Uma Arquitetura Baseada em Políticas para Gerência de Falhas em Redes Ópticas

Este exemplar corresponde à redação final da Dissertação devidamente corrigida e defendida por Cláudio Siqueira de Carvalho e aprovada pela Banca Examinadora.

Este exemplar corresponde à redação final da Tese/Dissertação devidamente corrigida e defendida por: Cláudio Siqueira de Carvalho
e aprovada pela Banca Examinadora.
Campinas, 28 de 07 de 2006
COORDENADOR DE PÓS-GRADUAÇÃO
CPG-IC

Campinas, 27 de julho de 2006.

Edmundo R M Madeira

Prof. Dr. Edmundo Roberto Mauro Madeira
(Orientador)

Dissertação apresentada ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Carvalho, Cláudio Siqueira de
C254a Uma arquitetura baseada em políticas para gerência de falhas em redes ópticas / Cláudio Siqueira de Carvalho -- Campinas, [S.P. :s.n.], 2006.

Orientador : Edmundo Roberto Mauro Madeira
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Computação.

1. Redes de computação – Gerência. 2. Engenharia de tráfego. 3. Comunicações óticas. 4. Tolerância a falha (Computação). I. Madeira, Edmundo Roberto Mauro. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Título em inglês: A policy-based architecture for fault management in optical networks.

Palavras-chave em inglês (Keywords): 1. Network management. 2. Traffic engineering. 3. Optical communications. 4. Fault-tolerant computing.

Área de concentração: Redes de computadores

Titulação: Mestre em Ciência da Computação

Banca examinadora: Prof. Dr. Edmundo Roberto Mauro Madeira (IC-UNICAMP)
Prof. Dr. Maurício Ferreira Magalhães (FEEC-UNICAMP)
Prof. Dr. Nelson Luis Saldanha Fonseca (IC-UNICAMP)
Prof. Dr. Paulo Lício de Geus (IC-UNICAMP)

Data da defesa: 27/07/2006

Programa de Pós-Graduação: Mestrado em Ciência da Computação

Termo de Aprovação

Dissertação defendida e aprovado em 27 de julho de 2006, pela Banca Examinadora composta pelos Professores Doutores:

Prof. Dr. Edmundo Roberto Mauro Madeira
IC/UNICAMP

Prof. Dr. Maurício Ferreira Magalhães
FEEC/UNICAMP

Prof. Dr. Nelson Luis Saldanha Fonseca
IC/UNICAMP

Instituto de Computação
Universidade Estadual de Campinas

Uma Arquitetura Baseada em Políticas para Gerência de Falhas em Redes Ópticas

Cláudio Siqueira de Carvalho[1]

Julho de 2006

Banca Examinadora:

- Prof. Dr. Edmundo Roberto Mauro Madeira (Orientador)
- Prof. Dr. Maurício Ferreira Magalhães
  FEEC – UNICAMP
- Prof. Dr. Nelson Luis Saldanha Fonseca
  IC – UNICAMP
- Prof. Dr. Paulo Lício de Geus (Suplente)
  IC – UNICAMP

[1]Suporte financeiro da CAPES e da Ericsson.

Resumo

A rede óptica é considerada uma solução para o congestionamento encontrado nas redes da atualidade. Cada fibra óptica é capaz de comportar de dezenas a centenas de canais ópticos que operam a taxas de 51 Mb/s a dezenas de terabits por segundo. Estes canais ópticos são elementos básicos para a formação de circuitos ópticos, o mecanismo padrão para transmissão de tráfego em redes ópticas. No contexto das redes ópticas, a ocorrência de uma falha de rede pode provocar a perda de um grande volume de dados. Este trabalho propõe que o problema das falhas também seja tratado durante o processo de admissão de tráfego e, para tanto, a solução proposta é utilizar políticas que considerem aspectos de falhas para gerenciar a agregação de tráfego em circuitos ópticos.

A solução proposta é aplicada no contexto de redes IP sobre redes WDM (*Wavelength Division Multiplexing*) e constituída por uma arquitetura baseada em políticas e grupos de políticas de agregação que consideram aspectos de falha para admissão de tráfego na rede. A arquitetura é composta por quatro módulos e um repositório de políticas. Estes módulos são: o controle de admissão (AC), o gerente de falhas (FM), o gerente de recursos (RM) e o gerente de políticas (PM). Todos estes módulos são utilizados para tratar o envio de um volume de requisições e, ao final, um evento de falha (rompimento de uma fibra). O PM conta com três grupos de políticas de agregação (G1, G2 e G3) de diferentes complexidades armazenados no repositório de políticas. O grupo G1 considera apenas aspectos de falha (esquema requerido de proteção) para admissão de tráfego. O grupo G2, uma extensão do G1, considera também a classe de serviço do fluxo para admissão de tráfego. O grupo G3, uma extensão do G2, permite que fluxos de tráfego sejam instalados em circuitos que ofereçam uma qualidade de serviço (esquema de proteção mais robusto) maior do que a requerida pela requisição.

Um simulador foi desenvolvido na linguagem Java para validar a solução proposta e doze experimentos foram realizados. Os resultados destes experimentos apresentaram-se relevantes para tratar o problema das falhas em redes ópticas. As políticas permitiram priorizar a admissão de determinados fluxos de tráfego e reduzir o volume de tráfego bloqueado após a ocorrência de uma falha, em várias cargas de rede. Porém, se o administrador tiver algum conhecimento prévio sobre o tipo de tráfego da rede (ex: matriz de tráfego), as políticas podem ser utilizadas para melhor planejar o uso dos recursos da rede.

Abstract

In these last few years, optical networking technology has been considered as a solution for bottlenecks found in today's networks. Each optical fiber is capable to have from ten to hundreds of optical channels that operate at rates from 51 Mb/s to ten of terabits per second. These channels are important elements in the composition of lightpaths, the default mechanism for traffic trasmition in optical networks. In the optical networks context, the occurence of a single failure can cause a huge of data loss. This work proposes that this problem is worth to be treated also during the traffic admission process. A solution for it is to use policies that consider fault aspects to manage the traffic grooming within lightpaths.

The proposed solution is applied in the context of IP networks over optical WDM (Wavelength Division Multiplexing) networks and is composed of a policy based architecture and groups of grooming policies that consider fault aspects for traffic flow admission in the network. The architecture is formed by four modules and a policy repository. These modules are the admission control (AC), fault management (FM), resource management (RM) and the policy management (PM); and are used to treat the sending of a volume of requisitions and a failure event (fiber cut) to the optical network management system. The PM takes account with three groups of grooming policies (G1, G2 and G3) of different complexities stored in the policy repository. The group G1 considers only fault aspects (required scheme of protection) to admit a traffic flow. The group G2, an extension of G1, also considers the class of service to admit the flow in the network. The group G3, an extension of G2, allows that traffic flows can be installed in lightpaths that offer a higher quality of service (a scheme of protection more robust) than that required by the requisition.

A simulator was developed in Java to validate the proposed solution and twelve experiments was simulated. The results of these experiments showed relevants to treat the fault problem in optical networks. The defined policies allowed to priorize the admission of specific traffic flows in the network and to reduce blocked traffic volume after the failure occurrence in many network loadings. However, if the administrator has a previous knowledge about the type of network traffic (e.g.: traffic matrix), the policies can be used to better plan the usage of network resources.

À minha mãe Luzia,
meu padrasto Mauro
e meu irmão Rodrigo.

Agradecimentos

Agradeço, primeiramente, a Deus, causa primária de todas as coisas. A Ele sou grato pelo dom da vida. Agradeço, com muito amor e carinho, à minha querida mãe Luzia, ao meu padrasto Mauro e ao meu irmão Rodrigo, pela educação, orientação e apoio que sempre me deram. Dedico este trabalho a vocês como forma de agradecimento ao universo de coisas boas que me proporcionaram ao longo do meu aprendizado. E ainda com tamanho amor e carinho, agradeço em memória ao meu pai Luis de Carvalho pelo amor que sempre teve por mim e meu irmão. Embora minha infância não me reporte lembranças a seu respeito, tenho a felicidade e orgulho de escutar depoimentos de grandes amigos e familiares que, com muita estima e carinho, relatam algumas de suas preciosidades.

Agradeço à minha família pelo carinho e apoio recebido em mais esta etapa da minha vida. Obrigado pelas palavras amigas que me fortaleceram para suportar a distância que nos separa e as dificuldades que encontrei em Campinas.

Agradeço, em especial, ao meu orientador Prof. Edmundo Madeira, cuja ajuda foi fundamental em todas as fases deste trabalho. O meu muito obrigado pela sua compreensão, ensinamentos, cobranças elegantes, críticas construtivas, esforço e preocupação com meu desempenho e aprendizado. Guardo comigo, e comento sempre que tenho oportunidade, a importância de seus atos de respeito e consideração com o próximo. Tenho o hábito de qualificar estes atos como nobres.

Agradeço aos professores da Universidade Católica de Goiás pela formação acadêmica recebida. Em particular, ao Prof. Paulo André, Prof. Luis Carlos e Prof. Leonardo Guedes, pela amizade e também por terem me recomendado no processo de seleção do mestrado. Ao Prof. Paulo André, meu orientador de iniciação científica, agradeço ainda aos seus ensinamentos que foram de grande importância para minha vida e para o ingresso no mestrado.

Agradeço aos amigos de graduação por todo apoio recebido durante o curso de mestrado. Em particular, agradeço aos amigos Adriano Cortes, Glênio Fujioka, Augusto Xavier, Elizeu Junior e Leonardo Rassi, pelas inúmeras ajudas recebidas e conversas que sempre adicionavam novos horizontes para meu conhecimento.

Agradeço aos amigos do Laboratório de Sistemas Distribuídos, da sala de doutorado número 92, e aos funcionários do Instituto de Computação pela convivência agradável e inúmeros favo-

res. Por auxílios em específico, agradeço ao Patrick Brito, Carlos Senna, Ulisses Silva, Camila Rocha, Rodrigo Tomita, Tiago Moronte, Luiz Bittencourt, Leonardo Tizzei, Lasaro Camargos, Gregório Tramontina, Fernando Castor, Irineu Sotoma, Luciano Digiampietri, Diogo Kropiwiec e Flávio Luzia.

Agradeço ao Prof. Maurício Magalhães e aos participantes do projeto da Ericsson pela amizade e contribuições para meu aprendizado na universidade. Em especial, agradeço ao amigo Fábio Verdi pelas inúmeras ajudas recebidas durante o mestrado, pela confiança e pela consideração.

Agradeço à Ana Chaves e família, e amigos das repúblicas em que morei. Em especial, agradeço aos amigos da república EhNoiz, Arthur Castro, Daniel Manzato, Eric Hainer e Felipe Massia pela ótima convivência, consideração e conversas amigas. A legítima amizade dos senhores é algo inestimável e marcante que guardarei nas boas lembrança da minha vida.

É bem provável que eu tenha esquecido, injustamente, de mencionar alguns nomes importantes nestes agradecimentos. Peço a essas pessoas, portanto, que relevem a minha falha e que aceitem meus sinceros agradecimentos da mesma forma.

Agradeço à CAPES e à Ericsson pelo apoio financeiro.

Sumário

Lista de Tabelas

Lista de Figuras

Lista de Acrônimos

ADM *Add-Drop Multiplexors*

ASON *Automatic Switched Optical Network*

CIM *Common Information Model*

COPS *Common Open Policy Service*

DEN *Directory Enable Networks*

DWDM *Dense Wavelength Division Multiplexing*

E-NNI *External Network-to-Network Interface*

GLASS *GMPLS Lightwave Agile Switching Simulator*

GMPLS *Generalized Multiprotocol Label Switching*

I-NNI *Internal Network-to-Network Interface*

IETF *Internet Engineering Task Force*

ITU-T *International Telecommunication Union - Telecommunication Standardization Sector*

LDAP *Lightweight Directory Access Protocol*

LER *Label Edge Routers*

LSP *Label Switching Paths*

LSR *Label Switch Routers*

MANs *Metropolitan Area Networks*

MPLS *Multiprotocol Label Switching*

NMS *Network Management System*

OIF *Optical Internetworking Forum*

OSLA *Optical Service Level Agreement*

OXC *Optical Cross Connects*

PCIM *Policy Core Information Model*

PDP *Policy Decision Point*

PEP *Policy Enforcement Point*

PMT *Policy Management Tool*

PONs *Passive Optical Networks*

PXC *Photonic Cross-Connects*

RWA *Routing and Wavelength Assignment*

SDH *Synchronous Digital Hierarchy*

SNMP *Simple Network Management Protocol*

SONET *Synchronous Optical Network*

TDM *Time Division Multiplexing*

UNI *User to Network Interface*

WANs *Wide Area Networks*

WDM *Wavelength Division Multiplexing*

Capítulo 1

Introdução

1.1 Contexto

A comunicação sobre fibras ópticas tem uma grande importância na história da evolução das redes de computadores. Desde a antiguidade existe a necessidade por sistemas de comunicação confiáveis. Ao longo do tempo, os sistemas de comunicação evoluíram gradualmente dos sinais de fumaça para os telégrafos, e finalmente para os primeiros cabos coaxiais em 1940. À medida que estes sistemas evoluíam, diversas limitações eram apresentadas entre eles. Os sistemas elétricos eram limitados pela necessidade de amplificação do sinal em pequenas distâncias, e os sistemas de microondas possuíam taxas de transmissão limitadas pela freqüência da portadora do sinal. Na segunda metade do século XX, a comunidade de pesquisa constatou que utilizar uma portadora de sinais ópticos para transmissão de dados teria vantagens significantes sobre as portadoras de sinais elétricos e de microondas existentes.

Após um período de pesquisa intenso entre 1975 e 1980, o primeiro sistema comercial de comunicação baseado em fibras ópticas foi desenvolvido. Esta primeira geração do sistema operava a uma taxa de 45 Mb/s com amplificadores espaçados em 10 km. Várias gerações de sistemas de comunicação óptica foram desenvolvidos. Recentemente, na quarta geração, foi alcançada a taxa de 14 Tb/s com amplificadores a uma distância de 160 km [10]. Para a quinta geração, o foco de desenvolvimento é estender a faixa de operação dos comprimentos de onda dos sistemas *Wavelength Division Multiplexing* [4]. Os sistemas WDM já existiam em gerações anteriores, WDM permite dividir a grande capacidade de uma fibra óptica em múltiplos canais de comunicação de forma a enviar mais de um sinal sobre a mesma fibra. Estes canais ópticos também são chamados de canais de comprimento de onda (*wavelength* ou *lambda*).

Atualmente, as fibras ópticas são utilizadas por várias empresas de telecomunicações para transmitir sinais telefônicos, sinais de televisão, e sinais de dados, as vezes todos na mesma fibra. Geralmente, a escolha por fibras ópticas é feita para sistemas com mais alta largura de banda ou que atravessam distâncias maiores do que a provida pelos cabos de cobre, por exemplo

para os *backbones*. Em alguns casos específicos, mesmo que a largura de banda ou distância sejam relativamente pequenas, as fibras ópticas ainda são utilizadas devido a algumas de suas características: imunidade à interferência eletromagnética, alta resistência elétrica, baixo peso, não emitem centelha e radiação eletromagnética.

1.2 Definição do Problema

O circuito óptico é o mecanismo padrão para transmissão de tráfego ao longo do domínio óptico. Chamado também de *lightpath*, sua largura de banda é determinada conforme a capacidade de seus canais ópticos, de aproximadamente 51Mb/s a dezenas de gigabits por segundo. Alguns problemas surgem à medida que uma quantidade considerável de clientes não necessita de toda a largura de banda de um circuito óptico. Nas redes IP, por exemplo, apenas parte dos clientes requisita grandes volumes de largura de banda. Alguns destes problemas são o desperdício de largura de banda e a grande perda de dados provocada por falhas.

O uso eficiente da largura de banda dos circuitos ópticos é um desafio bastante abordado na literatura [55, 35, 18]. Tipicamente, a agregação de tráfego é uma técnica que participa de várias soluções encontradas para este desafio. *Traffic Grooming* ou agregação de tráfego consiste em agregar mais de um fluxo de tráfego em um único circuito óptico. Alguns trabalhos propõem sistemas de engenharia de tráfego baseados puramente na agregação de tráfego [35] e outros buscam resolver o problema utilizando políticas para gerenciar a agregação de tráfego. No trabalho do nosso grupo de pesquisa [55], considerando que existem vários circuitos ópticos entre o par (origem, destino) de uma requisição, as políticas decidem em qual circuito óptico a requisição deve ser agregada.

Reduzir o impacto gerado por uma falha também é um desafio de grande importância em redes ópticas. Pequenas falhas como o mal funcionamento de um transmissor ou o rompimento de uma fibra podem provocar a perda de um grande volume de dados. Atualmente, os esforços para resolver este desafio estão baseados em mecanismos de proteção e restauração [45, 64, 41, 47, 26]. Estes mecanismos definem esquemas entre circuitos ópticos primários e circuitos ópticos de *backup* para a gerência de falhas. Nos mecanismos de proteção, os circuitos de *backup* são pré-estabelecidos embora exista a probabilidade de não serem utilizados antes da ocorrência de uma falha. Nos mecanismos de restauração, os circuitos de *backup* são estabelecidos após a ocorrência da falha, mesmo que exista o risco de não haver recursos disponíveis.

Canhui *et. al.* [45] definem dois métodos de proteção para 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 recursos requeridos e similares em termos de provisionamento de proteção fim-a-fim. Alangar *et. al.* [64, 41] apresentam uma revisão sobre a gerência de falhas em redes ópticas, abordando tópicos como aplicação de políticas, mecanismos de proteção e restauração e disponibilidade de recursos. Ramamurthy *et. al* [47] também discutem

sobre mecanismos de proteção para o tratamento de falhas em redes ópticas.

1.3 Objetivos

A agregação de tráfego é uma técnica que, combinada com o uso de heurísticas e políticas, permite otimizar a alocação de recursos em redes ópticas. Verdi *et. al* [55], em um trabalho anterior do nosso grupo de pesquisa, propõem um conjunto de políticas de agregação para reduzir a preempção de tráfego e o desperdício de largura de banda na rede. Outros trabalhos também consideram o uso de políticas para gerenciar a agregação de tráfego [35], no entanto, não foi encontrado nenhum que explore o uso de políticas de agregação para reduzir o impacto gerado após a ocorrência de uma falha.

O objetivo deste trabalho é:

- Estudar e analisar as contribuições do uso de políticas de agregação de tráfego para reduzir o impacto de uma falha após a sua ocorrência.

1.4 Contribuições

As contribuições desta dissertação incluem:

- estudo de políticas para redução do impacto gerado por uma falha. Neste tópico inclui-se o uso de modelos de informações para aplicação de políticas, o controle de admissão e a gerência de falhas em redes ópticas, a agregação de tráfego, e mecanismos de proteção e recuperação;
- proposta de uma arquitetura baseada em políticas para a gerência de admissão e falhas;
- proposta de um conjunto de políticas que buscam reduzir o impacto de uma falha;
- implementação de um simulador para validar a solução proposta.

1.5 Organização do Texto

O conteúdo desta dissertação está organizado em 8 capítulos, incluindo este capítulo de introdução:

1. *Introdução*: Capítulo atual.

2. *Redes Ópticas*: Este é um capítulo de conceitos básicos que discute as principais características de uma rede óptica WDM. Uma rede óptica é dividida em três planos conceituais: o plano de transporte, o plano de controle e o plano de gerência. No plano de controle são discutidos os elementos básicos de uma rede óptica e o funcionamento de cada um destes elementos. No plano de controle são discutidas as recomendações para controle da sinalização e roteamento em redes ópticas: o ASON (*Automatic Switched Optical Network*) e o GMPLS (*Generalized Multiprotocol Label Switching*). No plano de gerência é feita uma breve explicação sobre a integração IP/MPLS (*Multiprotocol Label Switching*) e as redes ópticas.

3. *Controle de Admissão baseado em Políticas*: Este capítulo também é de conceitos básicos, porém, apresenta o paradigma de gerência de redes baseada em redes ópticas especificamente para o controle de admissão. Este paradigma tem o apoio de um arcabouço onde são definidos uma ferramenta para edição de políticas, pontos de decisão e de aplicação de políticas e um repositório de políticas. As características básicas de uma política (ex: conceito e ciclo de vida) e um modelo para implementação de políticas (*Policy Core Information Model* - PCIM) também são discutidos neste capítulo.

4. *Trabalhos Relacionados*: Neste capítulo são discutidos alguns trabalhos relacionados com redes ópticas e aplicação de políticas, e que participam do domínio ou serviram de inspiração para a solução proposta.

5. *Solução Proposta*: Este capítulo discute os tópicos que participam da solução proposta: o cenário de referência considerado, uma arquitetura baseada em políticas e um conjunto de políticas. Consideramos o cenário IP/MPLS como referência para esta dissertação. A arquitetura baseada em políticas é composta pelo controle de admissão, gerente de falhas, gerente de políticas, gerente de recursos e um repositório de políticas. Por fim, três grupos de políticas foram desenvolvidos.

6. *Simulador Desenvolvido*: Houve a necessidade de desenvolver um simulador para validar a solução proposta. Este capítulo apresenta a arquitetura e funcionamento deste simulador, além de alguns artefatos de software gerados em sua implementação.

7. *Experimentos e Resultados*: Doze experimentos foram realizados para analisar as contribuições das políticas de agregação para reduzir o impacto gerado por uma falha, após a sua ocorrência. Este capítulo apresenta a configuraçã e os resultados destes experimentos.

8. *Conclusão e Trabalhos Futuros*: O uso de políticas de agregação apresentou várias contribuições para gerência de redes ópticas. Dentre elas estão a capacidade de priorizar a admissão de determinados fluxos, facilidades para a implementação de estratégias de gerência, dinamismo na admissão de tráfego, e reduzir o bloqueio de tráfego após a

ocorrência de uma falha na infra-estrutura da rede. Este capítulo discute sobre estas e outras contribuições obtidas ao se utilizar um controle de admissão baseado em políticas, em especial, para gerência de falhas. Os trabalhos futuros também são apresentados neste capítulo.

Capítulo 2

Redes Ópticas

2.1 Introdução

Atualmente, as redes ópticas apresentam contribuições em diversos segmentos da área de redes. No âmbito das aplicações, por exemplo, são encontrados diversos serviços avançados que ganharam visibilidade com a maturidade e difusão das redes ópticas, vide os serviços de monitoramento de processos industriais em tempo real, serviços de multimídia (ex: voz sobre IP, teleconferências e vídeo sob demanda) e serviços de home virtual, dentre outros. De uma forma geral, são serviços que exploram, principalmente, a grande largura de banda, os pequenos tempos de resposta e/ou imunidade a interferências eletromagnéticas das redes ópticas.

Um dos fatores que mais contribui para a oferta destes serviços é a ocupação da tecnologia óptica nas redes da atualidade. Na Internet, a maior concentração de redes ópticas está no núcleo, isto é, nas redes metropolitanas (ou *Metropolitan Area Networks* - MANs) e *backbones* (ou *Wide Area Networks* - WANs). Nas redes de acesso à Internet, estão as *Passive Optical Networks* (PONs) que embora sejam recentes, são tecnologias promissoras para ocupar as redes de acesso [39, 38]. Existem também várias instâncias de redes ópticas em redes de pesquisa, por exemplo: *Canarie Network* (CANet), Cooperação Latino-Americana de Redes Avançadas (CLARA), *Advanced Networking for Leading-edge Research and Education* (ABILENE) e Tecnologia da Informação no Desenvolvimento da Internet Avançada (TIDIA).

Várias tecnologias podem ser utilizadas para transmissão de sinal em redes ópticas. Neste capítulo apresentaremos uma visão geral sobre as redes ópticas baseadas na tecnologia *Wavelength Division Multiplexing* (WDM). A Seção 2.2 apresenta uma visão geral sobre as redes ópticas WDM, sua arquitetura e os circuitos ópticos. A Seções 2.3 e 2.4 discutem sobre as duas principais tecnologias para o controle da sinalização e roteamento de redes ópticas, as recomendações *Automatic Switched Optical Network* (ASON) e *Generalized Multiprotocol Label Switching* (GMPLS), respectivamente. A Seção 2.5 discute sobre a integração entre as redes ópticas WDM e as redes IP/MPLS (*Multiprotocol Label Switching*).

2.2 Redes Ópticas WDM

A tecnologia das redes ópticas surgiu como uma solução para os problemas de banda e gargalo encontrados nas redes atuais. Organizações e comunidades internacionais tais como o IETF (*Internet Engineering Task Force*), ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*) e OIF (*Optical Internetworking Forum*) estão criando especificações a fim de definir padrões para possibilitar o desenvolvimento de novas soluções relacionadas às redes ópticas.

Em redes ópticas são definidos três planos funcionais: plano de transporte, plano de controle e plano de gerência. A recomendação ASON definida pela ITU-T, além de definir uma arquitetura para o plano de controle óptico, identifica a relação básica entre os três planos.

- *Plano de transporte*: inclui todos os equipamentos de rede, fibras e elementos responsáveis pelo envio dos dados através dos canais ópticos;
- *Plano de controle*: provê a inteligência da rede através das capacidades de roteamento e sinalização para o estabelecimento de circuitos ópticos. Algumas das atividades deste plano são a descoberta de topologia, a notificação de falhas e o estabelecimento de circuitos ópticos;
- *Plano de gerência*: responsável por receber e realizar as requisições para o estabelecimento, remoção e manutenção das circuitos ópticos. Além disso, o plano de gerência implementa (em conjunto com o plano de controle) as cinco áreas funcionais de gerenciamento FCAPS.

As cinco áreas de gerenciamento FCAPS, recomendada pelo ITU-T, são:

1. *Gerência de falhas* (GF): Um dos principais objetivos da GF é aplicar estratégias para que na ocorrência de falhas futuras, a qualidade de serviço oferecida pela rede óptica seja pelo menos igual à qualidade de serviço contratada.
2. *Gerência de configuração* (GC): Na admissão de tráfego são encontradas várias atividades da GC. Um exemplo é a provisão de recursos, onde os recursos são configurados conforme a qualidade de serviço exigida pelo cliente.
3. *Gerência de contabilização* (GA): A principal função da GA é contabilizar eventos ocorridos na rede. Como resultado desta atividade podem ser gerados relatórios para diversas finalidades. Um exemplo é o relatório de conta de pagamento.
4. *Gerência de desempenho* (GP): Uma função importante da GP é monitorar eventos ocorridos na rede relacionados com o desempenho. Variações no desempenho obtido podem resultar em novos eventos para ajuste da rede.

5. *Gerência de segurança* (GS): A preocupação da GS está relacionada em como manter um ambiente seguro, considerando aspectos e mecanismos para garantir a autenticidade e anonimato de usuários (clientes), integridade, privacidade e confidencialidade dos dados.

As redes ópticas consistem basicamente de elementos como roteadores, *switches*, sistemas DWDM (*Dense Wavelength Division Multiplexing*), multiplexadores Add-Drop (ADM - *Add-Drop Multiplexors*), comutadores fotônicos (PXC - *Photonic Cross-Connects*) e comutadores ópticos (OXC - *Optical Cross Connects*) [40].

O OXC é um elemento que concentra várias funcionalidades. Cada OXC possui módulos para: multiplexação e demultiplexação de sinais ópticos, malhas de comutação para encaminhamento e adição/remoção de tráfego, e possíveis módulos do plano de controle e do plano de gerência, ver Figura 2.1. O trabalho [68] faz um amplo estudo da tecnologia dos futuros OXCs.

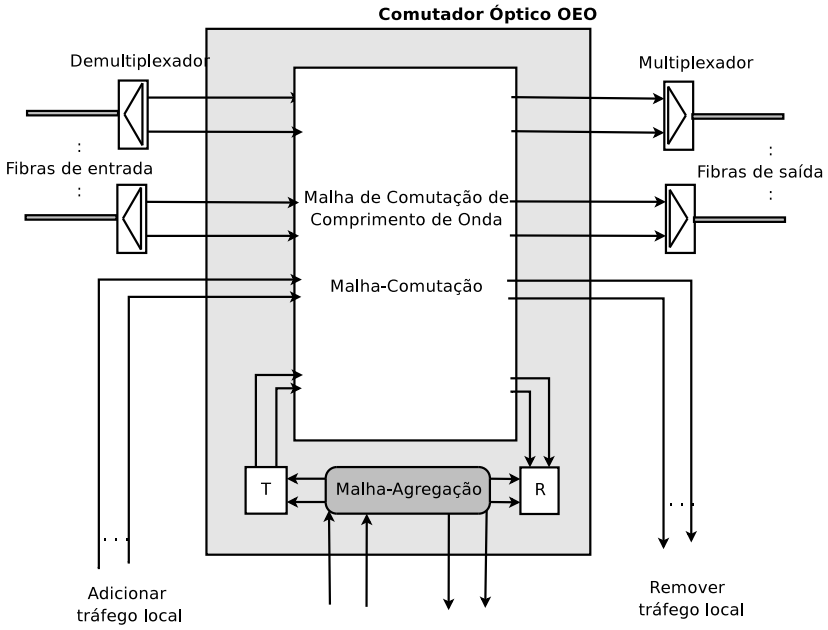


Figura 2.1: Arquitetura simplificada de um OXC.

Os sistemas WDM permitem a multiplexação e demultiplexação de canais de comprimento de onda (*wavelength* ou *lambdas*). Cada lambda de entrada é comutado para um lambda de saída com ou sem conversão, ver a Figura 2.2. A necessidade de conversão de lambda é definida por restrições físicas da rede (Seção 2.2.1) ou restrições do cliente. Algumas delas podem ser mapeadas através do contrato especificado entre o provedor de serviço e o cliente, *Optical Service Level Agreement* (OSLA) [30].

Um lambda pode ser exclusivo ou compartilhado entre vários clientes. A tecnologia *Time Division Multiplexing* (TDM) permite que a transmissão/recepção em um canal óptico seja

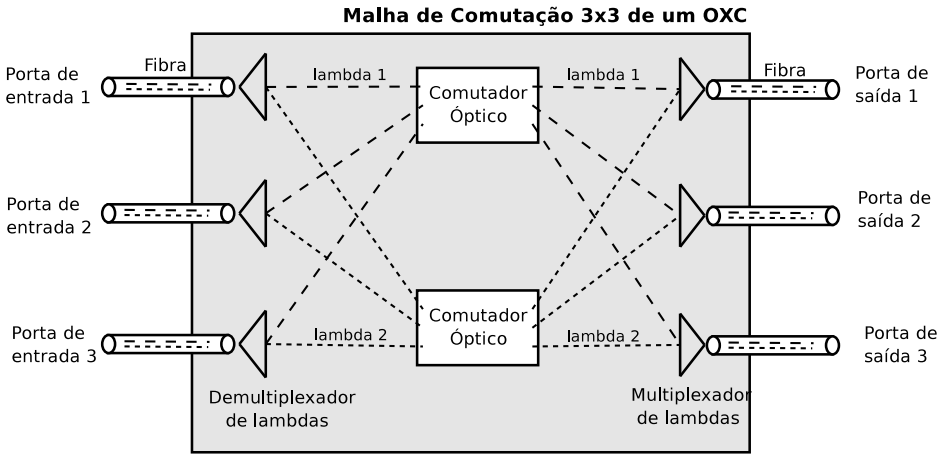


Figura 2.2: Malha de comutação 3x3.

síncrona e realizada em *slots* de tempo, isto é, cada cliente possui um intervalo de tempo reservado para transmitir e receber dados no canal.

Algumas funcionalidades dos OXC exigem a necessidade de conversão de sinal entre os meios eletrônico e óptico, originando a classificação OEO (óptico-eletrônico-óptico) para aqueles capazes de converter sinais entre os meios de transmissão e OOO (totalmente óptico) para os OXCs que não são capazes de realizar tal conversão. A agregação de tráfego, inserção e remoção de tráfego são exemplos de ações realizadas por OXCs OEO. Na malha de agregação, a inserção/remoção de tráfego é feita realizando a conversão de sinal e atribuindo/liberando um canal para transmissão. A instalação de mais de um fluxo de tráfego em um circuito óptico (agregação de tráfego) é feita seguindo a mesma idéia.

2.2.1 Circuitos Ópticos

O circuito óptico é o mecanismo padrão para transmissão de sinal entre dois pontos quaisquer da rede óptica. Para um fluxo de tráfego atravessar o domínio óptico pode ser utilizados um ou mais circuitos ópticos, ou seja, um circuito que entregue o tráfego diretamente para o destino (circuitos *single-hop*), ou vários circuitos ópticos que componham uma rota capaz de entregar o tráfego para o destino (circuitos *multihop*). A Figura 2.3 apresenta estes tipos de circuitos. L1 é um circuito *single-hop* enquanto o circuito L2, L3 e L4 é *multihop*.

A formação de circuito óptico é composta por uma rota e canais WDM inter-conectados ao longo desta rota, configurando o problema conhecido como *Routing and Wavelength Assignment* (RWA) [63]. Primeiramente encontra-se uma rota que satisfaça as exigências do fluxo de tráfego cliente (*routing*) e, posteriormente, escolhe-se e sinaliza (inter-conecta) os lambdas escolhidos ao longo da rota (*wavelength assignment*).

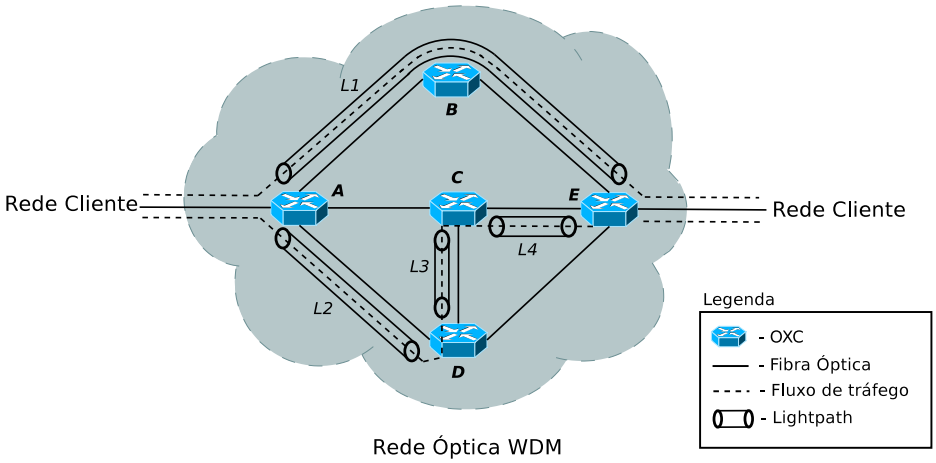


Figura 2.3: Circuitos ópticos *single-hop* e *multihop* em uma rede óptica WDM.

A largura de banda de um circuito está fortemente relacionada com a capacidade dos canais ópticos que o constituem, não é possível transmitir um volume de dados maior do que o suportado pelos seus canais ópticos. Algumas tecnologias definem hierarquias padrão para taxa de trasmissão síncrona de dados em redes ópticas: *Synchronous Digital Hierarchy* (SDH) e *Synchronous Optical Network* (SONET). SONET é a versão norte americana publicada pela *American National Standards Institute* (ANSI) e SDH é a versão internacional publicada pelo ITU. De forma resumida, em nível de camada física, as taxas de transmissão definidas para alguns canais são: OC-1 a 51.84Mb/s, OC-3 a 155.52Mb/s, OC-12 a 621.84Mb/s, OC-24 a ∼1.24Gb/s, OC-48 a ∼2.48Gb/s, OC-96 a 4.97Gb/s, OC-192 a ∼9.95Gb/s, OC-768 a 39.8Gb/s, etc. Em 2005, as conexões com OC-192 eram as mais comuns para uso em *backbones* de grandes provedores de serviço, e o uso de canais OC-768 são raramente utilizados fora das redes de pesquisa ou de teste.

O estabelecimento de um circuito óptico na rede pode ser estático, incremental ou dinâmico. Estático quando o circuito é estabelecido *off-line* com base em informações previamente conhecidas sobre o tráfego predominante da rede. Por exemplo, informações extraídas de uma matriz de tráfego. No tipo incremental e dinâmico os circuitos são estabelecidos à medida que as requisições são recebidas, no entato, é incremental se a ordem de chegada das requisições é conhecida. Os problemas de roteamento e atribuição de lambdas são discutidos a seguir nas duas seções seguintes, respectivamente.

Roteamento

O problema do roteamento resume-se em encontrar uma rota entre um par origem-destino que satisfaça as exigências de uma dada requisição presentes no O-SLA. Sobre o aspecto de ro-

teamento, exemplos de exigências são: conter ou não um determinado conjunto de enlaces e oferecer alguma garantia sobre o tempo de transmissão (isto é refletido no comprimento ou número de *hops* ou saltos da rota).

A literatura atual sugere três métodos ou soluções para o problema do roteamento em redes ópticas: roteamento-fixo, o roteamento-fixo-alternado e roteamento-adaptativo. O roteamento-fixo é considerado o mais simples, no entanto, o roteamento-adaptativo oferece o melhor desempenho. A seguir é feita uma breve discussão sobre cada um destes métodos e maiores detalhes são encontrados em [16, 33, 37, 46].

- *Roteamento-fixo*: Neste método as rotas são calculadas *off-line*. Para cada origem-destino é calculado uma única rota utilizando, por exemplo, os algoritmos de menor caminho como o *Dijkstra* e *Bellman Ford*. Uma requisição é bloqueada se não houver disponibilidade de lambdas na rota. O roteamento fixo pode potencialmente resultar em uma alta probabilidade de bloqueio de requisições se utilizado de forma dinâmica.

- *Roteamento-fixo-alternado*: No roteamento-fixo-alternado são calculadas várias rotas *off-line*. Cada nó da rede mantém uma tabela contendo as rotas de menor caminho para cada nó de destino. Por exemplo, nesta tabela inclui-se a rota de menor caminho, a segunda rota de menor caminho, a terceira rota de menor caminho, etc. Outros critérios também podem ser utilizados para ordenação da tabela de rotas.

- *Roteamento-adaptativo*: No roteamento adaptativo as rotas são calculadas e escolhidas de acordo com o tráfego atual da rede, buscando, por exemplo, balancear a carga dos enlaces da rede. Embora o roteamento-adaptativo tenha o melhor desempenho dos três métodos [63], este método possui um tempo maior para o cálculo da rota, além de possuir a demanda de protocolos de controle e de gerência para manter atualizadas as tabelas de rotas dos nós da rede. O roteamento adaptativo de menor caminho é um exemplo de roteamento adaptativo onde é utilizado o parâmetro custo para o cálculo de rotas. Outro exemplo é o roteamento adaptativo de menor congestionamento [16].

Atribuição de Comprimentos de Onda

O problema da atribuição de comprimentos de onda é dividido em dois sub-problemas: *(i)* escolha de lambdas e *(ii)* sinalização dos lambdas escolhidos. Primeiramente, para cada enlace de uma determinada rota, escolhe-se qual fibra e lambda serão utilizados; posteriormente, configura-se cada OXC da rota sinalizando a comutação dos lambdas de entrada e saída escolhidos. A fase *(i)* é executada através de heurísticas encontradas na literatura e a fase *(ii)* por meio de algum protocolo de sinalização do plano de controle.

A complexidade da fase de escolha de lambdas em redes ópticas é definida com base em duas restrições [48]: a *restrição de continuidade do lambda* e a *restrição de distinção dos*

lambdas. A *restrição de continuidade do lambda* define que um circuito óptico deve utilizar o mesmo lambda ao longo da rota. A rigidez desta restrição pode implicar no aumento do bloqueio de conexões se os OXCs da rede não suportarem a conversão de lambdas. A *restrição de distinção dos lambdas* define que todos os circuitos ópticos de uma mesma fibra devem ser alocados em lambdas distintos.

Nos OXCs que implementam a conversão de lambdas, um lambda de entrada λ_{in} recebido por uma porta P_{in} pode ser convertido para um lambda de saída λ_{out} diferente de λ_{in} antes que o sinal seja multiplexado para a porta de saída P_{out}. A conversão é feita sem que a informação carregada pelo lamba seja alterada. A Figura 2.4 apresenta alguns tipos de conversão de lambda considerando apenas uma porta de entrada e uma porta de saída. O caso de várias portas é mais complexo, porém similar.

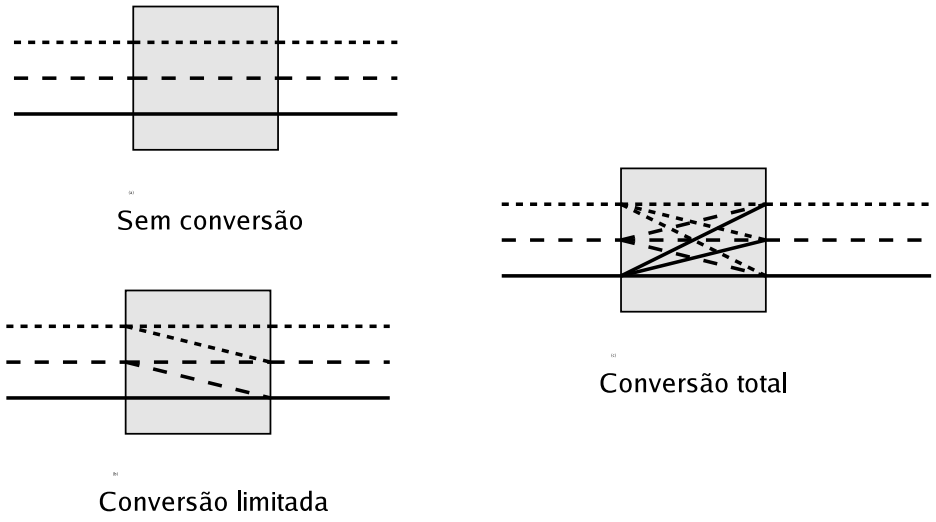


Figura 2.4: Capacidades de conversão de lambda dos OXCs.

O tipo sem capacidade de conversão é auto-explicável. Para OXCs com a capacidade total de conversão, cada lambda de entrada pode ser convertido para qualquer lambda de saída. A restrição de continuidade de lambda pode ser desconsiderada se todos os OXCs da rede suportarem este tipo de conversão, resultando em uma menor probabilidade de bloqueio de conexões. A desvantagem desta abordagem é o preço de equipamentos com a capacidade total de conversão. Um OXC com a capacidade limitada implica que apenas um conjunto de lambdas pode sofrer conversões.

Embora o preço de um OXC com capacidade total de conversão seja elevado, não é necessário que toda a rede tenha esta capacidade para se obter uma porcentagem de bloqueio aceitável. O trabalho [53] faz uma análise entre a probabilidade de bloqueio de conexões e a quantidade de OXCs capazes de realizar a conversão de lambdas na rede.

A atribuição de lambda é um tópico bastante explorado na literatura. Considerando os aspectos estático e dinâmico no estabelecimento de circuitos ópticos, a técnica de coloração de grafos é bastante utilizada no caso estático [63]. Para o caso dinâmico foram propostas várias heurísticas [63], incluindo as descritas abaixo. Estas heurísticas podem ser combinadas com qualquer solução de roteamento.

- *Random*: A primeira tarefa desta heurística é fazer um levantamento dos lambdas disponíveis na rota. A seleção de qual lambda será utilizado é feita de forma aleatória.
- *First-Fit* (FF): Nesta heurística, os lambdas são enumerados para facilitar a análise e a escolha de um lambda disponível. A análise dos lambdas é feita seqüencialmente, priorizando aqueles de menor número. Por final, é escolhido aquele que primeiro estiver disponível.
- *Least-Used* (LU): A heurística LU busca balancear o uso dos lambdas da rede, dando prioridade aos lambdas menos utilizados. Esta heurística não é muito utilizada na prática devido ao seu baixo desempenho comparado com as duas heurísticas anteriores, além do *overhead* de mensagens gasto para encontrar o lambda menos utilizado.

2.3 ASON

A arquitetura ASON [1] serve como modelo de referência para o provisionamento automático de conexões ópticas, definindo um modelo abstrato e funcionalidades necessárias para prover conexões ópticas de forma automática. A recomendação ASON, além de definir uma arquitetura para o plano de controle óptico, também identifica a relação básica entre os planos de controle gerência e transporte.

O plano de controle ASON não é uma coleção de protocolos, mas sim, uma arquitetura que define diferentes componentes funcionais para realizar funções específicas, dentre elas, sinalização e roteamento (ver Figura 2.5). As interações entre estes componentes e o fluxo de informações requerido para a comunicação entre componentes trafegam via interfaces. Estas interfaces (UNI, I-NNI e E-NNI) são conhecidas no ASON como "pontos de referência". A interface UNI (*User to Network Interface*) permite a troca de informações de sinalização entre um cliente (por exemplo, uma rede IP/MPLS) e a rede óptica. As interfaces I-NNI (*Internal Network-to-Network Interface*) e E-NNI (*External Network-to-Network Interface*) permitem o fluxo de mensagens para sinalização e roteamento dentro e entre domínios, respectivamente. A interface NMI é responsável pela troca de informações entre o sistema de gerência (NMS - *Network Management System*) e os planos de controle e transporte.

No contexto do ITU-T, o ASON define dois conceitos importantes:

- *Call*: É uma associação entre elementos de rede que provê uma instância de um serviço;

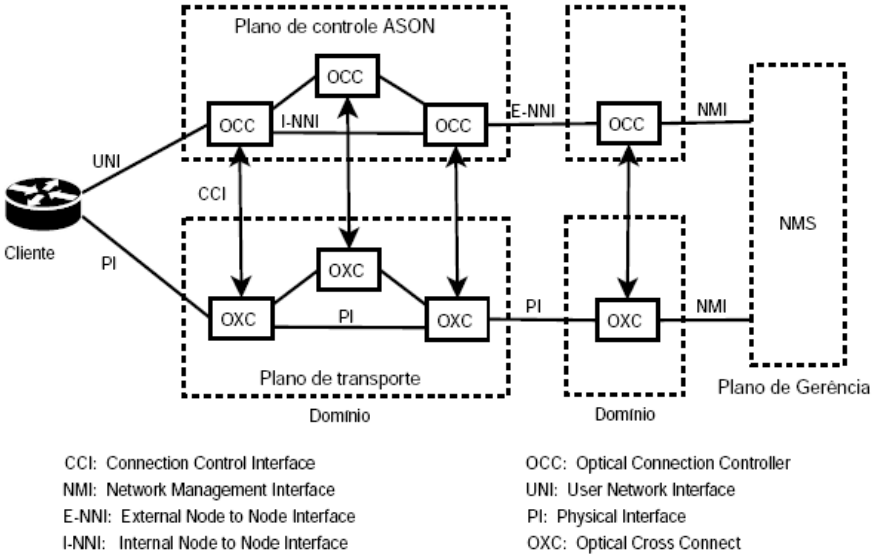


Figura 2.5: Arquitetura ASON.

- *Connection*: É uma concatenação de conexões em enlaces e sub-redes que permite o transporte de informações do usuário entre os pontos de ingresso e egresso de uma sub-rede.

Uma *call* não provê uma conectividade real para transmissão de tráfego do usuário, mas apenas constrói um relacionamento pelo qual futuras conexões poderão ser estabelecidas. Desta forma, uma call pode conter zero, uma ou múltiplas conexões. O ASON permite o estabelecimento de três tipos de conexões ópticas (ver Figura 2.6):

- *Permanent Connection* - PC: É uma conexão estabelecida pela configuração de todos os elementos de rede ao longo do caminho com os parâmetros requeridos para estabelecer uma conexão fim-a-fim. Tal provisionamento é feito pelo sistema de gerência ou intervenção manual;

- *Soft-permanent Connection* - SPC: É uma conexão pela qual um sistema de gerência configura o nó de origem enquanto os protocolos de roteamento e sinalização são utilizados para estabelecer a conexão fim-a-fim ao longo do caminho dentro do domínio;

- *Switched Connection* - SC: É uma conexão iniciada por uma rede cliente (exemplo, redes IP/MPLS) e estabelecida através dos protocolos de roteamento e sinalização. Neste caso há uma interação entre o lado cliente UNI (UNI-C) e o lado de rede UNI (UNI-N) a fim de trocarem mensagens de sinalização.

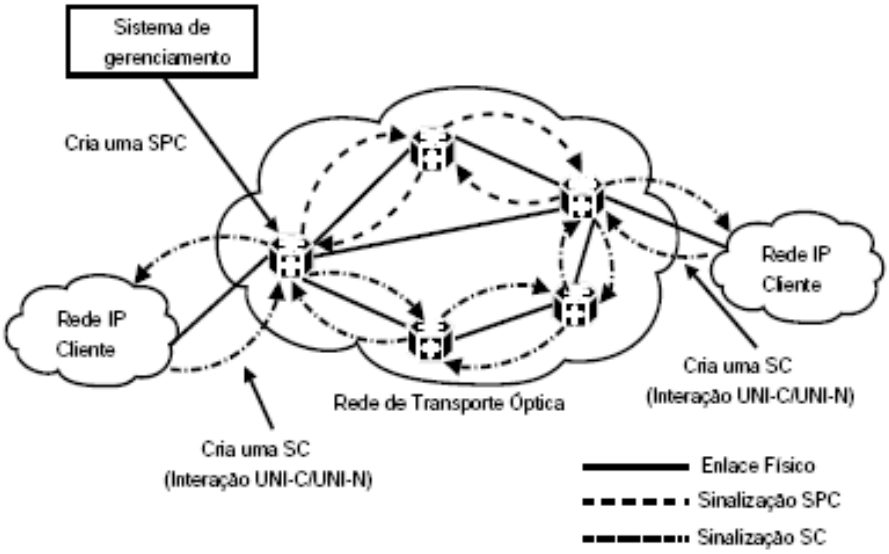


Figura 2.6: Sinalização SPC e SC.

Embora ocorra a mesma sinalização para o estabelecimento das conexões SPC e SC, uma conexão SPC é solicitada somente através de um sistema de gerenciamento, enquanto uma conexão SC é solicitada por uma rede cliente (Figura 2.6).

2.4 GMPLS

A arquitetura GMPLS [40], diferentemente do modelo ASON, propõe um conjunto de protocolos para o provisionamento automático de conexões ópticas. Esta arquitetura estende o MPLS para prover um plano de controle (sinalização e roteamento) não somente para dispositivos que realizam a comutação de pacotes, mas também, dispositivos com capacidade de comutação em slots de tempo, comprimentos de onda e fibras. Estes dispositivos são roteadores (LSRs - Label Switching Routers) com um conjunto de interfaces que executam outras operações de comutação além da comutação de pacotes. Estas interfaces podem ser classificadas como [40]:

- Interfaces PSC (*Packet Switch Capable*): são interfaces que recebem pacotes de entrada e encaminham os dados baseados no conteúdo (conhecido como rótulo) do cabeçalho do pacote. Exemplo, roteadores MPLS;

- Interfaces L2SC (*Layer-2 Switch Capable*): são interfaces que recebem quadros/células e comutam os dados baseados no conteúdo do cabeçalho do quadro/célula. Exemplos, interfaces em pontes (bridges) Ethernet que comutam dados baseados no conteúdo do

cabeçalho MAC e interfaces em comutadores ATM (ATM-LSRs) que encaminham dados baseados no VPI/VCI ATM;

- Interfaces TDM (*Time-Division Multiplex Capable*): são interfaces que comutam dados baseados nos slots de tempo em um ciclo de repetição. Exemplos, interfaces em comutadores SONET/SDH (XC - SONET/SDH Cross-Connect), multiplexadores (TM - *Terminal Multiplexer*) e multiplexadores Add-Drop (ADM - *Add-Drop Multiplexer*);

- Interfaces LSC (*Lambda Switch Capable*): são interfaces que comutam o comprimento de onda em que o sinal é recebido. Exemplos, comutadores fotônicos (PXCs) e comutadores ópticos (OXCs);

- Interfaces FSC (*Fiber-Switch Capable*): são interfaces que comutam dados baseadas na posição dos dados no espaço físico (fibra, porta). Exemplo, PXC e OXC podem operar no nível de fibras simples ou múltiplas.

Deve ser observado que há uma correlação entre a operação de comutação de rótulos, definido em interfaces PSC e que tem como exemplo roteadores MPLS, com as demais operações de comutação. Enquanto o rótulo utilizado no MPLS para comutação é explícito, em outras operações de comutação o rótulo foi substituído por outros esquemas similares de encaminhamento, baseados em slots de tempo, comprimentos de onda e fibra.

Desde que o termo Generalized MPLS (GMPLS) foi adotado para denotar a generalização do plano de controle MPLS a fim de prover múltiplos tipos de redes comutadas, o termo "LSP" (*Label Switch Path*) é utilizado no GMPLS para denotar diferentes tipos de circuitos, tais como, conexões SONET/SDH, um caminho óptico, um LSP MPLS e assim por diante.

No GMPLS, um conjunto de protocolos foi definido para o plano de controle a fim de atender três funções principais: gerenciamento de enlace, roteamento e sinalização [49]. O gerenciamento de enlaces é uma função implementada entre cada par de nós vizinhos. Esta é uma nova função que não existia no MPLS e que foi incorporada ao GMPLS através da criação do protocolo LMP (*Link Management Protocol*). O roteamento GMPLS foi estendido a partir do MPLS-TE para suportar a descoberta de recursos e topologias. O roteamento GMPLS é representado pelos protocolos OSPF-TE e IS-IS-TE e permite a alocação de vários atributos aos enlaces (por exemplo, proteção 1+1, 1:1, sem proteção, como veremos adiante) e a propagação de conectividades e informações de atributos (recursos) de um nó para todos os outros nós da rede. A sinalização GMPLS utiliza os protocolos de sinalização do MPLS-TE (RSVP-TE e CR-LDP) com extensões para manipulação de múltiplas tecnologias de comutação. Algumas extensões significativas incluem rótulo generalizado, bidirecionalidade e a separação dos planos de controle e dados.

Outra funcionalidade importante da arquitetura GMPLS é o tratamento de falhas. São definidas algumas fases para o tratamento de falhas: detecção, localização, notificação e recuperação.

Os protocolos RSVP-TE/CR-LDP e o LMP estão envolvidos no processo. O LMP é responsável por detectar uma falha e os protocolos RSVP-TE/CR-LDP são responsáveis por notificar a ocorrência da falha e recuperá-la aplicando mecanismos de proteção ou restauração.

A principal diferença entre os mecanismos de proteção e restauração está na reserva de recursos. Nos mecanismos de proteção são pré-estabelecidos circuitos de backup como tolerância a falhas ocorridas nos circuitos primários. Isto garante que, após a ocorrência de uma falha, o tráfego afetado poderá ser desviado para os circuitos de backup em pequenas escalas de tempo. A desvantagem destes mecanismos é a ociosidade dos recursos de backup. Por outro lado, nos mecanismos de restauração são estabelecidos circuitos de backup somente após a ocorrência de uma falha na rede. A vantagem destes mecanismos é o melhor aproveitamento da largura de banda da rede. As desvantagens são o tempo de recuperação e o risco de não existirem recursos disponíveis na rede para o tratamento da falha. O tempo de recuperação é basicamente o tempo de se estabelecer um novo circuito.

Na arquitetura GMPLS são implementados quatro tipos principais de proteções, os esquemas 1+1, 1:1, 1:N e M:N. O tipo mais robusto e de maior custo é o esquema 1+1. Esta proteção define que para cada circuito primário existe exatamente um circuito de backup responsável por carregar o mesmo tráfego contido no circuito primário, ao mesmo tempo. 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 circuito de backup. Os outros três tipos são variações do tipo M:N, onde os circuitos de backup não são utilizado para transmitir o tráfego dos circuitos primários, mas podem ser utilizados para trasmissão de tráfego de baixa prioridade, chamados de tráfego extra. Nestes três tipos, tanto o nó de ingresso quanto o de egresso precisam fazer o desvio do tráfego para o circuito de backup. No esquema M:N é definido que existe M circuitos de backup para N circuitos primários, onde $N > M \geq 1$. A definição dos outros tipos é feita de forma similar. No esquema 1:N existe 1 circuito de backup para N circuitos primários e no esquema 1:1 existe somente 1 circuito de backup para 1 circuito primário.

2.5 IP/MPLS sobre WDM

Tipicamente a integração IP/MPLS é feita em quatro camadas: IP para aplicações e serviços, ATM para engenharia de tráfego, SONET/SDH para transporte, e WDM para capacidade [34] (ver Figura 2.7). Embora cada uma destas camadas tenha sua função, as arquiteturas com múltiplas camadas (*multilayer*) reduzem a eficiência da rede e requerem um alto custo para a gerência. A tendência é eliminar camadas desta pilha de protocolos e oferecer suporte a vários protocolos para simplificar a arquitetura da rede.

As deficiências da arquitetura multi-camadas e o rápido crescimento do tráfego de dados em redes de comunicações estão motivando a criação de novos paradigmas arquiteturais. Uma integração de grande destaque é a IP-sobre-WDM. Neste contexto, um cenário bastante pro-

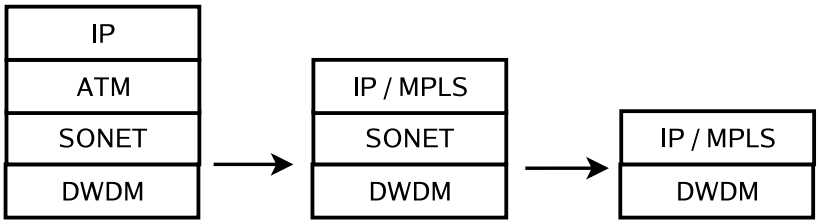


Figura 2.7: Evolução da pilha de protocolos.

missor é encontrar redes clientes MPLS baseadas em pacotes IP (redes IP/MPLS) requisitando serviços para redes ópticas WDM de forma a atravessar o domínio.

As redes MPLS são orientadas a conexão e têm como idéia básica a comutação baseada em rótulos. A intenção é substituir o roteamento IP feito na camada de rede pelo roteamento de rótulos feito entre as camadas de rede e enlace, alcançando maiores velocidades. O MPLS reconhece cada pacote IP recebido pelos roteadores de borda, chamados de LSR (*Label Switch Routers*), e adiciona um rótulo para que seja transmitido pelos circuitos MPLS, chamados de LSP (*Label Switching Paths*). Em outras palavras, o LSP é um circuito lógico que conecta dois LER (*Label Edge Routers*) distintos no domínio MPLS.

Capítulo 3

Controle de Admissão baseado em Políticas

3.1 Introdução

Grupos de trabalho do IETF têm desenvolvido extensões da arquitetura IP e do modelo de serviço de melhor esforço para a oferta de qualidade de serviço na Internet. Os grupos *Integrated Services* (int-serv) e RSVP [2] desenvolveram um modelo para que usuários possam requisitar níveis de qualidade de serviço específicos para suas aplicações. Recentes esforços no grupo *Differenciated Service* (diff-serv) também direcionaram esforços para a definição de mecanismos que suportem serviços agregados de qualidade de serviço.

No modelo int-serv, determinados fluxos de tráfego recebem tratamento preferencial sobre outros fluxos. O controle de admissão considera a requisição de reserva de recursos e a capacidade disponível da rede para determinar se a requisição de QoS é aceita ou rejeitada. No entanto, os mecanismos int-serv não consideram aspectos importantes do controle de admissão. Por exemplo, os gerentes da rede e do provedor de serviço devem ter suporte para monitorar, controlar, e ratificar o uso de recursos e serviços de rede baseados em políticas derivadas de critérios como a identidade de usuários e aplicações, características de tráfego, considerações de segurança e data e horário do dia/semana. De forma similar, os mecanismos diff-serv também precisam considerar políticas que envolvam critérios como indentidade do cliente e nós de ingresso [3].

Este capítulo apresenta os conceitos básicos para o controle de admissão baseado em políticas. A Seção 3.2 apresenta o arcabouço para aplicação de políticas definido pelo IETF. A Seção 3.3 discute as características básicas de um política e, por fim, a Seção 3.4 discute o *Policy Core Information Model* (PCIM), um modelo de informação que define uma hierarquia de elementos de softwares (ex: classes e esquemas XML) para implementação de políticas.

3.2 Arcabouço para Aplicação de Políticas

O IETF definiu um arcabouço que tem como objetivo controlar as decisões do controle de admissão através de políticas [62]. Este arcabouço é bastante utilizado na literatura e não inclui discussões sobre o comportamento de alguma política e sobre o uso de políticas específicas, discute apenas os elementos arquiteturais e mecanismos necessários para permitir a aplicação de uma variedade de políticas. Outros arcabouços são apresentados em [52].

O uso do arcabouço do IETF possui alguns requisitos. Os mecanismos desenvolvidos para prover o controle de decisões do controle de admissão devem satisfazer os seguintes requisitos: considerar o uso do RSVP para sinalização de largura de banda na rede, embora o arcabouço seja extensível para oferta de qualidade de serviços em outros contextos; suportar preempção de tráfego; suportar vários estilos de políticas (ex: políticas de configuração que incluem SLAs bilaterais e multi-laterais); suportar o monitoramento do estado da política e prover acesso à informação; incluir tratamento para tolerância e recuperação de falhas; prover pelo menos a escalabilidade provida pelo RSVP em termos de acomodar vários fluxos e nós de rede na rota do fluxo; e não ser mandatório para todos elementos de rede, em particular para os *policy-ignorant nodes* (PINs).

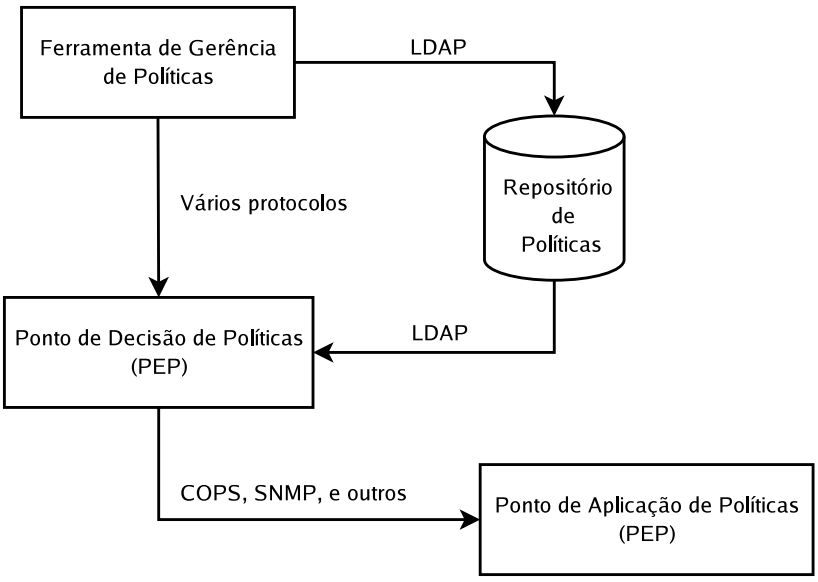


Figura 3.1: Arquitetura do arcabouço para aplicação de políticas definido pelo IETF.

A arquitetura do arcabouço é constituída pela ferramenta de gerência de políticas (*Policy Management Tool* - PMT), o repositório de políticas, o ponto de aplicação de políticas (*Policy Enforcement Point* - PEP) e o ponto de decisão de políticas (*Policy Decision Point* - PDP); ver Figura 3.1. Estes elementos são aplicados a um domínio administrativo, ou seja, uma coleção

de redes que estejam sobre o mesmo controle administrativo e agrupados para um propósito administrativo. Roteadores, *switches* e *hubs* são exemplos de elementos de rede considerados no domínio administrativo.

O PDP e o PEP são os dois principais elementos arquiteturais. O PDP é uma entidade remota que realiza as decisões de políticas e o PEP é um componente do nó de rede onde as decisões são aplicadas. A aplicação de políticas nos PEPs depende das decisões realizadas no PDP. Além do *Common Open Policy Service* (COPS) [28], um protocolo utilizado para comunicação entre o PDP e o PEP, o PDP também pode fazer uso de mecanismos e protocolos adicionais para alcançar funcionalidades adicionais como autenticação de usuário, contabilidade e armazenamento de informações de política. Por exemplo, o PDP pode utilizar o *Simple Network Management Protocol* (SNMP) [27] e serviços baseados em *Lightweight Directory Access Protocol* (LDAP) [29] para autenticação de usuário, armazenamento e resgate de informações de políticas.

A ferramenta de gerência de políticas é utilizada pelo administrador da rede para definir e editar políticas, e o repositório armazena as políticas definidas.

3.3 Características das Políticas

Uma política é definida de diversas formas. A recomendação para o controle de admissão baseado em políticas utiliza duas definições [62]:

1. Uma meta definida, direção ou método de uma ação para guiar e determinar decisões do presente e do futuro. Políticas são implementadas ou executadas dentro de um determinado contexto (ex: políticas de negócio);

2. Políticas como um conjunto de regras para administrar, gerenciar, e controlar o acesso para recursos de rede [7].

Tipicamente, uma política pode ser definida por vários atributos [20] e em vários níveis de abstração [43, 60]. Em sua essência, os atributos de uma política qualificam suas ações e condições, são eles:

- *Sujeito*: conjunto de gerentes (domínios) que devem aplicar as políticas;
- *Modalidade*: define se uma política é do tipo autorização a qual permite ou proíbe determinada ação, ou do tipo obrigação a qual exige ou impede determinada ação;
- *Disparador*: define um evento opcional o qual dispara a aplicação da política;
- *Ação*: especifica uma ou mais ações de gerência;

- *Alvo*: conjunto de objetos gerenciados nos quais as políticas serão aplicadas;
- *Restrição*: conjunto de restrições que devem ser satisfeitas antes da política ser aplicada. Este atributo representa as condições da política.

O texto abaixo apresenta um exemplo de política. As palavras sublinhadas são palavras-chave que identificam os atributos da política. *Sistema de gerência* é o sujeito, *deve* indica a modalidade, *quando* indica o disparador, *aumentar* expressa a ação, *para* faz referência ao alvo e *até* indica restrição.

O Sistema de gerência deve, quando fora de pico, aumentar a largura de banda em 10% para caminhos ou circuitos de baixa qualidade, até que largura de banda seja menor que 70% da banda total do caminho

Nos níveis de abstração de políticas inclui-se desde níveis de fácil compreensão para usuários até níveis mais próximos da linguagem de máquina. São eles: amigável, independente-equipamento, específico-equipamento e executável. As políticas dos níveis amigável e independente-equipamento podem ser disseminadas em vários domínios e para vários elementos de rede. O nível amigável descreve um formato independente de detalhes dos elementos de rede e de fácil entendimento pelo usuário do sistema. No nível independente-equipamento, as políticas são mais refinadas e, embora não sejam de fácil entendimento pelo usuário do sistema, ainda são independentes de detalhes dos equipamentos de rede. No nível específico-equipamento, por sua vez, as políticas são descritas em um formato específico para um particular tipo de equipamento. Por fim, o nível executável é o de maior refinamento. As políticas são definidas com um baixo nível de abstração, encontrando-se no formato de código executável ou instruções que serão enviadas para o sistema alvo.

Tipicamente as políticas são implementadas em mais alto nível de abstração. O administrador da rede pode utilizar uma linguagem específica para a implementação de políticas (ex: Ponder [22]) ou uma linguagem de uso geral (ex: Java). A Figura 3.2 apresenta uma visão detalhada do processo desde a definição até a aplicação das políticas no elemento de rede.

As políticas são refinadas gradualmente para um formato em que o módulo de gerência instalado no elemento de rede seja capaz de interpretar. Este refinamento é uma tarefa semi-automática e de grande complexidade pois envolve a decomposição de metas abstratas em instruções para um elemento de rede específico. Uma grande complicação é a resolução de conflitos estáticos e dinâmicos durante o refinamento. Um conflito ocorre quando duas políticas não podem existir simultaneamente no repositório de políticas, seja por causa de comportamentos contraditórios ou por algum motivo definido pelo administrador da rede. Ainda no sistema de

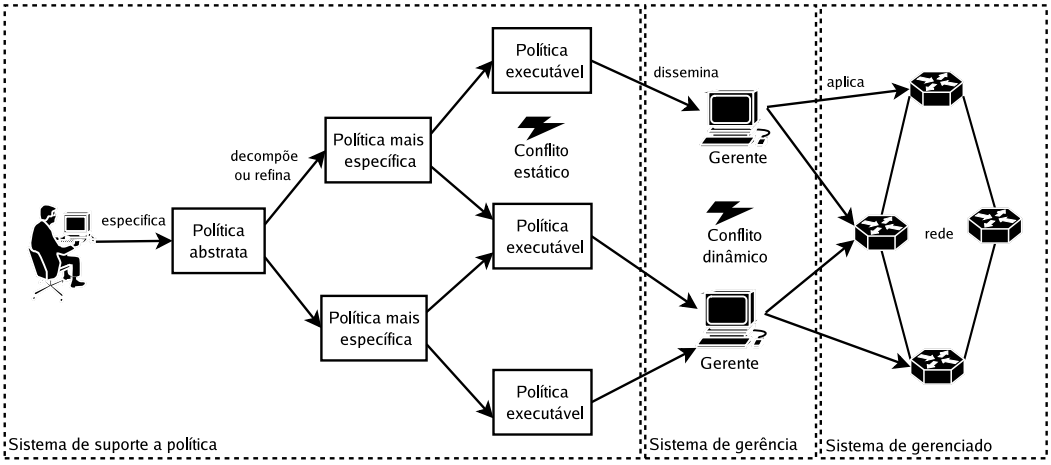


Figura 3.2: Ciclo de vida de uma política.

suporte a políticas, a detecção de conflitos é feita *off-line*, estática, examinando-se o conteúdo das declarações das políticas. Uma vez detectado, o conflito pode ser resolvido através da edição das políticas envolvidas, atribuição de prioridades ou provisão de meta-políticas. No sistema de gerência, os conflitos são detectados dinamicamente e tratados com técnicas como o estabelecimento de prioridades e meta-políticas definidas. Os trabalhos [24, 17, 23] discutem várias técnicas para tratamento de conflitos.

As políticas são disseminadas para os sistemas de gerência após terem sido definidas e refinadas. A função dos sistemas de gerência é armazenar e aplicar as políticas no sistema gerenciado (ex: elementos de rede).

3.4 Modelo de Informação PCIM

Organizações e comunidades internacionais tais como o IETF e DMTF tem definido especificações com o intuito de padronizar a modelagem de políticas, tipicamente em alto nível. Por exemplo, o IETF definiu o modelo de informação *Policy Core Information Model* (PCIM) [7] e o DMTF definiu os modelos *Common Information Model* (CIM) [6] e o *Directory Enable Networks* (DEN) [52].

O PCIM especifica um modelo de informação orientado a objetos utilizado para representar informações de políticas. Estendido do CIM, este modelo define hierarquias de classes estruturais que representam informações de políticas, e de classes de associação que indicam como as instâncias de classes estruturais estão relacionadas. As classes de políticas e associações definidas no PCIM são gerais o suficiente para representar políticas em qualquer contexto, porém, é esperado inicialmente que sejam utilizadas para representar políticas relacionadas com quali-

dade de serviço (int-serv e diff-serv) e IPSec [9].

O modelo CIM serve como um modelo que apresenta uma hierarquia de classes simples e de maior nível de abstração. Em sua extensão, o PCIM, são incorporadas novas classes onde suas especificações são mais próximas da implementação, ver Figura 3.3.

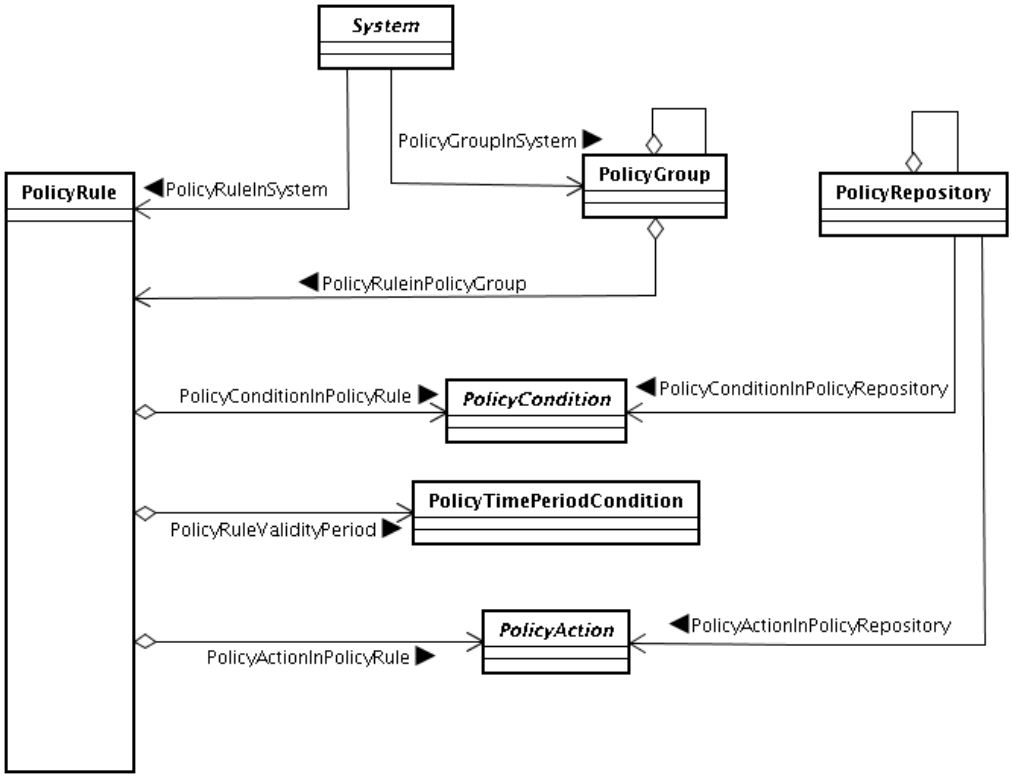


Figura 3.3: Hierarquia de classes do modelo de informação PCIM.

PolicyRule é a principal classe para representar a semântica "Se CONDIÇÃO então AÇÃO". As condições são representadas como conjuntos de AND de condições intercaladas por operações ORs (*Disjuntive Normal Form* - DNF), ou conjuntos de OR de condições intercaladas por operações AND (*Conjuntive Normal Form* - CNF). Condições individuais podem ser negadas e as ações especificadas pela *PolicyRule* são executadas se, e somente se, as condições forem verdadeiras.

As condições e ações de uma *PolicyRule* são modeladas, respectivamente, pelas classes *PolicyCondition* e *PolicyAction*. Uma *PolicyRule* pode ser associada com uma ou mais *PolicyTimePeriodCondition* indicando o perído em que a *PolicyRule* está ativa e inativa. A classe *PolicyRule* utiliza a propriedade *ConditionListType* para indicar se as condições estão no modo DNF ou CNF. A agregação *PolicyConditionInPolicyRule* contém duas propriedades para com-

pletar a representação das condições: *GroupNumber* e *ConditionNegated*. O inteiro *GroupNumber* indica o número do grupo em que a condição participa e o *boolean ConditionNegated* indica se a condição é negada (verdadeiro quando negada).

Suponha uma *PolicyRule* que agregue cinco *PolicyConditions*, de C1 a C5, com o seguintes valores de sua propriedades:

```
C1: GroupNumber = 1, ConditionNegated = FALSO
C2: GroupNumber = 1, ConditionNegated = VERDADE
C3: GroupNumber = 1, ConditionNegated = FALSO
C4: GroupNumber = 2, ConditionNegated = FALSO
C5: GroupNumber = 2, ConditionNegated = FALSO
```

A representação destas condições se *ConditionListType = DNF* é equivalente à expressão (C1 AND (NOT C2) AND C3) OR (C4 AND C5). Se *ConditionListType = CNF* a expressão equivalente é (C1 OR (NOT C2) OR C3) AND (C4 OR C5).

As *PolicyRules* podem ser priorizadas, utilizadas em *stand-alone* ou agrupadas. Uma política *stand-alone* é chamada de *PolicyRule*. *PolicyGroups* são agregações de *PolicyRules* ou de *PolicyGroup*, mas não ambos [7].

Capítulo 4

Trabalhos Relacionados

4.1 Introdução

Vários trabalhos estão relacionados com a solução proposta apresentada nesta dissertação. A Seção 4.2 discute aqueles que estão relacionados com a área de redes ópticas e a Seção 4.3 discute aqueles focados na gerência de redes baseada em políticas.

4.2 Redes Ópticas

Os estudos das comunicações ópticas têm seu início marcado na segunda metade do século XX quando a comunidade de pesquisa constatou que utilizar uma portadora de sinais ópticos para transmissão de dados teria vantagens significantes sobre as portadoras de sinais elétricos e de microondas existentes. Na década de 1970 é desenvolvido e instalado um sistema comercial baseado em comunicações ópticas como parte da primeira geração das comunicações ópticas. Nesta época, os problemas existentes em comunicações ópticas são evidenciados, vários deles decorrentes da grande largura de banda das fibras ópticas e outros relacionados com o que conhecemos por RWA.

Para se estabelecer uma conexão óptica é necessário encontrar uma rota e atribuir os lambdas para esta rota. Rouskas et. *al.* [48] e Zang et. *al* [63] discutem sobre alguns problemas existentes em RWA e soluções. [48] apresenta também uma visão geral sobre redes ópticas. Ambos os trabalhos foram importantes para uma compreensão geral da área.

O problema das falhas também é bastante discutido pela comunidade de pesquisa. Uma simples falha pode provocar a perda de um grande volume de tráfego. Zhang et. *al* [64] faz uma revisão sobre a gerência de falhas em redes ópticas incluindo aspectos como mecanismos de proteção e de restauração, e abordagens relacionadas com a disponibilidade de serviços, estratégias de provisionamento, tempo de restauração e a capacidade de se restaurar serviços.

Várias soluções são apresentadas na tentativa de resolver ou contribuir na solução do problema das falhas. Fumagalli et. *al* estudam a restauração IP e proteção WDM de forma a verificar suas vantagens e investigar qual destas seria a melhor abordagem. Wei et. *al* [59] estudam a integração de multi-camadas de rede sobre aspectos de falhas. Este problema é subdividido em três problemas menores, estratégias de modelagem, dimensionamento de capacidade e roteamento dinâmico, os quais buscam prover confiabilidade às conexões de largura de banda arbitrária em uma Internet óptica integrada. As simulações mostraram que os esquemas adaptativos para falhas obtiveram resultados melhores do que soluções encontradas na Internet sobre os critérios taxa de bloqueio de tráfego, reserva de recursos requeridos e taxa média de recuperação de tráfego. Ramamurthy et. *al* [47] discute diferentes métodos de proteção e restauração para o tratamento de falhas e os examina quanto ao tempo de recuperação. Os resultados obtidos mostraram que existe um limiar entre a utilização da capacidade e a susceptibilidade a múltiplas falhas de enlace. Zheng et. *al* [66] investigam métodos de proteção para o tratamento de falhas em um cenário IP/MPLS sobre redes WDM onde a demanda de tráfego é dinâmica. Dois algoritmos de roteamento são propostos para, de forma eficiente, garantir a largura de banda de caminhos de proteção.

À medida que as soluções para os problemas amadurecem, é observado que para resolver os problemas atuais as novas soluções precisam ser estendidas e considerar ou incorporar novos aspectos. A agregação de tráfego em circuitos ópticos é um tema que se apresentou estar relacionado com vários problemas. Por exemplo, para resolver problemas de falhas é importante obter informações sobre os fluxos de tráfego agregados nos circuitos ópticos que foram afetados pela falha. Da mesma forma, para se estabelecer uma conexão (problema RWA) deve-se ter informações sobre a capacidade dos OXCs quanto à agregação de tráfego.

Vários trabalhos buscam estudar a agregação de tráfego. Cinkler et. *al* [18] fazem uma revisão sobre a agregação de tráfego e de lambdas em um cenário de redes multi-camadas. Algumas vantagens e desvantagens destas técnicas também são apresentadas. Zhu et. *al* [67] discutem sobre a agregação de tráfego e a investigam em redes ópticas WDM em malha. O objetivo é aumentar a vazão da rede. Dutta et. *al* [25] apresentam uma visão geral comparativa entre trabalhos que revelam um volume de pesquisa significante em agregação de tráfego e, também, discutem novas direções e desafios neste tópico.

Outros trabalhos apresentam soluções para o problema das falhas considerando a agregação de tráfego. Canhui et. *al* [45] investigam a agregação de tráfego considerando aspectos de falhas em redes ópticas WDM em malha. Dentro de um contexto de provisionamento dinâmico onde conexões são estabelecidas, mantidas por um período de tempo e depois liberadas da rede óptica, são propostos dois métodos para proteção contra falhas, *protection-at-lightpath* (PAL) e *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.

Embora sejam encontrados trabalhos que façam co-relação entre o problema da agregação de tráfego e o problema das falhas [67, 45], não é encontrado algum que relacione políticas de agregação de tráfego para o tratamento de falhas.

Alguns trabalhos participam da solução apresentada nesta dissertação [30, 35, 65]. Fawaz *et. al.* [30] propõem 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. Esta dissertação considera o uso de OSLAs para aplicação de políticas.

Iovanna et. *al.* [35] discutem 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. Esta dissertação faz uso do conceito de elasticidade apresentado neste trabalho.

Zang et. *al.* [65] investigam métodos de RWA para o tratamento de falhas. Proteger um caminho fim-a-fim é uma solução bastante atrativa para servir conexões clientes na gerência de falhas em redes ópticas WDM em malha. Para proteger contra qualquer falha, duas rotas disjuntas são necessárias entre os nós de origem-destino, uma para o caminho primário e outra para o caminho secundário (*backup*). Geralmente, o caminho mais curto entre o par origem-destino é usado como caminho primário e o *backup* é calculado depois que os enlaces do caminho primário forem removidos. Esta abordagem é chamada de *two step approach*. [65] investiga o uso desta abordagem em redes ópticas utilizando OXC com e sem a capacidade de conversão. O método *two step approach* é utilizado no simulador desenvolvido nesta dissertação.

4.3 Gerência de Redes Baseada em Políticas

A gerência de redes baseada em políticas é uma área que tem despertado interesse da comunidade de pesquisa há alguns anos atrás. Morris Sloman, líder do grupo de Gerência de Sistemas Distribuídos da Universidade Imperial College, é um dos precursores da área. Vários projetos relacionados com políticas foram desenvolvidos neste grupo desde a década de 1980 [50, 51]. [20] e [60] apresentam as características básicas de políticas e as principais atividades das organizações envolvidas na época (ex: ITU, IETF e DMTF). Os conceitos básicos da gerência baseada em políticas foram obtidos nestes artigos.

Em 1989, o IETF também fez uso dos conceitos de políticas na RFC *Policy Routing in Internet Protocols* [19]. Estes conceitos foram reutilizados em áreas como *Internet Accounting* [42], *Integrated Services* [61], *Differenciated Services* [12], *AAA* [58] e *IP Security* [13]. Alguns anos depois, pesquisas em roteadores baseados em rótulo e no RSVP lideraram a especificação do protocolo *Open Outsourcing Policy Service* (OOPS) pela IBM. Mais tarde, o grupo *Resource Allocation Protocol* (RAP) do IETF padronizou o *Common Open Policy Service*, uma extensão do OOPS.

Em 2003, o DMTF especificou o *Common Information Model* [6], um modelo de informação que mantém informações de políticas e permite a gerência de redes. Entretanto, o DMTF não provê um guia arquitetural para sistemas de gerência de redes baseado em políticas. O IETF criou um arcabouço que pode ser reutilizado por vários outros grupos de trabalho. Ainda em 2003, o IETF especifica o PCIM, uma extensão do CIM utilizando conceitos da arquitetura de políticas do grupo de trabalho RAP. As políticas definidas nesta dissertação são baseadas no PCIM.

Recentemente, a gerência de redes baseada em políticas tem sido reforçada com a grande discussão sobre computação autonômica (*autonomic computing*). [11] faz uma revisão da gerência de políticas para o paradigma da computação autonômica e mostra como este paradigma pode ser usado para gerência de sistemas de rede. O segmento (*self-healing*) da computação autonômica é um trabalho futuro vislumbrado nesta dissertação.

Alguns artigos apresentam uma visão prática da aplicação de políticas em redes e foram importantes para mensurar a relevância da aplicação de políticas em casos mais concretos. [36] descreve um arcabouço para o entendimento e implementação de políticas na gerência de redes de empresas. Uma arquitetura geral para gerência de políticas é apresentada, assim como uma instância na gerência de configuração. [57] apresenta uma visão geral de como a administração de uma rede pode ser simplificada definindo dois níveis de políticas, de negócio e de tecnologia. Um método para tradução das políticas do nível de negócio para o nível de tecnologia e para verificação de conflitos entre políticas é apresentado no artigo. A arquitetura definida pode ser aplicada em duas áreas, a gerência de desempenho de SLAs e de suporte de comunicação utilizando o protocolo IPSec [9].

A aplicação de políticas no contexto da engenharia de tráfego e DiffServ tem apresentado vários trabalhos [21, 55]. Em especial, a pesquisa apresentada nesta dissertação é uma extensão de [55]. [55] busca reduzir o *overhead* da rede óptica para remover e rerotear tráfego IP/MPLS de baixa prioridade. A solução proposta inclui uma arquitetura baseada em políticas e grupos de políticas para agregação de tráfego IP/MPLS em circuitos ópticos. Os resultados das simulações mostraram que o número de remoções de tráfego é menor quando são utilizadas políticas para gerenciar a agregação de tráfego na rede. Este trabalho não considera aspectos de falha na agregação de tráfego.

A solução proposta nesta dissertação possui outros trabalhos como suporte [62, 5, 7]. [62] discute as metas e requisitos de um controle de admissão baseado em políticas e propõe um arcabouço de políticas composto por elementos conhecidos no COPS (ex: PDP e PEP). Este arcabouço é instanciado nesta dissertação. [7] também é uma recomendação IETF e define o modelo de informação PCIM. É apresentado um modelo de informação orientado a objetos para representação de informações de políticas desenvolvidas pelo grupo de trabalho *Policy Framework* do IETF e como uma extensão do modelo CIM especificado pelo DMTF. As definições da área de políticas apresentadas nesta dissertação seguem as terminologias descritas em [5].

Capítulo 5

Solução Proposta

5.1 Introdução

A largura de banda grande dos enlaces e dos circuitos ópticos é característica marcante das redes ópticas que traz benefícios e novos desafios. Um destes desafios é, na ocorrência de uma falha, reduzir a perda de dados na rede. Este capítulo propõe uma solução para este desafio. A idéia geral desta solução é admitir tráfego na rede óptica utilizando políticas de agregação que considerem aspectos de falha, e em caso de ocorrência de falha, priorizar a readmissão de fluxos de tráfego de maior importância ou relevância.

A solução proposta é composta por uma arquitetura de gerência baseada em políticas e um conjunto de políticas para agregação de tráfego. A Seção 5.2 apresenta o cenário considerado e as Seções 5.3 e 5.4 apresentam, respectivamente, a arquitetura e as políticas da solução.

5.2 Cenário de Referência

Atualmente, as redes ópticas são portadoras de tecnologias que permitem a interação com vários outros tipos de redes. Neste contexto, a integração com redes IP/MPLS tem se mostrado promissora para provedores de serviço [32]. As redes IP/MPLS clientes com seus LSPs baseados em pacotes requisitam recursos ópticos de forma a atravessar o domínio e alcançar seu destino. O cenário de referência desta dissertação considera a integração entre redes IP/MPLS e a rede óptica, ver Figura 5.1.

A requisição por recursos ópticos e a notificação de falha são eventos tratados pela solução proposta. O sistema de gerência da rede óptica recebe requisições por conexões e uma notificação de falha com a finalidade de analisar a contribuição das políticas de agregação para a redução do impacto da falha. As restrições das políticas são especificadas pelos seguintes parâmetros do contrato de serviço:

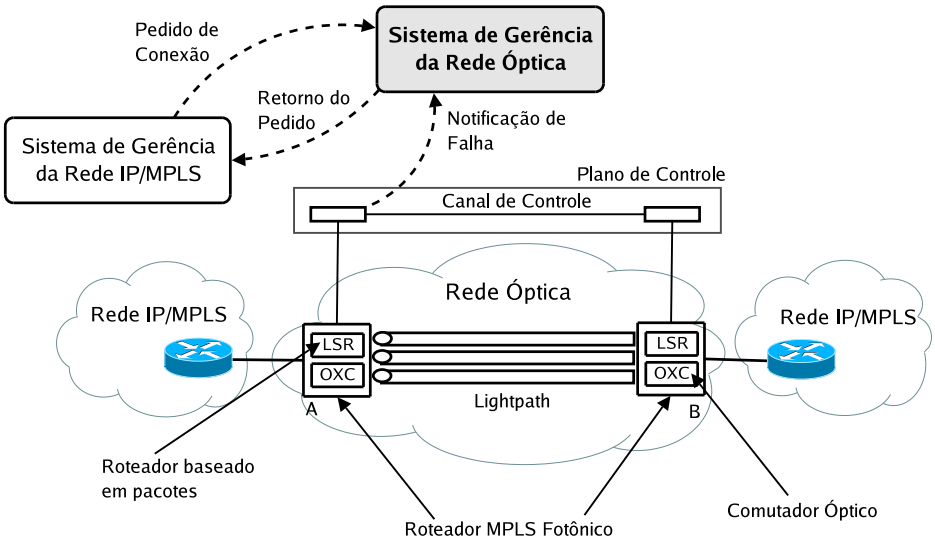


Figura 5.1: Cenário de Referência.

- *Classe de Serviço*: Define a prioridade de entrega do fluxo: alta prioridade (HP) ou baixa prioridade (LP).
- *Proteção*: Define o nível de proteção do fluxo podendo ser desprotegido ou ter a proteção 1+1, 1:1 ou 1:N.
- *Largura de banda requerida* (reqBw): Volume de tráfego real da conexão.
- *Largura de banda mínima* (minBw): Valor mínimo que a largura de banda do fluxo pode alcançar.
- *Largura de banda máxima* (maxBw): Valor máximo que a largura de banda do fluxo pode alcançar.

Os três níveis de largura de banda (reqBw, maxBw e minBw) foram especificados de forma a explorar o conceito da elasticidade utilizado no trabalho [35]. Uma das vantanges de se explorar este conceito é permitir a redução do número de preempções na rede. Por exemplo, dependendo da classe de serviço de um fluxo, pode-se alocar uma quantidade de banda maior do que a requerida (ex: maxBw), evitando que futuros pedidos de aumento da largura de banda provoque preempções na rede. A largura de banda equivalente à diferença entre *reqBw* e *maxBw* é chamada de largura de banda da elasticidade (*elastBw*) e ficará ociosa enquanto nenhum pedido de aumento de largura de banda for recebido.

A rede óptica deve prover mecanismos ou estratégias para todos os níveis de proteção exigidos pela rede IP/MPLS cliente. A ligação entre o tipo de proteção exigido no SLA é direta com o tipo de proteção oferecido pelo circuito óptico. Um circuito óptico pode participar

dos esquemas de proteção 1+1, 1:1 ou 1:N; ou ser desprotegido. Para simplicar a análise e a implementação consideramos que os circuitos ópticos são *single-hop*.

A notificação de uma falha é um evento do plano de controle óptico para o sistema de gerência. Embora o cenário de referência considere a existência de um plano de controle, nossa solução proposta está contida no contexto da gerência de redes ópticas e independe da tecnologia adotada para o plano de controle.

5.3 Arquitetura baseada em Políticas

A arquitetura proposta é constituída por quatro módulos de gerência e um repositório de políticas: Gerente de Recursos, Controle de Admissão, Gerente de Falhas e o Gerente de Políticas. A Figura 5.2 apresenta a arquitetura proposta.

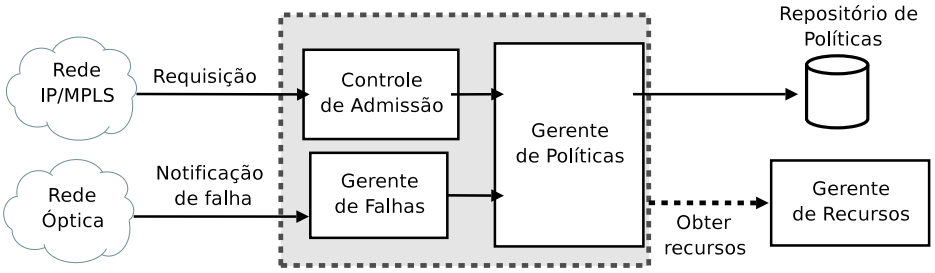


Figura 5.2: Arquitetura proposta.

- ▷ *Gerente de Recursos* (RM): O Gerente de Recursos é responsável por armazenar e prover informações sobre a topologia virtual e a topologia física da rede óptica. Os serviços do RM são requeridos pelos módulos AC, FM e PM (definidos em seguida). A topologia virtual representa o conjunto de circuitos ópticos estabelecidos entre os nós da rede óptica. Tipicamente, estes circuitos são conhecidos como *Forwarding Adjacencies* [8].

- ▷ *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 devidas políticas de admissão sejam aplicadas. O RM é invocado pelo AC para obter os circuitos ópticos que conectam o par (origem, destino) da requisição.

- ▷ *Gerente de Falhas* (FM): O Gerente de Falhas tem as funções de receber a notificação de falha enviada pelo plano de controle e decidir a ordem em que os fluxos afetados pela falha serão enviados 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 fluxos desprotegidos. A ordem

de prioridade para readmissão é estabelecida pela classe de serviço do fluxo, isto é, fluxos HP são enviados para readmissão antes de fluxos LP.

- *Gerente de Políticas* (PM): O Gerente de Políticas é equivalente ao *ponto de decisão das políticas* (PDP) do arcabouço para aplicação de políticas (Seção 3.2). Este módulo é responsável por receber fluxos IP/MPLS, decidir quais políticas serão executadas e instalar o fluxo caso exista algum circuito óptico que satisfaça as exigências da requisição. As condições das políticas decidem em qual circuito óptico o fluxo será admitido. As ações das políticas, por sua vez, instalam o fluxo na rede. Em alguns casos as ações removem fluxos de mais baixa prioridade em benefício da admissão de fluxos de mais alta prioridade. O *ponto de aplicação das políticas* (PEP) são os nós de borda da rede que, neste caso, são capazes de realizar a agregação de tráfego.

- *Repositório de Políticas* (PR): Armazena as políticas definidas. Este módulo é acessado somente pelo PM.

A requisição por recursos ópticos e a notificação de falha são eventos tratados de forma diferente pelos módulos da arquitetura. As Figuras 5.3 e 5.4 apresentam, respectivamente, como os módulos da arquitetura tratam estes eventos.

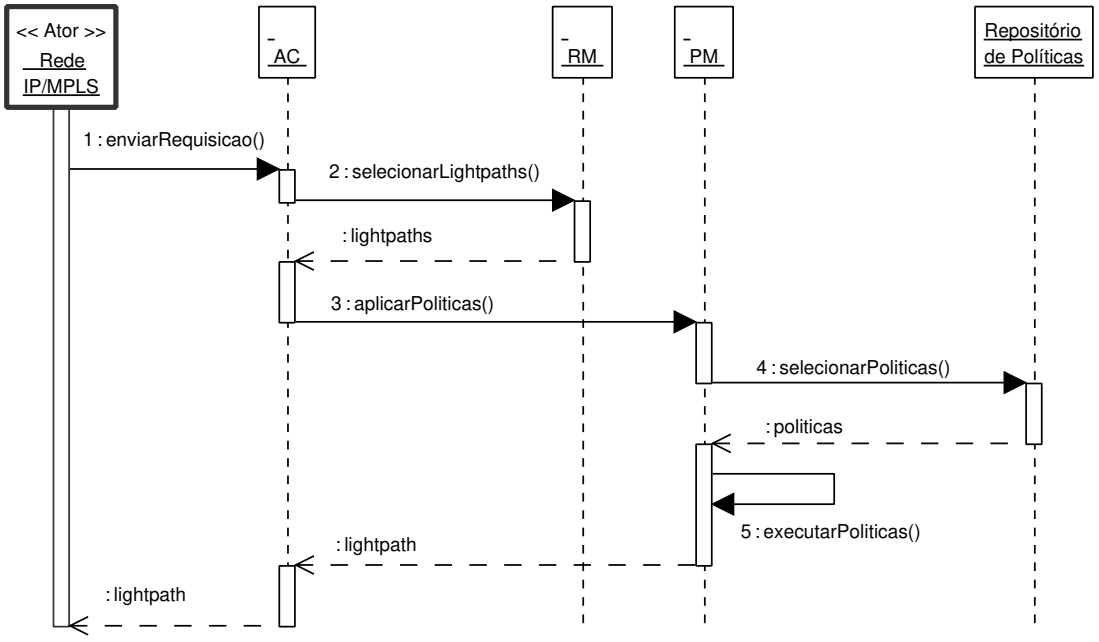


Figura 5.3: Tratamento do evento *requisição por recursos ópticos* pelos módulos da arquitetura.

Ao enviar uma requisição ao AC (1), a rede IP/MPLS cliente espera obter um circuito óptico que satisfaça as exigências do fluxo. O PM é o responsável por verificar a existência deste circuito. Os circuitos ópticos entre o par (origem,destino) são selecionados no AC (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 circuito óptico ou apenas um retorno vazio, o que significa que nenhum recurso foi encontrado e, então, a requisição é recusada.

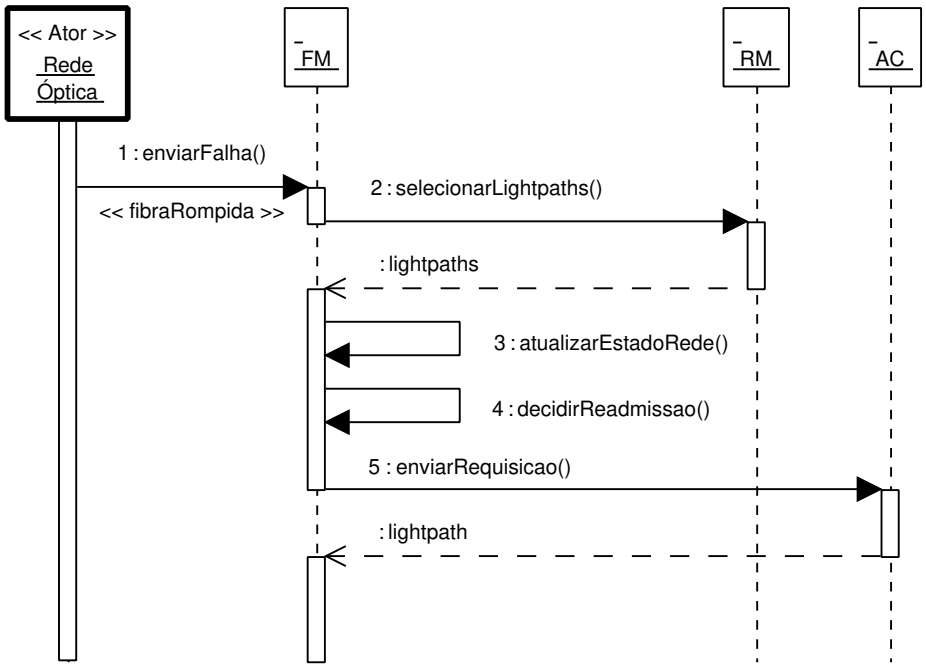


Figura 5.4: Tratamento do evento *notificação de falha* pelos módulos da arquitetura.

A notificação de falha sinaliza o rompimento de uma fibra. O plano de controle trata e notifica a falha ao FM após ter sido detectada. Ao enviar a notificação de falha (1), o FM obtém os circuitos ópticos contidos na fibra através do RM (2), sinaliza-os como falhos (3) e verifica quais fluxos não foram recuperados para que estes possam ser enviados ao PM (4). São enviados para readmissão 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 Figura 5.3.

5.4 Políticas

Não foi definida uma *ferramenta para edição e manipulação de políticas* (PMT). O papel das políticas propostas nesta dissertação é verificar a disponibilidade de circuitos ópticos que satisfaçam as restrições de largura de banda, proteção e classe de serviço especificadas no contrato de serviço. Em especial, as políticas analisam a proteção requerida e a disponível para admissão de tráfego como uma forma de buscar reduzir o impacto negativo gerado por uma falha. Esta é uma tarefa pró-ativa supostamente vinculada à gerência de falhas que, no entanto, está sendo realizada no controle de admissão. Instalar a requisição no circuito óptico também é uma responsabilidade das políticas.

As políticas de agregação também são utilizadas para readmissão de tráfego afetado por alguma falha ocorrida na infra-estrutura da rede. Para poder avaliar melhor a contribuição das políticas na redução tráfego bloqueado após uma falha, desenvolvemos três grupos de políticas. Cada um destes grupos possui diferentes capacidades de admissão. As características destes grupos são apresentadas em seguida.

- ▷ *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 circuito óptico com proteção 1+1 que tenha disponível a largura de banda requerida (ou largura de banda máxima se for o caso de uma requisição de alta prioridade). 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 circuito óptico desprotegido que tenha somente fluxos com a mesma classe de serviço da requisição. Em segundo, busca-se $(P2)$ admití-la em algum circuito óptico 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. Neste caso, são definidas três políticas. Caso a requisição desprotegida ainda não tenha sido admitida, então, primeiramente, busca-se $(P3)$ admití-la em algum circuito óptico desprotegido independente da classe de serviço dos fluxos já admitidos no circuito. Depois, busca-se admití-la $(P4)$ em algum circuito óptico desprotegido, preemptando, ou apenas removendo, fluxos de tráfego de mais baixa prioridade instalados no circuito. Por final, $(P5)$ busca-se admití-la em algum circuito

óptico protegido (exceto 1+1), preenchendo primeiro os circuitos 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). Nestas cinco políticas para admissão de tráfego desprotegido, a classe de serviço é um critério bastante utilizado durante o processo de admissão; porém, nas políticas definidas para tráfego protegido este critério não é bastante utilizado. Ao receber uma requisição protegida, o PM busca $(P6)$ admití-la em algum circuito óptico primário que tenha a mesma proteção requerida, independente da classe de serviço da requisição recebida. Depois, busca-se admití-la $(P7)$ em algum circuito óptico de mesma proteção, porém, preemptando, ou apenas removendo fluxos de tráfego desprotegidos de baixa prioridade instalados no circuito óptico.

- ▷ *Grupo de Políticas 3* (G3): Este grupo de políticas é o mais complexo, diferindo em dois pontos das políticas definidas no G2. O primeiro ponto é que se não houver algum circuito óptico com a mesma proteção requerida, então, busca-se admití-la em algum circuito que tenha um nível de proteção maior do que o requerido. Este método é utilizado especificamente para requisições 1:N que, neste caso, têm seus fluxos instalados em circuitos ópticos primários 1:1. Os circuitos 1+1 são exclusivos para tráfego 1+1. A segunda diferença é que o G3 permite a quebra de grupos de circuitos 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. Após a quebra de um grupo 1:N são liberados um grupo 1:1 e N-1 grupos de circuitos desprotegidos.

Além destes três grupos de políticas, outros tipos de políticas podem ser criados. Por exemplo, em seguida é apresentado um outro tipo de política que busca reduzir o volume de tráfego bloqueado após uma falha. Os resultados desta política não foram analisados.

- *Política extra*: Esta política busca priorizar a admissão de tráfego 1:N no circuito óptico 1:N disponível que apresentar a menor probabilidade de bloqueio após a ocorrência de uma falha. O cálculo desta probabilidade para um circuito primário 1:N é baseado na porcentagem de compartilhamento entre as fibras do seu grupo de proteção. Por exemplo, caso 70% das fibras de um circuito 1:N estejam compartilhadas com as fibras de outros circuitos 1:N do mesmo grupo, o rompimento de uma destas fibras implica na falha de mais de um circuito óptico. Neste caso, somente o tráfego de um dos circuitos afetados pela falha será desviado para o circuito de *backup*. A admissão de requisições 1:N é priorizada para circuitos que possuirem as menores probabilidades de compartilhamento entre fibras de seu respectivo grupo de proteção.

Capítulo 6

Simulador Desenvolvido

6.1 Introdução

Para validar a solução proposta simulou-se o cenário de referência. Existem alguns simuladores de redes ópticas disponíveis na literatura. O *GMPLS Lightwave Agile Switching Simulator* [44] é o mais completo deles. GLASS permite modelar e analisar o desempenho de algoritmos de roteamento, mecanismos de recuperação e protocolos de sinalização encontrados na área de redes ópticas. Dois fatores dificultaram o uso deste simulador em nossos experimentos: a falta de suporte aos mecanimos de proteção considerados e suas limitações para criação de topologias físicas. Adaptá-lo é uma opção, no entanto, o esforço de adaptação seria muito grande. Então, a abordagem escolhida foi desenvolver um novo simulador para realizar nossos experimentos.

O objetivo deste capítulo é apresentar o simulador desenvolvido. A arquitetura e o funcionamento do simulador são apresentados na Seção 6.2. Detalhes da modelagem do simulador são discutidos na Seção 6.3

6.2 Arquitetura e Funcionamento

Foi desenvolvido um simulador na linguagem Java para simular o cenário de referência e validar a solução proposta. Cada sistema externo ao sistema de gerência da rede óptica é representado por um módulo na arquitura, veja Figura 6.1. Estes módulos são: o gerador de requisições, gerador de falhas e o gerador de topologia virtual.

A numeração apresentada nos eventos da Figura 6.1 representam a ordem em que os eventos devem ocorrer para realizar um experimento. Alguns eventos necessitam de entradas e cada módulo obtém informações do RM para realizar sua função. A ordem e os eventos são: (1) carrega a topologia física, (2) gera a topologia virtual, (3) gera e envia as requisições, e (4) gera e envia a notificação de falha. Uma de duas topologias podem ser carregadas no simulador,

ambas implementadas diretamente em Java: a topologia preliminar ou a topologia da *National Science Foundation Network* (NSFNet). Estas topologias são apresentadas no Capítulo 7.

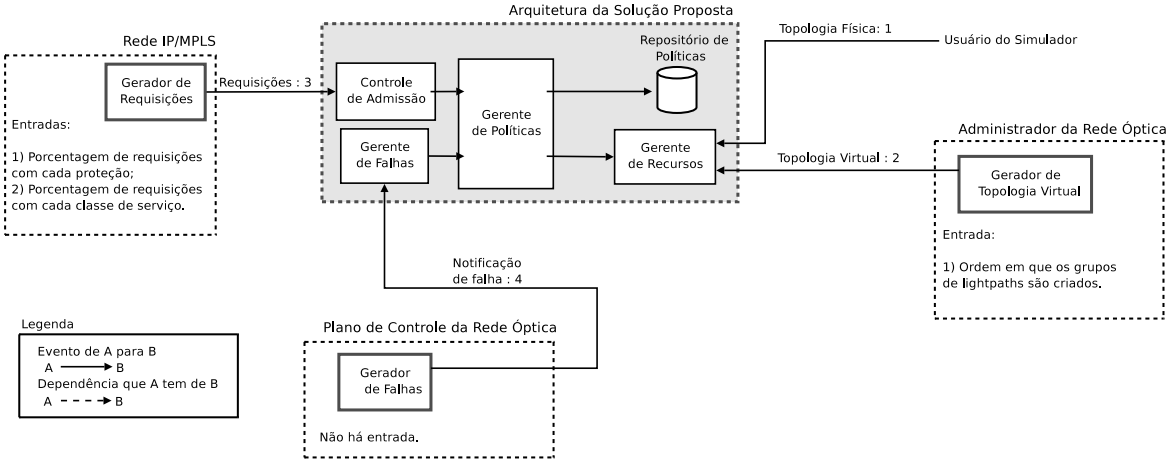


Figura 6.1: Arquitetura do simulador.

O evento (2) - gerar da topologia virtual - tem a carga da topologia física como dependência e possui a ordem de criação dos grupos de circuitos ópticos como entrada. No caso da ordem, por exemplo, primeiro tenta-se criar um grupo de circuitos ópticos 1:1, em segundo um grupo 1:N, em terceiro um grupo 1+1 e por fim um circuito desprotegido. Este ciclo existe até que não haja mais recurso óptico disponível e, conseqüemente, não seja mais possível criar um dos grupos de circuitos ópticos especificados.

O evento (3) - gerar requisições - tem a largura de banda total da rede como dependência e a porcentagem de requisições que deve ser gerada para cada proteção e classe de serviço. Por exemplo, 30% das requisições serão 1:1, 20% 1+1, 15% 1:N e 35% desprotegido; 50% das requisições serão HP e 50% LP. O evento (4) - gerar notificação de falha - não possui entrada. As Seções 6.2.1, 6.2.2 e 6.2.3 discutem respectivamente sobre como o gerador de requisições, gerador de falhas e gerador de topologia virtual executam suas funções.

No simulador, um fluxo pode assumir vários estados ao ser recebido pelo AC do sistema de gerência da rede óptica. Estes estados são: inicial, admitido, recusado, removido, falho, bloqueado, readmitido, recuperado e final, ver Figura 6.2.

O estado inicial representa a chegada de uma requisição e o estado final refere-se ao estado pelo qual o fluxo termina de forma normal (ex: cliente finaliza a transmissão). Após o estado inicial, a requisição pode ser admitida, recusada ou finalizada. Todo fluxo admitido pode passar para o estado removido, o qual requer decisão. Quando neste estado, o fluxo pode ser bloqueado (não pode ser agregado em outro circuito óptico) ou readmitido (o fluxo foi removido e pode ser agregado em outro circuito óptico). No estado readmitido, o fluxo pode ser removido outra vez e o ciclo continua ou o fluxo pode ser finalizado. De volta ao estado admitido, o fluxo pode ir

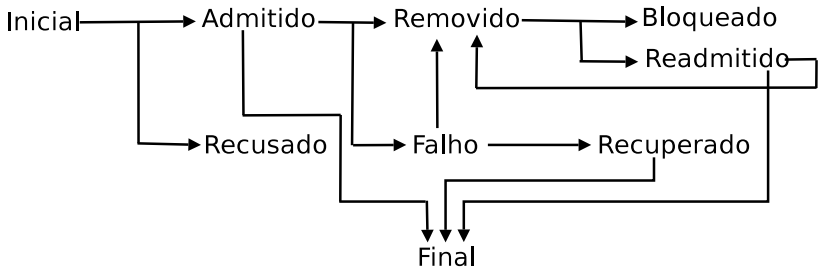


Figura 6.2: Estados e transições dos fluxos IP/MPLS.

para o estado falho. Este estado significa que o fluxo estava localizado em alguma fibra afetada por uma falha. No estado falho, o fluxo pode ser removido (tráfego desprotegido) continuando o ciclo assim como citado anteriormente. Por fim, o fluxo pode ser recuperado, isto é, o fluxo estava protegido e logo após a ocorrência da falha foi desviado diretamente para o circuito óptico de *backup*. No estado recuperado, o fluxo pode ser finalizado.

6.2.1 Gerador de Requisições

Várias cargas de rede são geradas para o AC, de 80% a 200% da capacidade total da rede com variação de 20%. Cada carga gera um experimento independente. As requisições de cada experimento são geradas de uma só vez, porém, a n-ésima requisição é enviada se, e somente se, for recebido o retorno da (n-1)-ésima requisição. Retorno nulo significa que a requisição foi recusada, caso contrário, é recebido o circuito óptico em que a requisição foi admitida.

O mecanismo utilizado para gerar as requisições é bastante simples, considere as seguintes porcentagens para os atributos proteção e classe de serviço: 30% 1:1, 20% 1+1, 15% 1:N e 35% desprotegido; 50% HP e 50% LP. A porcentagem de cada atributo é mapeada em um sub-intervalo de (0,1). Por exemplo, os intervalos para o atributo proteção são: (0,0.3] para 1:1, (0.3,0.5] para 1+1, (0.5, 0.65] para 1:N e (0.65,1) para desprotegido. O sorteio aleatório de um número entre (0,1) define a proteção da requisição. Por exemplo, o número 0.55 define a proteção 1:N. A geração da classe de serviço é equivalente à geração da proteção.

As larguras de banda da requisição (minBw, reqBw e maxBw) podem assumir qualquer valor inteiro do intervalo *[#LimiteInferior,#LimiteSuperior]*. Estes limites são definidos previamente antes da execução do experimento. O valor *reqBw* é sorteado do intervalo *[#LimiteInferior,#LimiteSuperior]*, e os valores *minBw* e *maxBw* são sorteados, respectivamente, dos intervalos *[#LimiteInferior,reqBw]* e *[reqBw,#LimiteSuperior]*.

6.2.2 Gerador de Falhas

O mecanismo para geração de uma falha também é bastante simples. Após obter a topologia física armazenada pelo gerente de recursos, o gerador de falhas escolhe aleatoriamente uma fibra desta topologia. O rompimento da fibra sorteada resulta na notificação do FM sobre a falha.

6.2.3 Gerador de Topologia Virtual

Os circuitos ópticos da topologia virtual são criados por grupos de proteção, isto é, grupos 1+1, 1:1 e 1:N. Cada grupo é formado pelos seus circuitos primários e *backups*. Para uniformizar o conceito, consideramos que um circuito desprotegido é equivalente a um grupo desprotegido.

A ordem especificada para os grupos de proteção define a ordem de criação dos circuitos ópticos. Por exemplo, {1:N, 1:N, 1:1, 1+1, desprotegido} define a ordem de criação dos circuitos, o primeiro e o último de um ciclo são respectivamente o 1:N e o desprotegido. Os grupos de proteção são criados seguindo ordem de grupos estabelecida até que não haja mais recursos disponíveis e, conseqüentemente, não seja possível criar nenhum dos grupos de proteção. Um grupo de proteção é criado se, e somente se, houver recursos disponíveis para estabelecer todos seus circuitos primários e o circuito de *backup*.

O método de dois passos (*two-step-approach* [65]) é utilizado para encontrar as rotas dos circuitos ópticos de cada grupo de proteção. Este método define que os circuitos primários devem ser disjuntos do circuito de *backup* e, para isso, os enlaces correspondentes às rotas dos circuitos primários ou de *backup* são removidos temporariamente do grafo da rede para garantir que os circuitos sejam disjuntos em enlace. Por exemplo, para um grupo de proteção: (1) encontra-se uma rota para o circuito de *backup*, (2) remove seus enlaces do grafo, (3) encontra-se uma rota para cada circuito primário, e (4) retorna os enlaces removidos para o grafo.

Devido à simplicidade e à praticidade, os algoritmos *Dijkstra* e *First-Fit* foram utilizados em conjunto com o método de dois passos. O *Dijkstra* encontra o menor caminho entre dois nós da rede e o *First-Fit* define que o primeiro lambda disponível da lista de lambdas de cada fibra deve ser atribuído para transmissão no enlace. Consideramos que todos os nós da rede são capazes de realizar a conversão completa de lambdas. Para maiores detalhes sobre estes algoritmos e a conversão de lambdas, ver o Capítulo 2.

6.3 Modelagem dos Módulos da Arquitetura Proposta

Os padrões (*patterns*) *singleton* e *factory* foram utilizados na modelagem dos módulos da arquitetura [31]. *Singleton* garante que uma classe é instanciada somente uma vez ao longo da execução do simulador. *Factory* define que somente serviços declarados pela interface de uma

classe poderão ser requisitados por outras classes. Este padrão garante o encapsulamento de serviços de uma classe. As três seções seguintes discutem sobre a modelagem dos módulos da arquitetura proposta.

Controle de Admissão e Gerente de Falhas

Cada um dos módulos AC e FM foi modelado em uma única classe, ver Figura 6.3.

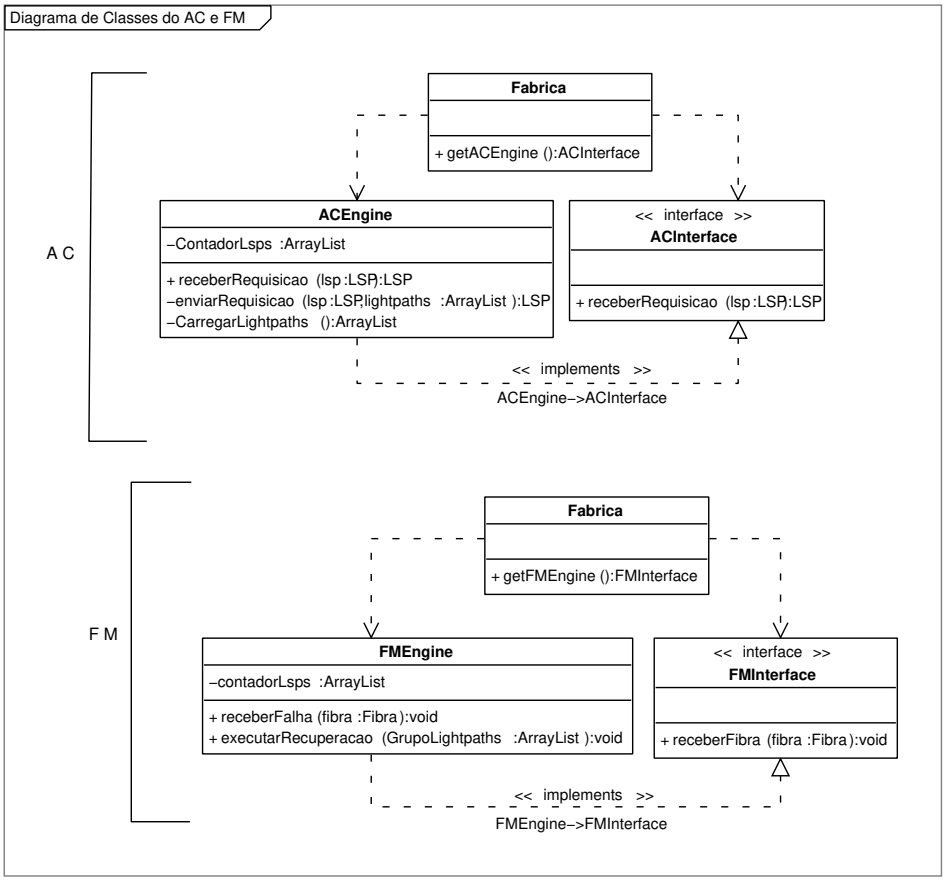


Figura 6.3: Diagrama de classes do AC e do FM.

Os principais métodos implementados pelo AC são:

- *ReceberRequisição()*: Recebe uma requisição da rede IP/MPLS e retorna nulo se a requisição for recusada ou o circuito óptico se a requisição for admitida. Este método invoca o método *CarregarLightpaths()*.

- *EnviarRequisição()*: Envia a requisição para o PM aplicar as devidas políticas. Um circuito óptico é retornado se a requisição for admitida, caso contrário é retornado nulo.
- *CarregarLightpaths()*: Requisita ao RM todos os circuitos ópticos entre a origem e destino especificados na requisição.

Os principais métodos implementados pelo FM são:

- *ReceberFalha()*: Recebe uma notificação do plano de controle da rede óptica sobre o rompimento de uma fibra.
- *ExecutarRecuperação()*: Este método possui várias tarefas: (1) verifica qual esquema de proteção está configurado para cada circuito óptico da fibra recebida, (2) desvia para o respectivo circuito de *backup* somente o tráfego do circuito primário que for eleito para proteção (grupos de proteção 1:N necessitam de uma eleição para decidir qual circuito primário será protegido caso a falha afete mais de um circuito do seu grupo), (3) retorna o tráfego afetado pela falha que não foi protegido.

Ambos os módulos AC e FM também contabilizam as requisições e seus respectivos estados com o intuito de medir os resultados do experimento.

Gerente de Recursos

Juntamente com o PM, o RM é um dos módulos mais complexos do protótipo. O RM define e gerencia classes que representam os recursos ópticos da topologia física e da topologia virtual, ver a Figura 6.4. O controle e armazenamento estão focados em recursos especificados pelas topologias física e virtual. Para a topologia física foram definidas as classes *Fibra* e *OXC*. Para a topologia virtual foram definidas as classes *Lightpath* e *LSP*.

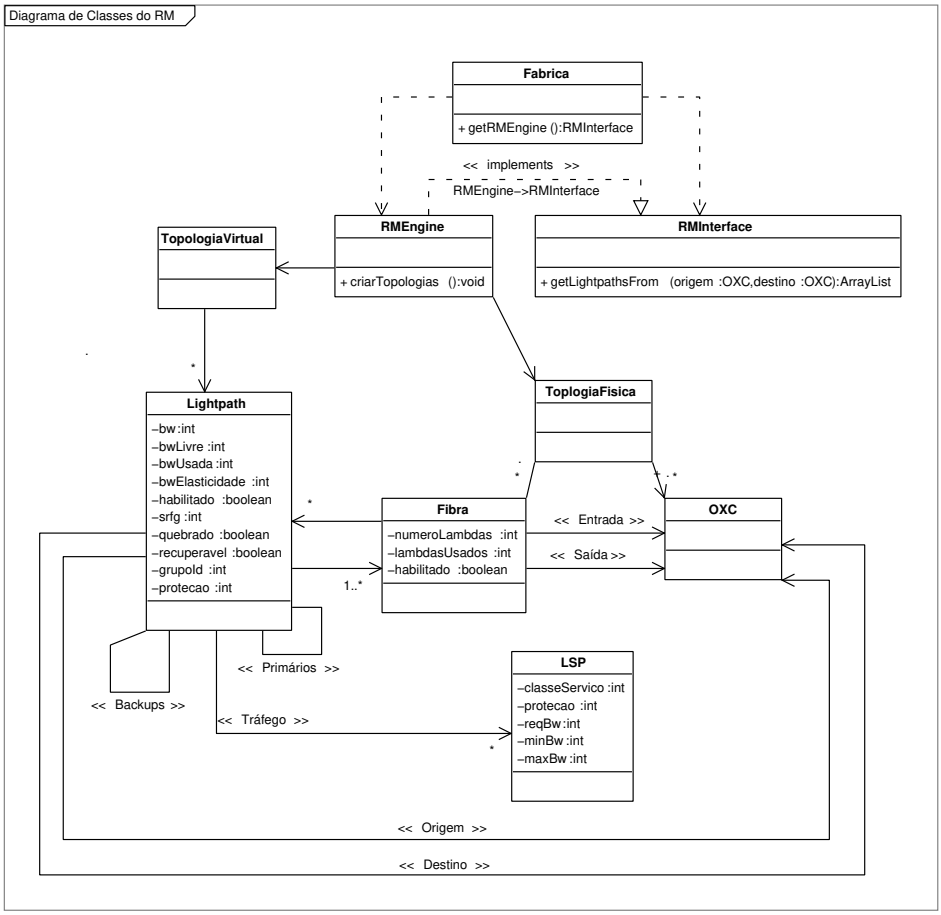


Figura 6.4: Diagrama de classes do RM.

Gerente de Políticas e Repositório de Políticas

A modelagem do PM foi baseada na especificação dos modelos de informação CIM [6] e PCIM [7], ver Figura 6.5. Uma breve discussão sobre o PCIM é encontrada na Seção 3.4.

A classe *PolicyRule* representa uma política e as classe *PolicyCondition* e *PolicyAction* representam suas respectivas condições e ações, as quais são construídas através de composições

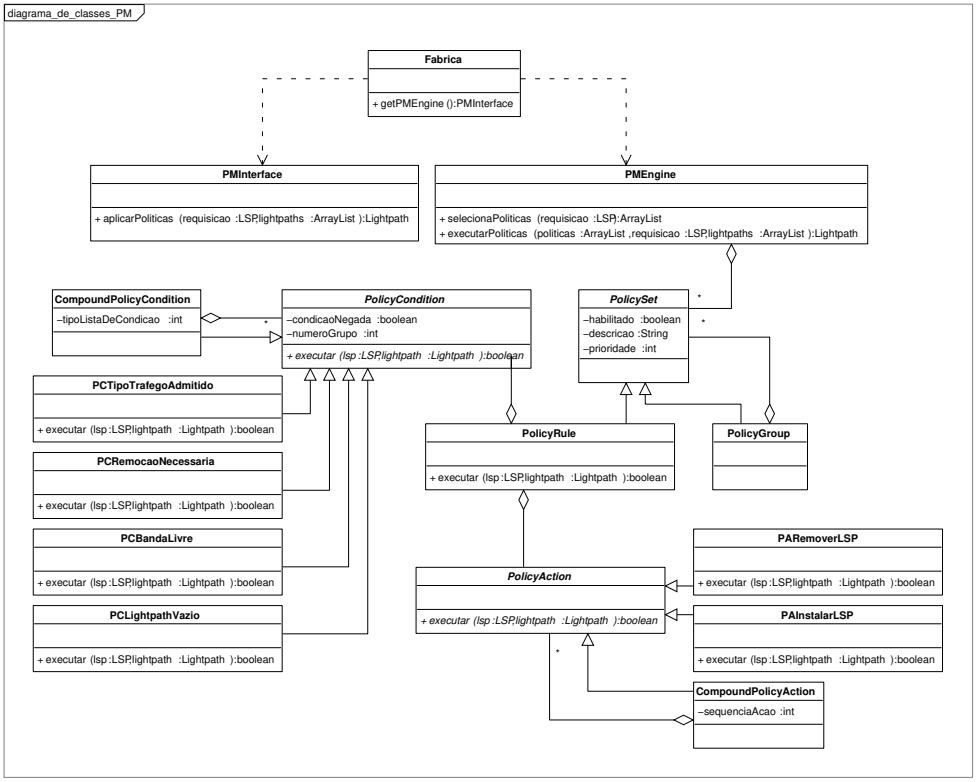


Figura 6.5: Diagrama de classes do PM.

a partir das classes *CompoundPolicyCondition* e *CompoundPolicyAction*. Por exemplo, para compor a política *(P1)* definida na Seção 3.3 é necessário instanciar a *CompoundPolicyCondition* a qual será composta por instâncias das classes *PCTypeOfProtection*, *PCTypeOfTrafficAdmitted*, *PCEmptyLightpath* e *PCFreeBandwidth*. No caso da classe *PCEmptyLightpath*, o atributo *conditionNegated* da classe *PolicyCondition* deve ser verdadeiro. Para as ações é preciso instanciar somente a classe *PAInstallLsp*. Os atributos *conditionListType* e *groupNumber* da classe *PolicyRule* combinados definem se as condições serão compostas na forma disjuntiva (DNF) ou conjuntiva (CNF). A Seção 3.4 apresenta detalhes sobre as composições DNF e CNF.

A forma como o PM foi modelado permite que os recursos de mais de um domínio sejam gerenciados. A Figura 6.6 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 simples, utilizando apenas um nível de grupo, ou sobre vários níveis de grupos, ver Figura 6.6. Para um 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 de políticas.

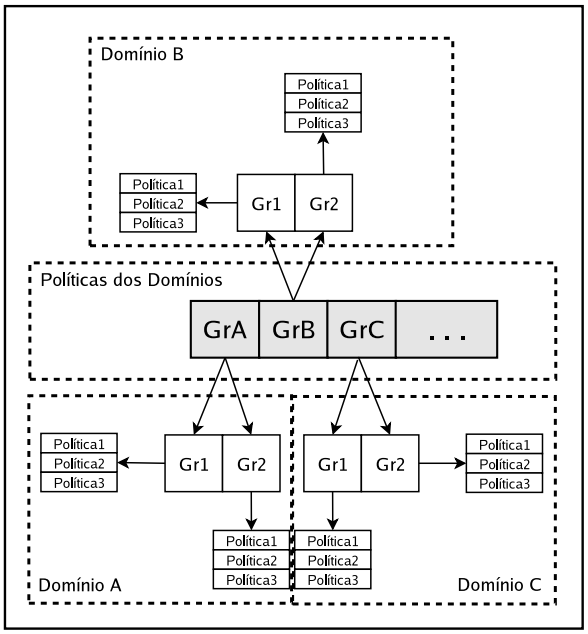


Figura 6.6: Exemplo para criação de um caso de políticas simples.

O PR foi incorporado ao PM. As políticas são instanciadas e armazenadas em um *ArrayList*. Foi discutida a abordagem de se modelar o PR como um módulo separado e utilizando o protocolo LDAP para o armazenamento das políticas, no entanto, a abordagem inicial é suficiente para cobrir a solução proposta.

Capítulo 7

Experimentos e Resultados

7.1 Introdução

O simulador apresentado no Capítulo 6 foi utilizado para realizar vários experimentos. A Seção 7.2 apresenta a configuração dos experimentos realizados, a Seção 7.3 discute os resultados obtidos, e, por fim, a Seção 7.3.3 faz uma análise geral dos resultados obtidos.

7.2 Experimentos

O objetivo dos experimentos apresentados a seguir é verificar se a solução proposta no Capítulo 5 permite reduzir o impacto negativo gerado pelo rompimento de uma fibra. Doze experimentos foram realizados em duas topologias físicas diferentes.

Os experimentos foram construídos a partir das variáveis de entrada do simulador: (1) a topologia física, (2) a ordem de criação dos grupos de proteção da topologia virtual, e (3) a porcentagem de requisições geradas para cada classe de serviço e proteção. A notificação de falha é uma entrada do simulador, porém não pode ser variável. Além destas variáveis de (1) a (3), algumas características embutidas no simulador também poderiam ser variadas, por exemplo, os algoritmos de roteamento e de atribuição de lambdas. Os experimentos realizados consideram somente a variação de (3) e (1). Considerar a variação de (2) implica em um grande número de experimentos. Esta atividade é um trabalho futuro.

A ordem de criação dos grupos de proteção (1) considerada para todos os experimentos é {1:N, 1:N, 1:1, 1+1, desprotegido}. Esta ordem foi escolhida para poder analisar melhor a política de quebra de grupos 1:N. Consideramos que a proteção 1:N é formada por um circuito óptico de *backup* e três circuitos ópticos primários, isto é, um grupo de proteção 1:3.

A atribuição das porcentagens para as proteções e as classes de serviços (3) são obtidas através de combinações de valores dos conjuntos $A = \{40\%, 20\%, 20\% \text{ e } 20\%\}$ e $B = \{20\%,$

80% e 50%}, ver Tabela 7.1. Os quatro tipos de proteções e os dois tipos de classes de serviço podem assumir somente valores do conjunto A e B, respectivamente. Desta forma, somente uma das proteções terá a porcentagem de 40% permitindo que esta proteção seja analisada separadamente das demais proteções. Para as classes de serviço são geradas combinações onde uma classe possui uma porcentagem maior ou menor do que a outra classe, ou ambas possuem a mesma porcentagem.

	Proteções				Classes de Serviço	
Cenário	Desprotegido	1:N	1:1	1+1	HP	LP
1	40%	20%	20%	20%	20%	80%
2	40%	20%	20%	20%	80%	20%
3	40%	20%	20%	20%	50%	50%
4	20%	40%	20%	20%	20%	80%
5	20%	40%	20%	20%	80%	20%
6	20%	40%	20%	20%	50%	50%
7	20%	20%	40%	20%	20%	80%
8	20%	20%	40%	20%	80%	20%
9	20%	20%	40%	20%	50%	50%
10	20%	20%	20%	40%	20%	80%
11	20%	20%	20%	40%	80%	20%
12	20%	20%	20%	40%	50%	50%

Tabela 7.1: Configuração dos experimentos realizados.

Os experimentos da Tabela 7.1 são independentes. Ao enviar as requisições e a notificação de falha do i-ésimo experimento, os circuitos ópticos são "reinicializados", isto é, o tráfego dos circuitos ópticos são desinstalados e os circuitos são reabilitados para que as requisições e a notificação de falha do (i-1)-ésimo experimento sejam enviados.

De uma forma geral, os experimentos são realizados sobre duas topologias físicas. Os circuitos ópticos de cada uma destas topologias são gerados somente uma vez e utilizando a mesma ordem de criação apresentada para os grupos de proteção. Cada experimento apresentado na Tabela 7.1 é simulado 7 vezes, uma para cada carga de rede (80%, 100%, 120%, 140%, 160%, 180% e 200%) e com as seguintes características: as requisições são geradas conforme a carga da rede, a notificação da falha é enviada após o envio das requisições e os circuitos ópticos são "reinicializados" ao término de cada simulação. Por exemplo, a quantidade de requisições desprotegidas geradas para a carga de 120% do experimento 1 é calculada da seguinte forma: 36 (capacidade da rede) * 1.2 (carga de tráfego a ser gerada) * 0.4 (porcentagem de requisições desprotegidas) = 17,28 Gb/s de tráfego gerado.

7.3 Resultados

Os resultados obtidos nos experimentos são apresentados em dois tipos de gráficos, específicos e gerais. O objetivo dos gráficos específicos, por exemplo a Figura 7.2(a), é apresentar as porcentagens relativas à admissão de tráfego, e ao bloqueio e tráfego afetado após uma falha. Estes gráficos foram obtidos a partir da média de 20 simulações para cada carga de tráfego dos experimentos. Os gráficos gerais, por exemplo a Figura 7.3(a), apresentam uma visão geral das vantagens da aplicação de políticas através de um comparativo do desempenho entre utilizar e não utilizar políticas para admissão de tráfego na rede óptica.

Devido à simplicidade, consideramos que o grupo G1 é equivalente a um caso sem políticas. As Seções 7.3.1 e 7.3.2 apresentam os resultados obtidos nas topologias físicas preliminar e NSFNet, respectivamente.

7.3.1 Topologia Física Preliminar

A topologia física preliminar é formada por 7 nós, ver Figura 7.1. Para a simulação, considera-se que cada enlace óptico possui duas fibras unidirecionais (uma para cada direção) e cada fibra possui 10 lambdas de 1 gigabit por segundo. Com esta infra-estrutura, o gerador de topologia virtual criou 37 circuitos ópticos entre o par de origem e destino (2,6): 9 grupos desprotegidos, 2 grupos 1+1, 2 grupos 1:1 e 5 grupos 1:3.

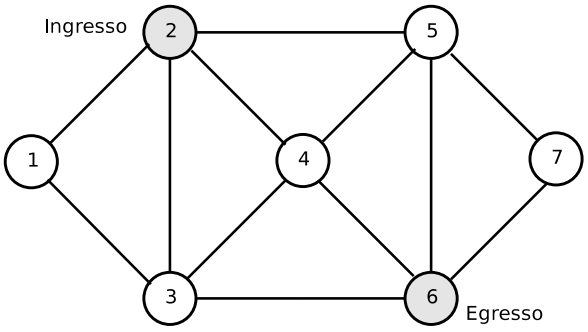


Figura 7.1: Topologia física preliminar.

De uma forma geral, a aplicação das políticas apresentou-se relevante na topologia preliminar, ver Figura 7.2.

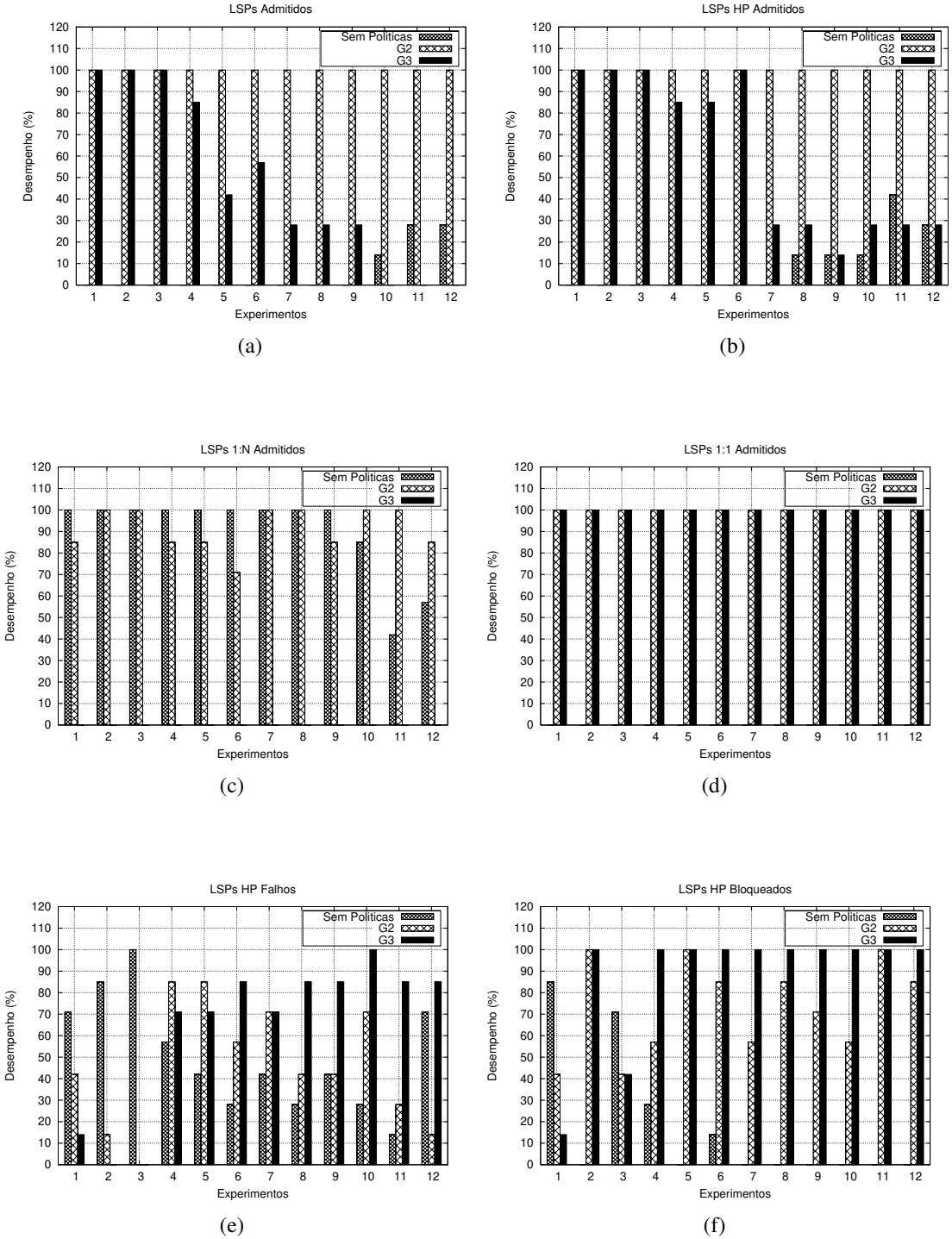


Figura 7.2: Visão geral do desempenho das políticas na topologia preliminar.

Os grupos de políticas G2 e G3 apresentaram um desempenho melhor do que o grupo "sem políticas" na admissão de tráfego. O grupo G2 em especial, obteve resultados melhores do que o grupo "sem políticas" em todos os experimentos. Ao analisar o desempenho das políticas sobre os tipos de tráfego admitidos, notamos que as políticas permitem priorizar tipos de tráfego específicos conforme a necessidade do administrador da rede. Porém, aumentar a prioridade de admissão de um tipo de tráfego implicou em reduzir a prioridade de admissão de outro tráfego. Fica a cargo do administrador querer ou não balancear a admissão dos diversos tipos de tráfego na rede.

O desempenho na admissão geral de tráfego é mantido na admissão de tráfego HP, Figura 7.2(b);porém, com uma melhora do grupo G3 nos experimentos de 4 a 6 (maior quantidade tráfego 1:N gerado) e de 10 a 12 (maior quantidade de tráfego 1+1 gerado). Isto significa que conforme planejado na definição dos grupos de políticas, o uso de políticas permitiu priorizar a admissão de tráfego HP. Para o grupo G3, os resultados não apresentaram superiores aos do grupo "sem políticas" para todas as cargas de rede, ver experimentos de 7 a 12.

Na admissão de tráfego 1:1, Figura 7.2(d), os grupos de políticas mostram resultados superiores aos do grupo "sem políticas" em todas das cargas de rede dos experimentos. Em especial, isto mostra que a capacidade do grupo G3 de quebrar grupos 1:N em benefício de fluxos 1:1 se demostrou eficiente quando comparado com o grupo "sem políticas".

O uso das políticas para admissão de tráfego 1:N teve seu desempenho afetado pelo bom desempenho da admissão de tráfego 1:1. O grupo "sem políticas" obteve um desempenho melhor do que os grupos de políticas em quase todas as cargas de rede. O grupo G3 não foi relacionado na Figura 7.2(c).

Os LSPs afetados pela falha foram contabilizados após o rompimento de uma fibra. O uso das políticas, neste contexto, apresentou-se relevantes somente para os experimentos de 4 a 12 (Figura 7.2(e)). Outras políticas poderiam ser desenvolvidas para reduzir o volume de tráfego afetado pela falha, por exemplo, desenvolver políticas que considerem a probabilidade de falha de um enlace.

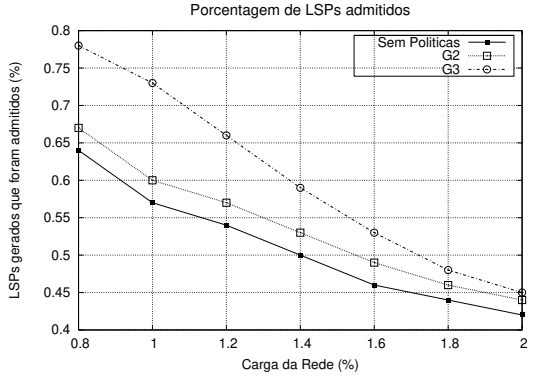
A Figura 7.2 mostra que o uso de políticas é importante para admissão de tráfego em redes ópticas, é possível priorizar a admissão de fluxos de tráfego específicos e admitir volumes de tráfego maiores do que o caso onde não são aplicadas políticas. Além disso, as políticas permitem reduzir o bloqueio de tráfego após a tentativa de readmissão do tráfego afetado pela falha. Mesmo que o grupo "sem políticas" tenha obtido um desempenho melhor do que os grupos de políticas quanto ao volume de tráfego afetado pela falha, a Figura 7.2(f) mostra que o uso de políticas não se apresentou relevante somente nos experimentos 1 e 3.

LSPs Admitidos

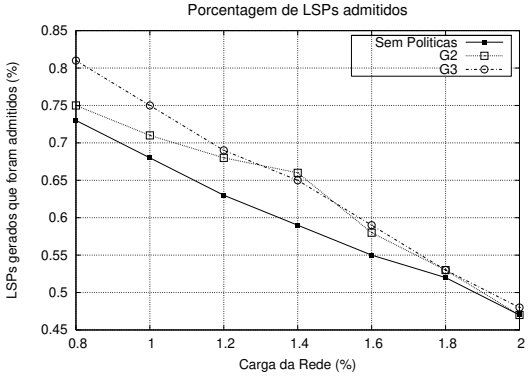
As políticas apresentaram bons resultados na admissão de tráfego quando comparados com o grupo "sem políticas", ver Figura 7.3. O grupo G3 mostrou-se relevante na admissão de tráfego

em baixas cargas de rede e nos experimentos de 1 a 6. O motivo principal para este desempenho é a sua grande capacidade de admissão de tráfego HP e tráfego 1:1. Nos experimentos de 7 a 12, o grupo G3 não apresentou bons resultados.

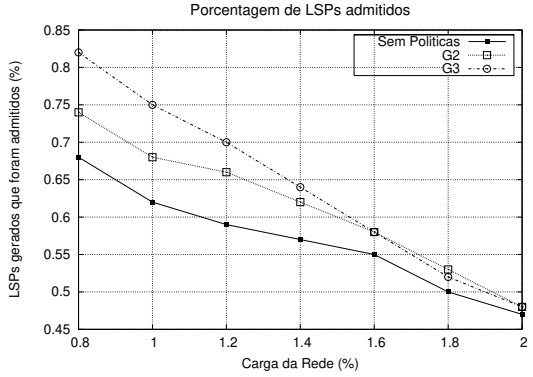
Ao contrário do grupo G3, as políticas do grupo G2 não são gulosas ao ponto de prejudicar a admissão de alguns fluxos de tráfego em benefício de outros fluxos. O G2 foi desenvolvido com o intuito de buscar satisfazer os diversos tipos de requisições, sem provocar grandes impactos na admissão de tráfego específico. Os resultados do G2 não são tão relevantes quanto os resultados obtidos pelo G3 nos experimentos de 1 a 4, mas são bons o suficiente para admitir um volume de tráfego maior do que o grupo "sem políticas" em todos os experimentos.



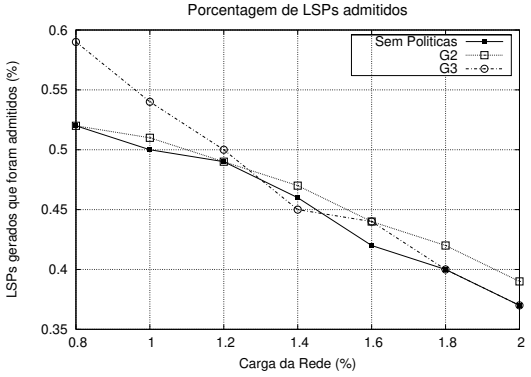
(a) Experimento 1.



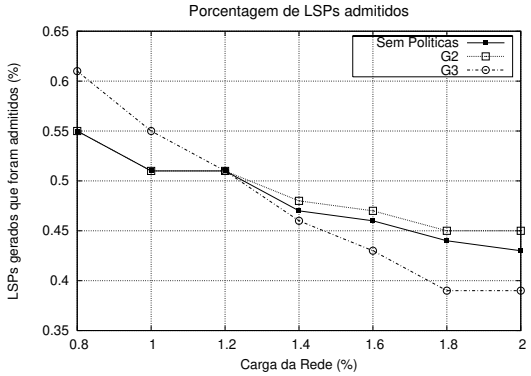
(b) Experimento 2.



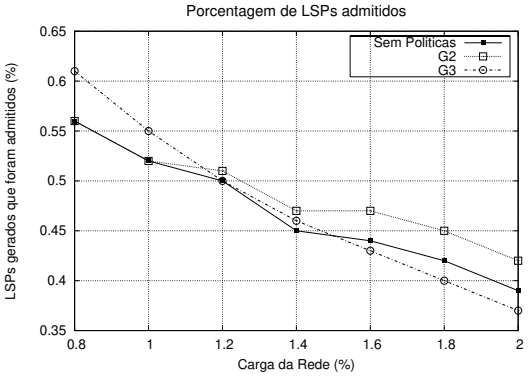
(c) Experimento 3.



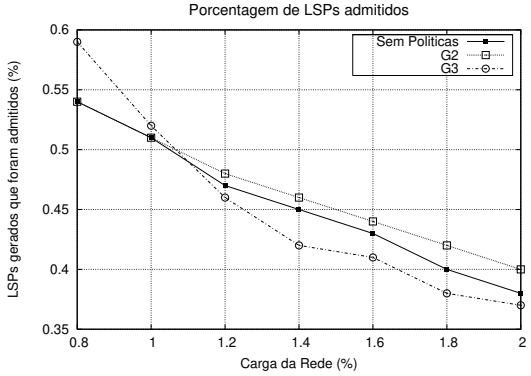
(d) Experimento 4.



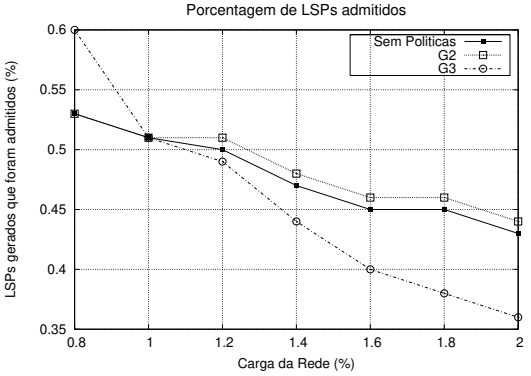
(e) Experimento 5.



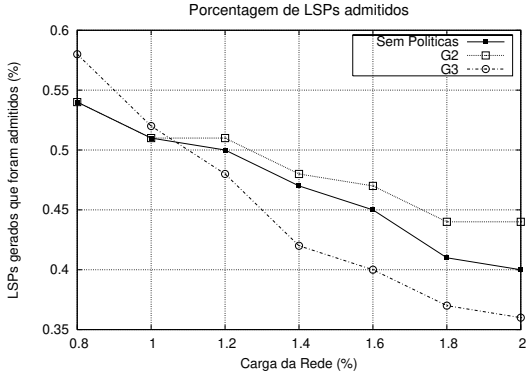
(f) Experimento 6.



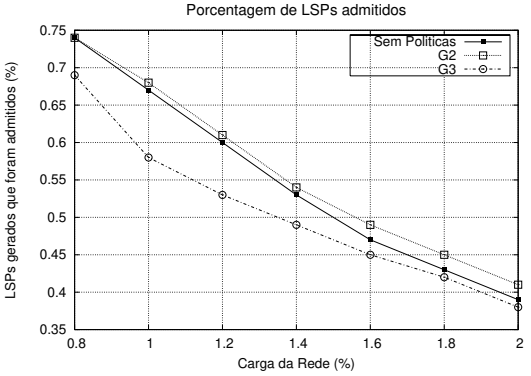
(g) Experimento 7.



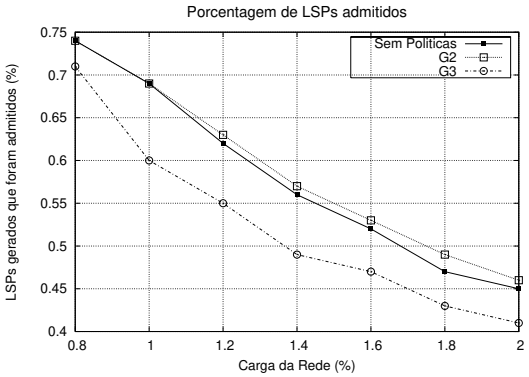
(h) Experimento 8.



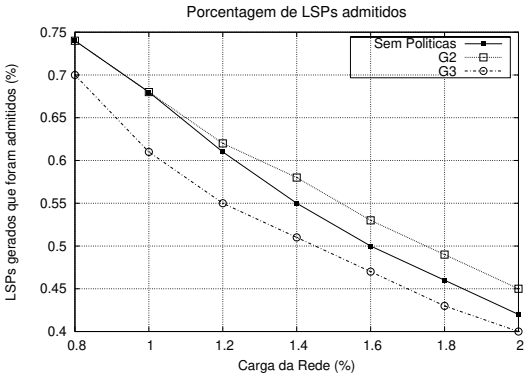
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



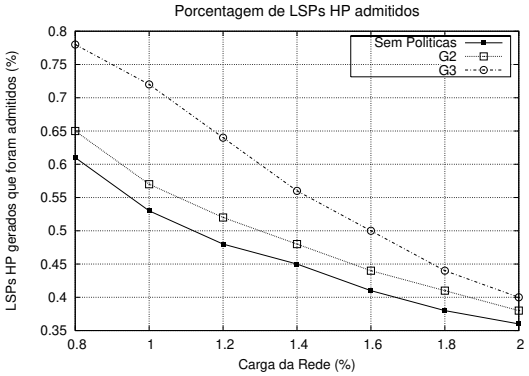
(l) Experimento 12.

Figura 7.3: Tráfego admitido na topologia preliminar.

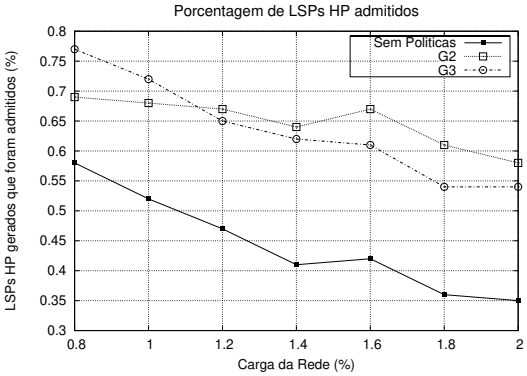
LSPs HP Admitidos

A admissão geral de tráfego possui um comportamento bastante similar ao da admissão de tráfego HP, ver Figura 7.4. O grupo G2 continua com o desempenho superior ao do grupo "sem políticas" em todos os experimentos e o desempenho do grupo G3 ainda é melhor nos experimentos de 1 a 4, porém, com melhoras nos experimentos de 4 a 6 e de 10 a 12. Isto mostra que ambos os grupos de políticas G2 e G3 permitem priorizar a admissão de tráfego HP na rede.

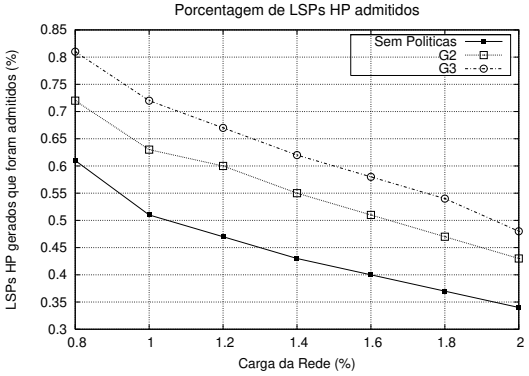
Em especial, os grupos de políticas obtiveram desempenhos melhores nos experimentos de 1 a 3, onde o volume de tráfego desprotegido é maior do que o tráfego gerado para os tráfegos protegidos (1:N, 1:1 e 1+1). Este comportamento é esperado pois a classe de serviço é considerada como um critério de admissão somente nas políticas para tráfego desprotegido. Nos outros experimentos, o bom desempenho das políticas é justificado somente pela capacidade de admissão das políticas.



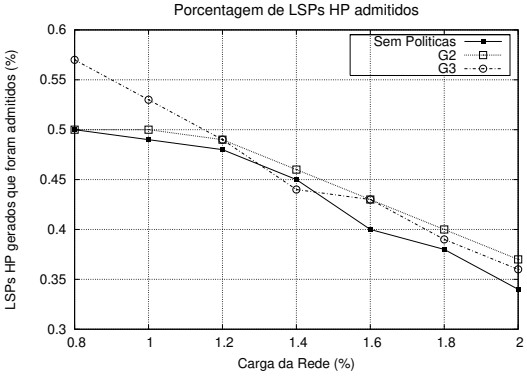
(a) Experimento 1.



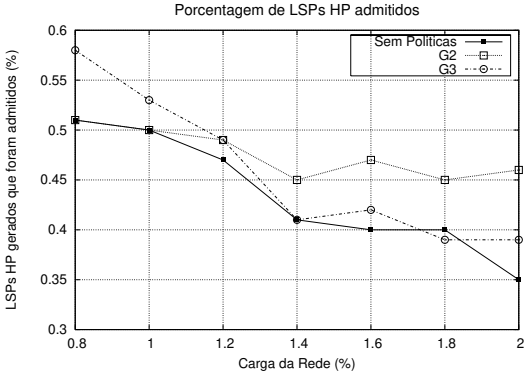
(b) Experimento 2.



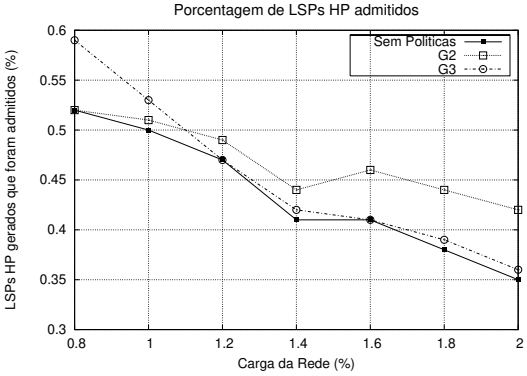
(c) Experimento 3.



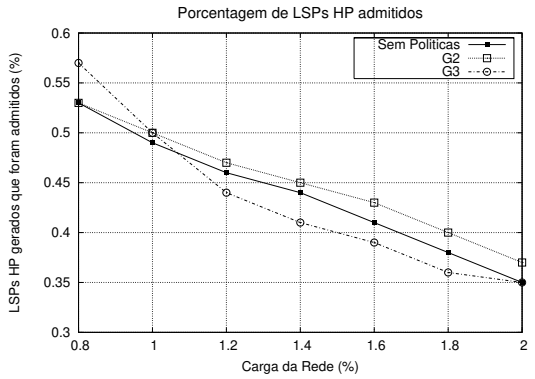
(d) Experimento 4.



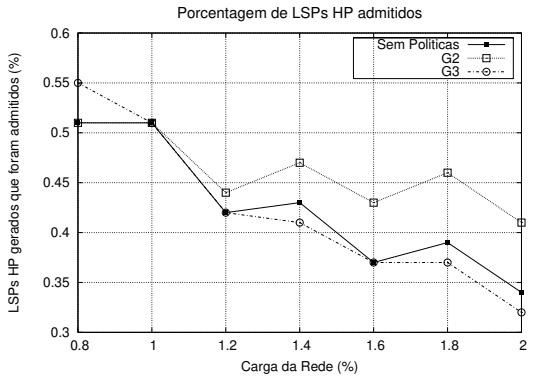
(e) Experimento 5.



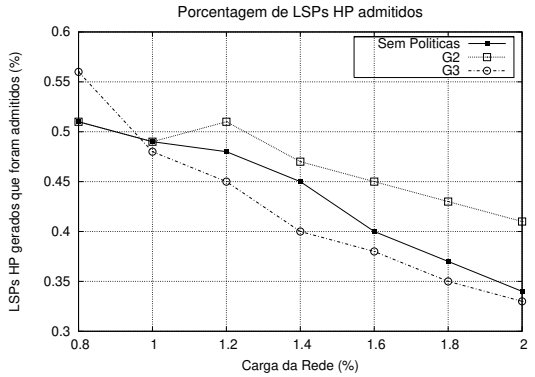
(f) Experimento 6.



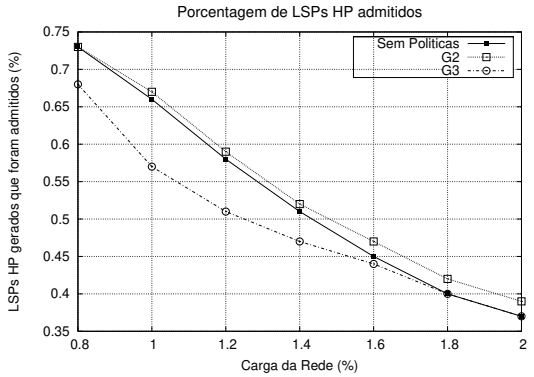
(g) Experimento 7.



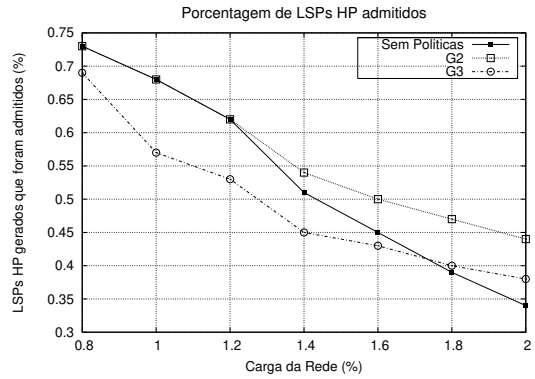
(h) Experimento 8.



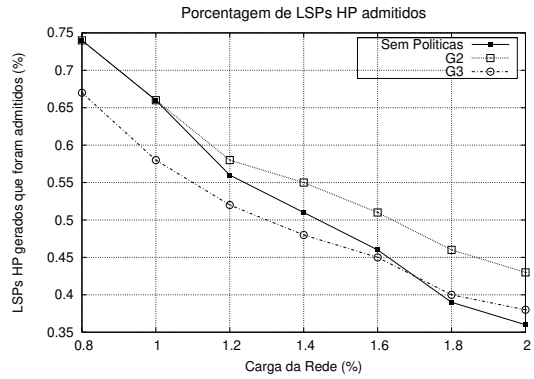
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



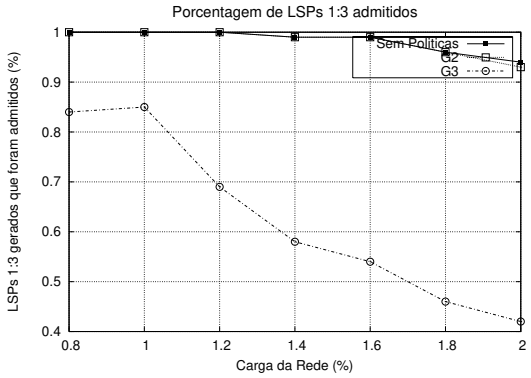
(l) Experimento 12.

Figura 7.4: Tráfego HP admitido na topologia preliminar.

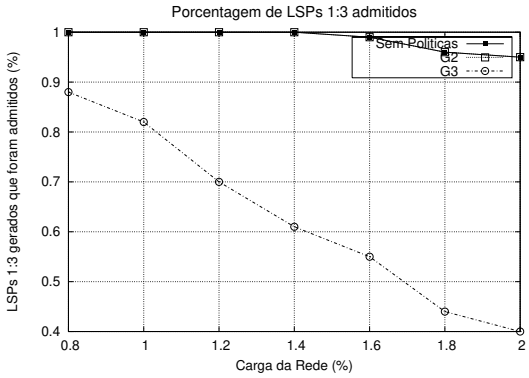
LSPs 1:N Admitidos

A admissão de tráfego 1:N utilizando as políticas não mostrou bons resultados, ver Figura 7.5. O desempenho do grupo G2 é muito similar ao do grupo "sem políticas". Dos experimentos de 1 a 9, os grupos G2 e "sem políticas" admitiram 100% do tráfego gerado em quase todas as cargas de rede. A abundância de circuitos ópticos na rede óptica é a principal explicação para este comportamento. No entanto, nos experimentos de 10 a 12, este desempenho é reduzido.

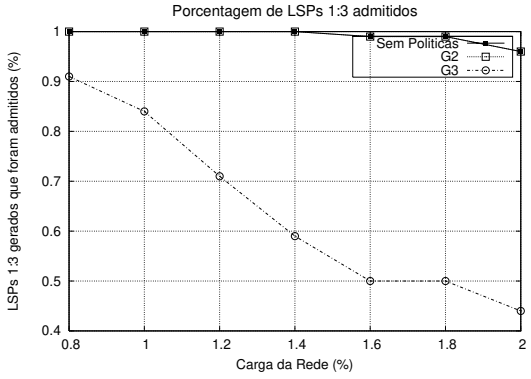
O desempenho do grupo G3 na admissão de tráfego 1:N é impactado pela quebra de circuitos ópticos 1:N em benefício de fluxos 1:1. Esta característica fez com que o desempenho do grupo G3 ficasse abaixo dos demais grupos em todos o experimentos.



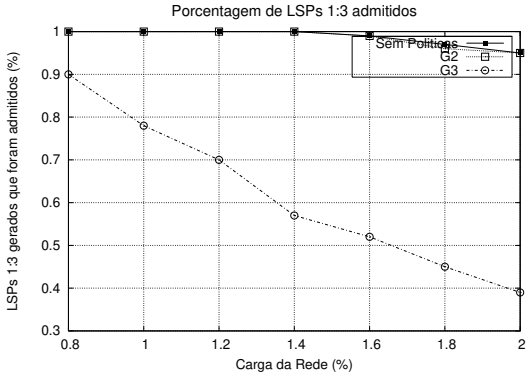
(a) Experimento 1.



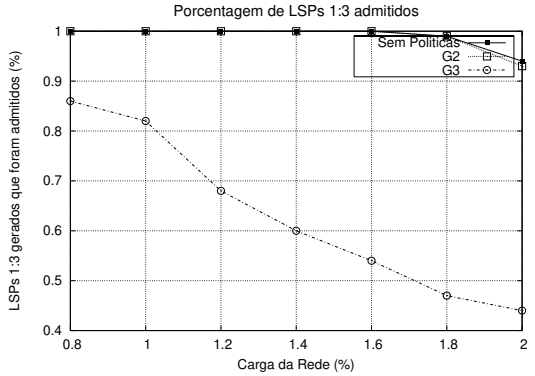
(b) Experimento 2.



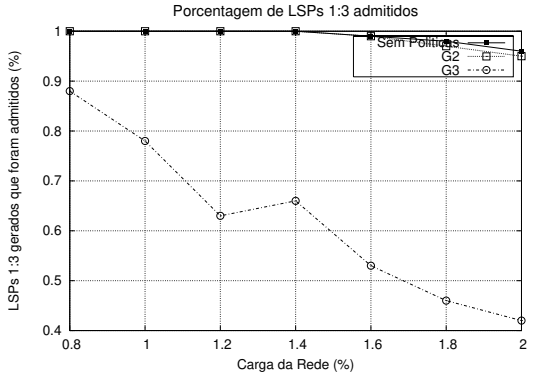
(c) Experimento 3.



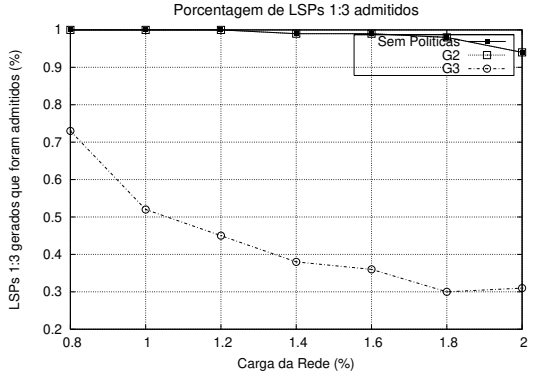
(d) Experimento 4.



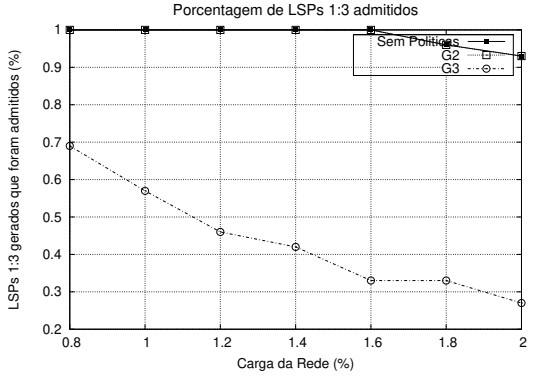
(e) Experimento 5.



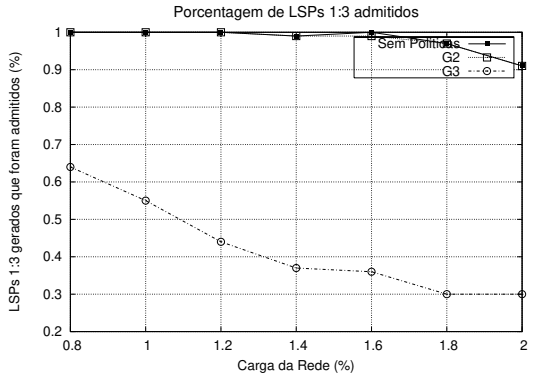
(f) Experimento 6.



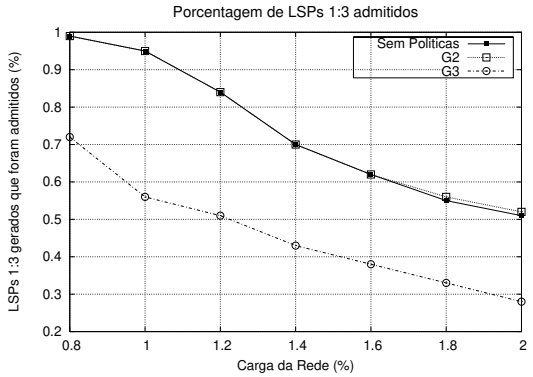
(g) Experimento 7.



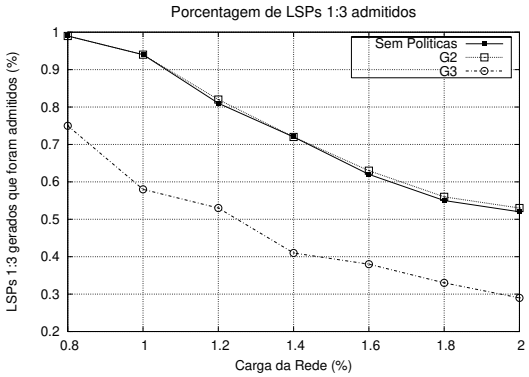
(h) Experimento 8.



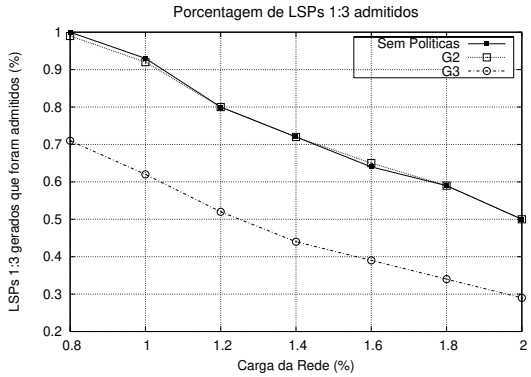
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



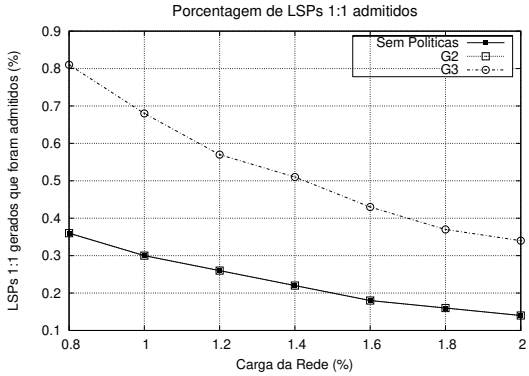
(l) Experimento 12.

Figura 7.5: Tráfego 1:3 admitido na topologia preliminar.

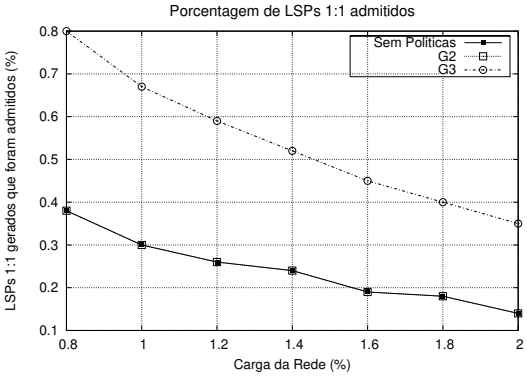
LSPs 1:1 Admitidos

O uso das políticas para admissão de tráfego 1:1 apresentou bons resultados, ver Figura 7.6. Comparando com os demais grupos, a quebra de grupos 1:N representou um ganho de pelo menos 15% nos resultados do grupo G3.

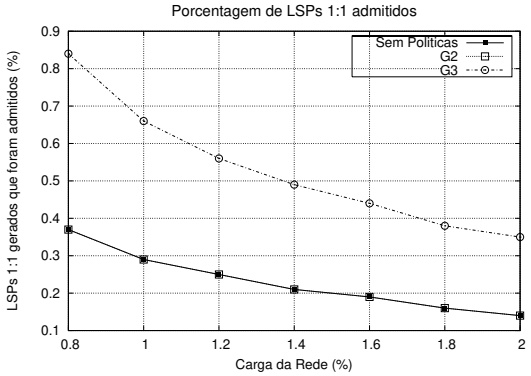
O grupo G2 apresentou o mesmo desempenho do que o grupo "sem políticas" em todos os experimentos. Isto acontece porque suas regras para admissão de tráfego 1:1 são bastante parecidas.



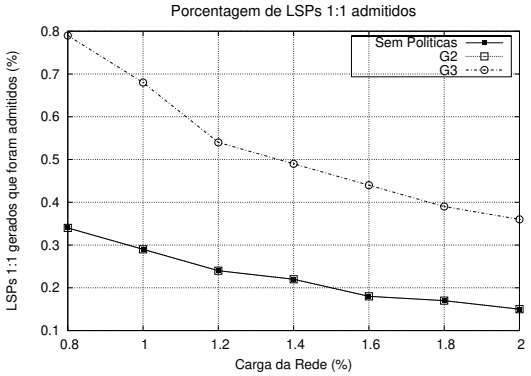
(a) Experimento 1.



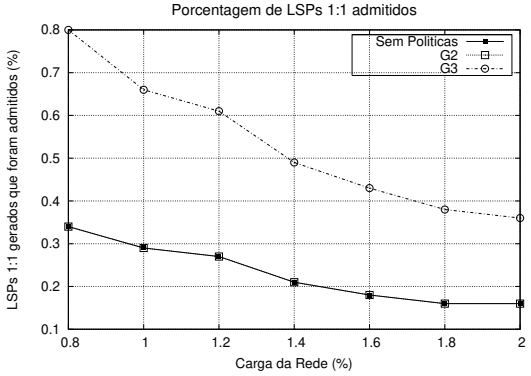
(b) Experimento 2.



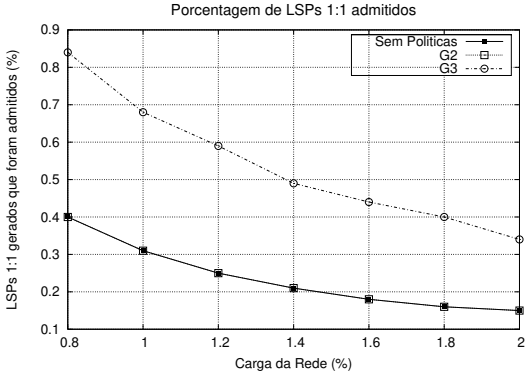
(c) Experimento 3.



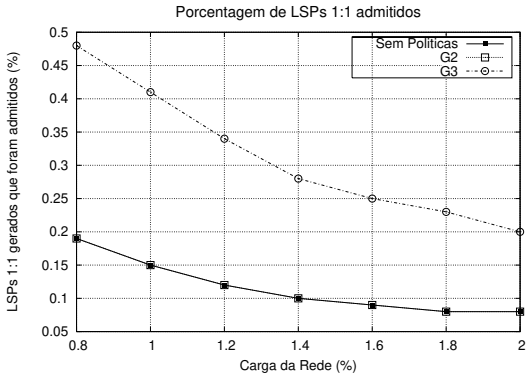
(d) Experimento 4.



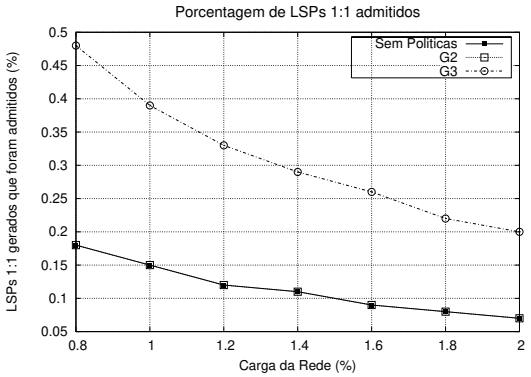
(e) Experimento 5.



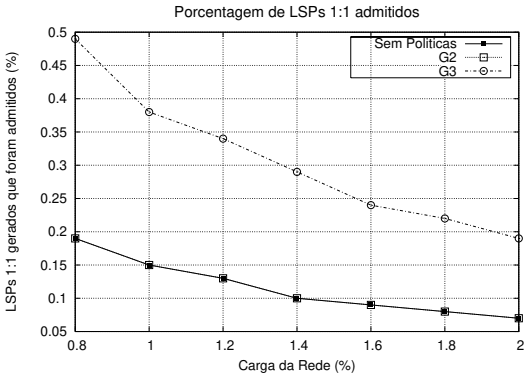
(f) Experimento 6.



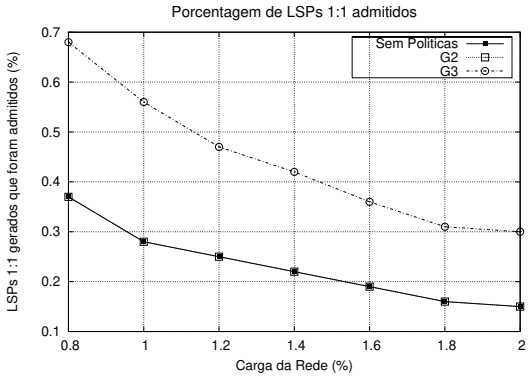
(g) Experimento 7.



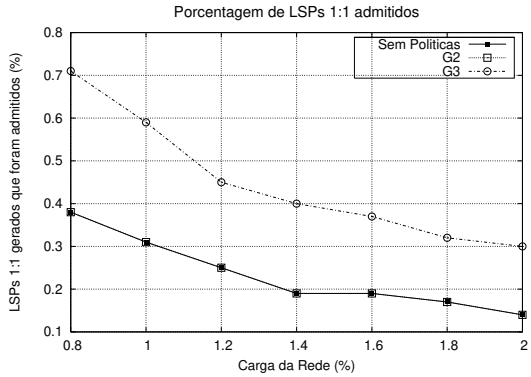
(h) Experimento 8.



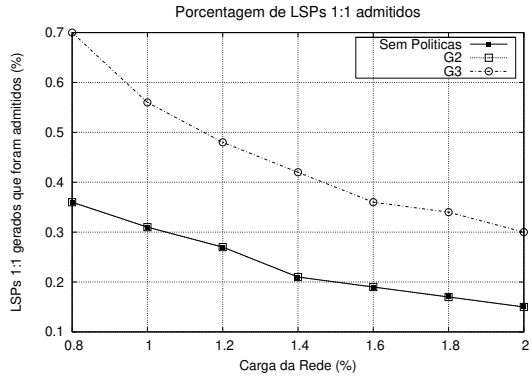
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.

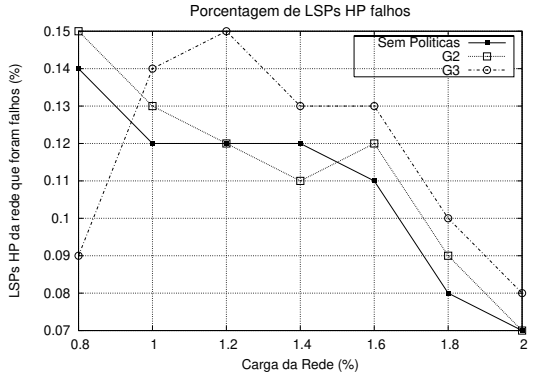


(l) Experimento 12.

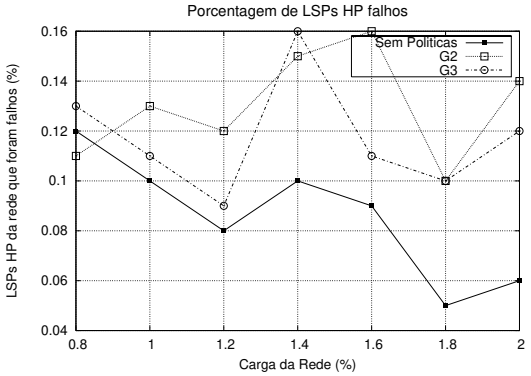
Figura 7.6: Tráfego 1:1 admitido na topologia preliminar.

LSPs HP Falhos

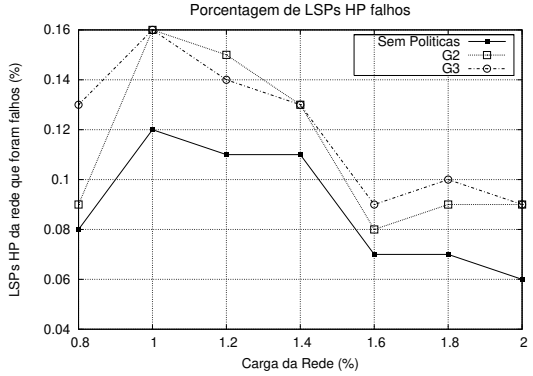
Devido ao comportamento aleatório da falha, o volume de tráfego apresentado em cada um dos experimentos é bastante particular, variando de 4% a 20%, ver Figura 7.7. Estes gráficos são utilizados para compreender os resultados obtidos no bloqueio de tráfego HP, mostrados a seguir.



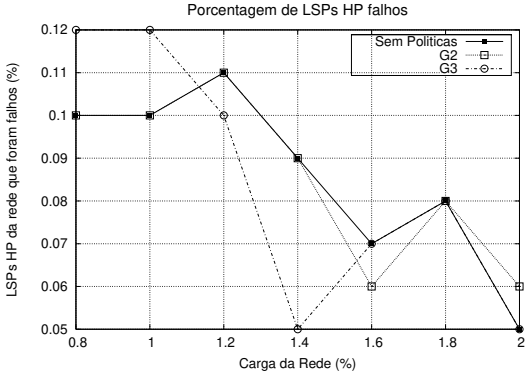
(a) Experimento 1.



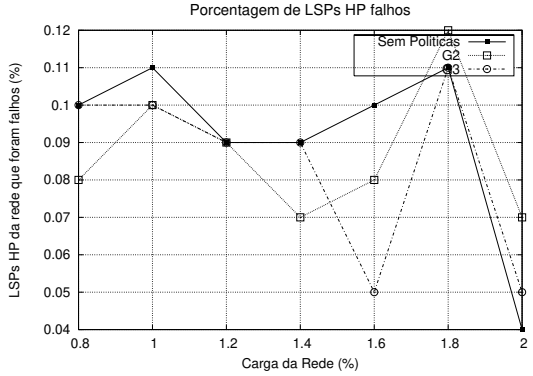
(b) Experimento 2.



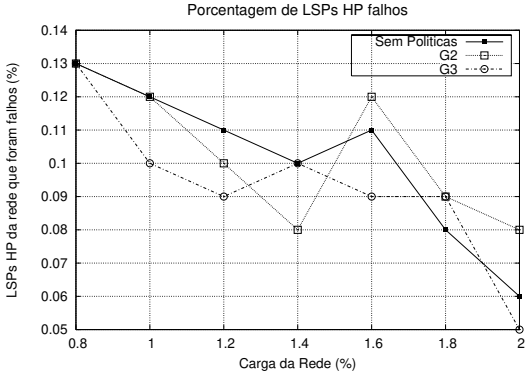
(c) Experimento 3.



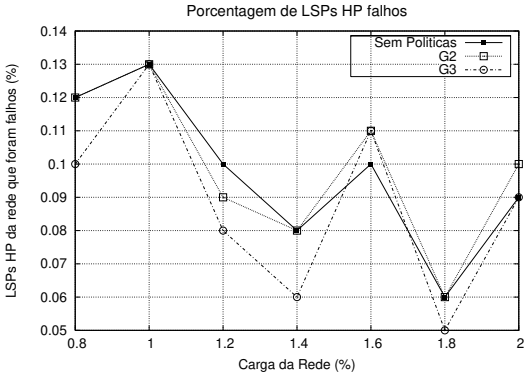
(d) Experimento 4.



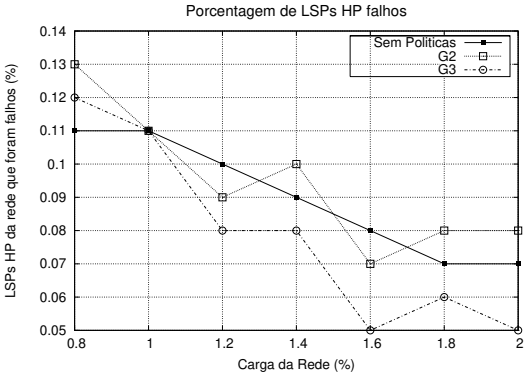
(e) Experimento 5.



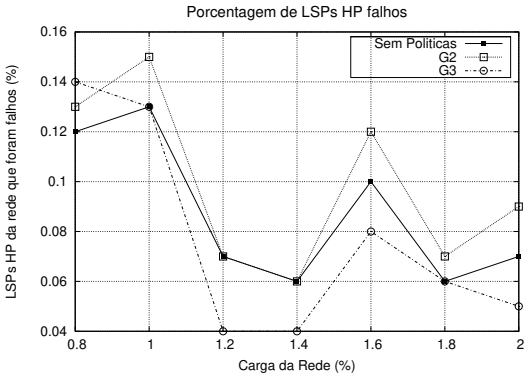
(f) Experimento 6.



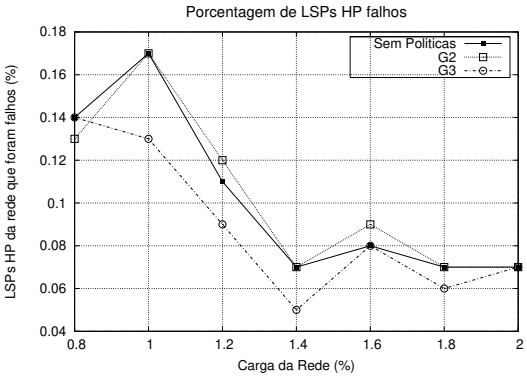
(g) Experimento 7.



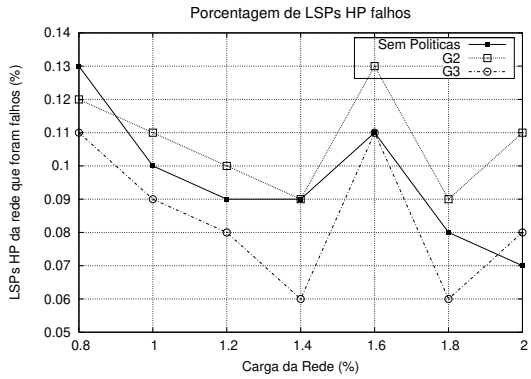
(h) Experimento 8.



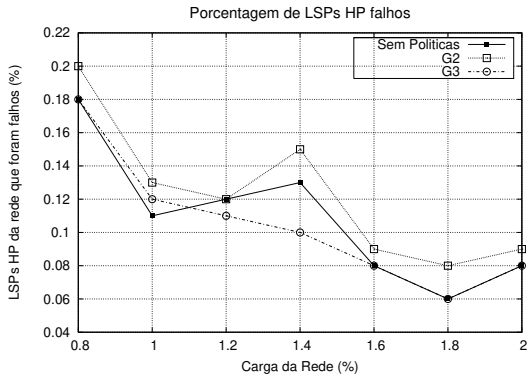
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



(l) Experimento 12.

Figura 7.7: Tráfego HP afetado pela falha gerada na topologia preliminar.

LSPs HP Bloqueados

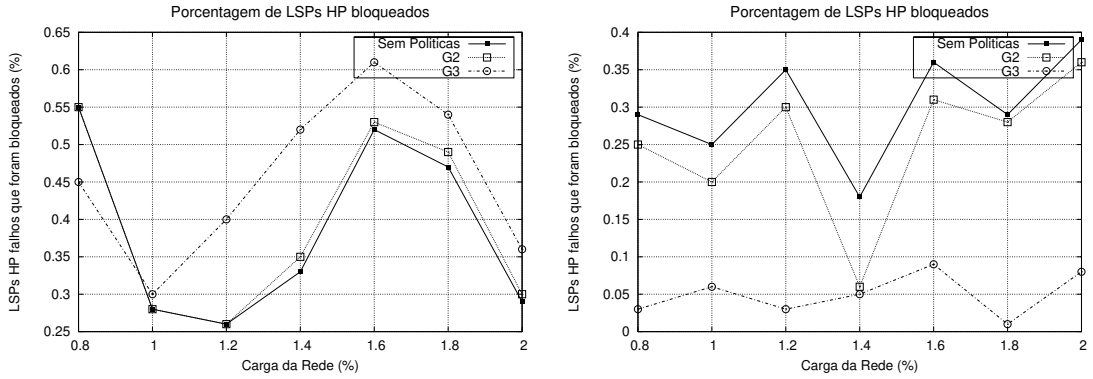
O uso de políticas apresentou-se relevante para reduzir o volume de tráfego HP bloqueado após a ocorrência de uma falha na rede, ver Figura 7.8. Em especial, o grupo G3 mostrou-se importante em quase todos os experimentos, apresentando resultados superiores aos dos demais grupos.

Os melhores resultados do grupo G3 estão nos experimentos de 5 a 12. Nestes experimentos participam aqueles onde o volume de tráfego admitido e afetado pela falha estão mais próximos aos dos resultados obtidos nos demais grupos. Isto significa que admitir um volume de tráfego não muito grande permitiu ao G3 bloquear um baixo volume de tráfego afetado pela falha. A quebra de grupos 1:N também contribuiu para estes resultados. Um maior volume de tráfego HP desprotegido foi admitido e readmitido após a ocorrência da falha, em detrimento dos fluxos de tráfego 1:N que tiveram sua admissão prejudicada.

Nos experimentos de 1 a 3 foi admitido um grande volume de tráfego HP, e também falhou um grande volume tráfego. O G3 obteve um bom resultado no experimento 2. Novamente, a quebra de grupos 1:N permitiu que futuros fluxos de tráfego 1:1 e desprotegidos (especialmente os fluxos HP) fossem admitidos.

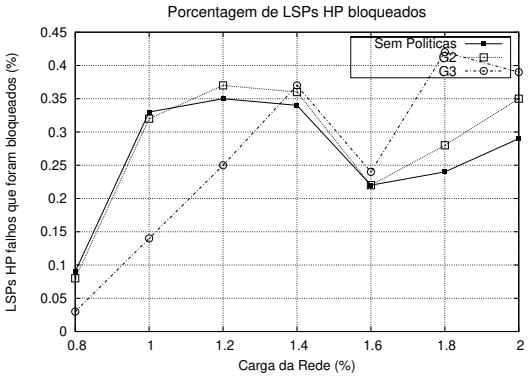
Os resultados obtidos pelo grupo G2 e o grupo "sem políticas" apresentaram-se bastante semelhantes. Este comportamento acontece em experimentos onde o volume de tráfego não é grande, experimentos 1, 3, 4, 6, 7, 9, 10 e 12. Nos demais experimentos 2, 5, 8 e 11 o grupo G2 mostrou, de uma forma geral, resultados melhores do que o grupo "sem políticas"; porém, não melhores do que os obtidos pelo grupo G3. O principal motivo para este comportamento é a preempção de fluxos LP em benefício do fluxos HP.

Em alguns experimentos o grupo de políticas G3 obteve um desempenho melhor do que os outros grupos somente em cargas de rede menores. No experimento 1, esta situação acontece para as cargas de 80% e 100%, e no experimento 3, entre as cargas de 80% e 140% da largura de banda total da rede.

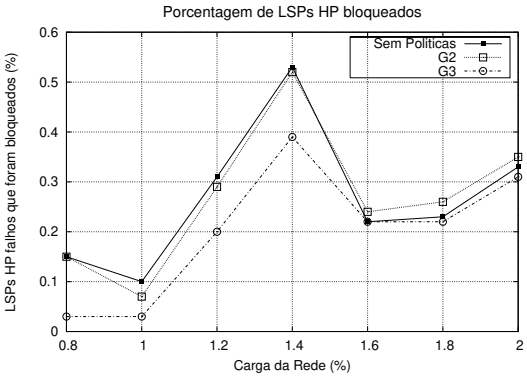


(a) Experimento 1.

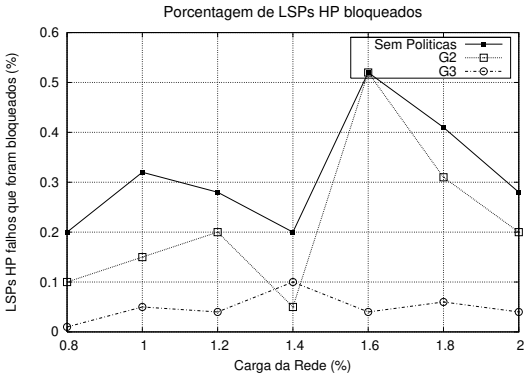
(b) Experimento 2.



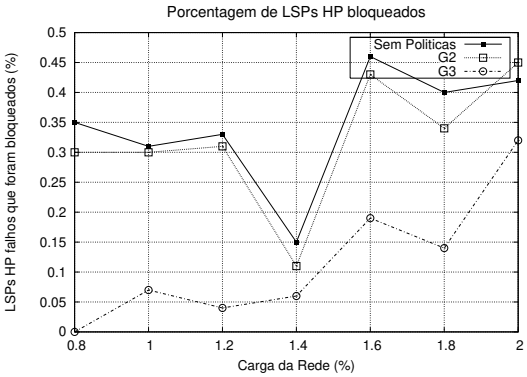
(c) Experimento 3.



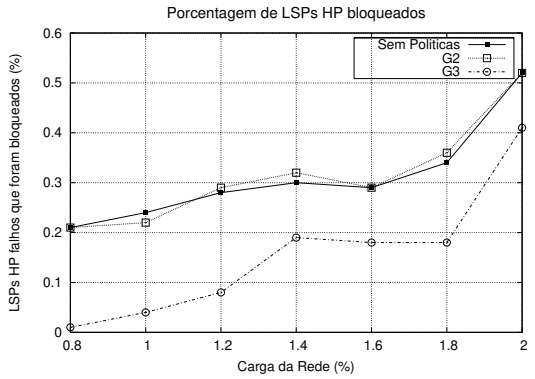
(d) Experimento 4.



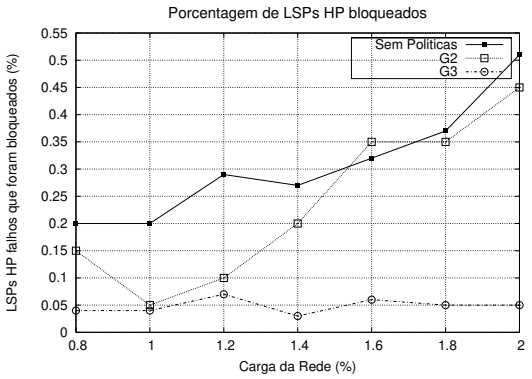
(e) Experimento 5.



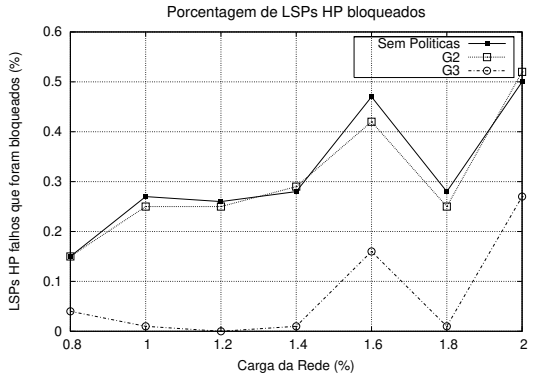
(f) Experimento 6.



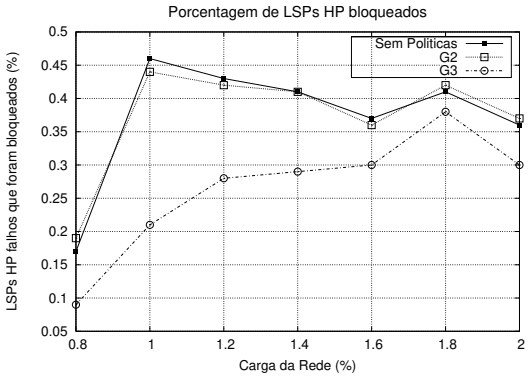
(g) Experimento 7.



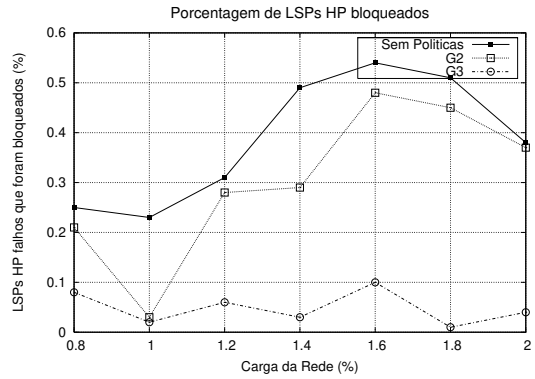
(h) Experimento 8.



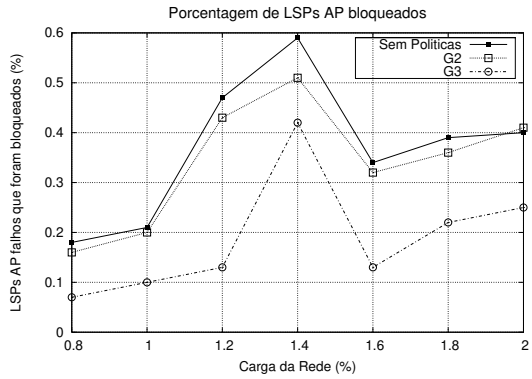
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



(l) Experimento 12.

Figura 7.8: Tráfego HP bloqueado após a tentativa de readmissão na topologia preliminar.

7.3.2 Topologia Física NSFNet

A topologia física NSFNet é formada por 16 nós, ver Figura 7.9. Para a simulação, considera-se que cada enlace óptico possui duas fibras unidirecionais (uma para cada direção) e cada fibra possui 10 lambdas de 1 gigabit por segundo. Com esta infra-estrutura, o gerador de topologia virtual criou 32 circuitos ópticos entre o par de origem destino (0,12): 4 grupos desprotegidos, 2 grupos 1+1, 2 grupos 1:1 e 5 grupos 1:3.

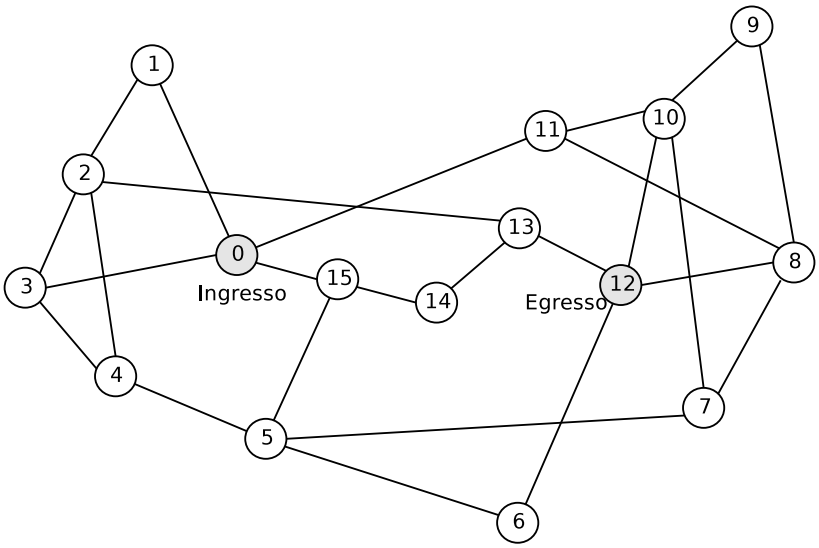
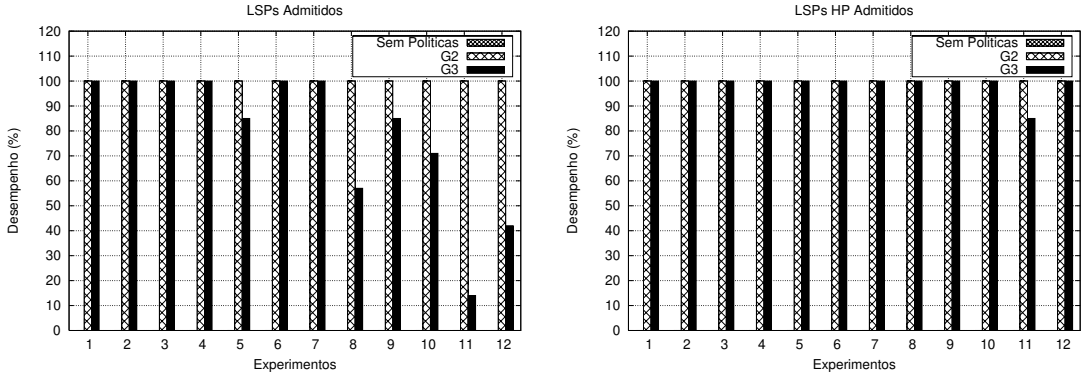


Figura 7.9: Topologia física NSFNet.

De uma forma geral, a aplicação das políticas apresentou-se relevante também na topologia NSFNet, no entanto, abaixo do desempenho obtido na topologia preliminar, ver Figura 7.10.



(a) (b)

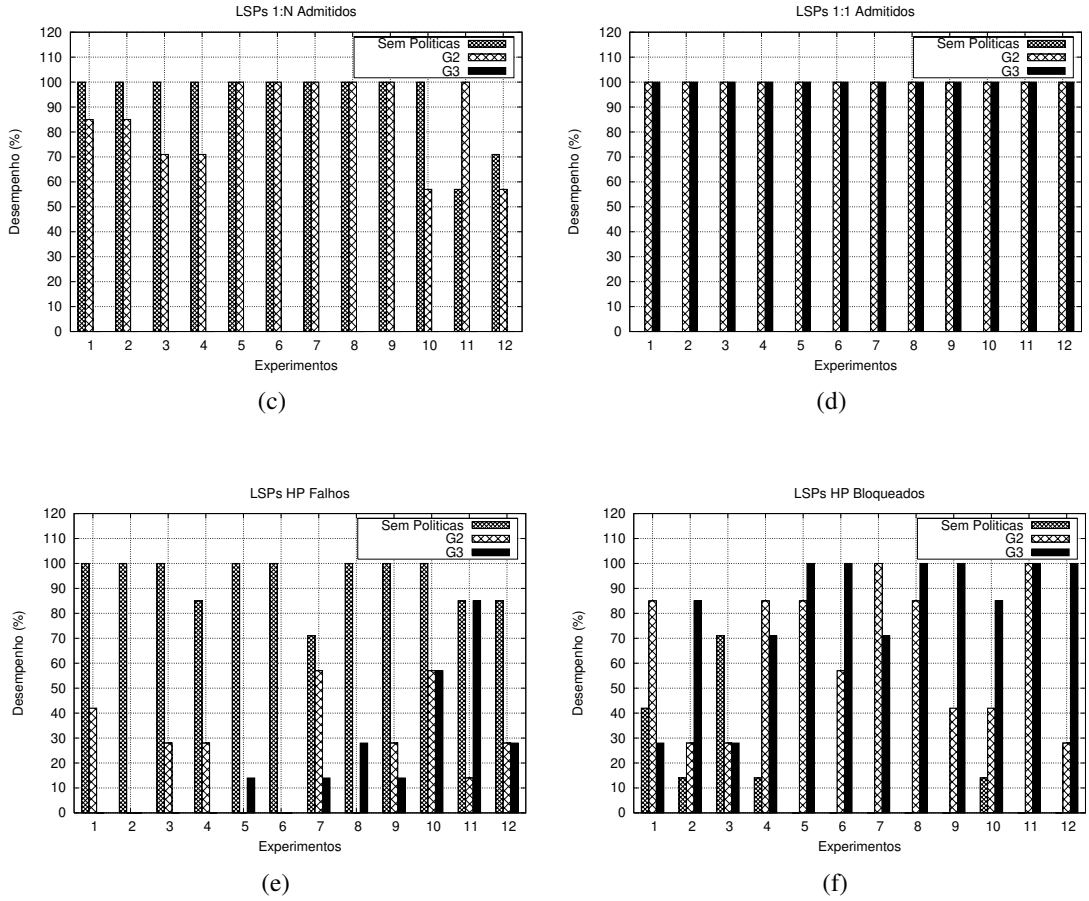


Figura 7.10: Visão geral do desempenho das políticas na topologia NSFNet.

Basicamente, a principal diferença entre os resultados obtidos na topologia NSFNet e na topologia preliminar é o ganho de desempenho do grupo G3 na maioria dos experimentos. O grupo G2 continua com o desempenho de 100% na admissão tráfego geral, tráfego HP e tráfego 1:1; e o grupo G3 obteve um ganho considerável na admissão do tráfego gerado nos experimentos de 4 a 12.

Observando a admissão de tráfego geral, HP e 1:1, o grupo G3 obteve um desempenho melhor do que o grupo "sem políticas" em todos os experimentos. Em particular, o desempenho do grupo "sem políticas" foi superado nos experimentos 10, 11 e 12 da admissão geral; e 7, 9 e 12 da admissão de HP. Na admissão de tráfego 1:1, o G3 continua com o desempenho de 100% em todos os experimentos.

A prioridade de admissão de tráfego HP apresentou-se mais eficiente para o grupo G3 na topologia NSFNet do que na topologia preliminar. A principal explicação para este fato é o aumento de 5 circuitos ópticos desprotegidos. Este aumento permitiu que as políticas do G3

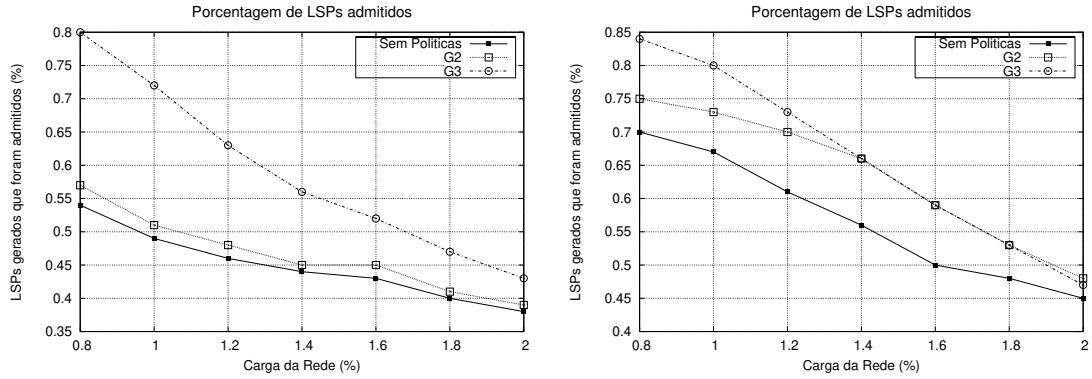
pudessem utilizar melhor os recursos da rede em benefício da admissão de tráfego HP.

De uma forma geral, o grupo "sem políticas" apresentou-se melhor para admissão de tráfego 1:N. Novamente, priorizar a admissão de tráfego 1:1 afetou o desempenho do grupo G3 na admissão de tráfego 1:N, ficando abaixo do desempenho de todos os demais grupos. O desempenho do grupo G2 oscila conforme as características do volume de tráfego gerado no experimento. O melhor desempenho encontra-se nos experimentos onde foram gerados grande volumes de tráfego 1:N e 1:1, isto é, experimentos 5, 6, 7 e 8, 9, respectivamente.

O uso de políticas para redução do bloqueio de tráfego HP após uma falha também apresentou-se relevante nos experimentos realizados sobre a topologia NSFNet.

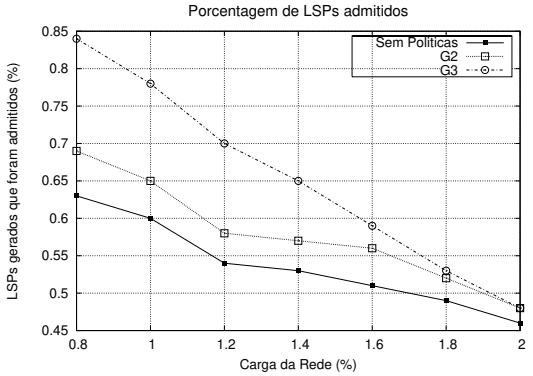
LSPs Admitidos

Embora não tenha admitido um volume de tráfego muito maior, o grupo G2 possui a melhor estabilidade em desempenho quando comparado com o grupo "sem políticas", em todos os experimentos, ver Figura 7.11. Comparado com os experimentos realizados sobre a topologia preliminar, o grupo G3 obteve bons resultados em um maior número dos experimentos, sendo, em alguns deles, com valores mais elevados. O maior número de circuitos ópticos desprotegidos contribuiu para o alto volume de tráfego admitido nos experimentos de 1 a 7. Em outros experimentos, de 8 a 12, o volume de tráfego não foi muito grande, porém, maior do que os resultados obtidos sobre a topologia preliminar.

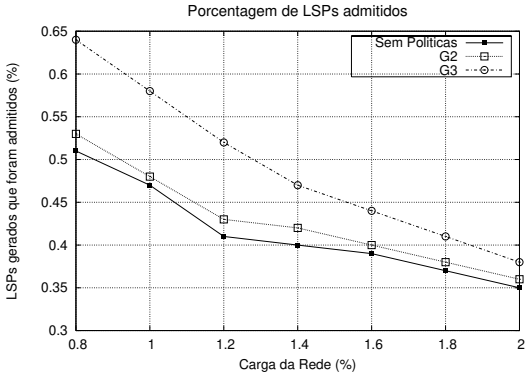


(a) Experimento 1.

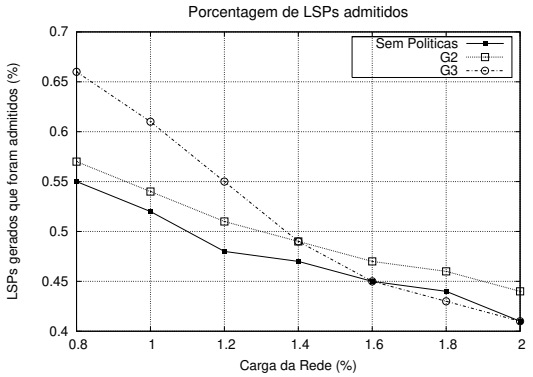
(b) Experimento 2.



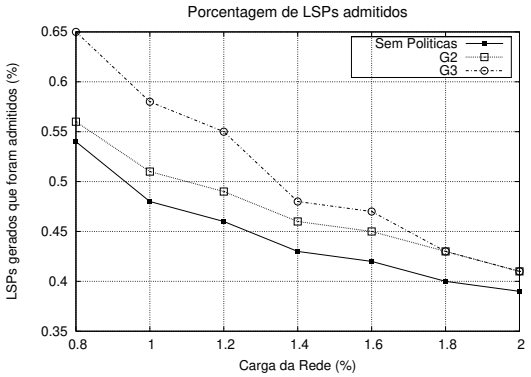
(c) Experimento 3.



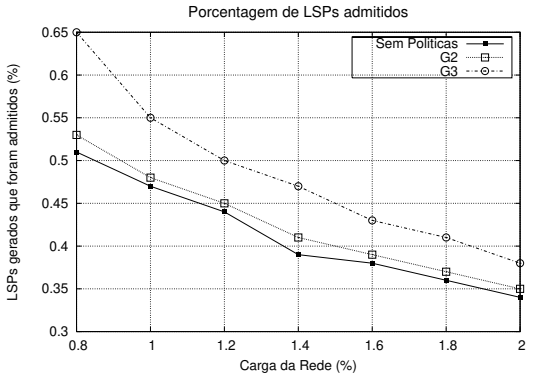
(d) Experimento 4.



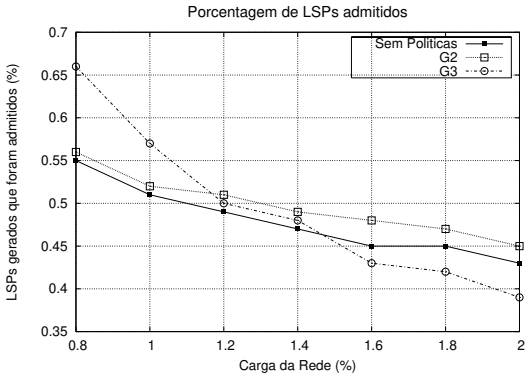
(e) Experimento 5.



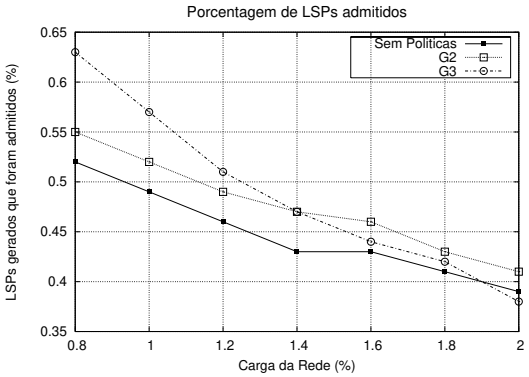
(f) Experimento 6.



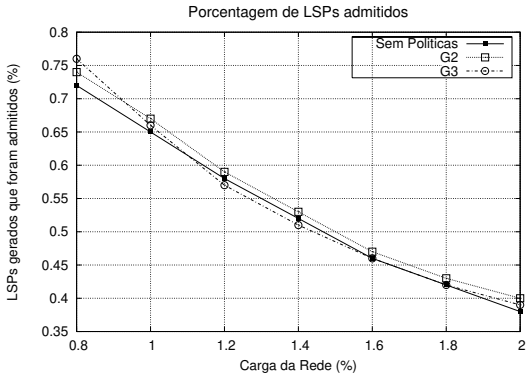
(g) Experimento 7.



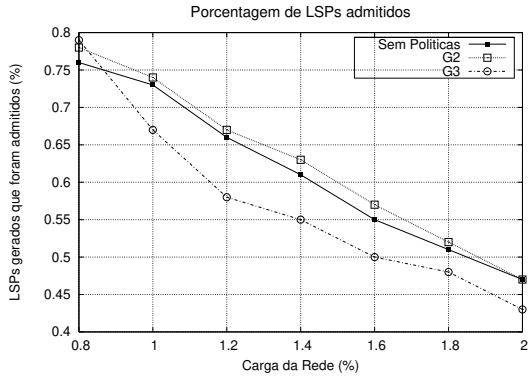
(h) Experimento 8.



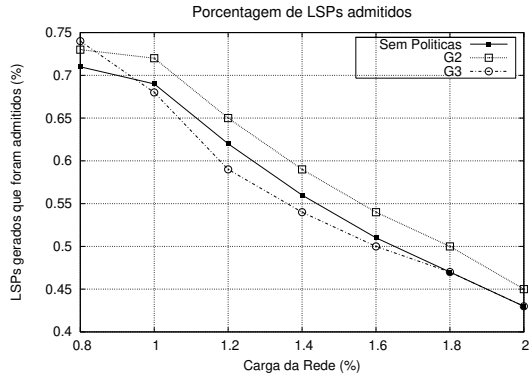
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



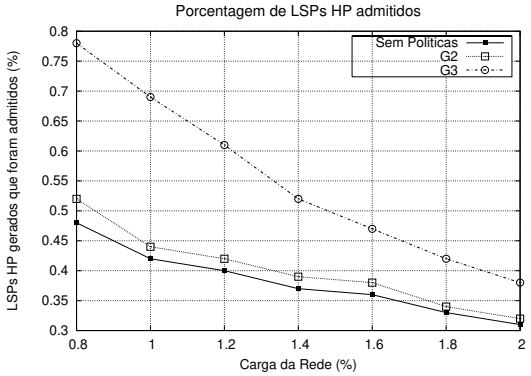
(l) Experimento 12.

Figura 7.11: Tráfego admitido na topologia NSFNet.

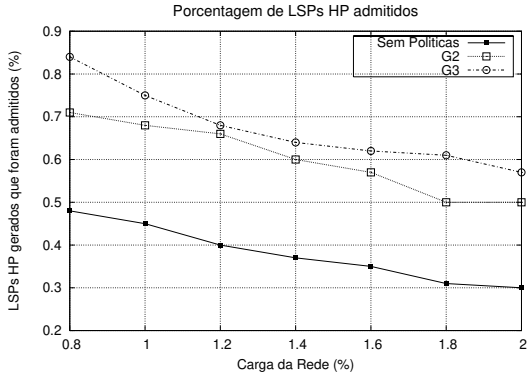
LSPs HP Admitidos

O fato de ter disponível um maior número de circuitos desprotegidos na topologia virtual contribuiu para que as políticas admitissem um volume de tráfego HP maior sobre a topologia NSFNet, ver Figura 7.12. Isto acontece pois ambos os grupos de políticas G2 e G3 priorizam a admissão de tráfego HP através da preempção de tráfego LP.

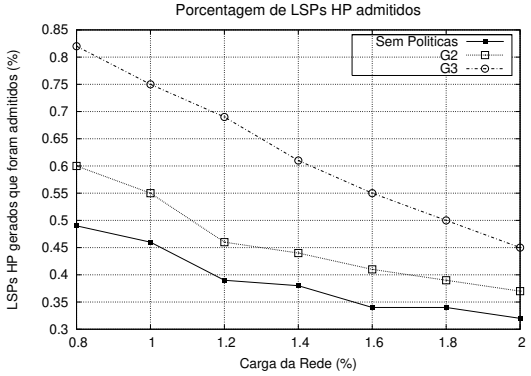
A proporção de tráfego HP admitido nos experimentos 1, 2, 3 e 4 é consideravelmente maior para o grupo de políticas G3, mantendo diferenças de até quase 30% comparado com os demais grupos, inclusive com o grupo G2. Nos demais experimentos, o desempenho não é significativo nesta proporção, porém, somente na carga de rede 1.2 do experimento 11 o grupo G3 possui valores inferiores ao grupo “sem políticas” para o volume de tráfego HP admitido.



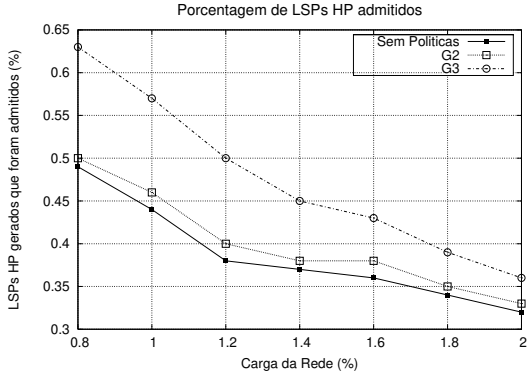
(a) Experimento 1.



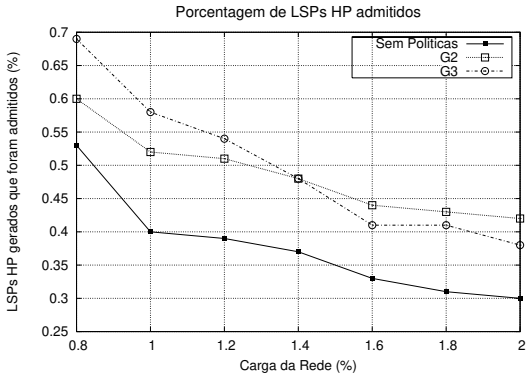
(b) Experimento 2.



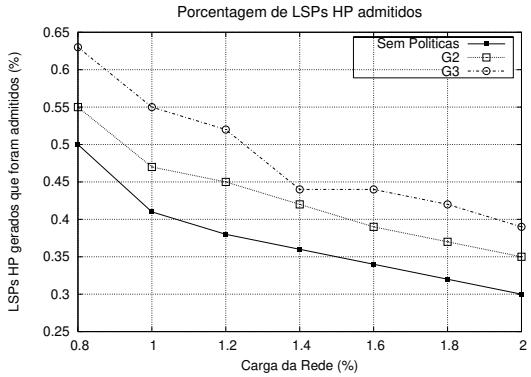
(c) Experimento 3.



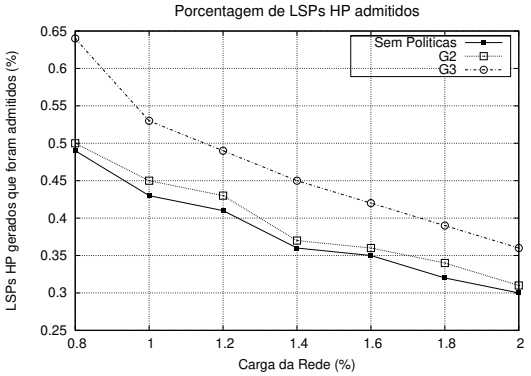
(d) Experimento 4.



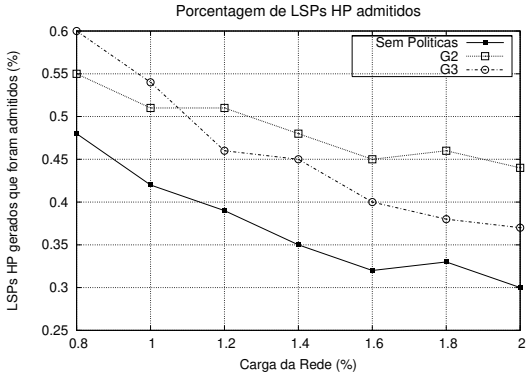
(e) Experimento 5.



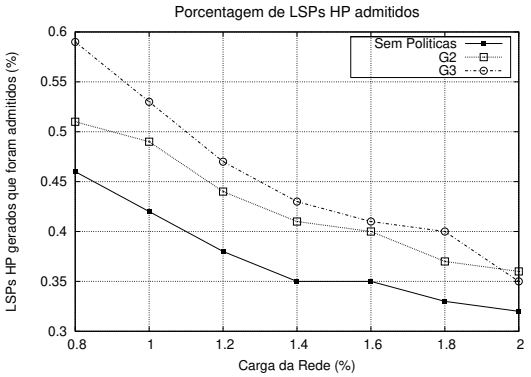
(f) Experimento 6.



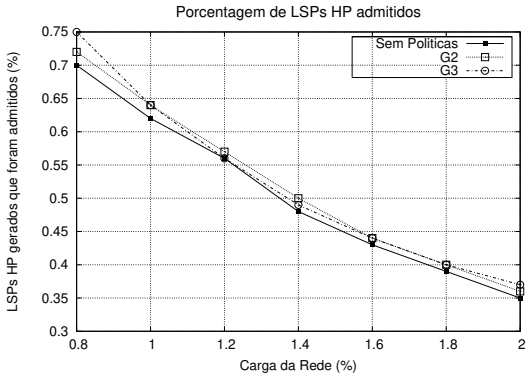
(g) Experimento 7.



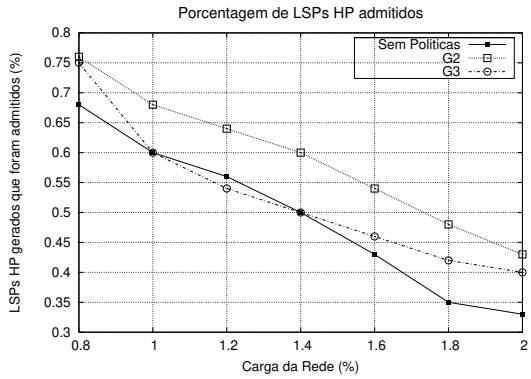
(h) Experimento 8.



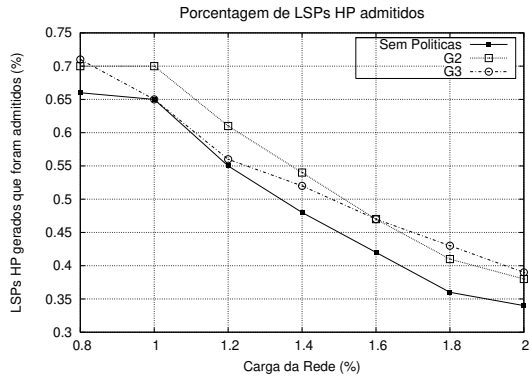
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



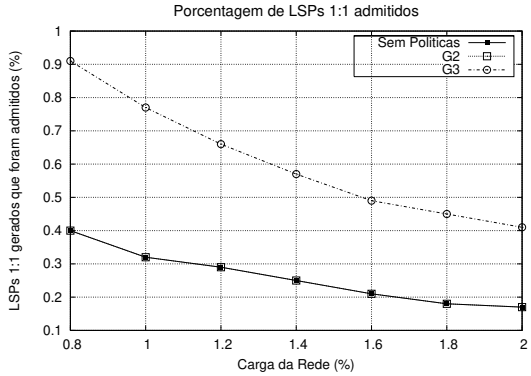
(l) Experimento 12.

Figura 7.12: Tráfego HP admitido na topologia NSFNet.

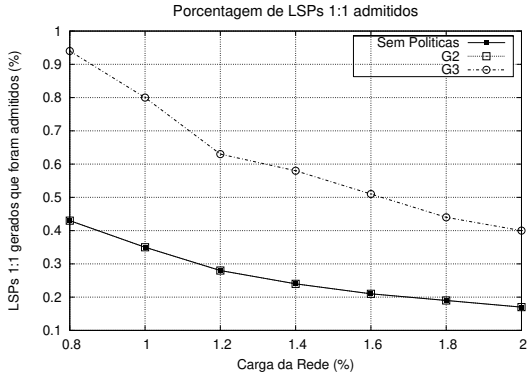
LSPs 1:1 Admitidos

O G3 é o grupo que admitiu o maior volume de tráfego 1:1, ver Figura 7.13. Comparando com a topologia preliminar, seus valores são maiores na topologia NSFNet, no entanto, a diferença de desempenho entre o G3 e os demais grupos continuam muito próxima. Em vários dos experimentos, o grupo G3 alcança a porcentagem de 90% de tráfego 1:1 admitido.

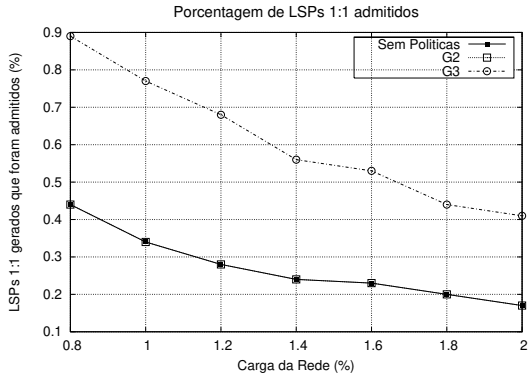
A quebra de grupos 1:N em benefício de fluxos 1:1 é, mais uma vez, o principal motivo para o bom desempenho do grupo G3. A ordem em que os fluxos de tráfego foram gerados e enviados também podem contribuir para o aumento da proporção dos resultados alcançados pelo G3. O grupo G2 e o grupo "sem políticas" possuem os mesmos resultados. Isto reflete a semelhança de suas políticas para admissão de tráfego 1:1.



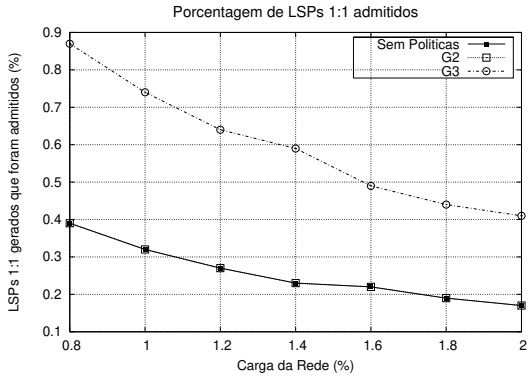
(a) Experimento 1.



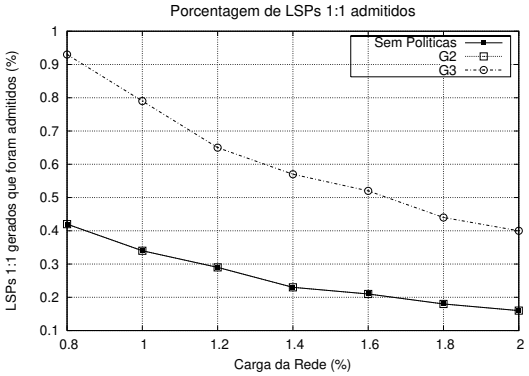
(b) Experimento 2.



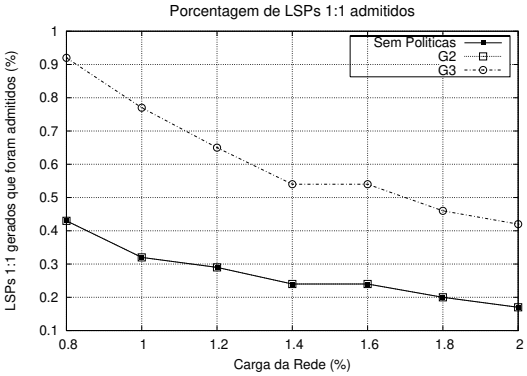
(c) Experimento 3.



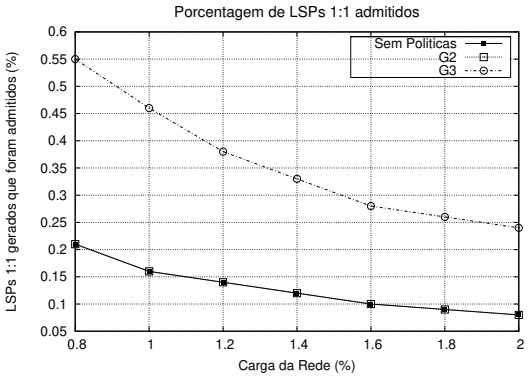
(d) Experimento 4.



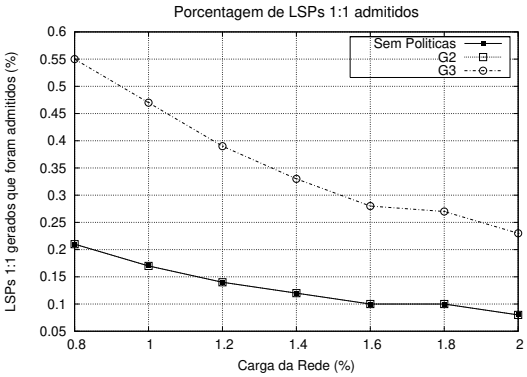
(e) Experimento 5.



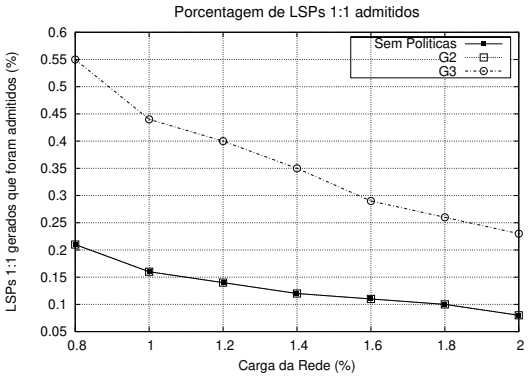
(f) Experimento 6.



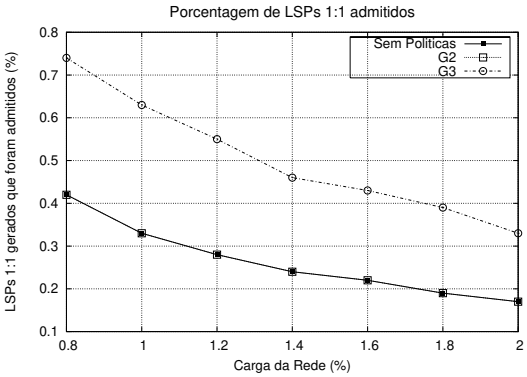
(g) Experimento 7.



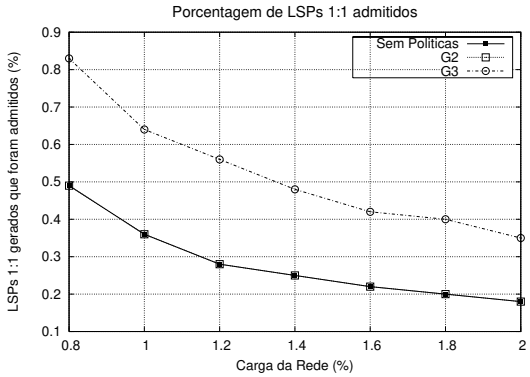
(h) Experimento 8.



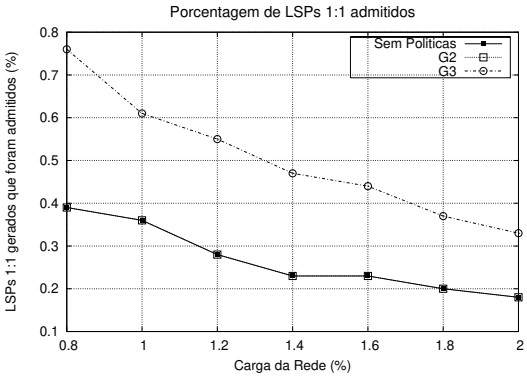
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



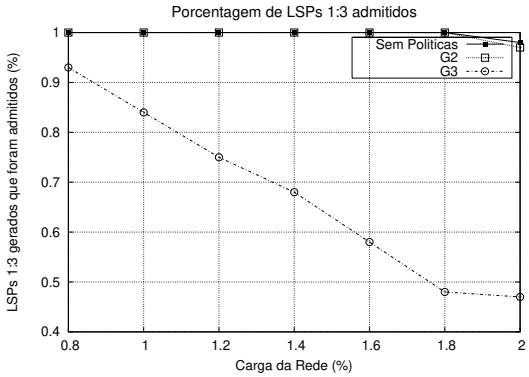
(l) Experimento 12.

Figura 7.13: Tráfego 1:1 admitido na topologia NSFNet.

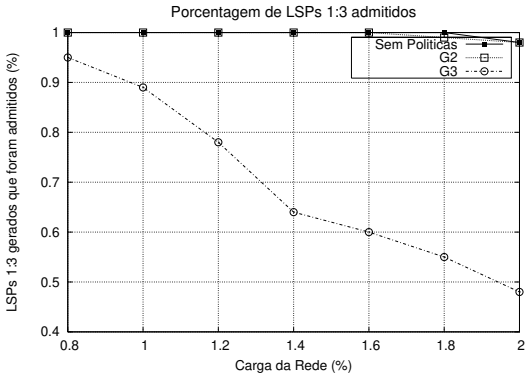
LSPs 1:N Admitidos

Os grupos de políticas não motraram-se eficientes para admissão de tráfego 1:N na topologia NSFNet, ver Figura 7.14. No grupo G3, a quebra de grupos 1:N permitiu priorizar a admissão de tráfego 1:1, porém, prejudicou a admissão de tráfego 1:N. A indisponibilidade de circuitos 1:N causou o baixo desempenho do grupo G3 em todos os experimentos.

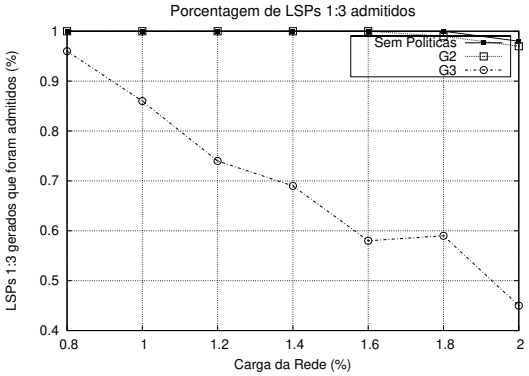
O grupo G2 obteve os melhores resultados, no entanto, iguais aos do grupo "sem políticas" em todos os experimentos. Este comportamento é refletido pela semelhança de suas políticas para admissão de tráfego 1:N. Para se obter melhores resultados com as políticas é necessário implementar regras mais aprimoradas.



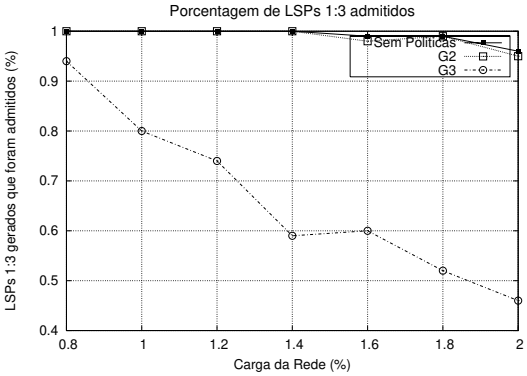
(a) Experimento 1.



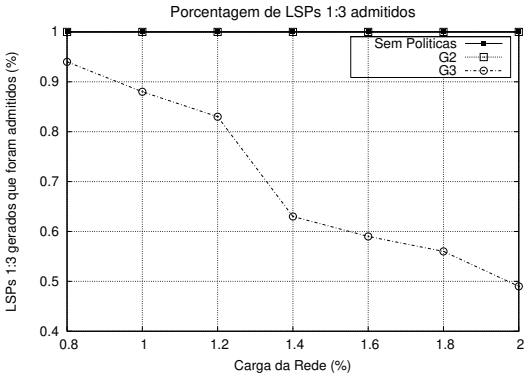
(b) Experimento 2.



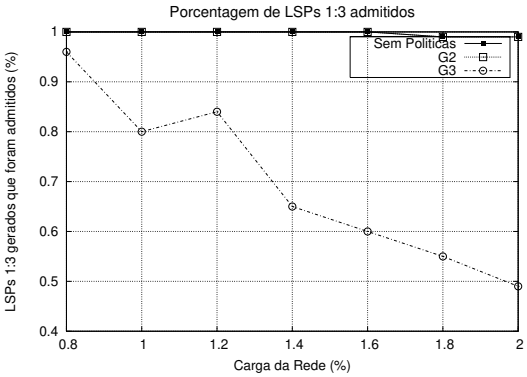
(c) Experimento 3.



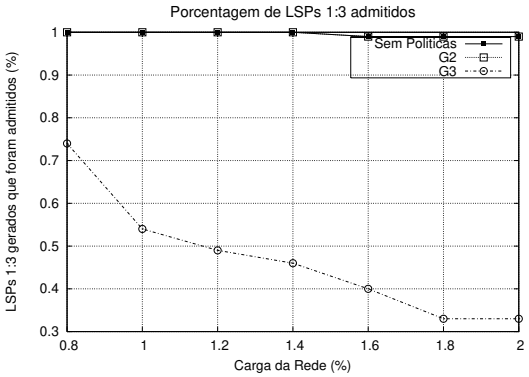
(d) Experimento 4.



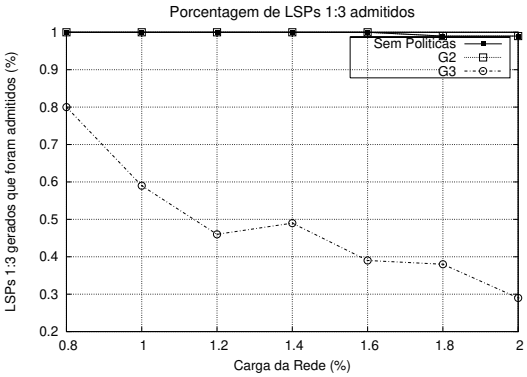
(e) Experimento 5.



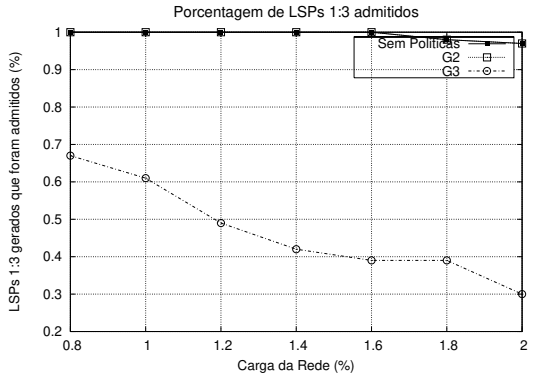
(f) Experimento 6.



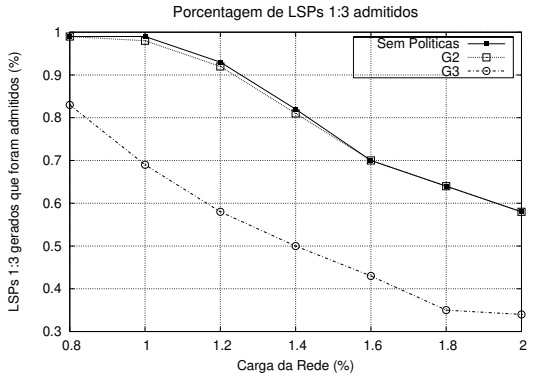
(g) Experimento 7.



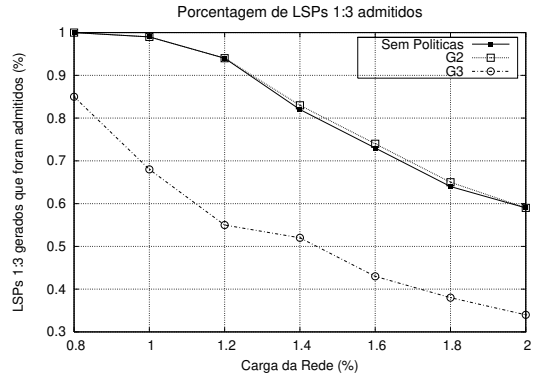
(h) Experimento 8.



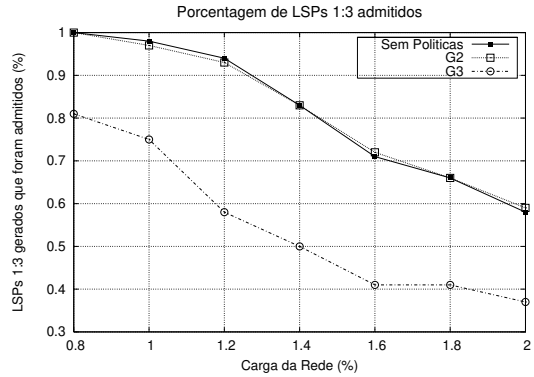
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



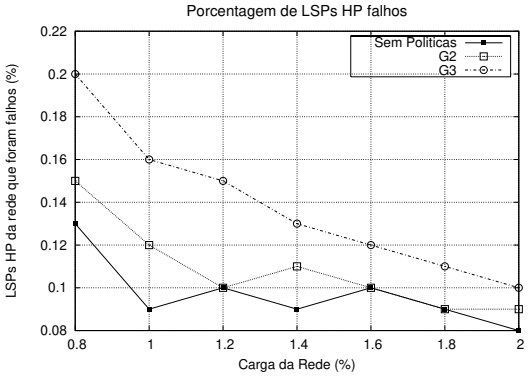
(l) Experimento 12.

Figura 7.14: Tráfego 1:3 admitido na topologia NSFNet.

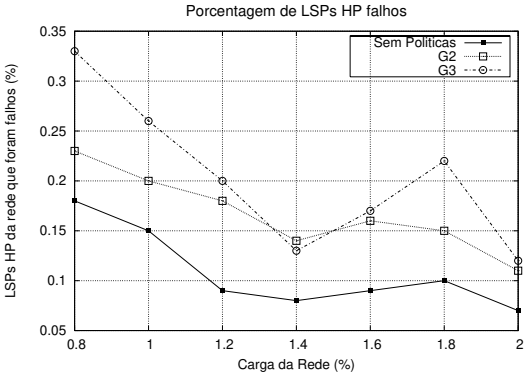
LSPs HP Falhos

A falha gerada de forma aleatória afetou um volume de tráfego menor ao utilizar o grupo "sem políticas". No entanto, em vários experimentos estes valores não apresentam grandes diferenças comparado com os demais grupos, ver Figura 7.15. Nos experimentos 1, 2 e 3, os valores alcançaram uma diferença de até $\sim$18%, mas nos experimentos de 5 a 12 as diferenças são menores.

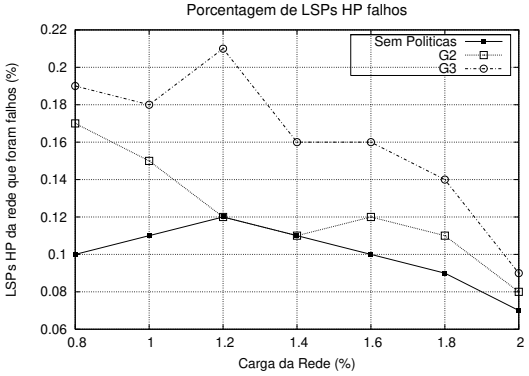
O volume de tráfego afetado pela falha é utilizado na análise do tráfego HP bloqueado após a tentativa de readmissão.



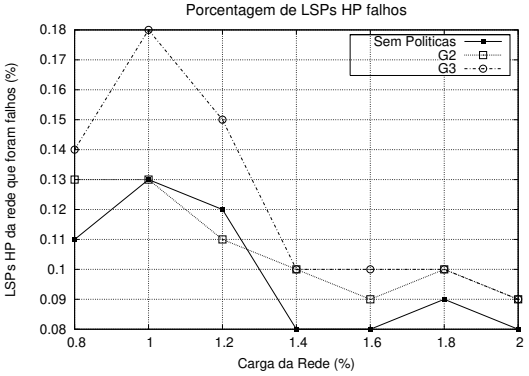
(a) Experimento 1.



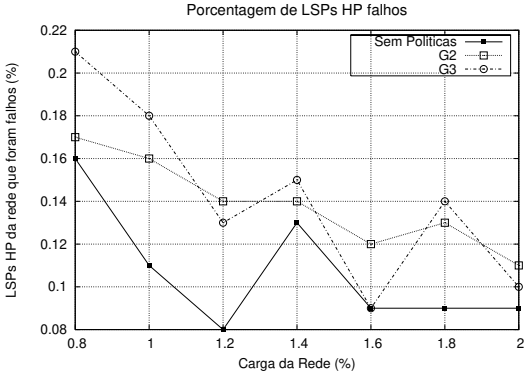
(b) Experimento 2.



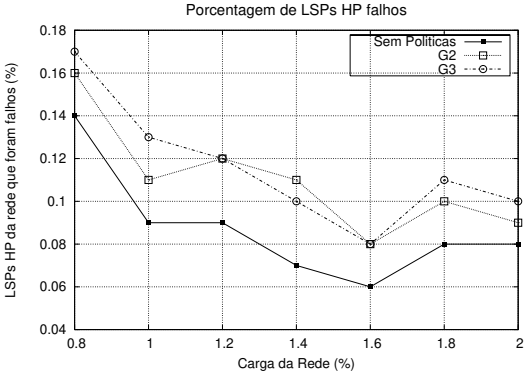
(c) Experimento 3.



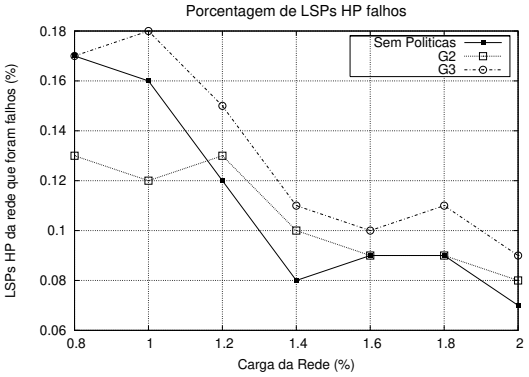
(d) Experimento 4.



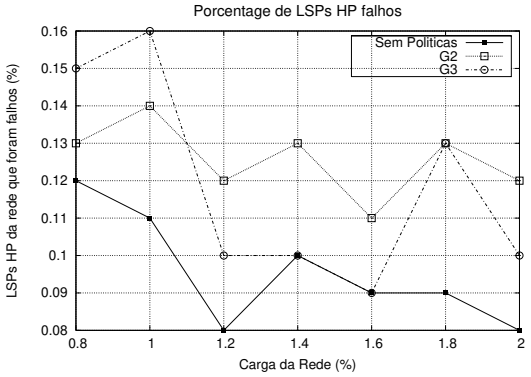
(e) Experimento 5.



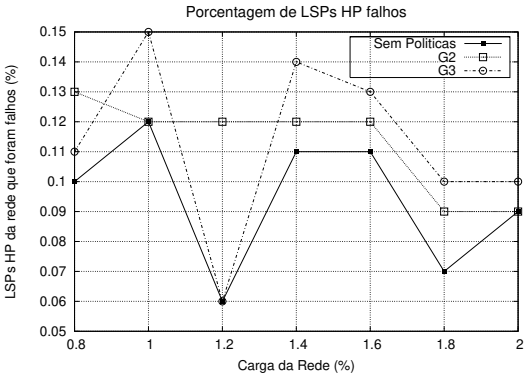
(f) Experimento 6.



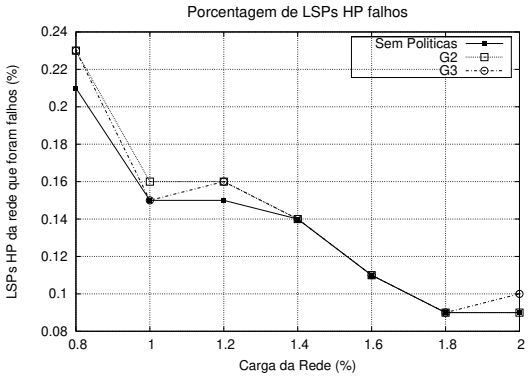
(g) Experimento 7.



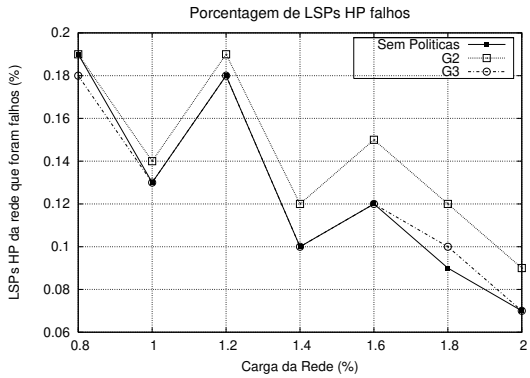
(h) Experimento 8.



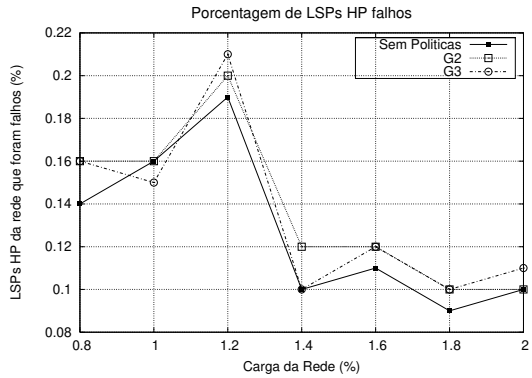
(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11.



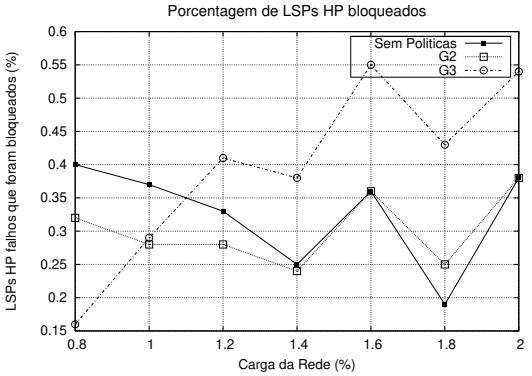
(l) Experimento 12.

Figura 7.15: Tráfego HP afetado pela falha gerada na topologia NSFNet.

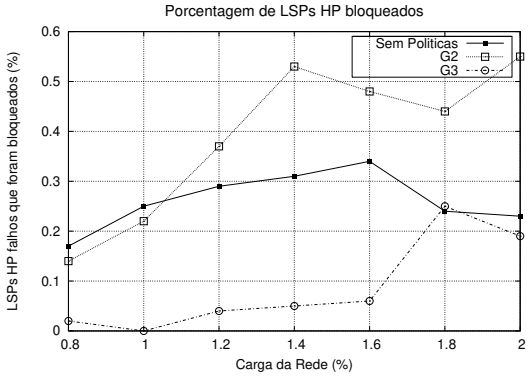
LSPs HP Bloqueados

O uso das políticas permitiu a redução de bloqueio do tráfego HP afetado pela falha em quase todos os experimentos realizados na topologia NSFNet, ver Figura 7.16. Nos experimentos 1, 3, 4, 7 e 10, o desempenho do grupo G3 é melhor do que dos demais grupos somente para cargas de rede mais baixas. Nos experimentos 5, 6, 8 e 9, o desempenho do grupo G3 é melhor em todas as cargas de rede.

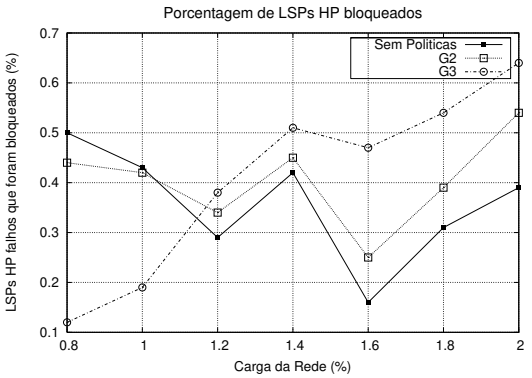
De uma forma geral, o grupo G2 obteve resultados melhores do que o grupo "sem políticas". Somente para as cargas de rede mais altas de alguns experimentos, o grupo "sem políticas" obteve resultados melhores do que o do grupo G2, veja os experimentos 1, 3, 6, 9, 10 e 12, onde estes resultados são melhores evidenciados. Nos outros experimentos, os resultados obtidos pelo grupo G2 são melhores do que o do grupo "sem políticas" para todas as cargas de rede.



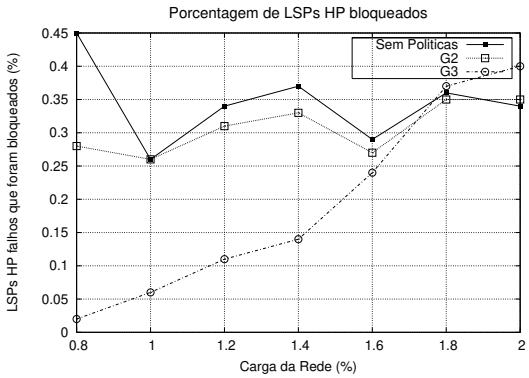
(a) Experimento 1.



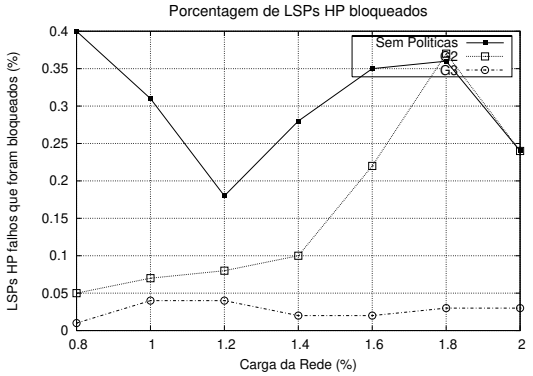
(b) Experimento 2.



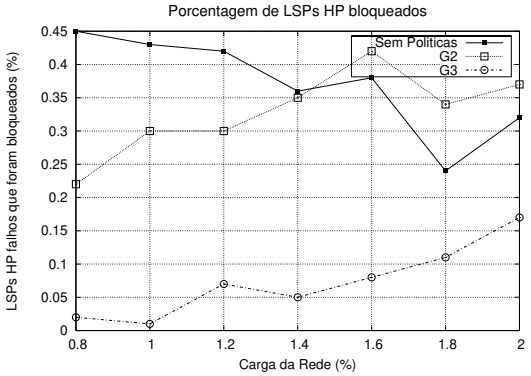
(c) Experimento 3.



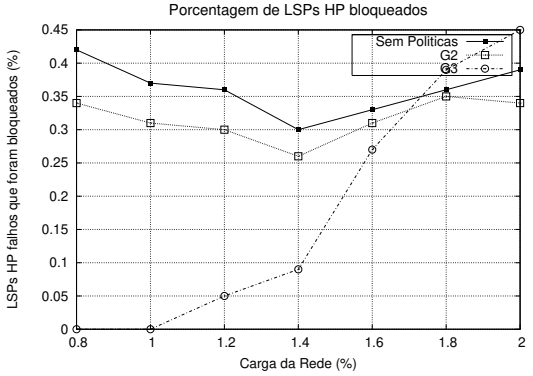
(d) Experimento 4.



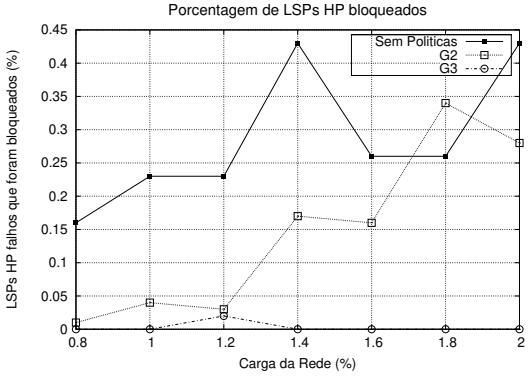
(e) Experimento 5.



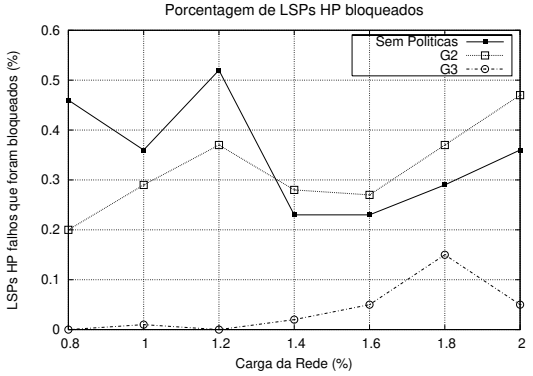
(f) Experimento 6.



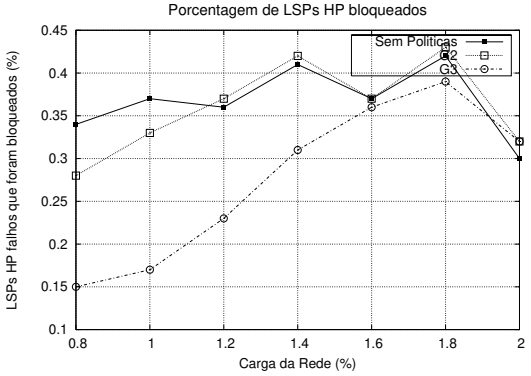
(g) Experimento 7.



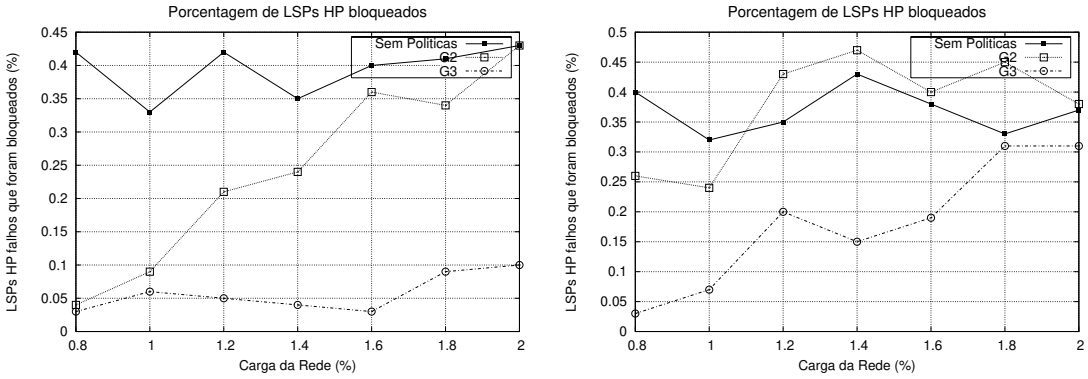
(h) Experimento 8.



(i) Experimento 9.



(j) Experimento 10.



(k) Experimento 11. (l) Experimento 12.

Figura 7.16: Tráfego HP bloqueado após a tentativa de readmissão na topologia NSFNet.

7.3.3 Análise Geral

Os resultados obtidos neste capítulo mostraram que é possível definir políticas de agregação que apresentem resultados relevantes tanto para a admissão de tráfego quanto para a gerência de falhas, conforme as necessidades do administrador da rede. Ter uma noção prévia das caracterísiticas das requisições através de, por exemplo, uma matriz de tráfego, pode ajudar em vários aspectos nestes resultados. O uso dos recursos da rede pode ser melhor planejado e as necessidades do administrador podem ser alcançadas de uma forma mais eficiente.

O uso de políticas de agregação apresentou vários ganhos na aplicação em ambas as topologias físicas, comparando-se com um caso onde não são aplicadas políticas. Estes ganhos são: admitir um volume de tráfego maior, priorizar determinados tipos de fluxos de tráfego e reduzir o volume de tráfego bloqueado após a tentativa de readmissão do tráfego afetado pela falha. A grande diferença destes ganhos para as duas topologias está em suas respectivas proporções. Na topologia NSFNet o uso de política apresentou resultados mais significativos do que os resultados obtidos na topologia preliminar.

Fazendo uma comparação geral entre os grupos de políticas definidos, o grupo G3 permitiu admitir maiores volumes de tráfego em vários experimentos, porém, em alguns experimentos, este resultado é prejudicado pela alta prioridade de admissão de determinados tipos de tráfego. Nestes casos, os grupos G2 e/ou “sem políticas” tiveram resultados melhores do que o G3. O grupo G3 também permitiu, na maioria dos experimentos, reduzir o volume de tráfego bloqueado após readmissão dos fluxos afetados pela falha.

O grupo G2 não obteve resultados melhores do que o G3 na admissão de tráfego, no entanto, os seus resultados são mais estáveis do que o do G3 quando comparados com os do grupo “sem políticas”. Os resultados obtidos pelo G2 são, em todos os experimentos, melhores ou iguais

aos do grupo “sem políticas”, na admissão de tráfego. Após a ocorrência de uma falha, o grupo G2 apresentou resultados mais significativos do que o grupo “sem políticas” somente em alguns experimentos.

Capítulo 8

Conclusão

8.1 Conclusão

A maturidade atual das redes ópticas permite conectar redes clientes através de circuitos ópticos de alta capacidade de transmissão. Para se ter uma idéia desta capacidade, as empresas Nippon Telegraph e Telephone Corporation do Japão demonstraram a transmissão de 14 Tb/s com amplificadores a uma distância de 160 km [10]. Além da alta capacidade de transmissão das fibras ópticas, elas também possuem atrativos como a baixa perda na transmissão de sinal e a imunidade a interferências eletromagnéticas.

Embora vários problemas sejam resolvidos com o uso de redes ópticas, novos problemas são trazidos para a comunidade de pesquisa. Por exemplo, (1) o fato de que não são todos os clientes que necessitam de toda a largura de banda de um circuito óptico pode provocar um desperdício relevante de largura de banda, e (2) uma falha simples pode provocar a perda de um grande volume de dados. Esta dissertação propõe uma solução para o segundo problema. Agregar mais de um fluxo de tráfego em um único circuito óptico é uma técnica que pode ser utilizada na solução de ambos os problemas. O problema (1) pode ser tratado utilizando-se políticas para gerenciar a agregação de tráfego e obter um melhor aproveitamento da largura de banda da rede. Esta dissertação propõe que o problema das falhas também seja tratado durante o processo de admissão de tráfego e, para tanto, a solução proposta é utilizar políticas que considerem aspectos de falhas para gerenciar a agregação de tráfego em circuitos ópticos.

A solução proposta é aplicada no contexto de redes IP sobre redes WDM e constituída por uma arquitetura baseada em políticas e grupos de políticas de agregação que consideram aspectos de falha para admissão de tráfego na rede. A arquitetura é composta por quatro módulos e um repositório de políticas. Estes módulos são: o controle de admissão (AC), o gerente de falhas (FM), o gerente de recursos (RM) e o gerente de políticas (PM). Todos estes módulos são utilizados para tratar um determinado volume de requisições e, ao final, um evento de falha (rompimento de uma fibra). O PM conta com três grupos de políticas de agregação (G1, G2

e G3) de diferentes complexidades armazenados no repositório de políticas. O grupo G1 considera apenas aspectos de falha (esquema requerido de proteção) para admissão de tráfego. O grupo G2, uma extensão do G1, considera também a classe de serviço do fluxo para admissão de tráfego. O grupo G3, uma extensão do G2, permite que fluxos de tráfego sejam instalados em circuitos que ofereçam uma qualidade de serviço (esquema de proteção mais robusto) maior do que a requerida pela requisição.

Um simulador foi desenvolvido em Java para validar a solução proposta e doze experimentos foram realizados sobre duas topologias físicas distintas. Os resultados destes experimentos apresentaram-se relevantes para tratar o problema das falhas em redes ópticas. O grupo G3 permitiu, em vários dos experimentos realizados, reduzir o volume de tráfego bloqueado e admitir volumes de tráfego maiores do que os outros grupos. O grupo G2 não obteve resultados melhores do que o G3 na admissão de tráfego, mas os seus resultados mostram-se mais estáveis quando comparado com os outros grupos. Os resultados obtidos pelo G2 são, em todos os experimentos, melhores ou iguais aos do grupo G1 na admissão de tráfego. Entretanto, o grupo G1 apresentou resultados mais significativos do que o grupo G2 em vários experimentos quanto a redução de tráfego bloqueado após a ocorrência de uma falha.

De uma forma geral, a aplicação de políticas demonstrou ser uma boa prática para alcançar resultados importantes para a gerência de redes ópticas. Por exemplo, as políticas permitiram priorizar a admissão de determinados fluxos de tráfego na rede e reduzir o volume de tráfego bloqueado após a ocorrência de uma falha. E ainda, como uma otimização, o administrador pode fazer uso de conhecimentos prévios sobre o tipo de tráfego da rede (ex: uma matriz de tráfego) para melhor planejar o uso dos recursos da rede.

O modelo de políticas apresentado nesta dissertação é geral o suficiente para suportar a adição de novas políticas ao repositório de políticas. Por exemplo, podem ser criadas políticas para priorizar outros tipos de tráfego ou até mesmo definir níveis de políticas mais abstratos.

8.1.1 Contribuições

As contribuições deste trabalho foram:

- estudo de políticas para redução do impacto gerado por uma falha. Neste tópico inclui-se o uso de modelos de informações para aplicação de políticas, o controle de admissão e a gerência de falhas de redes ópticas, a agregação de tráfego, e mecanismos de proteção e recuperação;
- proposta de uma arquitetura baseada em políticas para a gerência de admissão e falhas;
- proposta de um conjunto de políticas que buscam reduzir o impacto de uma falha;
- implementação de um simulador para validar a solução proposta.

8.1.2 Publicações

Esta dissertação gerou quatro artigos. [14] apresenta alguns resutados iniciais sobre a topologia preliminar. [54] discute sobre resultados obtidos na topologia NSFNet. [15] apresenta uma versão mais detalhada da implementação e dos resultados obtidos na topologia NSFNet. [56] discute sobre a aplicação de políticas de agregação em dois contextos: no contexto das falhas e no contexto da admissão (sem falhas). Neste último, aproveitar melhor a largura de banda da rede e reduzir a preempção de tráfego são desafios relevantes.

8.2 Trabalhos Futuros

Alguns trabalhos futuros são:

- O sucesso da readmissão do tráfego afetado pela falha está relacionado com volume de tráfego afetado pela falha e com o volume de tráfego admitido nos circuitos ópticos. Se os circuitos ópticos estiverem completamente utilizados, o resultado da readmissão de tráfego afetado pela falha será prejudicado. Um trabalho futuro é analisar este limiar e propor políticas que o considerem na admissão.

- O objetivo do administrador pode variar conforme as características das requisições e a disponibilidade de recursos na rede. Um trabalho futuro é construir metapolíticas para satisfazer esta necessidade. Uma solução é utilizar metapolíticas para analisar e escolher o grupo de políticas que melhor se adapta ao comportamento das requisições e das falhas recebidas. Considerar históricos também pode ajudar nas decisões efetuadas pelas políticas.

- Desenvolver políticas que considerem outros aspectos de falhas, por exemplo, probabilidade de falha de um enlace.

- Estender as políticas para considerar vários domínios.

- Considerar a existência de circuitos ópticos *multihop* na rede óptica.

- Aplicar os conceitos de computação autonômica (*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.

- Simular outros cenários de simulação. Ao invés de variar a topologia física da rede, simular com outras topologias virtuais. Isto implica em alterar a ordem de criação dos grupos de circuitos ópticos para os experimentos.

Referências Bibliográficas

[1] ITU-T: Architecture for the Automatically Switched Optical Network (ASON). Recomendação G.8080/Y.1340.

[2] Resource Reservation Protocol (RSVP) - Version 1 Functional Specification. http://www.ietf.org/rfc/rfc2205.txt, Setembro 1997. RFC-2205.

[3] SNMP Applications. http://www.ietf.org/rfc/rfc2573.txt, Abril 1999. RFC-2573.

[4] Interface for the Optical Transport Network (OTN). ITU-T, Fevereiro 2001. Recomendação G.709, versão 1.

[5] Terminology for Policy-Based Management. http://www.ietf.org/rfc/rfc3198.txt, Novembro 2001. RFC-3198.

[6] CIM Policy Model White Paper. http://www.dmtf.org/standards/, Junho 2003. CIM version 2.7, atualizado.

[7] Policy Core Information Model (PCIM) Extensions. http://www.ietf.org/rfc/rfc3460.txt, Janeiro 2003. RFC-3060.

[8] A Framework for Inter-Domain MPLS Traffic Engineering. http://www.ietf.org/, Julho 2005. draft-ietf-ccamp-inter-domain-framework-04.txt.

[9] Security Architecture for the Internet Protocol. http://www.ietf.org/rfc/rfc4301.txt, Dezembro 2005. RFC-4301.

[10] 14 Tbps over a Single Optical Fiber: Successful Demonstration of World's Largest Capacity. http://www.ntt.co.jp/news/news06e/0609/060929a.html, Setembro 2006.

[11] Dakshi Agrawal e Kang-Won Lee ad Jorge Lobo. Policy-Based Management of Networked Computing Systems. *IEEE Communications Magazine*, 43(10):69–75, Outubro 2005.

[12] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang e W. Weiss. An Architecture for Differentiated Services. http://www.ietf.org/rfc/rcf2475.txt, Dezembro 1998. RFC-2475.

[13] M. Blaze, A. Keromytis, M. Richardson e L. Sanchez. IP Security Policy (IPSP) Requirements. http://www.ietf.org/rfc/rcf3586.txt, Agosto 2003. RFC-3586.

[14] Cláudio Carvalho, Fábio Verdi, Edmundo Madeira e Maurício Magalhães. Policy-based Fault Management for Integrating IP over Optical Networks. *Fifth IEEE International Workshop on IP Operations & Management (IPOM 05)*, pp. 88–97, Outubro 2005. Barcelona, Espanha.

[15] Cláudio Carvalho, Fábio Verdi, Edmundo Madeira e Maurício Magalhães. Gerência de Falhas baseada em Políticas para Redes Ópticas. *Simpósio Brasileiro de Redes de Computadores (SBRC 06)*, Maio/Junho 2006. Curitiba-PR, Brasil.

[16] K. Chan e T. P. Yum. Analysis of Least Congested Path Routing in WDM Lightwave Networks. Em *IEEE INFOCOM 94*, volume 2, pp. 962–969, Abril 1994.

[17] Marinos Charalambides, Paris Flegkas, George Pavlou, Arosha Bandara, Emil Lupu, Alessandra Russo, Naranker Dulay, Morris Sloman e Javier Rubio-Loyola. Policy Conflict Analysis for Quality of Service Management. Em *Sixth IEEE International Workshop on Policy for Distributed Systems and Networks*, pp. 99–108, Junho 2005.

[18] Tibor Cinkler. Traffic and Lambda Grooming. *IEEE Network*, 03:16–21, Março/Abril 2003.

[19] D. Clark. Policy Routing in Internet Protocols. http://www.ietf.org/rfc/rcf1102.txt, Maio 1989. RFC-1102.

[20] Michel Cox e Rob Davison. Concepts, Activities and Issues of Policy-based Communications Management. *BT Technology Journal*, 17(3):155–169, Julho 1999.

[21] Elionildo da Silva Menezes, Djamel Fawzi Hadj Sadok e Judith Kelner. A Policy Management Framework Using Traffic Engineering in DiffServ Networks. Em *International Workshop on Quality of Service in Multiservice IP Networks*, pp. 331–346. Springer-Verlang, 2001.

[22] Nicodemos Damianou, Naranker Dulay, Emil Lupu e Morris Sloman. The Ponder Policy Specification Language. Em *Third IEEE International Workshop on Policies for Distributed System and Networks (POLICY'01)*, pp. 18–38, Junho 2001.

[23] Nicole Dunlop, Jadwiga Indulska e Kerry Raymond. Methods for Conflict Resolution in Policy-Based Management Systems. Em *Seventh IEEE International Enterprise Distributed Object Computing Conference*, pp. 98–109, Setembro 2003.

[24] Taner Dursun e Bülent Örencik. POLICE Distributed Conflict Detection Architecture. Em *IEEE International Conference on Communications*, pp. 2081–2085, Junho 2004.

[25] R. Dutta e N. G. Rouskas. Traffic Grooming in WDM Networks: Past and Future. *IEEE Network*, 16(6):46–56, Novembro/Dezembro 2002.

[26] Canhui Ou et. al. Traffic Grooming for Survivable WDM Networks - Shared Protection. *IEEE Journal on Selected Areas in Communications*, 21(9):1367–1383, Novembro 2003.

[27] D. Harrington et al. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Framework. http://www.ietf.ort/, Dezembro 2002. RFC-3411.

[28] K. Chan et al. COPS Usage for Policy Provisioning (COPS-PR). http://www.ietf.org/rfc/rfc3084.txt, Março 2001. RFC-3084.

[29] M. Pana et al. Policy Core Extension Lightweight Directory Access Protocol Schema (PCELS). http://www.ietf.org/rfc/rfc4104.txt, Junho 2005. RFC-4104.

[30] Wissan Fawaz, Belkacem Daheb, Oliver Audouin, Michel Du-Pond e Guy Pujolle. Service Level Agreement and Provisioning in Optical Networks. *IEEE Communications Magazine*, 42:36–43, Janeiro 2004.

[31] Erich Gamma, Richard Helm, Ralph Johnson e John Vlisside. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, Reading, Massachusetts, 1995.

[32] Nasir Ghani, Sudhir Dixit e Ti-Shiang Wang. On IP-over-WDM Integration. *IEEE Communications Magazine*, 38:72–84, Março 2000.

[33] H. Harai, M. Murata e H. Miyahara. Performance of Alternate Routing Methods in All-Optical Switching Networks. Em *IEEE INFOCOM 97*, volume 2, pp. 516–524, Abril 1997.

[34] Mohammad Ilyas e Hussein T. Mouftah. *The Handbook of Optical Communication Networks*. CRC Press, 2003.

[35] Paola Iovanna, Roberto Sabella e Marina Settembre. A Traffic Engineering System for Multilayer Networks Based on the GMPLS Paradigm. *IEEE Network*, pp. 28–37, Março/Abril 2003.

[36] Lundy Lewis. Implementing Policy in Enterprise Networks. *IEEE Communications Magazine*, 34(1):50–55, Janeiro 1996.

[37] L. Li e A. K. Somani. Dynamic Wavelength Routing Using Congestion and Neighborhood Information. Em *IEEE/ACM Transactions on Networking*, volume 2, 1999.

[38] Michael MacGarry, Martin Maier e Martin Reisslein. Ethernet pons: A survey of dynamic bandwidth allocation (dba) algorithms. *IEEE Optical Communications*, pp. 2–9, Agosto 2004.

[39] Michael MacGarry e Martin Reisslein. Bandwidth Management for WDM EPONs. *Journal of Optical Networking*, 5(9):637–654, Setembro 2006.

[40] E. Mannie. Generalized Multi-Protocol Label Switching Architecture. *RFC 3945*, Outubro 2004.

[41] E. Mannie. Generalized Multi-protocol Label Switching (GMPLS) Architecture. http://www.ietf.org/rfc/rfc3945.txt, Outubro 2004. RFC-3945.

[42] C. Mills. Internet Accounting: Background. http://www.ietf.org/rfc/rcf1272.txt, Novembro 1991. RFC-1272.

[43] Jonathan Moffet e Morris Sloman. Policy Hierarchies for Distributed Management Systems. *IEEE Journal on Selected Areas in Communications*, 11(9):1404–1414, Dezembro 1993.

[44] National Institute of Standards e Tecnologies. GMPLS Lightwave Agile Switching Simulator (GLASS). http://snad.ncsl.nist.gov/glass/. Página acessada em 21 de março de 2006.

[45] Canhui (Sam) Ou, Keyao Zhu, Jing Zhang, Hongyue Zhu e Biswanath Mukherjee. Traffic Grooming for Survivable WDM Networks: Dedication Protection. *Journal of Optical Networking*, 3(1):50–74, Janeiro 2004.

[46] S. Ramamurthy e B. Mukherjee. Fixed-Alternate Routing and Wavelength Conversion in Wavelength-Routed Optical Networks. Em *IEEE GLOBECOM 98*, volume 4, pp. 2295–2302, Novembro 1998.

[47] S. Ramamurthy, Laxman Sahasrabuddhe e Biswanath Mukherjee. Survivable WDM Mesh Networks. *Journal of Lightwave Technology*, 21(4):870–883, Abril 2003.

[48] George N. Rouskas e Harry G. Perros. A Tutorial on Optical Networks. Em E. Gregori, G. Anastasi e S. Basagni, editors, *Advanced Lectures on Networking : NETWORKING 2002 Tutorials*, volume 2497/2002, pp. 155–193. Springer-Verlag, 2002.

[49] Debanjan Saha, Bala Rajagopalan e Greg Bernstein. The Optical Network Control Plane: State of the Standards and Deployment. *IEEE Optical Communications*, 41(8):S29–S34, Agosto 2003.

[50] Morris Sloman. Policy Driven Management for Distributed Systems. *Journal of Network and Systems Management*, 2(4):333–360, Dezembro 1994.

[51] Morris Sloman e Emil Lupu. Security and Management Policy Specification. *IEEE Network*, 16(2):10–19, Março/Abril 2002.

[52] John Strassner. DEN-ng: Achieving Business-Driven Network Management. Em *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pp. 753–766, Abril 2002.

[53] S. Subramaniam, M. Azizoglu e A. K. Somani. All Optical Networks with Sparse Wavelength Conversion. *IEEE/ACM Transaction on Networking*, 4:544–557, Agosto 1996.

[54] Fábio Verdi, Cláudio Carvalho, Maurício Magalhães e Edmundo Madeira. Policy-based Grooming in Optical Networks. *Fourth Latin American Network Operations and Management Symposium (LANOMS)*, Agosto 2005. Porto Alegre, Brasil.

[55] Fábio Verdi, Edmundo Madeira e Maurício Magalhães. Policy-based Admission Control in GMPLS Optical Networks. *First IEEE Broadnets'04 (formalmente OptiComm)*, pp. 337–339, Outubro 2004. San Jose - Estados Unidos.

[56] Fábio L. Verdi, Cláudio Carvalho, Maurício Magalhães e Edmundo Madeira. Policy-based grooming in optical networks. *Journal of Network and Systems Management*, Junho 2008. Aceito para publicação.

[57] Dinesh C. Verma. Simplifying Network Administration Using Policy-Based Management. *IEEE Network*, 16(2):20–26, Março/Abril 2002.

[58] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege e D. Spence. AAA Authorization Framework. http://www.ietf.org/rfc/rcf2904.txt, Agosto 2000. RFC-2904.

[59] Wei Wei, Qingji Zeng e Yun Wang. Multi-Layer Differentiated Integrated Survivability for Optical Internet. *Photonic Network Communications*, pp. 267–284, Novembro 2004.

[60] René Wies. Policies in Network and Systems Management - Formal Definition and Architecture. *Journal of Network and Systems Management*, 2(1):333–360, Março 1994.

[61] J. Wroclawski. The Use of RSVP with IETF Integrated Services. http://www.ietf.org/rfc/rcf2210.txt, Setembro 1997. RFC-2210.

[62] R. Yavatkar, D. Pendarakis e R. Guerin. A Framework for Policy-based Admission Control. http://www.ietf.org/rfc/rfc2753.txt, Janeiro 2000. RFC-2753.

[63] Hui Zang, Jason P. Jue e Biswanath Mukherjee. A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks. *Optical Networks Magazine*, 1(1):47–60, Janeiro 2000.

[64] Jing Zhang e Biswanath Mukherjee. A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges. *IEEE Network*, 18(2):41–48, Março/Abril 2004.

[65] Jing Zhang, Keyao Zhu, Laxman Sahasrabuddhe, S. J. Ben Yoo, e Biswanath Mukherjee. On the Study of Routing and Wavelength Assignment Approaches for Survivable Wavelength-Routed WDM Mesh Networks. *Optical Network Magazine*, pp. 16–27, Novembro/Dezembro 2003.

[66] Qin Zheng e Gurusamy Mohan. Protection Approaches for Dynamic Traffic in IP/MPLS-over-WDM Networks. *IEEE Optical Communications*, pp. S24–S29, Maio 2003.

[67] Keyao Zhu e Biswanath Mukherjee. Traffic Grooming in an Optical WDM Mesh Network. *IEEE Journal on Selected Areas in Communications*, 20(1):122–133, Janeiro 2002.

[68] Keyao Zhu, Hui Zang e Biswanath Mukherjee. A Comprehensive Study on Next-Generation Optical Grooming Switches. *IEEE Journal on Selected Areas in Communications*, 21(7):1173–1186, Setembro 2003.