteamento com o cliente *vpn* conectado ao roteador *ce* e com a rede do provedor de serviço. A troca de informações com o roteador *ce* (cliente *vpn*) ocorre através de roteamento estático ou com o uso de protocolos de roteamento, como; *rip* (*routing information protocol*), *ospf* (*open shortest path*) ou *bgp* (*exterior border gateway protocol*). Já a troca de informações com a rede do provedor de serviços ocorre através do uso de dois protocolos de roteamento, o primeiro para troca de informações de rota da rede do provedor, como: *rip* ou *ospf*, e o segundo para troca de informações de roteamento dos cliente *vpn*, através do protocolo *mp-bgp*.

Cada roteador *pe* mantém uma tabela de roteamento independente para cada cliente *vpn* diretamente conectado, denominada tabela *vrf* (*virtual routing and forwarding*). Após a instalação das rotas locais do cliente *vpn* na tabela *vrf*, o roteador *pe* troca estas informações de roteamento com outros roteadores *pe* que possuem *sites* pertencentes a mesma *VPN*.

Na figura 1, os equipamentos de núcleo do provedor, denominados roteadores *p* (*provider*), são roteadores que não estão ligados diretamente aos roteadores *ce*. Roteadores *p* exercem a função de roteadores comutadores de rótulos *mpls*, ou roteadores *lsr* (*label switching routers*), comutando os tráfegos de dados dos clientes *vpn* entre os roteadores *pe*. Como o tráfego é enviado através do *backbone mpls* usando hierarquia de rótulos, os roteadores *p* somente necessitam manter rotas para os roteadores *pe*, não necessitando manter informações de roteamento *vpn*, aumentando assim a escalabilidade no *backbone mpls* [11].

A. Qualidade de Serviço na Arquitetura VPN MPLS

Comparadas as estratégias de *vpn* nível 2 (*vpn* com uso da tecnologia *frame relay* ou *atm*), as *vpns* nível 3 herdam a flexibilidade e a simplicidade das redes *IP*, refletindo-se em uma arquitetura escalável [11], devido ao grande potencial de crescimento das redes *IP*. Deve-se ressaltar que este não é o tipo ideal de rede com suporte a qualidade de serviço [12], devido à característica implícita de melhor esforço (*best effort*) das redes *IP*.

Segundo o IETF [4], a implementação de qualidade de serviço na arquitetura *vpn-mpls* pode ocorrer com o uso da arquitetura de serviços diferenciados (arquitetura *diffserv* [17]) na rede do cliente *vpn*, combinado ao uso do *mpls* no *backbone* do provedor. Através desta combinação, as aplicações dos clientes *vpn* são tratadas na borda da rede do provedor de serviço pelos mapeamentos de prioridades da arquitetura *diffserv* no cabeçalho *mpls*, de acordo com o nível de qualidade de serviço contratado pelo cliente [5]. Alguns trabalhos como [13], [6], [7] e [12] discutem esta forma de provimento de qualidade de serviço para arquitetura *vpn-mpls*. É importante ressaltar que estes trabalhos levam em consideração um mapeamento estático entre as prioridades do cliente e os acordos de nível de serviço contratados, ou seja, o cliente *vpn* não consegue estabelecer novos níveis de qualidade de serviços em tempo real.

A medida que o cliente *vpn* possui aplicações que em determinados horários ou por determinados instantes de tempo não necessitem da mesma prioridade na rede do provedor, se torna importante a possibilidade de modificação dos parâmetros de prioridades, a fim de reduzir custos com a contratação do serviço *vpn* ou garantir qualidade de serviço a outras aplicações que antes não eram prioritárias. Com o intuito de possibilitar esta implementação, foi desenvolvido neste artigo a proposta de expansão da arquitetura *vpn mpls* possibilitando a criação e/ou modificação dos parâmetros de prioridade dos clientes *vpn* através da criação do mapeamento dinâmico de prioridades a ser utilizado pela rede do provedor de serviço.

B. Proposta de Expansão da Arquitetura VPN MPLS

Este trabalho propõe uma expansão da arquitetura *vpn-mpls* para provimento em tempo real de qualidade de serviço fim-a-fim. A proposta de expansão está baseada na possibilidade de estabelecimentos de mapeamento dinâmico de prioridades (mapeamento da arquitetura de *serviços diferenciados* no *mpls*) de acordo com a necessidade do cliente *vpn*.

A criação deste mapeamento dinâmico de prioridades entre os clientes *vpn* (roteador *ce*) e o provedor de serviço (roteador *pe*) é realizado através da inserção de parâmetros na tabela *vrf* implementada no roteador *pe*. Estes parâmetros representam as prioridades das rotas dos clientes *vpn*, e através de uma modificação do protocolo *mp-bgp* é possível a troca destes

valores de prioridade das rotas entre o roteador *ce* e *pe*. Estas modificações são realizadas através do uso da especificação formal em *SDL*.

De acordo com a proposta, a troca de informações de prioridade entre o roteador *ce* e o roteador *pe* possibilita o estabelecimento de novos níveis de qualidade de serviço através da inserção de novos mapeamentos, ou modificação de mapeamentos já existentes. Os valores de prioridade das rotas a serem informados pelo cliente *vpn* são obtidos a partir do campo *dscp* da arquitetura de serviços diferenciados, e transportados pela modificação realizada no protocolo *mp-bgp*, dentro dos estados *open sent* e *established* da maquina de estado do protocolo. As modificações dos estados visam proporcionar o estabelecimento de sessões *mp-bgp* através da troca de mensagens *keepalive* e conseqüentemente a troca de informações de prioridade de rotas através do uso do campo *route target* da mensagem *update*, entre o roteador *ce* e o roteador *pe*.

Com as informações de rotas e prioridades das rotas, o roteador *pe* monta a tabela de mapeamento de prioridades do cliente *vpn*. De acordo com a necessidade do cliente, cada mapeamento contido nesta tabela pode ter seus valores de prioridade alterados através da troca de mensagens *update*, criando-se assim o conceito de mapeamento dinâmico de prioridades do cliente *vpn*.

III. Especificação Formal da Proposta de Expansão da Arquitetura VPN MPLS

A proposta de expansão sugerido neste trabalho é representado através da especificação formal utilizando as estruturas em *SDL* de sistemas, blocos, processos e procedimentos, com orientação à objetos através do uso da ferramenta *SDL TAU Suite* [2]. A proposta, representada pelo sistema denominado *basicarquitecture-scenario2* é apresentado na figura 2.

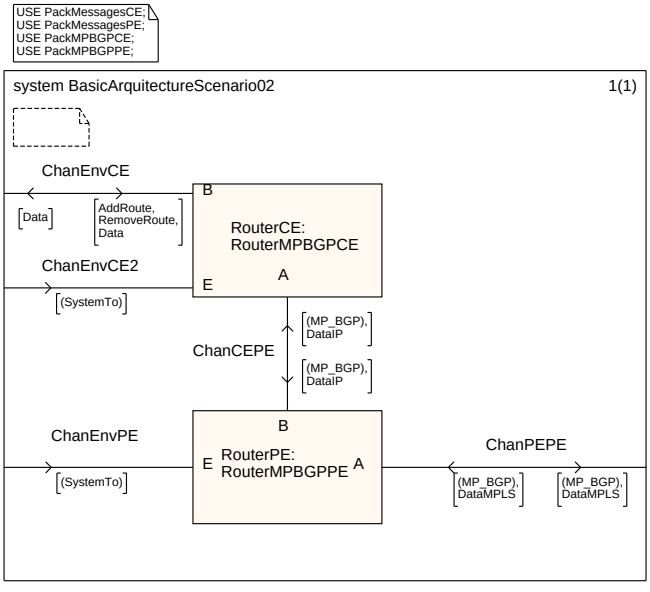

Fig. 2. Sistema *basicarquitecture-scenario2*

Os dois componentes principais da arquitetura *vpn-mpls* (roteador *ce* e roteador *pe*) são representados no sistema da figura 2 pelos blocos *routermpbgp-ce* e *routermpbgp-pe*. Através do retângulo com uma borda dobrada localizado na parte superior esquerda da figura 2, o sistema *basicarquitecture-scenario2* faz uso dos pacotes(*packmessage-ce*, *packmessage-pe*, *packbasicrouter-pe*, *packmpbgp-ce* e *packmpbgp-pe*) especificados através da cláusula USE. As interações entre o bloco *routermpbgp-ce*, bloco *routermpbgp-pe* e o ambiente externo são representados pelos canais de comunicação *chan-cepe*, *chan-envce*, *chan-envce2*, *chan-envpe* e *chan-pepe*.

O bloco *routermpbgp-pe*, que faz parte do pacote *packmpbgp-pe*, é a especificação do roteador *pe* da proposta de expansão da arquitetura *vpn-mpls*. Este bloco é responsável por trocar informações de rotas e prioridades de rotas do cliente *vpn* via protocolo *mp-bgp* com o roteador *ce* (bloco *routermpbgp-ce*) via canal *chan-cepe*, e com os roteadores *pe* pertencentes a rede do provedor de serviço, representado nesta especificação pelo ambiente externo, via canal *chan-pepe*.

Na linguagem SDL, através do uso de técnicas de orientação à objetos, é possível reutilizar especificações e redefini-las integral ou parcialmente. Redefinições de blocos e processos foram utilizadas com o propósito de se criar a proposta de expansão a partir da padronização da arquitetura *vpn-mpls*. As redefinições feitas no processo *prouter-pe* (redefinição dos estados *open sent* e *established*) visam permitir o roteador *pe* estabelecer sessões *mp-bgp* com o roteador *ce*, e através destas sessões trocar informações de prioridade sugeridas pelo cliente *vpn* através do roteador *ce*. A redefinição feita no estado *open sent* permiti o processo *prouter-pe* estabelecer sessões *mp-bgp* com o processo *prouter-ce*(roteador *ce*) e com o ambiente externo (roteadores *pe* da rede do provedor) através da troca de sinais *keepalive*. A troca de informações de prioridade de rotas se torna possível através da redefinição do estado *established*, mostrada na figura 3, que passa a tratar o campo *route target* do sinal *update* proveniente do roteador *ce* como valor de prioridade da rota.

De acordo com a figura 3, estando o processo no estado *established*, ao receber um sinal *update*, o processo verifica se existe rota a ser removida da tabela *vrf*, através da variável *droute* do sinal *update*. Se existir rota a ser removida, esta é removida através da chamada ao procedimento *vrf-uninstall*. Após a remoção da rota, o processo *prouter-pe* checa se o sinal *update* é proveniente do roteador *ce*, ou do ambiente externo, através da verificação do número do sistema autônomo do sinal *update*. Para ambos os casos a nova rota transportada no sinal *update* é instalada na tabela *vrf* (procedimento *vrf-install*), e informada ao roteador *ce* (bloco *routermpbgp-ce*) para o sinal *update* vindo do roteador *pe* (ambiente externo), ou informada aos roteadores *pe* para o sinal *update* vindo do roteador *ce* (bloco *routermpbgp-ce*).

IV. Análise de Desempenho

A análise de desempenho realizada visa estudar o comportamento das aplicações dos clientes *vpn* para cenários sem nenhuma implementação de qualidade de serviço e com a implementação de qualidade de serviço através do uso do mapeamento de prioridades da arquitetura de serviços difer-

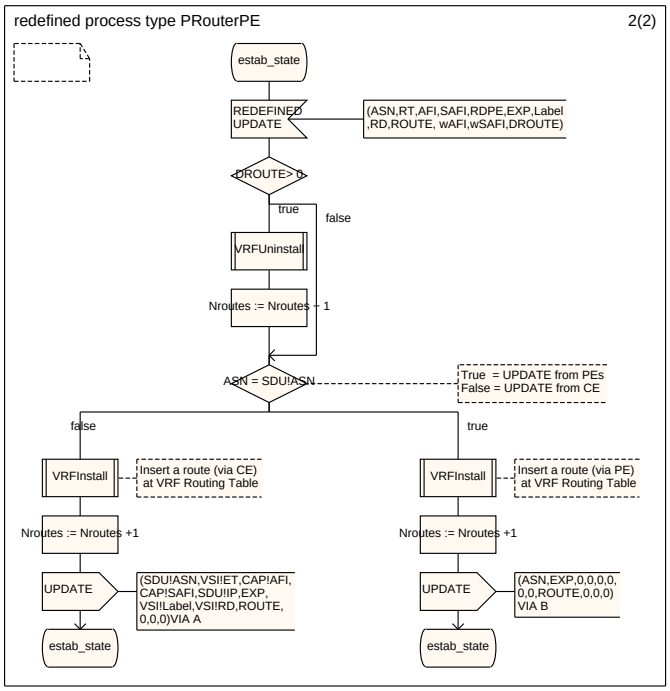

Fig. 3. Redefinição do processo *prouter-pe* - estado *established*

enciados (arquitetura *diffserv*) na rede *mpls* do provedor de serviço.

Esta análise apresenta simulações do transporte de diferentes serviços como voz, vídeo e dados, sobre uma infraestrutura de provedor baseado na arquitetura *vpn-mpls*, com e sem a implementação de qualidade de serviço. Tendo como finalidade a comparação do desempenho das aplicações frente a implementação de qualidade de serviço, utilizada na proposta de expansão da arquitetura *vpn mpls*. É importante ressaltar que os cenários simulados visam validar a proposta de expansão da arquitetura *vpn-mpls*, através do uso do mapeamento da arquitetura de serviços diferenciados nos rótulos *mpls* da rede do provedor de serviço.

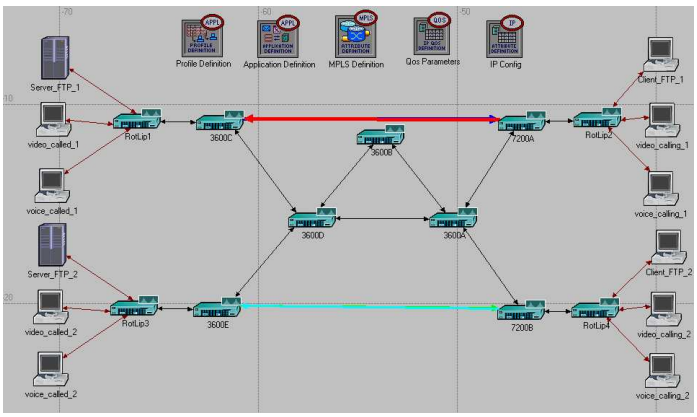

Fig. 4. Topologia da rede simulada no *Opnet*

Os cenários simulados fazem uso da mesma topologia de rede (figura 4), mas distinguem-se basicamente pelo tipo de implementação de qualidade de serviço utilizada, descritos como:

- *Cenário de melhor esforço*: também denominado cenário *best effort*, representa o cenário da arquitetura *vpn-mpls* sem nenhuma implementação de qualidade de serviço.
- *Cenário com combinação de serviços diferenciados e mpls*: expansão do cenário de melhor esforço com a implementação do mapeamento entre as classes de serviço da arquitetura de serviços diferenciados implementado no cliente *vpn*, nos rótulos *mpls* da rede do provedor.
- *Cenário com engenharia de tráfego*: expansão do cenário com combinação de serviços diferenciados e *mpls*, onde técnicas de engenharia de tráfego também são aplicadas.

A análise de desempenho dos cenários baseou-se nos resultados de vazão (bits/segundo) e atraso fim-a-fim (segundos) das aplicações dos clientes *vpn*. Os cenários analisados correspondem a um tempo de simulação de 3600 segundos (1 hora).

Na topologia da rede simulada, os roteadores *3600a*, *3600b* e *3600d* representam os roteadores de núcleo do provedor de serviço (roteadores *p* da arquitetura *vpn-mpls*). Os roteadores *3600c*, *3600e*, *7200a* e *7200b* representam os roteadores de borda do provedor de serviço (roteadores *pe*). Os roteadores *rotlip1*, *rotlip2*, *rotlip3* e *rotlip4* são roteadores dos clientes *vpn* (roteadores *ce*). Os servidores e estações utilizados na construção da topologia são elementos de rede dos clientes *vpn*(*cliente-1* e *cliente-2*).

Nesta topologia os enlaces são *full duplex* de forma que o "gargalo"da rede ocorra no *backbone*, onde os enlaces entre os roteadores *3600a*, *3600b* e *3600d*, que representam o núcleo (*backbone*) da rede do provedor de serviços, são de 6.5 Mbps. Os demais enlaces entre os roteadores, que representam a borda da rede e a rede dos clientes *vpn* (roteadores *pe* e roteadores *ce*), são de 10 Mbps. Entre os servidores de *ftp* , clientes *ftp* e estações de *vídeo* e de voz, que estão ligados aos roteadores dos clientes (*rotlip1*, *rotlip2*, *rotlip3* e *rotlip4*) são configurados enlaces de 10 Mbps.

Com o intuito de simular cenários reais, onde aplicações não prioritárias compartilham a rede com aplicações prioritárias, foram definidas três aplicações; aplicação de transferência de arquivo ou *ftp* (*file transfer protocol*) gerando 2.0 Mbps de tráfego, aplicação de *vídeo* (*vídeo conferência*) gerando 1.5 Mbps e aplicação de voz sobre *IP* (*voip*) gerando 20.0 Kbps, para cada cliente *vpn*.

O cenário de melhor esforço funciona como cenário de referência para os outros cenários de simulação, e representa o cenário da arquitetura *vpn-mpls* sem nenhuma implementação de qualidade de serviço. De acordo com a topologia da rede apresentada na figura 4 e as configurações das aplicações *ftp*, *vídeo* e *voip* , o *cliente-1* gera um tráfego total de 3.5 Mbps do instante de tempo de simulação 180 segundos até o final da simulação (instante 3600 segundos). As aplicações *ftp*, *vídeo* e *voip* do *cliente-2*, iniciadas nos instantes de tempo 1800, 900 e 900 segundos respectivamente, possuem as mesmas configurações feitas no *cliente-1*. Logo, o *cliente-2* também gera um tráfego total de 3.5 Mbps. Os tráfegos dos clientes *vpn* totalizam uma carga de tráfego de 7.0 Mbps imposta ao núcleo do provedor de serviço, que apresenta enlaces de 6.5 Mbps, ocorrendo concorrência entre as aplicações no acesso

a rede do provedor.

No segundo cenário, as redes dos clientes *vpn* implementam a arquitetura de serviços diferenciados, através do uso do campo *type of service* do *IP* para priorização das aplicações a fim de serem mapeados nos rótulos *mpls* da rede do provedor.

De acordo com a arquitetura de serviços diferenciados [17], as classes de serviço são classificadas como AF (*Assurance Forwarding*), EF (*Expedited Forwarding*) e BE (*Best Effort*). Dentro da classe AF, quatro sub-classes são padronizadas, indo da mais prioritária AF4x até a menos prioritária AF1x. O valor x nestas sub-classes podem variar de 1 a 3, representando a prioridade dentro de cada sub-classe, sendo a classe AF43 de maior prioridade dentro das sub-classes AF. A classe EF é a classe com o maior índice de prioridade, superando todas as sub-classes AF e a BE, sendo utilizada pela arquitetura de serviços diferenciados para priorizar o tráfego de sinalização da rede e tráfego de voz. A classe BE, também denominada classe de melhor esforço, é utilizada para tráfegos não prioritários, como transferência de arquivos (*ftp*).

Neste cenário, a priorização das aplicações no campo *type of service* são configuradas como sendo AF11 para todas as aplicações do *cliente-2* e AF21, AF41 e EF para as aplicações de *ftp*, *video* e *voip* do *cliente-1*, respectivamente. Para este cenário, a aplicação de *voip* do cliente-1 é a mais prioritária seguida da aplicação de *video* e *ftp*, e as aplicações do cliente-2 (*ftp*, *video* e *voip*) são as menos prioritárias.

O cenário com engenharia de tráfego tem como objetivo analisar os resultados de desempenho de cada aplicação fazendo uso da engenharia de tráfego na combinação de serviços diferenciados e *mpls*. A aplicação de engenharia de tráfego neste cenário visa a construção de caminhos comutados por rótulos (*lsp - label switching path*) com restrições mínimas de banda na rede *mpls* do provedor de serviço. Os *lsps* estáticos criados na simulação, que interligam os sites dos clientes *vpn*, passam a possuir restrição mínima de banda com valor de 4 Mbps para estabelecimento do *lsps*. Os *lsps* estáticos utilizados pela simulação são representados na figura 4 pelas setas horizontais que interligam os roteadores *3600c* e *7200a* para o *cliente-1*, e os roteadores *3600e* e *7200b* para o *cliente-2*.

A figura 5 apresenta os resultados de vazão dos enlaces do núcleo da rede, entre os roteadores *3600d* e *3600a* (parte superior da figura 5) e entre os roteadores *3600d* e *3600b* (parte inferior da figura 5) para o primeiro e segundo cenário. Para os dois cenários, toda a carga média imposta à rede durante a simulação é transmitida no núcleo da rede pelo menor caminho (enlace *3600d-3600a*), devido ao uso do algoritmo de caminho mais curto (*spf - shortest path first*) utilizado pelo protocolo *ospf* (*open shortest path*) implementado nos roteadores da rede do provedor de serviço, deixando subutilizado o enlace *3600d-3600b*, por onde trafega apenas a sinalização de roteamento.

Para o cenário com engenharia de tráfego, apresentado pela figura 6, o uso da rede do provedor de serviço é otimizado e garantido pelo parâmetro de banda mínima configurado no estabelecimento dos *lsps*. Neste cenário os *lsps* do *cliente-1* são estabelecidos entre os roteadores *3600c* e *7200a* (figura 4) passando pelo enlace *3600d-3600a*, e os *lsps* do *cliente-2* são estabelecidos entre os roteadores *3600e* e *7200b* (figura 4) passando pelo enlace *3600d-3600b*, pois o enlace *3600d-3600a* não suporta o estabelecimento dos *lsps* dos dois clientes devido a limitação de banda. Com isso, pode-se analisar na parte superior da figura 6 todo o tráfego das aplicações do *cliente-1* gerados desde o início da simulação com carga média de 3.5 Mbps sendo transmitidos através do enlace *3600d-3600a*. A parte inferior da figura 6 apresenta a vazão do enlace *3600d-3600b*, que é de 1.5 Mbps a partir do tempo de 15 minutos (900 segundos) representando as aplicações de *vídeo* e *voip* do *cliente-2*, e aumenta para aproximadamente 3.5 Mbps a partir do tempo de 30 minutos (1800 segundos) com o início da aplicação *ftp* do *cliente-2*.

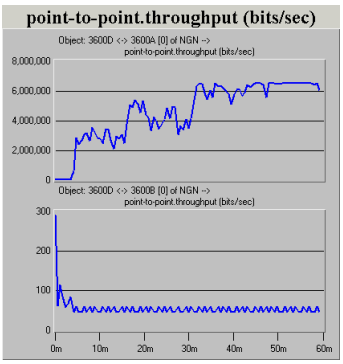

Fig. 5. Vazão dos enlaces *3600d-3600a* e *3600d-3600b* para o cenário de melhor esforço

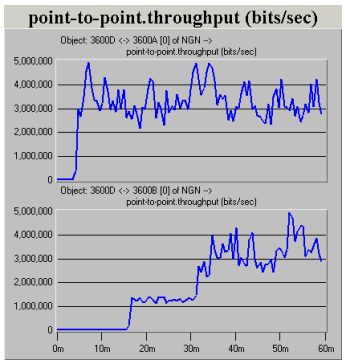

Fig. 6. Vazão dos enlaces *3600d-3600a* e *3600d-3600b* para o cenário com engenharia de tráfego

A figura 7 apresenta os resultados de atraso fim-a-fim da aplicação de *vídeo* do *cliente-1* para os três cenários simulados. Para o cenário de melhor esforço todas as aplicações são tratadas pela rede da mesma forma, o valor de atraso fim-a-fim de *vídeo* (figura 7), assim como o valor de atraso fim-a-fim da aplicação de *voip* (figura 9) do *cliente-1*, começam a piorar a partir do tempo de 30 minutos devido ao aumento da carga imposta a rede do provedor pelo início das aplicações do *cliente-2*. Para o cenário com combinação de serviços diferenciados e *mpls*, a aplicação de *vídeo* do *cliente-1* é mapeada na classe AF41 que apresenta uma prioridade alta na rede em comparação com as outras aplicações, perdendo apenas para classe EF de *voip*. Com isso, o valor de atraso fim-a-fim da aplicação de *vídeo* do *cliente-1* para este cenário (figura 7) apresenta valores pequenos em comparação com os valores de atraso fim-a-fim da aplicação de *vídeo* do *cliente-2* (figura 8). O mesmo fato ocorre para o atraso fim-a-fim da aplicação de *voip* do *cliente-1*(figura 9), mapeada na classe EF, que apresenta resultados melhores em comparação com aplicação de *voip* do *cliente-2*(figura 10) mapeada na classe AF11.

No cenário com engenharia de tráfego, os valores de atraso fim-a-fim da aplicação de *vídeo* do *cliente-1* (figura 7) e do *cliente-2* (figura 8) permanecem estáveis durante toda a simulação, visto que as aplicações do *cliente-2* não disputam o mesmo enlace com o *cliente-1*. O mesmo ocorre para a aplicação *voip* do *cliente-1* (figura 9) e do *cliente-2* (figura 10).

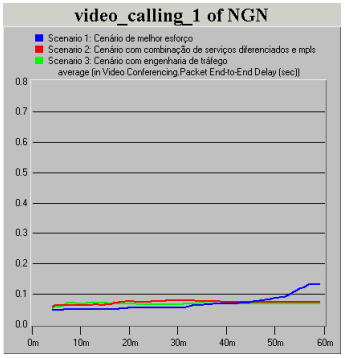

Fig. 7. Atraso fim-a-fim de pacote de *vídeo* do *cliente-1*

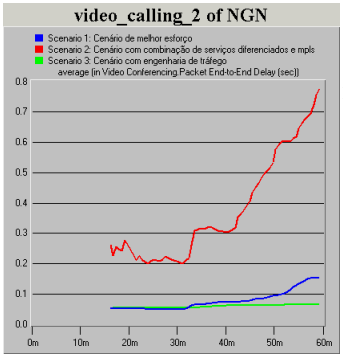

Fig. 8. Atraso fim-a-fim de pacote de *vídeo* do *cliente-2*

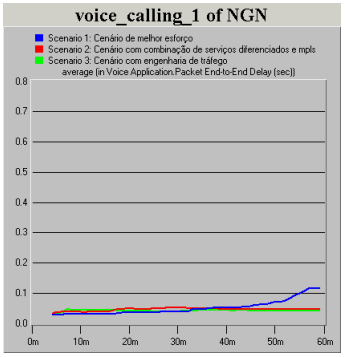

Fig. 9. Atraso fim-a-fim de pacote de voz do *cliente-1*

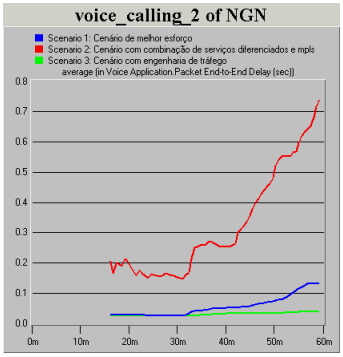

Fig. 10. Atraso fim-a-fim de pacote de voz do *cliente-2*

V. Conclusões

A provisão de qualidade de serviço é parte intrínseca dos serviços emergentes, como as redes privadas virtuais (*VPNs*). De acordo com a padronização do IETF para arquitetura *vpn-mpls* [4], uma solução de provimento de qualidade de serviço para esta arquitetura é a combinação da arquitetura de serviços diferenciados no cliente *vpn* com a rede *mpls* do provedor de serviço, estabelecendo-se um mapeamento estático de prioridade de tráfego na borda da rede do provedor de serviço.

Visando o estabelecimento de um mapeamento dinâmico de prioridades na borda da rede do provedor de serviços, onde o cliente *vpn* pode a qualquer instante criar e/ou modificar mapeamentos de prioridade, desenvolveu-se neste trabalho uma proposta de expansão da arquitetura *vpn-mpls* utilizando-se a linguagem de especificação formal *SDL*. Com a proposta de expansão da arquitetura criou-se um mecanismo de mapeamento dinâmico entre as prioridades dos clientes *vpn* e os acordos de nível de serviço contratados do provedor, através da inserção do parâmetro de prioridade de rota do cliente *vpn* na tabela *vrf*, e a modificação do protocolo *mp-bgp* para o transporte dos valores de prioridade de rota. Sendo assim, a medida que o cliente *vpn* possui aplicações que em determinados horários ou por determinados instantes de tempo não necessitem da mesma prioridade na rede do provedor, se torna possível a modificação dos parâmetros de prioridades a fim de reduzir custos com a contratação do serviço *vpn* ou garantir qualidade de serviço a outras aplicações que antes não eram prioritárias.

Com a análise de desempenho realizada através do Opnet pode-se comparar o comportamento das aplicações dos clientes *vpn* para cenários sem nenhuma implementação de qualidade de serviço e com a implementação de qualidade de serviço, através do uso do mapeamento de prioridades da arquitetura de serviços diferenciados na rede *mpls* do provedor de serviço, técnica esta utilizada na proposta de expansão da arquitetura *vpn mpls*.

Referências

[1] M. Suzuki P. Knight B. Schliesser A. Nagarajan, J. Sumimoto. Applicability Statement for Virtual Router-based Layer 3 PPVPN approaches, February 2004. draft-ietf-l3vpn-as-vr-01.txt.

[2] Telelogic AB. Telelogic TAU 4.2 SDL Suite Getting Started. Technical report, Telelogic AB Sweden, September 2001.

[3] M. C. Castro. Propostas de implementação de qualidade de serviço na arquitetura VPN MPLS, utilizando linguagem de especificação formal SDL orientada a objetos e análise de desempenho utilizando o simulador OPNET. Msc, UNICAMP, Dezembro 2004. Tese de Mestrado em Engenharia Elétrica.

[4] S. John Brannon C. J. Chase J. Clercq P. Hitchen D. Marshall M. J. Morrow A. Vedrenne E. C. Rosen, Y.Rekhter. BGP/MPLS IP VPNs, October 2004. draft-ietf-l3vpn-rfc2547bis-03.txt.

[5] Y. Rekhter D. Farinacci T. Li A. Conta E. Rosen, G. Fedorkow. RFC 3032 - MPLS Label Stack Encoding, January 2001.

[6] S. Ganti W. C. Lau N. S. S. Van den Bosch F. Chiussi, J. Clercq. Framework for QoS in Provider-Provisioned VPNs, March 2003. draft-chiussi-ppvpn-qos-framework-01.txt.

[7] B. Kang K. Jun H. Lee, J. Hwang. End-to-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network. In *IEEE MILCOM 2000*, pages 479–483, 2000.

[8] ITU-T. Rec. Y.1311.1 - Network-based IP VPNs over MPLS Architecture, July 2001. Rec. Y.1311.1.

[9] ITU-T. Rec. Y.1311 - Network-based VPNs - Generic Architecture and Service Requirements, March 2002. Rec. Y.1311.

[10] A. Krywaniuk J. Clercq, O. Paridaens. An Architecture for Provider Provisioned CE-Based Virtual Private Networks Using IPSec, February 2004. draft-ietf-l3vpn-ce-based-02.txt.

[11] O. Paridaens J. Clrcq. Scalability Implications of Virtual Private Networks. *IEEE Communications Magazine*, pages 151–157, May 2002.

[12] N. Ansari J. Zeng. Toward IP Virtual Private Network Quality of Service: A Service Provider Perspective. *IEEE Communications Magazine*, pages 113–119, April 2003.

[13] J.Clercq. QoS considerations for L3 PPVPNs, February 2003. draft-declercq-ppvpn-l3vpn-qos-00.txt.

[14] W. C. Borelli M. C. Castro, N. A. Nassif. QoS Performance Evaluation in BGP/MPLS VPN. *International Information and Telecommunication Technologies Symposium - I2TS'2003, Florianópolis-SC*, Novembro 2003.

[15] G. Wright B. Gleeson T. Sloane R. Bubenik C. Sargor I. Negusse J. Yu P. Knight, H. Ould-Brahim. Network based IP VPN Architecture using Virtual Routers, April 2004. draft-ietf-l3vpn-vpn-vr-02.txt.

[16] E. C. Rosen. Applicability Statement for BGP/MPLS IP VPNs, October 2004. draft-ietf-ppvpn-as2547-07.txt.

[17] M. Carlson E. Davies Z. Wang W. Weiss S. Blake, D. Black. RFC 2475 - An Architecture for Differentiated Services, December 1998.

[18] R. Chandra D. Katz T. Bates, Y. Rekhter. RFC 2858 - Multiprotocol Extensions for BGP-4, June 2000.

[19] T. Li Y. Rekhter. RFC 1771 - A Border Gateway Protocol 4 (BGP-4), March 1995.