Gerência de Falhas baseada em Políticas para Redes Ópticas

Cláudio Carvalho[1], Edmundo Madeira[1],
Fábio Verdi[2] e Maurício Magalhães[2]

[1] Universidade Estadual de Campinas (UNICAMP) - Instituto de Computação (IC)
Caixa Postal 6176, 13084-971, Campinas-SP, Brasil

{carvalho,edmundo}@ic.unicamp.br

[2]UNICAMP - Faculdade de Engenharia Elétrica e de Computação (FEEC)
Caixa Postal 6101, 13083-970, Campinas-SP, Brasil

{verdi,mauricio}@dca.fee.unicamp.br

Abstract. *This paper presents a policy-based architecture for admission of IP/MPLS flows within an optical network taking into account the possibility of having to cope with further transport faults. The defined policies try to reduce the negative impact generated by an optical transport network. In our model, IP/MPLS flows are divided into High Priority (HP) and Low Priority (LP) traffic and the lightpaths are capable to work with the 1+1, 1:1 and 1:N schemes of protection. The type of the flow and the required protection are important criteria for traffic admission. Our approach was validated by an implementation and the results showed that the defined policies decrease the number of blocked LSPs after the ocurrrence of a failure.*

Resumo. *Neste artigo é apresentada uma arquitetura baseada em políticas para a admissão de fluxos IP/MPLS em redes ópticas, considerando a possibilidade de gerência de futuras falhas de rede. As políticas definidas buscam reduzir o impacto negativo gerado por uma falha. Em nosso modelo, os fluxos IP/MPLS são divididos em fluxos de alta prioridade (HP) e baixa prioridade (LP) e os lightpaths são capazes de trabalhar com os esquemas de proteção 1+1, 1:1 e 1:N. O tipo de fluxo e a proteção requerida são critérios importantes para a admissão de tráfego. Nosso método foi validado por uma implementação e os resultados mostraram que as políticas definidas reduzem o número de LSPs bloqueados após a ocorrência de uma falha.*

1 Introdução

As redes ópticas estão sendo consideradas como uma solução para o congestionamento encontrado nas redes atuais. As fibras ópticas e os sistemas DWDM (*Dense Wavelength Division Multiplexing*) são elementos importantes nesta solução. De forma complementar, cada fibra óptica é capaz de transmitir um grande volume de tráfego (potencialmente 50 Tbits por segundo) e a tecnologia DWDM é capaz de dividir esta grande largura de banda em algumas centenas de canais ópticos DWDM não sobrepostos e de menores capacidades. As fibras ópticas também são capazes de alcançar baixas atenuações e dispersões na transmissão [Mukherjee 2000].

Embora as redes ópticas resolvam vários problemas conhecidos, novos desafios são trazidos para a comunidade de pesquisa. Um problema bastante analisado está relacionado com a redução do impacto negativo gerado por uma falha de rede. Sabendo que uma fibra possui uma grande largura de banda, o rompimento de uma fibra pode causar a perda de um grande volume de dados. Definida pelo IETF e estendida da arquitetura MPLS (*Multiprotocol Label Switching*), a arquitetura GMPLS (*Generalized Multiprotocol Label Switching*) [Mannie 2004] define um conjunto de protocolos capaz de lidar com falhas. São definidos mecanismos para detectar a ocorrência de uma falha, notificá-la aos nós adjacentes e aos nós envolvidos no processo de recuperação de tráfego, e também, mecanismos para desviar o tráfego do *backup* para os recursos primários, quando estes forem reparados. Além de definir os mecanismos citados, a arquitetura GMPLS também implementa alguns mecanismos de proteção de tráfego já definidos na literatura.

Foram definidos quatro tipos de proteção. O tipo mais robusto quanto a falhas é a proteção 1+1. Esta proteção define que para cada recurso primário existe exatamente um recurso de *backup* dedicado carregando, simultaneamente, o mesmo tráfego contido no recurso primário. O nó de egresso seleciona o melhor sinal a ser aceito. No caso de uma falha, somente o nó de egresso precisa fazer o desvio do tráfego para o recurso de *backup*. Os outros três tipos são o 1:1, 1:N e o M:N, onde os tipos 1:1 e o 1:N são tipos específicos do M:N. No tipo 1:1, o tráfego é enviado somente no recurso primário e o recurso de *backup* pode ser utilizado para carregar tráfego extra (tráfego de baixa prioridade). Quando uma falha afetar o recurso primário, o tráfego extra que está sendo transmitido no recurso de *backup* precisa ser bloqueado para que o tráfego contido no recurso primário seja desviado para recurso de *backup*. Este desvio de tráfego é feito em ambos os nós de ingresso e egresso. O tipo 1:N define que existe somente um recurso de *backup* para os N recursos primários. Caso um destes recursos primários falhe, os N-1 recursos primários se tornam desprotegidos enquanto o recurso primário que falhou não for reparado. Por fim, o tipo M:N define que existem M recursos de *backup* para N recursos *primários*, onde M>N. Maiores detalhes sobre proteção podem ser encontrados em [Mannie and Papadimitriou 2004]. No caso das redes ópticas, o recurso considerado é o *lightpath*.

O *lightpath* é um circuito virtual utilizado para a transmissão de tráfego entre dois pontos quaisquer da rede óptica. Para melhor aproveitar a grande largura de banda da rede óptica, espera-se que mais de um fluxo de tráfego seja admitido em cada *lightpath*. A admissão eficiente de fluxos de baixa velocidade em recursos de alta velocidade é um problema bastante analisado e conhecido como agregação de tráfego ou *traffic grooming* [Verdi et al. 2005, Ou et al. 2004, Iovanna et al. 2003].

Dependendo de como a agregação de fluxos é feita nos *lightpaths*, o uso da largura de banda da rede pode ser maximizada ou desperdiçada. Fica claro que se algumas políticas forem definidas para gerenciar a agregação de tráfego, os recursos da rede podem ser melhor aproveitados e, conseqüentemente, um maior volume de tráfego pode ser admitido. Além de influenciar na admissão de tráfego, a agregação de tráfego também pode influenciar na gerência de falhas. Dependendo de como as políticas de agregação forem definidas, um maior ou menor volume de tráfego pode ser bloqueado após a ocorrência de uma falha.

Neste trabalho são propostas uma arquitetura baseada em políticas e um conjunto

de políticas para agregação de fluxos IP/MPLS na rede óptica que considera a possibilidade de gerência de futuras falhas de rede. O objetivo consiste na redução do impacto negativo gerado por uma falha ocorrida no domínio óptico.

Os fluxos IP/MPLS são classificados no modelo como fluxos de alta prioridade (HP) e baixa prioridade (LP) e os *lightpaths* são capazes de trabalhar com os esquemas de proteção 1+1, 1:1 e 1:N, ou serem desprotegidos. O tipo de fluxo e a proteção requerida são critérios importantes para a admissão de tráfego. O método proposto foi validado por uma implementação e os resultados mostraram que as políticas definidas reduzem o número de LSPs bloqueados após a ocorrência de uma falha. As políticas definidas foram estendidas de um trabalho anterior [Verdi et al. 2005], onde estávamos interessados somente em maximizar o uso de recursos e reduzir o impacto gerado por preempções de LSPs de baixa prioridade, sem considerar a ocorrência de falhas.

Embora exista um grande interesse na arquitetura GMPLS, o método proposto neste trabalho é geral o suficiente e independe da tecnologia utilizada no plano de controle.

O restante deste trabalho está organizado da seguinte forma. Na próxima seção são apresentados alguns trabalhos relacionados. Na Seção 3 são descritas a arquitetura e as políticas propostas. A Seção 4 faz uma breve discussão sobre a implementação e os resultados obtidos nas simulações. Finalmente, a Seção 5 conclui o trabalho e discute alguns trabalhos futuros.

2 Trabalhos Relacionados

Até onde sabemos não há trabalhos com uma proposta semelhante ao nosso método. Em seguida serão discutidos alguns trabalhos que motivaram a realização da nossa proposta.

O trabalho apresentado em [Iovanna et al. 2003] discute um sistema de engenharia de tráfego que considera os métodos de roteamento *on-line* e *off-line* para a instalação de tráfego na rede. Este sistema é capaz de reagir dinamicamente a mudanças de tráfego e conta com o conceito da elasticidade da largura de banda para conseguir um melhor aproveitamento dos recursos da rede óptica. Através da elasticidade busca-se reservar uma largura de banda maior do que a banda requerida para os fluxos de alta prioridade, permitindo que pedidos de alteração de largura de banda sejam atendidos com um menor índice de preempção. A diferença entre a banda requerida e a máxima que foi reservada é chamada de banda de elasticidade e pode ser utilizada por fluxos de baixa prioridade enquanto estiver ociosa. O uso de políticas e de mecanismos de proteção contra falhas não são considerados.

O trabalho apresentado em [Ou et al. 2004] discute a agregação de tráfego em redes WDM (*Wavelength Division Multiplexing*). Além da largura de banda menor do que a de um lambda (*wavelength*), uma conexão também pode requerer uma proteção contra alguma falha de rede, tipicamente o rompimento de uma fibra. São propostos dois métodos para a agregação de tráfego: o *Protection-at-Lightpath* (PAL) e o *Protection-at-Connection* (PAC). Estes métodos são diferentes em termos de roteamento e quantidade de recurso requerido. O método PAL provê uma proteção fim-a-fim de *lightpath* na qual, após a ocorrência de uma falha, os nós finais dos *lightpaths* afetados pela falha comutam para seus respectivos *lightpaths* de *backup*. O método PAC provê uma proteção fim-a-fim

com respeito a conexão. Neste caso, após a ocorrência de uma falha os nós finais das conexões afetadas pela falha comutam para seus respectivos *lightpaths* de *backup*. Os autores buscam otimizar o uso de recursos da rede através da agregação de tráfego. Não são considerados o uso de políticas e de diferentes classes de serviço.

Fawaz *et. al.* [Fawaz et al. 2004] propõe um contrato de serviço aplicado para redes ópticas (O-SLA). Os autores descrevem três classes de serviço e algums parâmetros de tráfego e desempenho para compor cada classe, por exemplo, o tempo de configuração da conexão, disponibilidade do serviço e restrições para roteamento e recuperação de falhas. O uso do O-SLA para aplicação de políticas em redes ópticas também é discutido.

Em [Verdi et al. 2005] são apresentados uma arquitetura e um conjunto de políticas para gerenciar a agregação de fluxos de tráfego de baixa velocidade em *lightpaths*. A agregação é feita dinamicamente considerando diferentes classes de serviço. As políticas definidas buscam reduzir o trabalho gasto para preemptar e remover fluxos de tráfego de baixa prioridade. A proteção contra falhas não é considerada como um critério para admissão de tráfego.

3 Solução proposta

Embora as redes ópticas sejam capazes de interagir com várias outras redes, existe um grande interesse na integração entre redes IP/MPLS e redes WDM [Ghani et al. 2000]. Neste contexto, o modelo *overlay* [Assi et al. 2001] é bastante indicado para os provedores de serviço (ex: Telecom's) uma vez que são a maior parte interessada em atuar como redes de transporte para redes IP clientes. Um cenário típico e promissor é ter redes MPLS clientes com seus LSPs baseados em pacotes requisitando por recursos ópticos de forma a atravessar o domínio e alcançar seu destino. A Fig. 1 apresenta o cenário considerado neste trabalho.

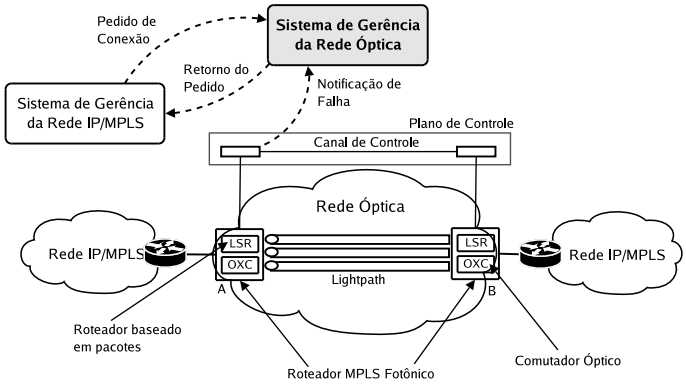

Figura 1. Cenário de referência.

No cenário de referência apresentado na Fig. 1 ocorrem eventos de pedido de conexão e seu respectivo retorno, ambos entre os sistemas de gerência da rede cliente e da rede óptica. Outro evento é a notificação de falha enviada pelo plano de controle ao sistema de gerência da rede óptica. Como pode ser observado, os *lightpaths* conectam o nó de ingresso "A" ao nó de egresso "B" do domínio óptico, conseqüentemente, a agregação de tráfego é realizada somente em nós de ingresso. As idéias iniciais sobre políticas de agregação para gerência de falhas foram apresentadas em [Carvalho et al. 2005]. As seções seguintes apresentam a arquitetura e o conjunto de políticas.

3.1 Arquitetura

A arquitetura proposta neste trabalho é composta por cinco módulos de gerência: Gerente de Recursos, Controle de Admissão (AC), Gerente de Falhas (FM), Gerente de Políticas (PM) e o Repositório de Políticas (PR). Estes módulos foram desenvolvidos com o intuito de oferecer uma infra-estrutura básica para a aplicação de políticas em redes ópticas assim como controlar as informações necessárias para gerenciar a integração entre redes IP/MPLS e redes DWDM.

Os módulos da arquitetura poderiam teoricamente ser implementados de uma forma distribuída. No protótipo desenvolvido, estes módulos são implementados em um único nó, caracterizando um *bandwidth broker* (BB) centralizado [Hamada et al. 2002]. O BB aplica políticas nos nós que realizam grooming através de módulos locais chamados de PEPs (*Policy Enforcement Point*). A definição dos PEPs está fora do escopo deste trabalho.

A arquitetura é apresentada na Fig. 2 e em seguida é feita uma breve explanação sobre cada módulo.

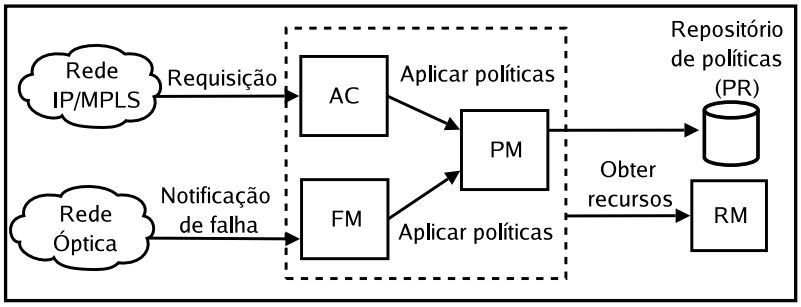

Figura 2. Arquitetura proposta.

- *Gerente de Recursos* (RM): O Gerente de Recursos é responsável por armazenar informações sobre a topologia virtual e a topologia física da rede óptica. Este módulo é acessado pelo AC, FM e PM (definidos em seguida) de forma a obter alguma informação relacionada com os recursos ópticos.
  A topologia virtual representa o conjunto de *lightpaths* estabelecidos entre os nós da rede óptica. Tipicamente, estes *lightpaths* são conhecidos como *Forwarding Adjacencies* [Farrel et al. 2005].

- *Controle de Admissão* (AC): O Controle de Admissão é responsável por receber requisições IP/MPLS e enviá-las para o Gerente de Políticas para que as políticas devidas sejam aplicadas. Antes de enviar uma requisição ao PM, o AC invoca o RM com o intuito de obter os *lightpaths* que conectam o par origem/destino desta requisição.

- *Gerente de Falhas* (FM): O Gerente de Falhas tem a função de receber as notificações de falha enviadas pelo plano de controle e manter a gerência atualizada sobre a ocorrência de falhas na rede e suas respectivas implicações, por exemplo, a indisponibilidade de um enlace. O FM também é responsável por decidir quais dos fluxos afetados pela falha deverão ser reenviados ao AC para readmissão.

Mesmo que a recuperação dos fluxos afetados pela falha seja prevista pelos mecanismos de proteção, para alguns fluxos esta recuperação não é garantida. Isto ocorre com fluxos 1:N e com fluxos desprotegidos. Com o intuito de alcançar um melhor aproveitamento da largura de banda da rede óptica foi definido como tarefa extra para a gerência de falhas, tentar readmitir os fluxos de tráfego que não foram recuperados. A ordem de prioridade para readmissão é estabelecida pela classe de serviço do fluxo, isto é, o tráfego HP é enviado para readmissão antes do tráfego LP.

- ▷ *Gerente de Políticas* (PM): O Gerente de Políticas é responsável por receber fluxos IP/MPLS e executar as devidas políticas para admissão deste fluxo. As condições das políticas decidem em qual *lightpath* o fluxo será admitido. As ações das políticas, por sua vez, executam a instalação deste fluxo e/ou remoção de fluxos na rede. Na Seção 4 são apresentados detalhes sobre o comportamento dos fluxos na rede.
- ▷ *Repositório de Políticas* (PR): Armazena as políticas definidas.

Como pôde ser observado na descrição da arquitetura, são previstos dois eventos no sistema: chegada de requisição e notificação de falha. Para visualizar o tratamento destes eventos e ter um melhor entendimento sobre a interação entre os módulos da arquitetura é apresentada a seguir uma breve explanação de cada evento.

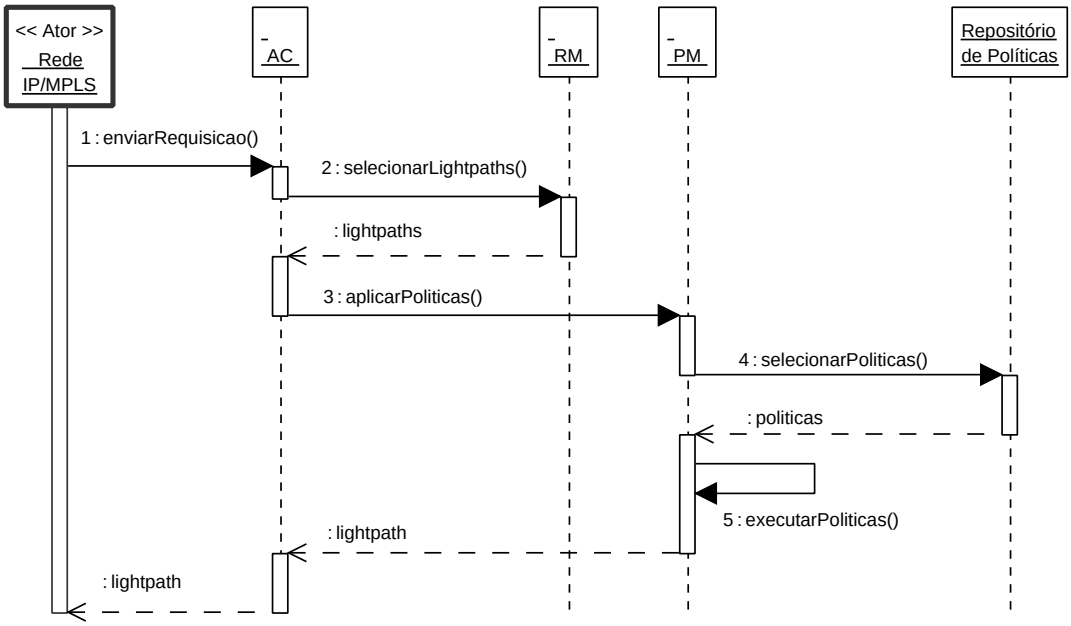

Figura 3. Interação entre os módulos para o evento *Chegada de requisição*.

A Fig. 3 apresenta as interações entre os módulos da arquitetura causadas pela chegada de uma requisição. Ao enviar uma requisição para o AC (1), a rede IP/MPLS cliente espera obter um *lightpath* que satisfaça as exigências do fluxo. O PM é o responsável por verificar se a rede óptica possui recursos para atender a requisição recebida. Antes

desta verificação, o AC seleciona os *lightpaths* entre o par origem/destino (2) para que o PM possa aplicar as políticas (3) e verificar se algum deles satisfaz as exigências do cliente. Para aplicar as políticas é necessário primeiramente selecionar aquelas que estão relacionadas com a requisição recebida (4) e posteriormente executá-las (5). O resultado deste processo pode ser um *lightpath* ou apenas um retorno vazio, o que significa que nenhum recurso foi encontrado.

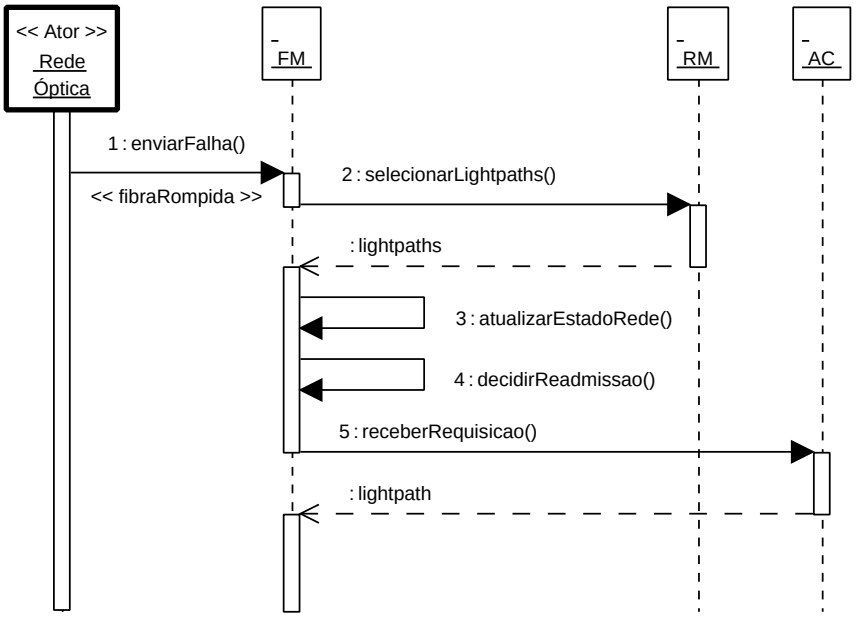

Figura 4. Interação entre os módulos para o evento *Notificação de falha*.

A Fig. 4 apresenta as interações entre os módulos da arquitetura causadas pela notificação de uma falha. O tipo de falha considerado neste caso é o rompimento de uma fibra. Uma vez detectada, o plano de controle trata e notifica a falha ao FM para que a atualização da gerência seja feita e alguma tarefa extra seja executada sobre os fluxos de tráfego que não foram recuperados. Ao enviar a notificação de falha (1), o FM obtém o conjunto de *lightpaths* contidos na fibra através do RM (2), atualiza o estado da rede (3) e verifica quais fluxos não foram recuperados para que estes possam ser enviados para o PM (4). São enviados primeiramente os fluxos de mais alta prioridade, isto é, fluxos HP. Ao chegar no PM, o processo de admissão do fluxo recebido é igual ao apresentado na Fig. 3.

3.2 Políticas

As políticas definidas neste trabalho têm como objetivo tentar encontrar um *lightpath* que satisfaça as exigências de uma requisição e admití-la caso o recurso tenha sido encontrado. Suas condições são responsáveis por encontrar o *lightpath*, analisando um conjunto de *lightpaths* e a requisição recebida. Suas ações são responsáveis por instalar a requisição no *lightpath* encontrado.

Para melhor explorar os resultados da aplicação de políticas, foram desenvolvidos três grupos de políticas, com diferentes complexidades. Em seguida é feita uma breve explanação sobre cada grupo de política.

- ▷ *Grupo de Políticas 1* (G1) : Este é o grupo de menor complexidade. Quando uma requisição é recebida pelo PM, a admissão é feita considerando apenas a proteção exigida. Por exemplo, se uma requisição 1+1 chegar ao PM, sua admissão poderá ser feita somente em algum *lightpath* com proteção 1+1 que tenha disponível a largura de banda exigida pela requisição. Esta analogia também é válida para a admissão de fluxos que exigem outros tipos de proteções;

- ▷ *Grupo de Políticas 2* (G2): O grupo G2 tem uma complexidade intermediária. Suas políticas estendem as políticas definidas no G1, considerando também a classe de serviço da requisição recebida como critério para a admissão. Este critério é somente na admissão de tráfego desprotegido. Ao receber uma requisição desprotegida, sua admissão é feita conforme a seguinte ordem de prioridade. Primeiro busca-se $(P1)$ admití-la em algum *lightpath* desprotegido que tenha somente fluxos com a mesma classe de serviço da requisição. Em segundo, busca-se $(P2)$ admití-la em algum *lightpath* desprotegido que esteja vazio. Estas duas políticas buscam admitir, tentando manter juntos os fluxos de tráfego de mesma classe de serviço; no entanto, quando os recursos da rede se tornam escassos, outras políticas são executadas. Para este caso, são definidas três políticas. Caso a requisição desprotegida ainda não tenha sido admitida, então, primeiramente, busca-se $(P3)$ admití-la em algum *lightpath* desprotegido independente da classe de serviço dos fluxos já admitidos no *lightpath*. Depois, busca-se admití-la $(P4)$ em algum *lightpath* desprotegido, preemptando, ou apenas removendo, fluxos de tráfego de mais baixa prioridade do *lightpath*. Por final, $(P5)$ busca-se admití-la em algum *lightpath* protegido (exceto 1+1), preenchendo primeiro os *lightpaths* de *backup* e posteriormente os primários. Para esta política existem duas restrições: $(P5a)$ a requisição recebida deve ser desprotegida e $(P5b)$ ser de baixa prioridade (LP). Descritas estas cinco políticas para tráfego desprotegido, observa-se que a classe de serviço foi um critério bastante utilizado durante o processo de admissão de tráfego desprotegido. Porém, nas políticas definidas para tráfego protegido, a classe de serviço não é considerada como um critério para a admissão. Ao receber uma requisição protegida, o PM busca $(P6)$ admití-la em algum *lightpath* primário que tenha a mesma proteção, independente da classe de serviço da requisição recebida. Depois, busca-se admití-la $(P7)$ em algum *lightpath* de mesma proteção, porém, preemptando, ou apenas removendo, fluxos de tráfego desprotegidos que sejam de baixa prioridade admitidos no *lightpath*.

- ▷ *Grupo de Políticas 3* (G3): Este grupo de políticas é o mais complexo, diferindo em dois pontos das políticas definidas no G2. O primeiro é que se não houver recurso disponível com o mesmo nível de proteção requerido, então busca-se admití-la em algum *lightpath* que tenha um nível de proteção maior do que o requerido. Este método é utilizado especificamente para 1:N e, como conseqüência, uma requisição 1:N pode ser instalada em um *lightpath* primário 1:1. Os *lightpaths* 1+1 são exclusivos para tráfego 1+1. A segunda diferença é que este grupo de políticas permite a quebra de um determinado grupo de *lightpaths* 1:N para atender requisições 1:1. Isto é, ao chegar uma requisição 1:1, o PM poderá admití-la em um grupo 1:N que não esteja sendo utilizado. Para isso é necessário

fazer a quebra deste grupo, resultando em um grupo 1:1 e N-1 grupos de *lightpaths* desprotegidos.

A quebra de grupos 1:N é feita somente na gerência, no entanto, é necessário ter algumas precauções durante o processo de recuperação de tráfego. Após a ocorrência de uma falha, não deve ser permitido ao plano de controle, realizar a recuperação de fluxos de tráfego admitidos em grupos de *lightpaths* que foram quebrados. Caso contrário, algum dos N-1 *lightpaths* desprotegidos poderia vir a receber a proteção 1:N que não mais o pertence.

4 Implementação e Resultados

Para testar as políticas definidas na Seção 3.2 foi desenvolvido um simulador utilizando a linguagem Java. A modelagem do PM foi baseada na especificação do modelo de informação CIM (*Common Information Model*) [CIM 2003] definido pelo DMTF (*Distributed Management Task Force*) e na especificação do modelo PCIM (*Policy Core Information Model*) [PCIM 2003]. Estas especificações definem um modelo para representar e gerenciar políticas, independente do ambiente de aplicação. Inicialmente, espera-se que sejam utilizados para representar políticas no ambiente de gerência de redes.

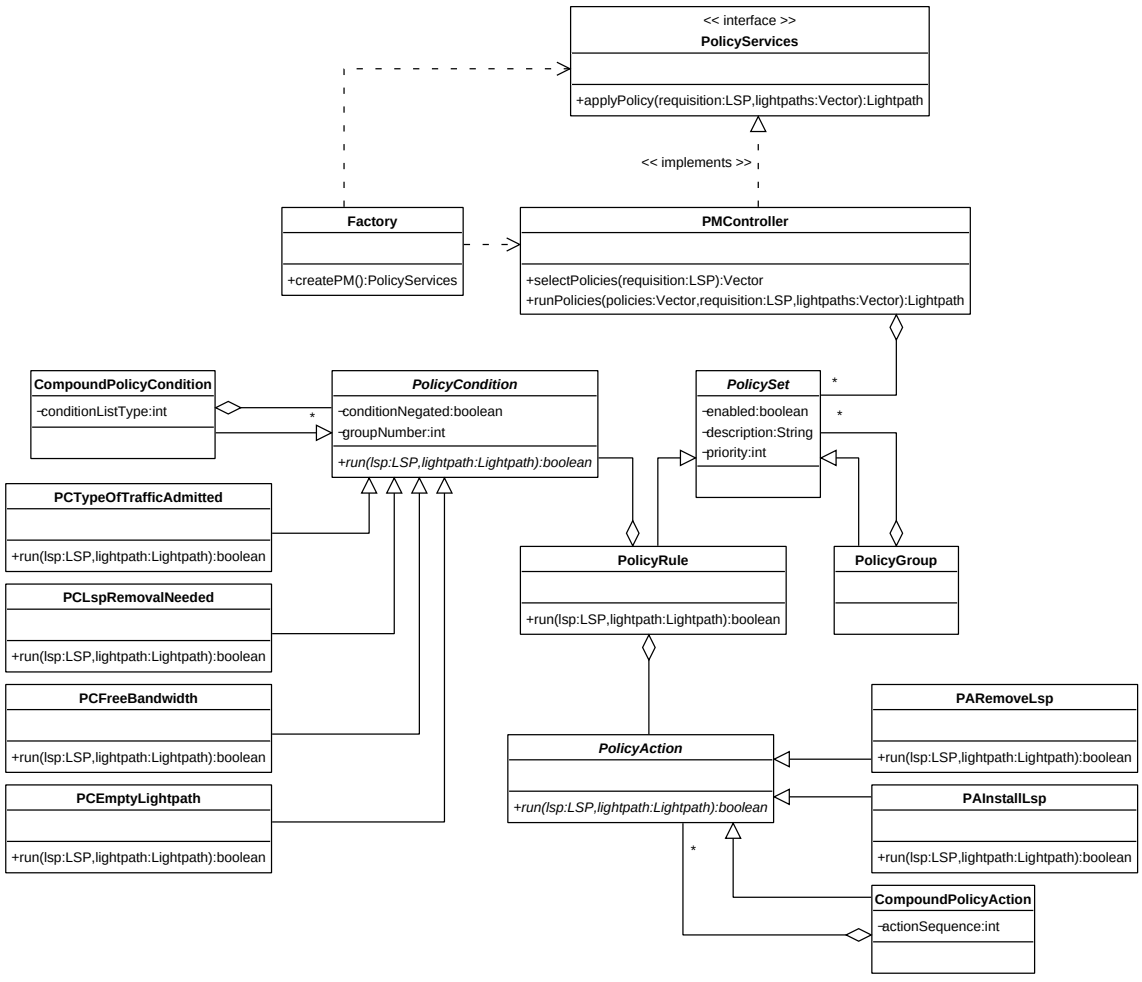

Figura 5. Diagrama de classes do Gerente de Políticas.

A Fig. 5 mostra o diagrama de classes parcial utilizado para implementar as políticas descritas na Seção 3.2. Considerada a classe que representa a política propriamente dita, a *PolicyRule* é formada por *PolicyConditions* e *PolicyActions*. Tanto as condições quanto as ações podem ser compostas através das classes *CompoundPolicyCondition* e *CompoundPolicyAction*, respectivamente. Por exemplo, para compor a política 1 $(P1)$ definida na Seção 3.2 é necessário criar uma *CompoundPolicyCondition* composta por instâncias das classes *PCTypeOfProtection*, *PCTypeOfTrafficAdmitted*, *PCEmptyLightpath* e *PCFreeBandwidth*. No caso da *PCEmptyLightpath*, o atributo *conditionNegated* da classe *PolicyCondition* deve ser verdadeiro. Para as ações é preciso instanciar somente a classe *PAInstallLsp*. A combinação dos atributos *conditionListType* e *groupNumber* da classe *PolicyRule* define se as condições serão compostas na forma disjuntiva (DNF) ou conjuntiva (CNF) [PCIM 2003].

O diagrama de classes apresentado na Fig. 5 permite que o PM gerencie os recursos de mais de um domínio. A Fig. 6 ilustra como isto pode ser feito. Primeiro é criado um conjunto para armazenar os grupos de políticas de cada domínio (*PolicySet*). Em seguida são criados os grupos de políticas (*PolicyGroup*), os quais permitem que as políticas (*PolicyRule*) de um dado domínio sejam organizadas e priorizadas conforme as exigências do administrador da rede. A definição das políticas pode ser feita sobre uma estrutura mais simples, utilizando apenas um nível de grupo, ou sobre vários níveis de grupos. A implementação do caso mais simples é apresentada na Fig. 6. Para o caso mais complexo, a definição das políticas pode ser feita sobre uma estrutura de árvore onde os nós internos são os grupos e os nós folha são as políticas. Mesmo que esta estrutura ofereça uma grande flexibilidade para a organização das políticas, nosso método considera apenas um domínio e apenas um nível de grupo para definição das políticas.

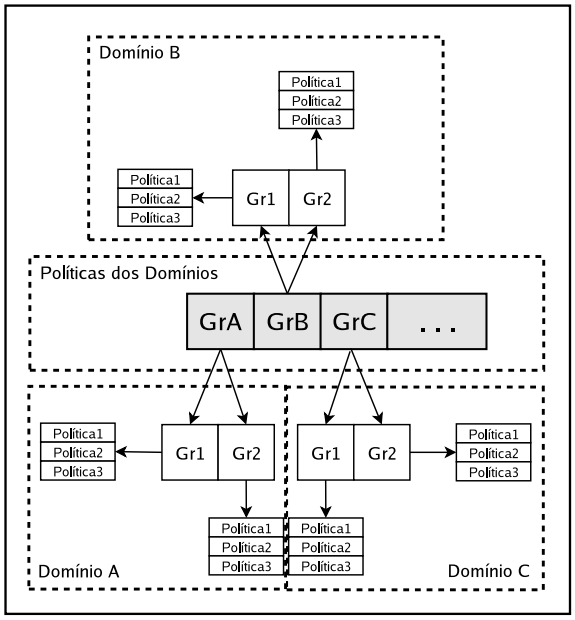

Figura 6. Criação de Políticas.

É importante mencionar que existem diferentes formas de agregar fluxos em *lightpaths* sem o uso de políticas. Neste trabalho foi assumido que as tarefas executadas pelas políticas do grupo 1 (G1) são equivalentes àquelas realizadas sem o uso de políticas.

Isto foi considerado pois o G1 é um grupo de baixa complexidade e apenas um critério (proteção) é utilizado para decidir em qual *lightpath* o fluxo recebido será agregado.

Para melhor compreender os resultados obtidos nas simulações é mostrado em seguida um diagrama de transição que representa os estados de um fluxo IP/MPLS considerados neste trabalho (Figura 7).

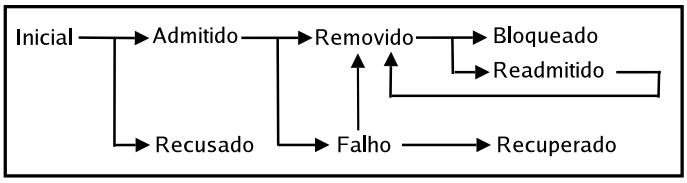

Figura 7. Transições de uma requisição IP/MPLS.

O estado inicial representa a chegada de uma requisição. A partir do estado inicial, uma requisição pode ser admitida ou rejeitada. Se admitida e se não ocorrerem falhas ou preempções, o fluxo permanece neste estado até o final da simulação. Caso contrário, o fluxo vai para o estado falho se ocorrer uma falha ou para o estado removido se um fluxo de mais alta prioridade for recebido e implicar a sua remoção. Também irá para o estado removido aquele fluxo que tiver sido afetado por uma falha e, além disso, seja desprotegido ou não tenha obtido a recuperação por algum motivo (ex: fluxos do tipo 1:N falhos que estão em primários distintos mas possuem o mesmo *backup*). A transição de um fluxo para o estado removido requer providências. Todo fluxo removido é enviado para readmissão podendo ser readmitido ou bloqueado conforme a disponibilidade dos recursos da rede. Isto significa que fluxos admitidos e readmitidos são potenciais candidatos a futuras remoções. Tarefas relacionadas com a decisão e execução das remoções são de responsabilidade das políticas. Voltando ao estado admitido, caso uma fibra seja rompida, os fluxos IP/MPLS contidos nos *lightpaths* desta fibra passarão para o estado falho. Somente aqueles previamente protegidos passarão para o estado recuperado, ou seja, serão desviados para seus respectivos *lightpaths* de *backup*. Os fluxos falhos que estiverem desprotegidos, serão removidos e enviados ao AC para a readmissão. Como pôde ser observado, o diagrama apresentado na Fig 7 permite a ocorrência de ciclos indeterminados (contínuos) envolvendo o estado removido, no entanto, o fato de que as políticas removem somente fluxos desprotegidos de mais baixa prioridade para admitir fluxos de mais alta prioridade descartam a possibilidade de ciclos com esta característica.

Em seguida são apresentadas as principais informações da simulação e os resultados obtidos. As métricas para análise dos resultados são a quantidade de tráfego admitido, juntamente com o tipo de tráfego admitido, e a quantidade de tráfego HP bloqueado após o rompimento de uma fibra.

A topologia física da rede NSFNet foi utilizada nas simulações (Figura 8). Os *lightpaths* são criados do nó 0 para o nó 12, seguindo diferentes rotas. Cada enlace físico tem duas fibras unidirecionais (uma para cada direção) e cada fibra tem 10 lambdas (*wavelengths*) de 1 Gb/s. Com a configuração desta rede física foi possível criar 36 *lightpaths* (36 Gb/s) entre o nó de ingresso e o nó de egresso, distribuídos da seguinte forma: quatro desprotegidos, vinte e quatro 1:N, quatro 1:1 e quatro 1+1. Para a proteção 1:N foi definido que existe um *lightpath* de *backup* para três primários, configurando uma proteção 1:3. Isto resulta em seis grupos de 1:3 ($6 * (1+3) = 24$ *lightpaths*). No caso de 1:1 e 1+1,

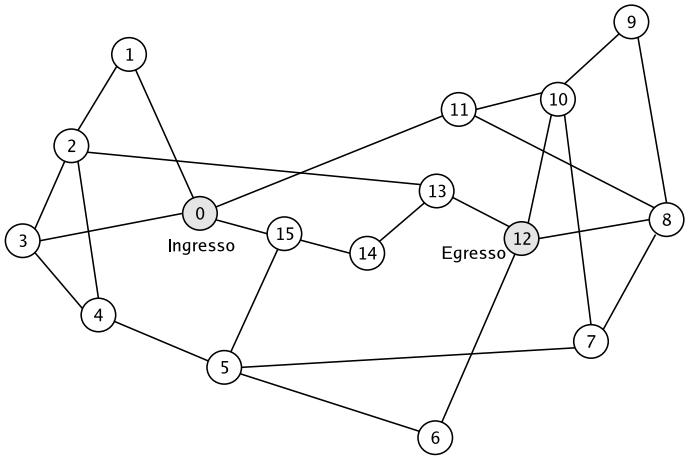

Figura 8. Topologia da rede NSFNet.

para cada *lightpath* primário existe um *lightpath* de *backup*. Resumindo, foram criados 36 *lightpaths*, são eles: 6 grupos 1:N, 2 grupos 1:1, 2 grupos 1+1 e 4 grupos desprotegidos. Em [Carvalho et al. 2005] são realizadas simulações com outra topologia física de rede.

Para validar as políticas, foram injetadas oito diferentes cargas de tráfego na rede, de 80% (0.8) a 200% (2.0) da largura de banda da rede (36 Gb/s). Com estas cargas foi possível avaliar o comportamento das políticas em cenários onde a quantidade de tráfego gerada é menor do que a capacidade da rede e, no outro extremo, quando a rede encontra-se em sobrecarga. A porcentagem de fluxo de tráfego gerada para cada requisição foi de: 35% para desprotegido, 15% para 1:N, 20% para 1+1 e 30% para 1:1. Estes fluxos de tráfego foram gerados levando-se em consideração a porcentagem da carga da rede. Por exemplo, a quantidade de requisições geradas para a carga de 120% (1.2) é aproximadamente: 36 Gb (capacidade da rede) $*$ 1.2 (carga a ser gerada) $*$ 0.3 (porcentagem de 1:1) = 13 Gb/s. A largura de banda mínima de uma requisição é 50 Mb/s e a máxima é 400 Mb/s. Estatisticamente, a largura de banda média para cada requisição é 225 Mb/s. No total 50% do tráfego gerado é HP e 50% é LP. As simulações foram executadas 20 vezes para que o resultado seja obtido através da média entre as iterações. Uma falha de fibra simples é gerada aleatoriamente para cada iteração.

A Figura 9 mostra a quantidade de fluxos admitidos na rede. Observe que o G1 é o grupo que admite a menor quantidade de tráfego. O G3, considerado o grupo mais sofisticado, tem o melhor desempenho quando comparado com os outros dois grupos. É importante ressaltar que a porcentagem de tráfego admitido depende de como as requisições são agregadas em cada *lightpath*.

A Figura 10 ilustra a quantidade de fluxos HP admitidos na rede. O G3 é o grupo que admitiu a maior quantidade de tráfego HP, por volta de 77% do tráfego HP gerado. Além disso, o G3 mantém uma diferença de aproximadamente 35% da quantidade de tráfego admitida pelo grupo G1. Observando a Fig. 10, é possível verificar que as políticas definidas no grupo G3 permitem que seja dada a preferência para a admissão de tráfego de mais alta prioridade.

A Figura 11 apresenta a quantidade de fluxos 1:1 admitidos na rede. Este gráfico reflete o resultado obtido com a quebra de grupos 1:N para atender requisições 1:1. Ob-

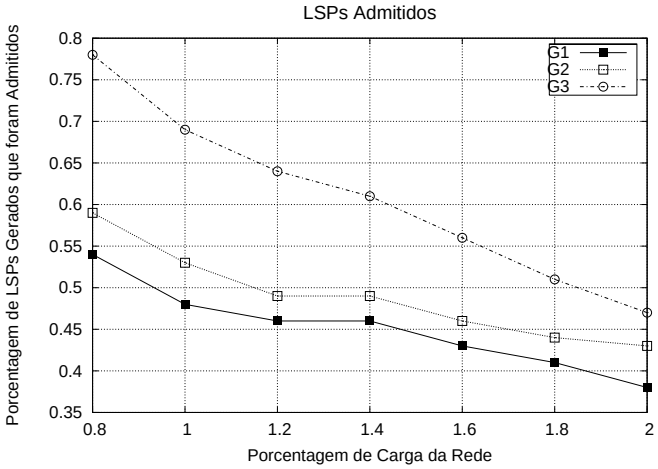

Figura 9. Porcentagem de tráfego admitido.

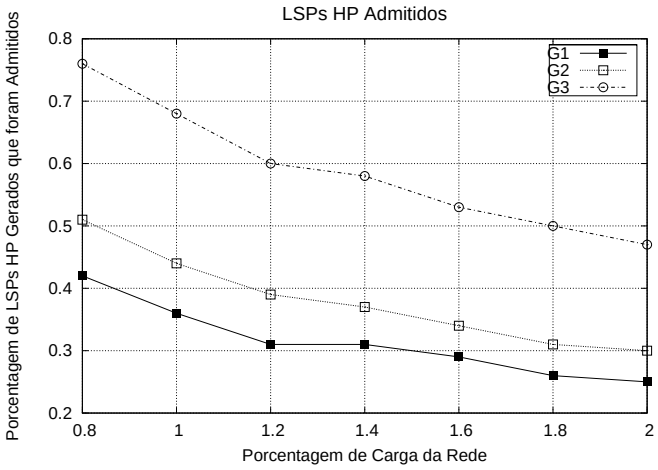

Figura 10. Porcentagem de tráfego HP admitido.

serve que o G3 foi o grupo que admitiu a maior quantidade de tráfego 1:1 enquanto os outros grupos admitiram a mesma quantidade de tráfego 1:1. Sabendo que foi gerada uma maior quantidade de tráfego 1:1 nas simulações, o grupo G3 provou ser eficiente para este tipo de cenário. O grupo G3 é fortemente indicado para cenários onde é encontrada uma grande quantidade de *lightpaths* com a proteção 1:N e a quantidade requisições 1:1 gerada é maior do que a quantidade de *lightpaths* 1:1 disponíveis.

A Figura 12 mostra a porcentagem de fluxos HP que estavam na rede e foram afetados pela ocorrência de uma falha. A informação mostrada nesta figura foi extraída da seguinte forma. Uma falha simples de fibra é gerada de forma aleatória e enviada ao FM. Após receber notificação da falha, são contados quantos fluxos (HPs e LPs) foram admitidos nesta fibra e então contados quantos destes fluxos são HP. Na Figura 12 é possível verificar que o grupo G1 apresenta uma menor porcentagem quando comparado com o G2 e o G3. Este comportamento é esperado pois na Fig. 9 é mostrado que a quantidade de tráfego HP admitido pelo grupo G1 é menor do que a quantidade de tráfego admitido pelo grupo G2 e G3.

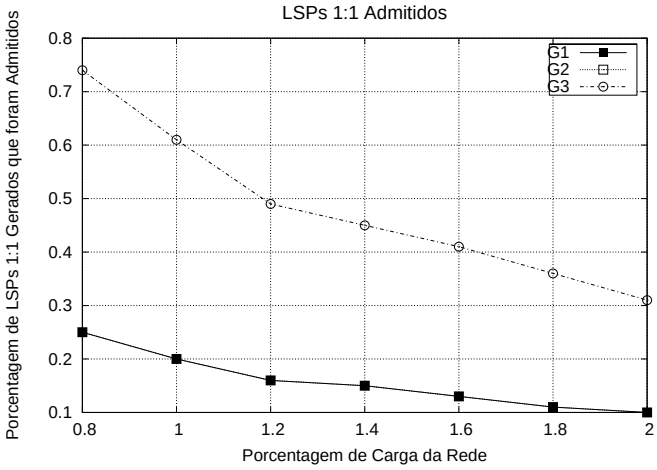

Figura 11. Porcentagem de tráfego 1:1 admitido.

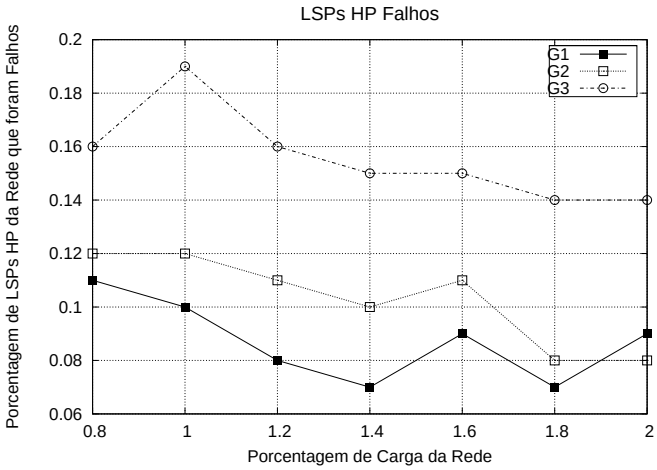

Figura 12. Porcentagem de tráfego HP afetado pela falha.

A Figura 13 mostra a quantidade de fluxos HP afetados pela falha e que foram bloqueados após a tentativa de readmissão. A análise desta figura deve ser feita em conjunto com a Fig. 12. Embora o grupo G3 tenha apresentado a maior quantidade de tráfego HP afetado pela falha, também foi o G3 que obteve o menor número de bloqueio até a carga de 1.4. Um dos principais fatores para este bom desempenho é a quebra de grupos 1:N. Observe que a medida que a carga da rede aumenta, o número de bloqueio apresentado pelo grupo G3 também aumenta. O grupo G2 se mostrou mais eficiente do que o G3 somente em cenários onde a rede estava sobrecarregada, carga acima de 1.4, bloqueando uma menor quantidade de fluxos HP.

De uma forma geral, considerando o cenário onde um dado domínio oferece uma quantidade razoável de *lightpaths* com a proteção 1:N e uma grande quantidade de tráfego 1:1, o grupo G3 apresentou um melhor desempenho quando comparado com o grupo G2 e o G1. Neste cenário o grupo G3 se mostrou bastante indicado para provedores interessados em admitir uma maior quantidade de tráfego, principalmente fluxos 1:1, e priorizar fluxos HPs. O grupo G3 também se mostrou interessante para reduzir a quantidade de tráfego bloqueado após a ocorrência de uma falha, considerando que a carga da rede es-

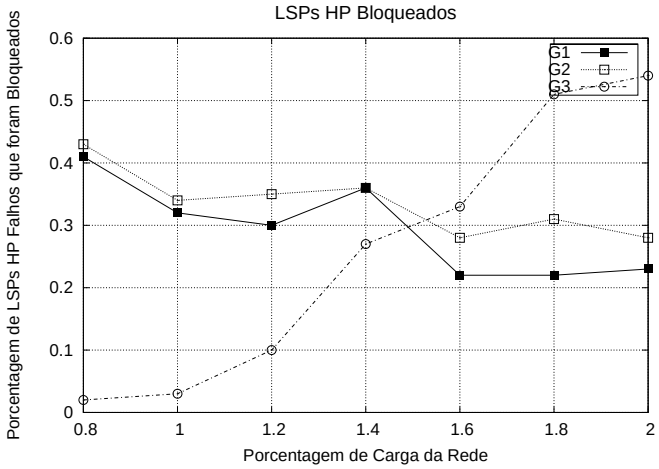

Figura 13. Porcentagem de tráfego HP bloqueado após a falha.

teja abaixo de 1.4. Para casos de sobrecarga, com uma carga acima de 1.4, o grupo G2 se mostrou mais eficiente, bloqueando uma menor quantidade de tráfego. G2 demontrou ser o grupo que mais admitiu tráfego 1:N, embora não tenha sido apresentado um gráfico para este caso.

5 Conclusão e Trabalhos Futuros

Neste trabalho foram apresentados uma arquitetura e um conjunto de políticas para gerência de falhas em redes ópticas. As políticas definidas buscam agregar fluxos IP/MPLS em *lightpaths* de forma que após a ocorrência de uma falha no plano de tranporte da rede, o impacto gerado por esta falha seja reduzido. A arquitetura é composta pelos módulos: Controle de Admissão, Gerente de Recursos, Gerente de Falhas, Gerente de Políticas e o Repositório de Políticas. As políticas são divididas em três grupos com diferentes complexidades. No grupo G1 é considerada apenas a proteção como critério de admissão. Além da proteção, no G2 também é considerada a classe de serviço. Por fim, no G3 são considerados ambos os critérios do G2, além de permitir realizar a quebra de grupos 1:N com a finalidade de atender grupos 1:1.

As políticas definidas neste trabalho consideram apenas um domínio e estão organizadas em somente um nível de política. No entanto, a abordagem apresentada é flexível ao ponto de permitir que outras políticas sejam incorporadas ao repositório de políticas. Por exemplo, caso exista a necessidade de priorizar outros tipos de tráfego ou construir vários níveis de políticas, formando uma hierarquia, novas políticas e novos grupos podem ser criados. A solução proposta foi validada por uma implementação.

Os resultados da simulação mostraram que o grupo G3 é bastante indicado para a admissão de tráfego, permitindo priorizar fluxos de alta prioridade e fluxos do tipo 1:1. O G3 também mostrou ser eficiente após a ocorrência de uma falha bloqueando uma menor quantidade de tráfego HP para cargas de rede abaixo de 1.4. Uma desvantagem de se utilizar o grupo G3 é o baixa admissão de tráfego 1:N. O grupo G2 apresentou um bom desempenho em casos de sobrecarga, acima de 1.4.

Como trabalho futuro pretende-se aplicar os conceitos de computação autônoma (*autonomic computing*) no cenário de gerência de falhas em redes ópticas. Um ponto

interessante a ser analisado é a auto-recuperação (*self-healing*) após a ocorrência de uma falha.

Agradecimentos

Os autores agradecem à Ericsson Brasil, CNPq e FAPESP pelo suporte.

Referências

Assi, C., Shami, A., Ali, M. A., Kurtz, R., and Guo, D. (2001). Optical Networking and Real-Time Provisioning: An Integrated Vision for the Next-Generation Internet. *IEEE Network*, pages 36–44.

Carvalho, C., Madeira, E., Verdi, F., and Magalhães, M. (2005). Policy-based Fault Management for Integrating IP over Optical Networks. *Fifth IEEE International Workshop on IP Operations & Management (IPOM), LCNS*, 3751:88–97. Barcelona, Espanha.

CIM (2003). Commmon Information Model. http://www.dmtf.org/standards/documents/CIM/DSP0108.pdf.

Farrel, A., Vasseur, J.-P., and Ayyangar, A. (2005). A Framework for Inter-Domain MPLS Traffic Engineering. *draft-ietf-ccamp-inter-domain-framework-04.txt*.

Fawaz, W., Daheb, B., Audouin, O., Du-Pond, M., and Pujolle, G. (2004). Service Level Agreement and Provisioning in Optical Networks. *IEEE Communications Magazine*, pages 36–43.

Ghani, N., Dixit, S., and Wang, T.-S. (2000). On IP-over-WDM Integration. *IEEE Communications Magazine*, 38:72–84.

Hamada, T., Czezowski, P., and Chujo, T. (2002). A Policy-Enabled GMPLS-Based Control Plane for Bandwidth Brokering. *Network Operations and Management Symposium (NOMS)*, pages 939–941.

Iovanna, P., Sabella, R., and Settembre, M. (2003). A Traffic Engineering System for Multilayer Networks Based on the GMPLS Paradigm. *IEEE Network*, 17:28–37.

Mannie, E. (2004). Generalized Multi-Protocol Label Switching (GMPLS) Architecture. ftp://ftp.rfc-editor.org/in-notes/rfc3945.txt.

Mannie, E. and Papadimitriou, D. (2004). Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS). *draft-ietf-ccamp-gmpls-recovery-terminology-05.txt*.

Mukherjee, B. (2000). WDM Optical Communication Networks: Progress and Challenges. *IEEE Journal on Selected Areas in Communications*, 18(10):1810–1824.

Ou, C., Zhu, K., Zhang, J., Zhu, H., and Mukherjee, B. (2004). Traffic Grooming for Survivable WDM Networks: Dedicated Protection. *Journal of Optical Networking*, 3(1):50–74.

PCIM (2003). Policy Core Information Model. RFC-3460.

Verdi, F., Carvalho, C., Magalhães, M., and Madeira, E. (2005). Policy-based Grooming in Optical Networks. *Fourth IEEE Latin American Network Operations and Management Symposium (LANOMS)*, pages 125–136. Porto Alegre-RS, Brasil.