SOBREVIVÊNCIA EM REDES ÓPTICAS TRANSPARENTES

Marco Dias Dutra Bicudo

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA ELÉTRICA.

Aprovada por:

Prof. Otto Carlos Muniz Bandeira Duarte, Dr.Ing.

Prof. Luís Henrique Maciel Kosmalski Costa, Dr.

Prof. Marcelo Gonçalves Rubinstein, D.Sc.

Prof. Antonio Jorge Gomes Abelém, D.Sc.

RIO DE JANEIRO, RJ - BRASIL

DEZEMBRO DE 2005

BICUDO, MARCO DIAS DUTRA

Sobrevivência em Redes Ópticas Transparentes [Rio de Janeiro] 2005

XIV, 75 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia Elétrica, 2005)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Redes Ópticas Transparentes
2. Multiplexação por Comprimento de Onda
3. Sobrevivência a Falhas

I. COPPE/UFRJ II. Título (série)

À minha família.

Agradecimentos

À minha família, principalmente meus pais, por todo o amor, orientação, incentivo e apoio ao longo da minha vida.

Ao professor Otto por toda a amizade, confiança e orientação, além de sempre estar presente, para dar conselhos e ajudar a superar todos os obstáculos.

Aos amigos Aurelio, Daniel, Guilherme, Igor, Miguel e Rafael pela amizade e pela ajuda nos diversos momentos de dificuldade encontrados no decorrer da tese.

A toda a equipe do GTA, em particular aos amigos, Bernardo, Italo, Kleber, Rezende, pela amizade e pela boa convivência durante toda a tese.

Aos professores Luís Henrique Costa, Marcelo Rubinstein e Antônio Abelém pela presença na banca examinadora.

À CAPES, RNP e FUNTTEL, pelo financiamento da pesquisa.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

SOBREVIVÊNCIA EM REDES ÓPTICAS TRANSPARENTES

Marco Dias Dutra Bicudo

Dezembro/2005

Orientador: Otto Carlos Muniz Bandeira Duarte

Programa: Engenharia Elétrica

O objetivo deste trabalho é analisar o desempenho dos mecanismos de sobrevivência a falhas nas redes ópticas transparentes. O impacto da conectividade da rede e da reversibilidade destes mecanismos é abordado nas análises. É proposto um novo mecanismo de sobrevivência que visa oferecer uma maior flexibilidade à rede no atendimento aos requisitos de sobrevivência e, conseqüentemente, torná-la mais adaptada às necessidades do usuário. A probabilidade de bloqueio e a disponibilidade de conexões são utilizadas como métricas de desempenho da rede. O mecanismo proposto adiciona à configuração da rede um parâmetro α, chamado fator de relaxação de restrições SRLG (*Shared Risk Link Group*). Através do ajuste desta variável é possível controlar o compromisso entre o ganho da probabilidade de bloqueio e a perda de disponibilidade. Os resultados da conectividade da rede mostram que o custo de uma rede de maior conectividade, associado à instalação de enlaces ópticos, é recompensado pelos ganhos tanto na probabilidade de bloqueio quanto na disponibilidade. Nas simulações de reversibilidade, os resultados mostram que os mecanismos não-reversíveis, ao contrário do que se previa, podem resultar em melhor disponibilidade, dependendo somente do tempo de comutação entre os canais ópticos, primário e de proteção, que constituem uma conexão óptica.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

SURVIVABILITY IN TRANSPARENT OPTICAL NETWORKS

Marco Dias Dutra Bicudo

December/2005

Advisor: Otto Carlos Muniz Bandeira Duarte

Department: Electrical Engineering

This work aims to analyze the performance of the survivability mechanisms of transparent optical networks. The node degree and the non-reversibility of such mechanisms are also addressed in the analysis. A novel mechanism is proposed envisaging a network more flexible and, consequently, more suitable to the user. The blocking probability and the connection availability are used as performance metrics. The proposed mechanism adds to the optical network configuration a parameter α for loosening the SRLG (Shared Risk Link Group) constraints. This parameter controls the tradeoff between the blocking probability gain and the availability loss is controlled. The results of the node degree simulation show that the implementation cost of a network with higher connectivity is rewarded by better blocking probability and availability. The results of the non-reversibility simulation show the non-reversible mechanism may present better availability, only depending on the switching time between primary and secondary optical channels, which constitute the optical connection.

Sumário

Lista de Figuras

Lista de Acrônimos

ATM:	*Asynchronous Transfer Mode*;
ASON:	*Automatic Switched Optical Network*;
DWDM:	*Dense Wavelength Division Multiplexing*;
EDFA:	*Erbium-Doped Fiber Amplifier*;
GMPLS:	*Generalized Multi-protocol Label Switching*;
IEEE:	*Institute of Electrical and Electronics Engineers*;
ILP:	*Integer Linear Programming*;
IP:	*Internet Protocol*;
LSP:	*Label Switched Path*;
MPLS:	*Multi-protocol Label Switching*;
MEMS:	*Micro-Electro-Mechanical Systems*;
NGN:	*Next Generation-Network*;
OEO:	*Optical-Electrical-Optical*;
OPSN:	*Optical Packet Switching Network*;
OXC:	*Optical Cross-Connect*;
QoS:	*Quality of Service*;
SLA:	*Service Level Agreement*;
SONET:	*Synchronous Optical Network*;
SRLG:	*Shared Risk Link Group*;
STL:	*Standard Template Library*;
UDP:	*User Datagram Protocol*;
V.A.:	Variável Aleatória;

VoIP: *Voice over IP*;

VPN: *Virtual Private Network*;

WDM: *Wavelength Division Multiplexing*;

WRON: *Wavelength Routing Optical Network*.

Capítulo 1

Introdução

AS redes ópticas permitem baixa latência e grande banda passante, proporcionando um ambiente favorável ao crescimento da Internet e a proliferação de aplicações cada vez mais sofisticadas que exigem maior desempenho da rede. As aplicações, tais como os jogos interativos, os programas de compartilhamento de arquivos e as conferências de áudio e vídeo, entre outras, estão presentes no cotidiano de praticamente todos os usuários de computadores que utilizam a Internet [1, 2]. Além da necessidade de banda passante e de baixo atraso, existe também uma tendência para que estas aplicações apresentem um comportamento cada vez mais dinâmico, modificando ao longo do tempo o conjunto de origens e destinos de tráfego na rede para uma única instância de aplicação [3, 4]. Outra tendência verificada é o aumento do período de duração de uma aplicação, que pode ser de horas e algumas de até 24 horas por dia. Assim, torna-se evidente que a disponibilidade e a confiabilidade são fundamentais para as redes ópticas.

1.1 Motivação

A maioria das redes ópticas atuais utiliza o ATM (*Asynchronous Transfer Mode*) e o SONET (*Synchronous Optical Network*) como tecnologias de transmissão óptica. Estas tecnologias baseiam-se em conexões de banda fixa, geralmente estabelecidas manualmente. Um novo modelo mais adequado às necessidades das aplicações atuais é o mo-

delo multicamadas IP/GMPLS (*Generalized Multiprotocol Label Switching*)-sobre-WDM (*Wave-length Division Multiplexing*). A multiplexação de comprimento de onda WDM é uma tecnologia que permite melhor utilizar a banda passante das fibras ópticas. Com esta tecnologia, dentro de uma única fibra podem ser estabelecidos diversos canais ópticos que operam em diferentes comprimentos de onda podendo atingir taxas de transmissão da ordem de 40 Gbps [5]. Cada canal óptico deste permite que dados sejam trasmitidos utilizando esquemas de modulação distintos e com taxas de transmissão diferentes uma das outras. Por sua vez, o GMPLS [6], proporciona o estabelecimento dinâmico de canais ópticos, introduzindo o conceito de Redes Ópticas de Comutação Automática (*Automatic Switched Optical Network* - ASON) [3,7,8]. A introdução do MPLS (*Multiprotocol Label Switching*) [9], que está contido na arquitetura GMPLS, agrega importantes funcionalidades à rede, pois suas conexões (*Label Switched Path* - LSP) fornecem a possibilidade de Engenharia de Tráfego [10, 11], de Redes Privadas Virtuais (VPN - *Virtual Private Network*) [12] e de Qualidade de Serviço (QoS - *Quality of Service*) [13, 14].

Conforme as redes ópticas migraram da topologia em anel, muito comumente encontrada em redes SONET/SDH (*Synchronous Digital Hierarchy*), para a topologia em malha, que visa solucionar problemas de escalabilidade e de redundância excessiva, as deficiências de implementação de sobrevivência na nova topologia se tornaram evidentes. A simplicidade nas decisões de envio da topologia em anel favorece a implementação da sobrevivência pois há somente duas alternativas para o envio de dados. Por outro lado, as redes em malha apresentam múltiplos caminhos e necessitam de estabelecimento de conexões para transferir dados da origem ao destino. Portanto, desde que esta tendência de migração de topologia se consolidou, pesquisas relacionadas à sobrevivência em redes WDM em malha se desenvolveram visando solucionar este problema que afeta a disponibilidade de conexões em redes ópticas em malha. Aliado a esta tendência, há também a consolidação da tecnologia de fabricação de comutadores ópticos transparentes. Uma rede constituída de comutadores transparentes encaminha os fluxos de dados sem necessitar de conversões do meio óptico para o meio eletrônico. Nas redes ópticas o encaminhamento realizado eletronicamente é o maior limitador da taxa de transmissão das conexões ópticas. Assim, a introdução desta tecnologia permite que as conexões ópticas obtenham uma largura de banda que não era possível anteriormente.

A multiplexação de vários canais em uma única fibra-óptica torna a rede óptica mais sensível ao evento de uma falha, pois a interrupção de uma única fibra pode interferir no serviço oferecido por diversas conexões. Neste contexto, a sobrevivência a falhas em redes ópticas é quesito essencial no projeto e operação destas redes. A sobrevivência a falhas, como o próprio nome já diz, é a capacidade de uma rede não prejudicar, ou não interromper, as conexões de seus usuários quando ocorrer a falha de algum recurso da rede. Nas redes ópticas em malha, os mecanismos que oferecem sobrevivência a falhas, também denominados mecanismos de sobrevivência, são classificados, basicamente, em dois tipos: a proteção, que pré-computam e pré-alocam os recursos de recuperação; e a restauração, que computam os recursos de recuperação de maneira reativa apenas quando ocorre a falha. Aplicando estes mecanismos de sobrevivência a falhas em uma rede IP/GMPLS-sobre-WDM, o leque de implementações distintas de sobrevivência se multiplica, pois agora estes mecanismos podem ser utilizados tanto na camada WDM, oferecendo recuperação de conexões WDM chamadas de canais ópticos, como na camada IP/GMPLS, oferecendo recuperação de conexões GMPLS.

A maioria dos trabalhos de sobrevivência a falhas realiza análises utilizando, a probabilidade de bloqueio e a disponibilidade. A probabilidade de bloqueio determina a probabilidade com que uma requisição de conexão não seja atendida pela rede, que pode ser devido à falta de recursos ou devido à falha de enlaces. Apesar de não estar no contrato do usuário, este parâmetro é do interesse das operadoras de redes ópticas, pois está associado à eficiência da rede. A disponibilidade mede a percentagem do tempo que o usuário obtém o serviço que foi contratado e que, portanto, deve ser respeitado a todo custo. A solução ideal para este problema seria obter a probabilidade de bloqueio mínima para a disponibilidade máxima. Como esta solução não foi alcançada ou levaria a um grande desperdício de recursos, as propostas nesta área buscam o compromisso entre estas duas variáveis.

1.2 Trabalhos Relacionados

A pesquisa na área de sobrevivência de redes ópticas em malha abrange diversos tópicos que incluem a sobrevivência na camada óptica [15–20], a sobrevivência na camada IP [21–25], análises comparativas entre proteção *versus* restauração [17, 19, 26], o segmentos do canal a ser recuperado [27, 28] e propostas de mecanismos de recuperação utilizando um modelo multicamadas [3, 22, 23, 29], entre outros. Ramamurthy *et al.* [15] realizam formulações de programação linear (*Integer Linear Programming* - ILP) para investigar os diferentes mecanismos de proteção de redes WDM em malha. São abordadas a proteção de enlace e a proteção de canal óptico (*lightpath*). As formulações ILPs analisam a quantidade necessária de recursos da rede para alocar uma determinada demanda estática de tráfego. Em um outro artigo, Ramamurthy *et al.* [16] analisam o tempo de recuperação de falhas e a eficiência de diferentes mecanismos de proteção e restauração. Zhang *et al.* [17] realizam um estudo geral sobre sobrevivência a falhas, comparando proteção e restauração de redes WDM em malha. Os mecanismos de sobrevivência são avaliados com base na confiabilidade, na disponibilidade, no tempo de restauração e na restaurabilidade do serviço. Os fatores que influem no desempenho e como melhorar a operação destes mecanismos são analisados. Mohan *et al.* [18] abordam a sobrevivência através de mecanismos de restauração de canais ópticos, afirmando que somente a restauração possibilita o uso eficiente dos recursos da rede. Os principais mecanismos de restauração são analisados e seus desempenhos comparados. Gerstel *et al.* [19], apresentam uma abordagem sob a perspectiva de serviço da sobrevivência de redes ópticas. O autor justifica a sobrevivência na camada óptica devido à necessidade de baixo tempo de recuperação, que não é possível para um mecanismo implementado na camada IP, dentre outros aspectos operacionais. O trabalho analisa as vantagens e desvantagens para a operadora da rede de cada um dos mecanismos, de proteção e restauração, discutindo aspectos como a topologia da rede adotada, contrapartidas econômicas para a operadora além dos benefícios adquiridos pelo cliente. Gerstel *et al.* [20] apresentam uma abordagem focada na implementação da sobrevivência em redes ópticas em malha e em anel. Detalhes como o posicionamento dos multiplexadores e demultiplexadores dentro da arquitetura do nó comutador óptico, o mapeamento das conexões dos clientes na camada

óptica e a interação entre o cliente e a rede são discutidos. Wang *et al.* [21] realizam uma análise sobre restauração de canal, sub-canal e enlace em redes ópticas IP-sobre-WDM em malha utilizando a plataforma de controle e sinalização GMPLS. É observado nas simulações que existe um compromisso entre a probabilidade de bloqueio, taxa de sucesso de restauração, tempo médio de restauração e disponibilidade, na decisão de qual dos três mecanismos de restauração deve ser implementado. Kodialam *et al.* [22, 30] e Ye *et al.* [24] utilizam uma abordagem de roteamento integrado, considerando informações das camadas WDM e IP simultaneamente para a implementação de sobrevivência em redes ópticas em malha. Zheng *et al.* [23] apresentam dois algoritmos de roteamento integrado para mecanismos de proteção. O BIRA (*Bandwidth-based Integraded Routing Algorithm*) visa a eficiência da rede através da minimização da banda passante necessária ao estabelecimento dos LSPs. O HIRA (*Hop-based Integraded Rounting Algorithm*) visa a eficiência da rede através da minimização do número de saltos necessários ao estabelecimento dos LSPs. Ou *et al.* [27] e Li *et al.* [28] apresentam esquemas de proteção de sub-canal como uma alternativa viável para reduzir o tempo de restauração, já que a sinalização não necessita percorrer toda extensão do canal óptico até o nó de origem para que seja iniciado o procedimento de recuperação.

Alguns trabalhos [3, 29] se utilizam das funcionalidades da plataforma GMPLS para estabelecer conexões ópticas automaticamente. Segundo os autores, a introdução deste plano inteligente de gerenciamento e de controle torna estas redes, as ASON, mais capazes de implementar sobrevivência a falhas. Este tipo de rede é considerado a próxima geração de redes (*Next Generation Network* - NGN) [31, 32], pois proporcionam, além da sobrevivência a falhas, o estabelecimento dinâmico de conexões ópticas, satisfazendo requisitos das aplicações mais exigentes e dinâmicas.

Por fim, Ali *et al.* [33] aplica o conceito de compartilhamento para qualquer recurso da rede que possa sofrer escassez, como conversores, regeneradores de sinal e dispositivos óptico-eletrônico-óptico (*Optical-Eletronic-Optical* - OEO). Segundo Ali *et al.* [33], o compartilhamento de recursos de proteção pode ir muito além do compartilhamento convencional de comprimento de onda em fibras ópticas.

1.3 Objetivos

O principal objetivo deste trabalho é realizar análises de desempenho de mecanismos de proteção em redes ópticas WDM em malha e propor um novo mecanismo de proteção. Os mecanismos de proteção são uma das possíveis abordagens à implementação de sobrevivência a falhas em redes ópticas. O aprimoramento destes mecanismos visa uma maior eficiência da rede, proporcionando à operadora da rede economia de recursos de custo elevado, como comprimentos de onda, por exemplo. O mecanismo proposto foi desenvolvido para aumentar o compartilhamento entre recursos de proteção e assim possibilitar que a rede atinja esta maior eficiência.

O mecanismo proposto e as análises de desempenho são apresentados em [34, 35]. As análises de desempenho utilizam dois parâmetros: a probabilidade de bloqueio de conexões, e a disponibilidade das conexões que foram estabelecidas com sucesso. As análises são divididas em duas partes. Primeiramente o desempenho da rede é analisado com o mecanismo proposto e com os mecanismos convencionais de proteção. Através do parâmetro de relaxação de risco α, introduzido pelo mecanismo proposto, é possível obter um compromisso entre a probabilidade de bloqueio e a disponibilidade, como é discutido ao longo do trabalho.

Em seguida, é analisado o impacto da conectividade da rede e da não-reversibilidade dos mecanismos no desempenho geral dos mecanismos de proteção implementados em uma rede. Para as simulações de conectividade, os mecanismos de proteção são implementados em topologias de redes ópticas de diferentes conectividades, para medir o quanto uma rede mais conexa afeta positivamente os parâmetros de desempenho. As simulações de reversibilidade buscam ponderar as vantagens e as desvantagens da implementação de mecanismos não-reversíveis, que afetam, principalmente, a disponibilidade das conexões ópticas. Um simulador próprio é desenvolvido para a realização das análises de desempenho comparando os mecanismos convencionais e o mecanismo proposto. O simulador é desenvolvido em C++ e utiliza a biblioteca de programação genérica STL (*Standard Template Library*) [36, 37].

1.4 Objetivos

Esta tese está organizada da seguinte forma. O Capítulo 2 introduz conceitos básicos de redes ópticas, de multiplexação de comprimento de onda e de redes ópticas transparentes. A arquitetura de rede considerada neste trabalho, os componentes que compõem esta arquitetura de rede e as características das tecnologias aplicadas que afetam o desempenho desta arquitetura são detalhados. O Capítulo 3 apresenta os principais mecanismos de sobrevivência a falhas em redes ópticas em malha e propõe o novo mecanismo, discutindo quais os impactos no desempenho da rede para os diferentes mecanismos de sobrevivência. Outros aspectos como a conectividade da rede e a reversibilidade dos mecanismos de sobrevivência são discutidos. O Capítulo 3 também realiza uma análise funcional destes mecanismos e determina os principais fatores que afetam o desempenho da rede. No Capítulo 4 são apresentados os detalhes referentes às simulações, os detalhes de implementação do simulador e as análises dos resultados. Todo o ambiente de simulação, incluindo a estrutura de dados do simulador, os algoritmos de roteamento utilizados e os procedimentos efetuados pelo simulador para sorteio de variáveis aleatórias, é detalhado. No Capítulo 4 também são apresentados os resultados obtidos da comparação do mecanismo proposto e das análises de desempenho relativas à conectividade da rede e à reversibilidade dos mecanismos. Por fim, no Capítulo 5, são apresentadas as conclusões e os trabalhos futuros.

Capítulo 2

Redes Ópticas

AS tecnologias de redes ópticas são responsáveis pela enorme largura de banda disponível hoje no mundo todo e elas continuam evoluindo rapidamente em termos de funcionalidades e de capacidade. Os centros de pesquisa, a indústria de equipamentos de telecomunicações e as organizações de padronização, tais como o IEEE (*Institute of Electrical and Electronics Engineers*) e o ITU-T (*International Telecommunications Union Telecommunication Standardization Sector*), são os principais atores no desenvolvimento das redes ópticas.

Neste capítulo, são abordados alguns conceitos básicos de redes ópticas, as tecnologias de transmissão em fibra óptica, as redes ópticas totalmente transparentes e seus principais componentes. A tecnologia de multiplexação por comprimento de onda é também apresentada neste capítulo.

2.1 Os Serviços das Redes Ópticas

Existe uma classificação fundamental que divide as infra-estruturas de rede em relação à comutação na rede: as redes de comutação de circuito e as redes de comutação de pacotes. As redes de comutação de circuito oferecem circuitos dedicados para seus clientes. Estas conexões, depois de estabelecidas, têm banda passante garantida e dedicada até que seja efetuada a desconexão. Nestas redes, a soma da banda passante de todas as conexões

em um enlace deve ser menor ou igual à capacidade de transmissão do enlace. A aplicação mais comum deste tipo de rede são as redes de telefonia pública, que oferecem uma conexão de banda fixa, tipicamente de 4 kHz, aos seus usuários finais. Esta conexão é, então, convertida para um canal digital de 64 kbps. Porém, estas redes oferecem diversas outras taxas de transmissão. Os serviços de linha privada, como são chamados, podem apresentar taxas de transmissão de algumas dezenas de kbps a até dezenas de gigabits por segundo (Tbps).

O principal problema das redes de comutação de circuito é a ineficiência de utilização dos recursos da rede, que ficam ociosos quando um usuário não transmite dados, o que é comum em tráfegos em rajadas. Os tráfegos em rajadas são comumente encontrados em redes de dados, como a Internet. As redes de comutação de pacotes foram propostas para lidar mais eficientemente com tráfegos em rajadas. Nestas redes, os pacotes dos fluxos de diferentes usuários são multiplexados em um enlace, que tem sua capacidade compartilhada entre todos os fluxos. Desta maneira, a capacidade de transmissão do enlace é utilizada eficientemente, porque quando um usuário não transmite pacotes outro poderá transmitir além do usual. Porém, não é possível garantir banda nem latência, pois a utilização dos recursos da rede não é controlada, não é previsível e, principalmente, não necessita de estabelecimento de circuitos ou conexões que garantem reserva de recursos.

As redes ópticas, como implementadas atualmente, são baseadas em comutação de circuitos, apesar desta comutação ainda ser implementada eletronicamente. Isto se deve a algumas deficiências tecnológicas atuais, principalmente, à incapacidade de processar opticamente um pacote, o que faz com que a informação óptica seja convertida para um plano eletrônico e processada eletronicamente. Além disso, em uma rede óptica em malha, um nó pode estar ligado a diversos outros nós ópticos por dezenas de fibras ópticas. Processar, encaminhar e comutar eletronicamente todos esses pacotes ópticos gera, atualmente, latência e, conseqüentemente, ineficiência na utilização da banda das fibras. As Redes de Comutação Óptica de Pacotes (*Optical Packet Switching Network* - OPSN) [38–40] podem apresentar um futuro promissor, mas esta tecnologia ainda precisa amadurecer para ser implementada, pois não há como processar informação de outra maneira que não seja eletrônica. Portanto, implementar uma Rede Óptica de Comutação/Roteamento de Lambda (*Wavelength Routing Optical Network* - WRON) [41, 42] é uma solução de com-

promisso entre a atual falta de tecnologia de processamento óptico de pacotes, porque estabelece circuitos ópticos, e a baixa velocidade do processamento eletrônico, pois devido ao estabelecimento de circuitos, não necessita de processamento eletrônico em seus nós.

O modelo de serviço oferecido pelas empresas operadoras de redes ópticas está mudando rapidamente conforme as tecnologias evoluem e a concorrência entre empresas se intensifica. A largura de banda passante alocada para cada concessão de linha privada está crescendo. Taxas de 155 Mbps, 2,5 Gbps e até 10 Gbps, que até poucos anos atrás eram muito pouco comuns para transmissão em longas distâncias, tornam-se cada vez mais utilizados. Além disto, os clientes diretos destas redes ópticas estão assinando contratos cada vez mais curtos, pois a expectativa é de conseguir taxas mais alta com menores custos em um curto período de tempo. Também já é possível encontrar situações onde os contratos têm duração de dias ou horas, seja para realizar um *backup* de dados imprevisto, cobrir uma falha eventual, ou até devido a algum evento especial. Devido a esta dinâmica crescente no estabelecimento de conexões ópticas, existe a necessidade de um modelo que supra estas necessidades.

Outro aspecto muito importante em redes ópticas é a disponibilidade de conexões, que é definida como a percentagem do tempo que a conexão permanece operacional. A disponibilidade vem aumentando ano a ano e é cada vez mais comum encontrar operadoras de redes ópticas que oferecem cinco 9's (99,999%) [5, 43] de disponibilidade, que corresponde a um período de inoperacionalidade de 5 minutos ao ano. Já se fala em sete 9's e até nove 9's para se definir disponibilidade. Para atingir este nível de disponibilidade, a rede deve implementar mecanismos de sobrevivência a falhas de rápida recuperação. Este assunto é discutido no Capítulo 3.

2.2 Terminologia e Conceitos

Nesta seção são introduzidos conceitos e terminologias pertinentes à arquitetura de rede óptica utilizada neste trabalho. Algumas das definições apresentadas nesta seção são baseadas em [44] e podem apresentar definições diferentes fora do escopo deste trabalho,

em outra abordagem de redes ópticas.

2.2.1 Transparência e Opacidade

Uma rede óptica consiste em um conjunto de nós interconectados entre si através de fibras ópticas. Estes nós, os comutadores OXC (*Optical Cross-Connect*), incluem uma matriz de comutação óptica e um controlador desta matriz. As matrizes de comutação óptica podem ser opacas ou transparentes. As opacas realizam conversões óptico-eletrônico-óptico (*Optical-Eletronic-Optical* - OEO) para efetuar a comutação. Uma rede que utilize comutadores opacos, ou seja, que sejam constituídos de matrizes de comutação opacas, pode manipular eletronicamente os sinais ópticos que atravessam um nó, como, por exemplo, efetuar operações de reformatação, regeneração, retemporização e amplificação do sinal. A rede óptica transparente transporta os sinais ópticos do emissor ao receptor ao longo da rede totalmente no domínio óptico, sem conversões OEO. Conseqüentemente, os nós do núcleo de uma rede transparente, apesar de poderem amplificar opticamente os sinais, através de EDFAs (*Erbium-Doped Fiber Amplifier*) por exemplo, não obtém acesso aos dados transportados pelos sinais ópticos.

2.2.2 A Multiplexação por Comprimento de Onda

A multiplexação por comprimento de onda (*Wavelength Division Multiplexing* - WDM) é uma técnica que permite que múltiplos sinais ópticos, de diferentes comprimentos de onda ou lambdas, sejam multiplexados em uma única fibra e, portanto, possam ser transmitidos em paralelo nesta fibra. O funcionamento da técnica de muliplexação é ilustrado na Figura 2.1.

Um lambda pode transportar diferentes conteúdos digitais a taxas de transmissões variadas, como OC-3 (155 Mbps), OC-12 (622 Mbps) etc, e a diferentes formatos ou encapsulamentos, como SONET, Ethernet e ATM. Desta forma, a tecnologia WDM permite alta capacidade e flexibilidade devido à transmissão paralela de diversos lambdas onde, por exemplo, em um lambda pode trafegar um sinal SONET OC-48 de aproximadamente 2,5 Gbps e, na mesma fibra óptica, em outro lambda pode trafegar Ethernet OC-192 de

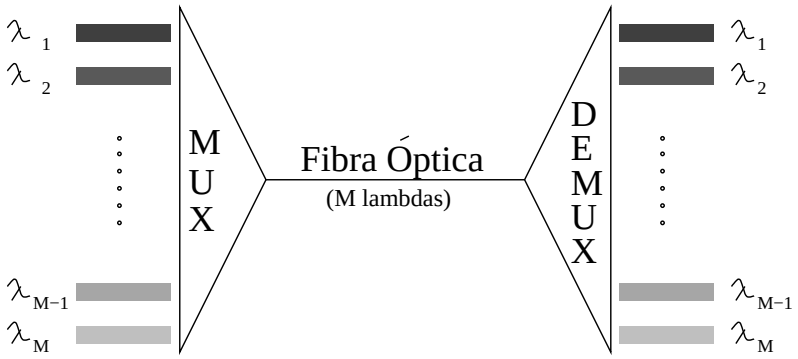


Figura 2.1: Multiplexação e demultiplexação de comprimento de onda.

aproximadamente 10 Gbps. As pesquisas em WDM denso (*Dense WDM* - DWDM) não param de derrubar os recordes do número de lambdas multiplexados em uma única fibra, que já ultrapassam o milhar, assim como da taxa máxima transmitida, que já ultrapassou o Tbps. Em pouco tempo será possível fabricar comercialmente equipamentos capazes de transmitir até 160 lambdas com capacidade superior a OC-192, atingindo, em uma única fibra, até 1,6 Tbps [5, 45].

O WDM é uma técnica responsável pela transmissão em fibras ópticas, não especificando, porém os requisitos necessários aos nós da rede e os procedimentos na comutação destes sinais ópticos. Tipicamente, nas redes ópticas mais avançadas, esta comutação é realizada através de dispositivos ópticos, como as matrizes de comutação ópticas, as OXCs (*Optical Cross-Connect*), apresentadas na Seção 2.2.5. A arquitetura das redes ópticas WDM em malha é apresentada na Seção 2.3.

2.2.3 O Canal Óptico

Canal óptico (*lightpath*) é uma conexão da camada óptica fim-a-fim entre dois nós da rede, geralmente localizado na borda, como a Figura 2.2 ilustra. O conceito de canal óptico não se aplica somente a redes ópticas com comutadores OXCs transparentes. Uma rede que apresenta somente comutadores opacos também resulta em canais ópticos, apesar das conversões OEO. Neste trabalho o termo canal óptico tem o mesmo significado de caminho óptico.

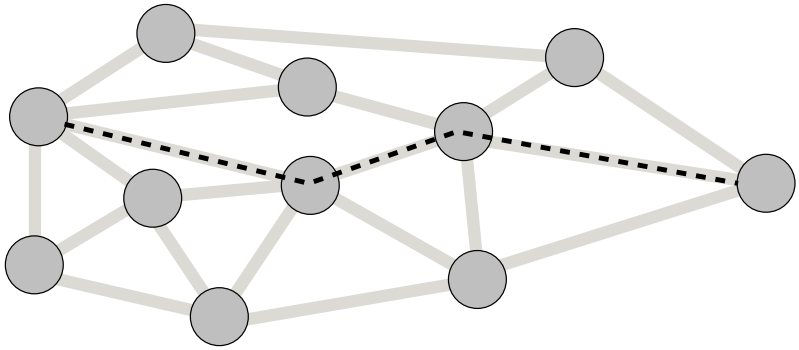


Figura 2.2: Exemplo de Canal Óptico

2.2.4 A Propriedade de Continuidade Obrigatória de Lambda

Um canal óptico satisfaz as restrições da propriedade de continuidade obrigatória de comprimento de onda, ou simplesmente continuidade de lambda, se é transportado pelo mesmo lambda, por toda a sua extensão, em todos os enlaces.

Para redes opacas esta restrição não é problema, pois como a comutação do feixe de luz é realizada através de conversões OEO a conversão eletrônico-óptica da porta de saída pode escolher o lambda disponível na fibra. As redes transparentes, em contrapartida, não apresentam conversões OEO e, portanto, a restrição de continuidade de lambda pode acarretar em altas probabilidades de bloqueio. Uma alternativa é a introdução de conversores ópticos de lambda em seus nós [46, 47], que não apresenta as limitações de banda dos dispositivos eletrônicos e reduz a probabilidade de bloqueio, devido à eficiência de utilização dos lambdas da rede. Uma rede transparente que apresenta comutadores OXCs sem conversores ópticos de lambda acarreta uma maior probabilidade de bloqueio porque a disputa por recursos ocorre com maior freqüência. Por outro lado, esta disputa não ocorre em redes opacas ou redes transparentes com conversores, pois se o lambda escolhido estiver indisponível basta utilizar outro.

Uma rede de conversão total de lambda é uma rede que inclui em cada nó, ou OXC, conversores ópticos de lambda para cada comprimento de onda de cada interface óptica, ou fibra óptica. Desta forma, não existe a possibilidade de faltar conversores de lambda e, conseqüentemente, bloquear o estabelecimento de uma conexão. Os conversores ópticos de lambda apresentam um custo relativamente elevado, e, portanto, seu uso deve ser

minimizado no projeto e na implementação destas redes ópticas.

Alcançar uma baixa probabilidade de bloqueio com a mínima quantidade de conversores é necessário para que as redes ópticas sejam eficientes e relativamente baratas. Neste contexto, o posicionamento esparso de conversores [48], a utilização parcial de conversores nos nós da rede [49] e a combinação destas duas técnicas [50] vêm obtendo resultados significativos na redução do custo de implementação de redes ópticas e na melhora da probabilidade de bloqueio. Segundo Chu *et al.* [50], não é necessário que todos os nós da rede sejam habilitados com a conversão total de lambda para que a rede obtenha uma baixa probabilidade de bloqueio equivalente a uma rede transparente de conversão total.

2.2.5 O Comutador Óptico OXC

O comutador óptico OXC (*Optical Cross-Connect*) [51–53] é um dispositivo que permite a comutação de um feixe de luz de uma porta de entrada para uma porta de saída. Ele é constituído, basicamente, de duas entidades: uma entdidade da camanda WDM, a matriz de comutação óptica e uma entidade da camada IP que controla a matriz de comutação óptica. Esta comutação pode utilizar uma conversão óptico-eletrônica na porta de entrada e uma conversão eletrônico-óptica na porta de saída, ou realizar a comutação totalmente óptica. No primeiro caso, a denominada conversão OEO apresenta limitações, como a banda passante, que não é desejada em redes de alta velocidade. No segundo caso, a comutação é dita OOO (*Optica-Optical-Optical*).

O OXC é um dispositivo que funciona no plano óptico comutando sinais ópticos, sem decodificar os sinais ópticos em dados, para obtenção de endereços para a comutação, como acontece em comutadores Ethernet, por exemplo. Esta função é realizada pela matriz de comutação óptica, que, por ser totalmente passiva, necessita de uma unidade de controle. Esta unidade controladora deve implementar protocolos de sinalização e de roteamento que são necessários para computar e estabelecer as conexões do plano óptico. É através deste controlador que os nós da rede trocam informações de estado de enlace e de ocorrência de falhas de recursos, além de sinalizar o estabelecimento de canais ópticos.

2.2.6 Matriz de Comutação Óptica de Larga Escala

Atualmente matrizes de comutação com quantidades de portas de comutação óptica, ou portas comutadoras, variando de poucas centenas a até alguns milhares são empregados pelas empresas de telecomunicações para suas redes ópticas. É importante ressaltar que um cabo de fibra óptica pode conter dezenas de fibras ópticas e cada fibra pode conter dezenas ou até centenas de lambdas. Assim, há a necessidade de desenvolver uma matriz comutadora de larga escala para fornecer dinamicamente o estabelecimento de canais primários e os canais de proteção.

As principais considerações no desenvolvimento destes dispositivos de larga escala são: o número de portas comutadoras necessárias para a fabricação do dispositivo; a uniformidade na atenuação dos possíveis caminhos na matriz de comutação; o número de cruzamentos de sinais (*crossover*); e as características de bloqueio do dispositivo. Maiores detalhes sobre as portas comutadoras serão apresentados na seção seguinte.

As matrizes comutadoras são construídas usando múltiplas portas comutadoras, ou portas de comutação óptica. O número de portas necessárias para a fabricação destas matrizes deve ser considerado porque o custo e a complexidade da matriz dependem deste número. Diversas arquiteturas de matrizes comutadoras foram propostas visando à redução deste número de portas, acarretaram em detrimento de outros parâmetros, também importantes, como a complexidade do algoritmo de controle ou as características de bloqueio do dispositivo.

A uniformidade da atenuação, ou perda de sinal, na matriz de comutação é outro fator importante a ser considerado. Como mencionado, estas matrizes comutadoras podem apresentar diferentes atenuações para diferentes combinações de entrada e saída. Esta característica é acentuada em matrizes de larga escala, pois as variações de possíveis combinações são maiores. Uma medida de uniformidade pode ser obtida considerando os números mínimo e máximo de portas comutadoras para todas as possíveis combinações de entrada e de saída. Desta maneira é possível definir a variação de atenuação associada a uma matriz de comutação óptica.

Muitas das matrizes descritas a seguir são fabricadas pela integração de múltiplas por-

tas ópticas em um único substrato. Diferentemente de circuitos eletrônicos integrados, onde as conexões entre os vários componentes podem ser realizadas em múltiplas camadas, em circuitos ópticos integrados todas estas conexões são realizadas em uma única camada, devido à utilização de guias de onda (*waveguides*). Nesta única camada, se dois guias de onda se cruzam, dois efeitos podem ocorrer: a atenuação do sinal e o cruzamento de sinais (*crosstalk*). Portanto, no projeto e na fabricação destas matrizes, estes cruzamentos (*crossovers*) devem ser evitados para minimizar, ou eliminar completamente, estes efeitos. Vale notar que estes cruzamentos não dizem respeito às portas comutadoras ditas *free-space*, como as portas ópticas que constituem as matrizes de comutação óptica MEMS (*Micro-Electro-Mechanical System*), descritos mais adiante.

Uma matriz comutadora é denominada não-bloqueante se uma porta não utilizada puder ser conectada simultaneamente a qualquer outra porta não utilizada. Assim, uma matriz não-bloqueante pode realizar toda requisição de conexão de uma porta de entrada para uma de saída. Se existe alguma combinação de par entrada-saída que não possa ser conectada, então a matriz comutadora é denominada bloqueante. A maioria das aplicações requisita matrizes não-bloqueantes. Porém, mesmo entre matrizes comutadoras não-bloqueantes existem diferenciações. Uma matriz é denominada amplamente não-bloqueante (*wide-sense nonblocking*) se todas as conexões entre entrada e saída podem ser realizadas sem requisitar que outras conexões sejam rearranjadas, mas nada impede que o controlador verifique a disponibilidade das portas para escolher a melhor configuração. Uma matriz comutadora estritamente não-bloqueante (*strict-sense nonblocking*), por sua vez, permite que qualquer conexão entre portas de entrada e de saída não utilizadas sejam realizadas sem ao menos ter que considerar quais foram as conexões previamente alocadas na matriz comutadora. Ou seja, uma matriz estritamente não-bloqueante também é amplamente não-bloqueante, porém um amplamente não-bloqueante não é estritamente não-bloqueante.

Uma matriz comutadora que requisita o rearranjo de conexões é denominada não-bloqueante rearranjável (*rearrangeable nonblocking*). A vantagem desta matriz é o menor número de portas comutadoras necessárias, tornando-a economicamente mais competitiva. A maior complexidade do algoritmo de controle e a necessidade de interrupção de conexões para o rearranjo desta matriz são as principais desvantagens das arquiteturas

que apresentam esta característica.

A Porta de Comutação Óptica

A porta de comutação óptica, ou porta comutadora, é o elemento que constitui uma matriz de comutação óptica. Este elemento é responsável pelo redirecionamento, ou alteração do curso, de um feixe de luz ou laser dentro da matriz de comutação óptica. Existem diversos tipos de portas ópticas e estes tipos de portas podem ser organizados em arquiteturas distintas, como veremos mais adiante. As portas de comutação óptica são utilizadas em redes ópticas para diversos tipos de aplicações. A aplicação para a qual o tipo de porta será utilizado depende de alguns parâmetros de desempenho do tipo de porta, como o tempo de comutação e números de portas comutadoras, apresentados na Tabela 2.1. Uma das aplicações destas portas é a provisão de canais ópticos. Para este fim, as portas ópticas são utilizadas como componentes das matrizes de comutação que constitui as matrizes de comutação óptica, presente nos comutadores OXCs (*Optical Cross-Connect*), e reorganizam a arquitetura de controle interno, permitindo o estabelecimento de novos canais ópticos. Nesta aplicação, estas portas funcionam como substituições aos cabos (*patch cables*) manuais, mas exigem softwares de gerenciamento de conexões fim-a-fim. Portanto, para este tipo de aplicação é aceitável um tempo total de comutação de alguns milissegundos.

Tabela 2.1: Tipos de aplicações para as portas de comutação óptica.

Aplicação	Tempo de Comutação de uma Porta	Número de portas Necessárias
Provisão de Canal	1-10 ms	>1000
Comutação para Proteção	1-10 ms	2-1000
Comutação de Pacotes	1 ns	>100
Modulação Externa	10 ps	1

Uma outra importante aplicação é para a comutação de proteção de fibra ou de lambda, discutida no Capítulo 3. Estes dispositivos são utilizados para comutar o tráfego de um

recurso, que pode ser uma fibra ou um lambda, primário para um recurso secundário no caso da falha do primário. Esta operação deve ser efetuada em um tempo total de algumas dezenas de milissegundos, que deve incluir o tempo de detecção da falha, a comunicação da falha para os elementos apropriados da rede, o tempo de comutação e configuração destes elementos.

Existem outras aplicações para as portas de comutação óptica, tais como encaminhar pacotes ópticos ou até modular dados definindo os estados *on* e *off* na saída do laser. A comutação de pacotes ópticos necessita de portas que comutem na ordem de poucos nanossegundos para um funcionamento eficiente [5]. Já a modulação do laser necessita de tempo de comutação da ordem de picossegundos [5].

Além do tempo de comutação e ao número de portas necessárias, outros parâmetros são utilizados para caracterizar a adequação da porta ao tipo de aplicação em redes ópticas. Estes parâmetros são apresentados a seguir.

A fração de extinção *on-off* de uma porta é a razão entre a intensidade do sinal no estado *on* e a intensidade do sinal no estado *off*. Esta fração deve ser a maior possível e é importante para aplicações em moduladores. Outro parâmetro é a atenuação inserida por um comutador, que é definida como a fração de potência que é dissipada ou perdida pelo comutador, geralmente expressada em decibéis (dB).

A atenuação é uma característica indesejável porque aumenta a faixa dinâmica do nível do sinal na rede. Este parâmetro deve ser o menor possível, pois, como as conexões atravessam um número variável de portas dentro das matrizes de comutação, é necessária a introdução de atenuadores variáveis para equalizar a perda de potência entre estes diferentes caminhos dentro de comutador.

A diafonia (*crosstalk*) é outro parâmetro importante. Como uma porta comutadora não é um dispositivo ideal, um feixe de luz que é comutado da entrada x para a saída y pode interferir em outra saída diferente de y, ocasionando uma diminuição da relação sinal ruído.

A confiabilidade do comutador é um parâmetro muito utilizado em aplicações de telecomunicações. Este parâmetro mede o quanto o dispositivo segue as especificações de

funcionamento mesmo que em situações extremas, como reconfiguração de rotas. São testes pertinentes para medir este parâmetro, o teste de exaustividade, que força no comutador um número grande de vezes a execução de procedimentos de reconfiguração, e o teste de ociosidade, que efetua comandos de reconfiguração após um grande período de inatividade.

O *latching* é uma característica presente nos comutadores ópticos que permite que o comutador mantenha seu estado de configuração mesmo durante uma interrupção no fornecimento de energia, permitindo, assim, que o tráfego da rede que passa por este comutador não seja interrompido.

A perda dependente de polarização (*polarization-dependent loss* - PDL) é outra característica a ser considerada na especificação de um comutador óptico, ou de uma porta óptica. Este parâmetro define se um comutador atenua excessivamente uma polarização do laser. Porém, este efeito pode ser tolerado se o comutador óptico for utilizado como modulador, pois, se posicionado imediatamente após o dispositivo emissor de laser, permite que a polarização do laser seja controlada utilizando uma fibra óptica chamada fibra óptica preservadora de polarização (*polarization-preserving fiber*), que adequa a luz do laser ao modulador.

A Arquitetura de uma Matriz de Comutação Óptica

Usualmente, existe um compromisso entre estes diferentes aspectos de projeto e implementação de uma matriz comutadora. As principais arquiteturas para o desenvolvimento de matrizes de larga escala são apresentadas a seguir. A Tabela 2.2 compara as características dessas arquiteturas.

CrossBar

Uma matriz comutadora com a arquitetura *crossbar*4×4, com 4 entradas e 4 saídas, é apresentado na Figura 2.3. Esta matriz utiliza 16 portas comutadoras 2×2 e a conexão da entrada para a saída é obtida através da configuração apropriada destas portas.

Tabela 2.2: Comparação entre as diferentes arquiteturas de matrizes comutadoras.

Arquitetura	**Não-Bloq.**	**Núm. de Comut.**	**Perda Máx.**	**Perda Mín.**
CrossBar	Amplamente	n^2	$2n-1$	1
Clos	Estritamente	$4\sqrt{2n^{1,5}}$	$5\sqrt{2n}-5$	3
Spanke	Estritamente	$2n$	2	2
Benes	Rearranjável	$n/2(2\log_2 n-1)$	$(2\log_2 n-1)$	$(2\log_2 n-1)$
Spanke-Benés	Rearranjável	$n/2(n-1)$	n	$n/2$

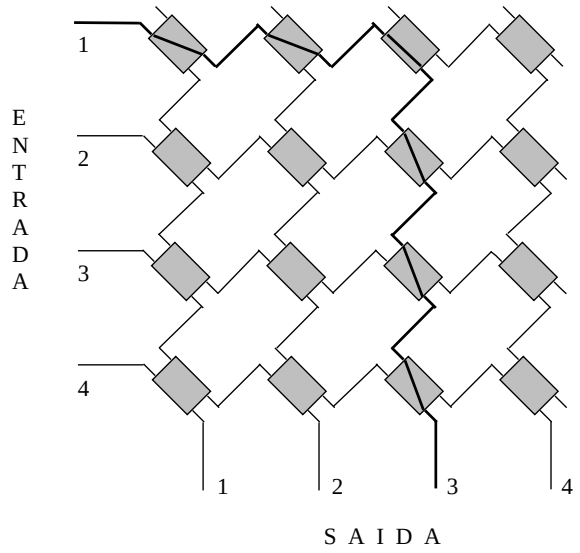


Figura 2.3: Uma matriz *Crossbar* 4x4 com 16 portas comutadoras 2x2.

Uma matriz comutadora em *crossbar* de $n \times n$ necessita de n^2 portas comutadoras de 2×2. A maior desvantagem desta arquitetura é a variação do tamanho do caminho, pois o menor caminho é 1 e o maior caminho é $2n-1$, tornando a perda de sinal, ou atenuação, através da matriz pouco uniforme. A principal vantagem é a ausência de cruzamentos de guias de onda na fabricação desta matriz e a característica de ser amplamente não-bloqueante.

Clos

A arquitetura *Clos* permite a fabricação de uma matriz comutadora estritamente não-bloqueante. A Figura 2.4 apresenta uma matriz *Clos* em três estágios de 1024 portas. A construção de uma matriz *Clos* $n \times n$ é baseada em três parâmetros de projeto, m, k e p. Primeiramente, faz-se $n = mk$. O primeiro estágio consiste em k portas comutadoras de $m \times p$. O estágio intermediário consiste em p portas comutadoras de $k \times k$. As p saídas de todos as portas comutadoras do primeiro estágio são ligadas às p portas do segundo estágio. De maneira análoga o terceiro estágio, composto de k portas comutadoras de $p \times m$, é ligado às saídas do segundo estágio. Nesta arquitetura, se a inequação $p \geq 2m-1$ for satisfeita, a matriz é estritamente não-bloqueante.

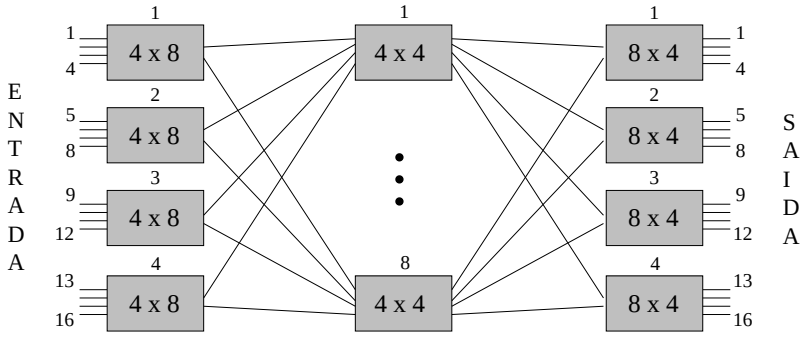


Figura 2.4: Uma matriz *Clos* 16x16 de três estágios com portas comutadoras de 4x4 e 4x8.

Esta arquitetura apresenta algumas vantagens que a torna adequada na implementação de matrizes de larga escala. A uniformidade da perda de sinal através da matriz entre uma entrada e uma saída e o número de portas comutadoras 2×2, que são necessárias para se obter os elementos de $m \times p$ e $k \times k$, são dois pontos favoráveis a esta arquitetura quando comparada com a *Crossbar*.

Spanke

A arquitetura *Spanke*, apresentada na Figura 2.5, é apontada como uma solução bastante comum hoje em dia utilizada nos projetos de matrizes comutadoras. Nesta arquitetura, uma matriz $n \times n$ é composta de $2n$ portas de comutação $1 \times n$. Esta arquitetura é

estritamente não-bloqueante e utiliza um outro paradigma para reduzir o custo de fabricação. Diferentemente das outras arquiteturas de matrizes comutadoras, esta arquitetura não busca diminuir o número de portas comutadoras 2×2. O que faz a arquitetura *Spanke* mais atrativa é a utilização de portas comutadoras $1 \times n$ que podem ser fabricados a partir de uma única porta e não é resultado da combinação de portas 1×2 ou 2×2, como as outras arquiteturas. Este é o caso da tecnologia de direcionamento de feixe de luz através de espelhos MEMS. Portanto, somente $2n$ portas destas são necessárias. Isto implica um custo que cresce linearmente com n, que é uma vantagem frente a outras arquiteturas de matrizes. Além do mais, cada conexão estabelecida passa por somente 2 elementos de comutação, o que apresenta vantagens em relação à uniformidade da perda de sinal e em relação à atenuação do sinal da porta de entrada à porta de saída.

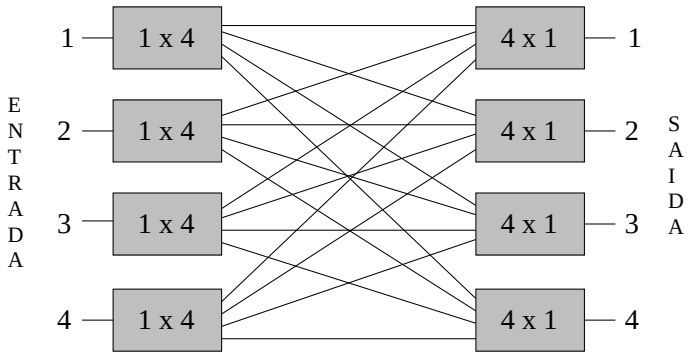


Figura 2.5: Uma matriz *Spanke* 4x4 com 8 portas comutadores 1x4.

Benes

A arquitetura *Benes* é não-bloqueante rearranjável e a mais eficiente em termos do número de portas comutadoras 2×2 necessárias para fabricação de matrizes comutadoras de larga escala. Uma arquitetura *Benes* 8×8 rearranjável, que usa somente 20 portas 2×2, é apresentada na Figura 2.6. Em comparação com uma arquitetura *Crossbar*, que necessita de 64 destas portas, *Benes* apresenta um ótimo resultado. Generalizando, esta arquitetura precisa de $(n/2)(2\log_2 n - 1)$ portas 2×2. A perda de sinal é a mesma através da matriz, independentemente do par de entrada e saída. As suas duas principais desvantagens são a sua não-bloqueabilidade que não é amplamente garantida e a quantidade de cruzamentos de guias de ondas (*waveguides crossovers*) que são requisitos de projeto, tornando a

integração óptica mais difícil de implementar.

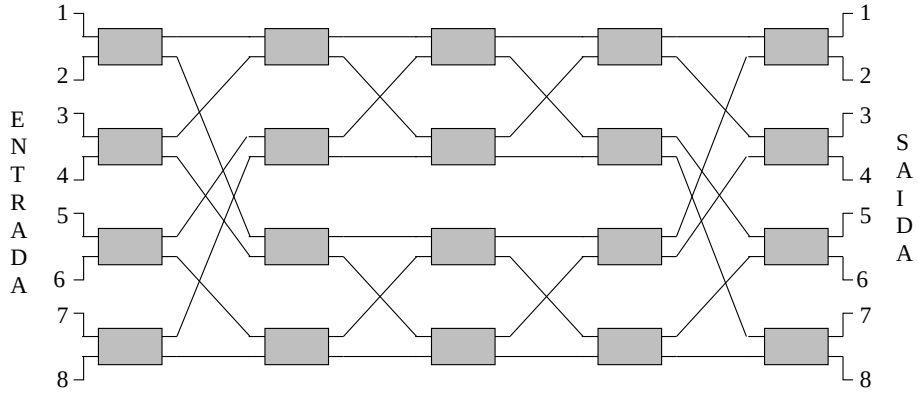


Figura 2.6: Uma matriz *Benes* 8x8 com 20 portas comutadoras 2x2.

Spanke-Benes

Uma boa relação de compromisso entre a arquitetura *Crossbar* e a *Benes* é apresentada na Figura 2.7, que é não-bloqueante rearranjável utiliza 28 portas 2×2 e não apresenta cruzamentos *crossover*. Esta arquitetura foi descoberta por Spanke e Benes e é chamada de arquitetura planar de n estágios, pois uma matriz de $n \times n$ necessita de n estágios, ou colunas. Ele necessita de $n(n-1)/2$ portas, o caminho mais curto é $n/2$ e o caminho mais longo é n. As suas desvantagens são a característica de não-bloqueabilidade e a não-uniformidade da perda do sinal.

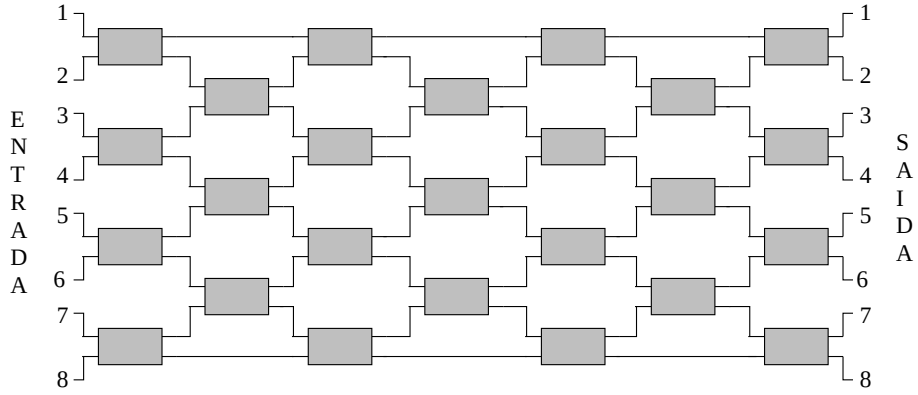


Figura 2.7: Uma matriz *Spanke-Benes* 8x8 com 28 portas comutadoras 2x2.

Tecnologias de Comutação Óptica

Atualmente, existem muitos tipos de tecnologias de comutação utilizadas na implementação de matrizes de comutação óptica. A Tabela 2.3 compara estas diferentes tecnologias, utilizadas para a fabricação de portas que são os principais componentes das matrizes de comutação óptica. Com exceção da tecnologia de comutação MEMS 3D, todas as tecnologias de portas descritas a seguir são aplicadas para uma arquitetura *Crossbar*.

Tabela 2.3: Comparação entre as diferentes tecnologias de fabricação de elementos comutadores.

Tecnologia	**Núm. de Portas** por Matriz	**Perda** (dB)	***C*rosstalk** (dB)	**PDL** (dB)	**Tempo de Comutação**
Mecânica	8×8	3	55	0,2	10 ms
MEMS 2D	32×32	5	55	0,2	10 ms
MEMS 3D	1000×1000	5	55	0,5	10 ms
Bolha	32×32	7,5	50	0,3	10 ms
Cristal Líquido	2×2	1	35	0,1	4 ms
Eletro-Óptico	4×4	8	35	1	10 ps
Termo-Óptico	8×8	8	40	baixo	3 ms
SOA	4×4	0	40	baixo	1 ns

Mecânica

Portas ópticas de tecnologia mecânica utilizam o posicionamento de espelhos para estabelecer seus canais ópticos. Através de alterações no posicionamento, que geralmente são alterações rotacionais, o espelho intercepta o laser que emergiu da fibra, alterando sua direção para a porta de saída desejada. Estes espelhos são chamados de espelhos de dois estados e, conseqüentemente, estão associados a somente uma saída, pois ou redirecionam o laser para a porta ou não modificam o curso do laser. No estado desativado a direção do laser não é alterada pelo espelho em questão, o que significa que a matriz de comutação

óptica alterará a direção do laser em espelhos posteriores. No estado ativo, o espelho é posicionado na frente do laser refletindo-o para a porta referente a este espelho, como apresentado pela Figura 2.8.

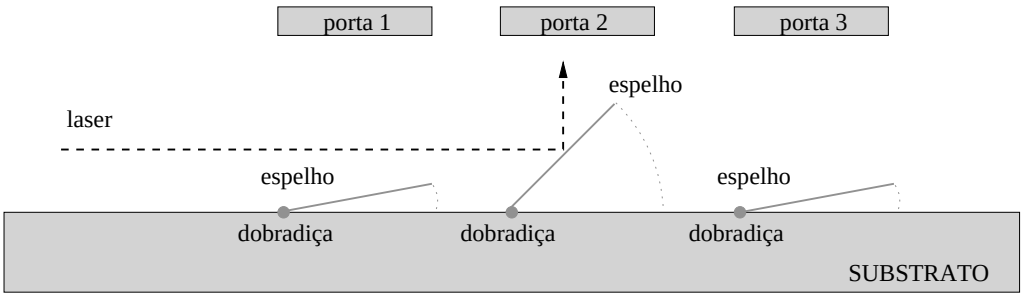


Figura 2.8: Um espelho de dois estados na posição ativa alterando a direção do laser.

As portas comutadoras mecânicas apresentam baixa atenuação, baixo PDL, baixa interferência cruzada e custo de fabricação relativamente barato quando comparadas com outras tecnologias. Como são utilizadas em uma arquitetura *Crossbar*, as matrizes que utilizam esta tecnologia apresentam baixa uniformidade de perda de sinal. Seu tempo de comutação é da ordem de poucos milissegundos e o número de portas é entre 8 e 16 portas. Como a maioria dos dispositivos mecânicos, apresenta deficiências em relação a confiabilidade e durabilidade, devido a desgastes físicos/mecânicos, mas apesar disto é a tecnologia mais economicamente viável e madura até o momento. Podem ser cascateados para atingir um maior número de portas, porém existem outras soluções como as MEMS.

MEMS

Os sistemas micro-eletro-mecânicos (*Micro-Eletro-Mechanical System* - MEMS) são dispositivos mecânicos miniaturizados, geralmente projetados usando substrato de silício, que em aplicações de matrizes de comutação óptica são mini-espelhos móveis com dimensões variando de micrometros a milímetros. Uma única placa de silício pode conter um grande número destes espelhos, o que possibilita a fabricação de matrizes com um maior número de portas de entrada e saída. Além disso, estes espelhos são fabricados utilizando procedimentos conhecidos e tecnologias já amadurecidas de semicondutores, reduzindo seu custo. Estes espelhos podem ser defletidos de uma posição para outra uti-

lizando diversas técnicas eletrônicas, tais como métodos eletromagnéticos, eletrostáticos ou pizoelétricos, por isso a denominação MEMS.

O modelo de espelho mais simples é o espelho de dois estados, como já comentado e apresentado na Figura 2.8. Este tipo de espelho, que é organizado em *Crossbar*, é fácil de controlar digitalmente pois permite somente duas posições: ativada, que reflete o laser para a porta de saída associada, e desativada, que não reflete o laser. Esta tecnologia é denominada MEMS 2D, devido a sua característica bidimensional.

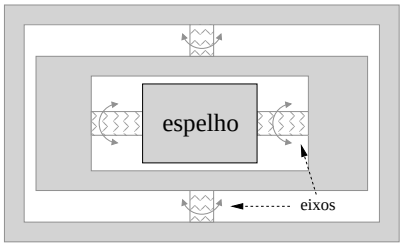


Figura 2.9: Um espelho direcionador analógico de feixe que é rotacionado livremente nos dois eixos.

Outro tipo de estrutura de controle do espelho refletor é apresentada na Figura 2.9. Nesta estrutura o espelho é posto em um quadro que apresenta um grau de liberdade rotacional no eixo horizontal. Este, por sua vez, é posto em um outro quadro que apresenta um grau de liberdade rotacional no eixo vertical. Com a combinação da rotação horizontal, da rotação vertical e de um controle analógico de posicionamento, o espelho pode apontar para qualquer direção, diferentemente do porta comutadora 2D. Este espelho é denominado espelho direcionador analógico de feixe, ou espelho 3D. Vale notar que o controle deste tipo de espelho não é trivial e requisita sofisticados servo-mecanismos para defletir o espelho e mantê-lo na posição desejada.

No projeto de matrizes comutadora que utilizam a tecnologia MEMS 3D é comum a utilização da arquitetura *Spanke*, discutida na Seção 2.2.6. Cada espelho está associado a uma fibra, ou lambda, de entrada. Através de uma lente acopladora, o laser da fibra é direcionado para o espelho, que reflete o laser para outro conjunto de espelhos. Este segundo conjunto de espelhos reflete o feixe para outra lente que acopla/adapta o laser de volta para a porta de saída, que corresponde a uma fibra, ou lambda. Portanto, para

conectar a porta i à porta j, basta alinhar o espelho i em direção ao espelho j e vice-versa. Note que o feixe de laser desta conexão pode cruzar com outros feixes, porém não ocasionará interferência cruzada.

Entre as diversas tecnologias apresentadas nesta seção, os dispositivos direcionadores analógicos MEMS 3D oferecem as melhores condições para a fabricação de matrizes de larga escala. Estas portas comutadoras são compactas, têm boas características ópticas e têm o menor consumo de energia. Outra vantagem é o maior número de portas de entrada e saída que a tecnologia permite. Atualmente, utilizando portas MEMS 3D conseguir dispositivos com 256 a 1000 portas de entrada e saída é comercialmente viável.

Guia de Onda Baseada em Bolhas

Outra tecnologia bastante promissora utiliza uma abordagem com guias de ondas em uma topologia planar, onde o elemento atuante, ou seja, o elemento responsável pela reflexão do feixe de laser, é baseado em uma tecnologia similar à utilizada pelas impressoras jato de tinta. A Figura 2.10 apresenta a matriz de comutação óptica. A matriz consiste em guias de onda que se cruzam. Na interseção destas guias de onda existe um líquido que apresenta o mesmo índice de refração que as guias de onda. Sob condições normais, o laser atravessa as interseções sem ser desviado da guia de onda em questão. Contudo, se o líquido presente nas interseções for aquecido, uma bolha de ar é formada. Esta bolha de ar quebra a continuidade do índice de refração, o que faz com que o laser seja refletido para a guia de onda que atravessa. A figura apresenta uma matriz 2×2 e, utilizando esta abordagem, é possível fabricar uma matriz de 32×32 em um mesmo substrato plano. Esta tecnologia promete matrizes comutadoras de custo relativamente baixo, de fácil implementação, de dimensões reduzidas com tempo de comutação da ordem de dezenas de milissegundos.

Cristal Líquido

A tecnologia de cristal líquido também é outra alternativa eficiente para fabricação de matrizes de comutação óptica. Aplicando uma voltagem em uma célula de cristal líquido

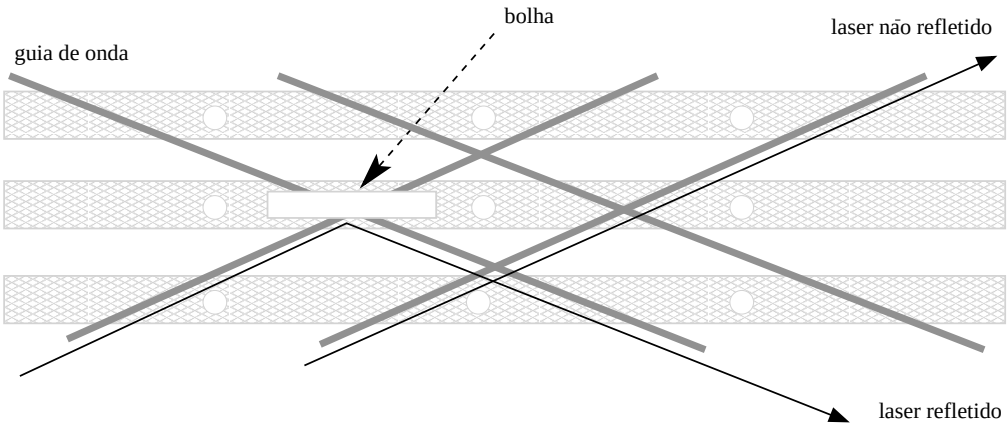


Figura 2.10: Uma matriz de comutação óptica de guia de onda baseado em bolha.

é possível polarizar o laser que passa pela célula. Esta característica pode ser combinada com separadores passivos de polarização resultando em uma matriz independente da polarização. O tempo de comutação de um dispositivo deste é da ordem de dezenas de milissegundos. Como a tecnologia de guia de onda baseada em bolha, a matriz de cristal líquido pode ser fabricada em grande quantidade e a um baixo custo.

Eletro-Óptico, Termo-Óptico e SOA

Outra tecnologia ainda em amadurecimento é a utilização do niobato de lítio ($LiNbO_3$), muito comumente encontrado em moduladores externos eletro-ópticos. Apesar de ser capaz de mudar de estado muito rapidamente, tipicamente em menos de 1 picossegundo, a perda de sinal, a perda dependente da polarização (PDL) e o custo são grandes desvantagens desta tecnologia. Por esta razão, esta tecnologia ainda tem um longo caminho antes de se consolidar como tecnologia de comutação óptica.

As matrizes de comutação óptica termo-ópticos são interferômetros 2×2 construídos em um material de guia de onda que tem um índice de refração variável em função da temperatura. Estes dispositivos já foram construídos em substratos de silício e de polímero, mas apresentam grande interferência cruzada. Além disso, o efeito termo-óptico é relativamente lento, o que torna o tempo de comutação da ordem de milissegundos, o que não o torna vantajoso comercialmente ante as outras tecnologias.

Os amplificadores ópticos de semicondutores (*Semiconductor Optical Amplifier* - SOA) podem ser utilizados como portas comutadoras *on-off* variando-se a tensão aplicada. Quando a tensão é reduzida, não existe população reversa de elétrons e o dispositivo absorve o sinal de entrada. Quando a tensão é suficiente, o dispositivo amplifica o sinal na saída. Esta combinação de amplificação no estado *on* e a absorção no estado *off* permite que esta tecnologia alcance uma alta fração de extinção *on-off*. Este dispositivo pode atingir tempo de comutação da ordem de 1 nanossegundo. Apesar da fabricação de grandes matrizes comutadoras ser possível, esta tecnologia ainda não é comercialmente viável, pois este dispositivo apresenta elevado custo e é difícil torná-lo independente da polarização do laser.

2.3 As Redes Ópticas WDM

Uma rede WDM encaminha as mensagens da origem até o destino baseada no lambda associado ao canal óptico. Este paradigma de encaminhamento de mensagens em redes ópticas é também conhecido como Roteamento de Comprimento de Onda (*Wavelength Routing* - WR), utilizado nas redes WRON (*Wavelength Routing Optical Network*).

Para transportar os dados é necessário que antes seja estabelecida uma conexão na camada óptica, o canal óptico. Esta conexão define os enlaces da rede e os respectivos lambdas. Após seu estabelecimento, a banda passante do canal óptico fica totalmente disponível para a conexão, até que seja efetuada sua finalização, ou desconexão. O estabelecimento deste canal óptico consiste primeiramente na escolha dos enlaces. Este procedimento pode ser realizado através de qualquer protocolo de roteamento. Em seguida é necessário escolher os lambdas que serão utilizados em cada enlace do canal. Existem diversos algoritmos de escolha de lambda [54], mas visando manter o foco principal deste trabalho, este aspecto das redes WDM não foi abordado. A combinação destes dois procedimentos é denominada Roteamento e Associação de Lambda (*Routing and Wavelength Assignment* - RWA) [55, 56]. O roteamento e a associação de lambdas podem ocorrer simultaneamente e não serem seqüencialmente. Neste caso o roteamento poderia utilizar a disponibilidade dos comprimentos de onda das fibras ópticas [57].

Uma rede WDM transparente, que apresenta conversão total de lambda em todos os seus nós, realiza o encaminhamento de pacotes e o estabelecimento de conexões de maneira semelhante às redes convencionais de comutação de circuito de telefonia, por exemplo, sem a restrição de continuidade de lambda.

2.4 A Arquitetura IP/GMPLS-sobre-WDM

O modelo de interconexão de redes ópticas IP/GMPLS (*Generalized Multiprotocol Label Switching*)-sobre-WDM (*Wavelength Division Multiplexing*), apontado por Vassour *et al.* [4] e Maesschalk *et al.* [3], dentre outros, é mais adequado a às necessidades atuais de banda passante e dinâmica na conexão e desconexão. Neste novo paradigma de redes ópticas, a camada óptica utiliza a topologia física da rede para estabelecer canais de transmissão totalmente ópticos. O grafo da topologia física consiste em comutadores ópticos como vértices e em enlaces ópticos como arestas. O estabelecimento destas conexões ópticas gera uma topologia virtual da rede para a camada IP/GMPLS. O grafo da topologia virtual consiste em roteadores IP/GMPLS como vértices e em canais ópticos como enlaces. Esta camada, por sua vez, utiliza a topologia virtual para estabelecer os LSP (*Label Switched Path*), como a Figura 2.11 ilustra.

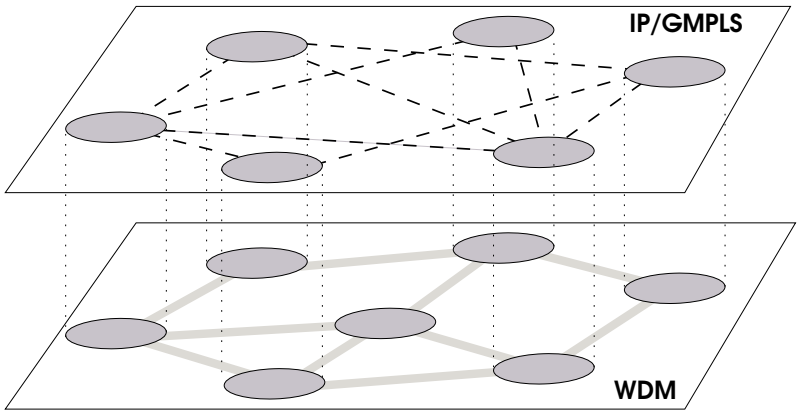


Figura 2.11: Topologia Física e Virtual

A introdução do GMPLS nesta arquitetura proporcionou aos operadores da rede uma maior dinâmica no estabelecimento e encerramento de conexão. O tempo reduzido de

estabelecimento de uma conexão, comparado com as tecnologias de redes ópticas anteriores, permite a computação, a sinalização e o estabelecimento de canais ópticos sob demanda. Com base nisto, diversos trabalhos estão utilizando o arcabouço GMPLS para justificar um mecanismo de sobrevivência que utilize os recursos da rede de maneira mais eficiente. Por outro lado, apesar deste período necessário para conectar um canal óptico entre dois nós da rede ter reduzido, o tempo de recuperação das redes SONET, da ordem de 50 ms, ainda está longe de ser alcançado.

O Plano de Controle GMPLS

Xin *et al.* [58] apresentam uma visão geral da arquitetura IP/GMPLS-sobre-WDM e seu plano de controle, que é composto de um módulo principal (MM - *Main Module*), módulos de gerência de recursos (RMM - *Resource Management Module*), módulo de conexão (CM - *Connection Module*) e módulos de proteção e restauração (PRM - *Protection and Restorarion Module*). O módulo RMM é utilizado para roteamento e alocação de lambda (RWA - *Rounting and Wavelength Assignment*), descoberta de topologia e de recursos e suporte a qualidade de serviço. O módulo CM é usado para sinalização e manutenção de conexões. Em redes GMPLS os protocolos CR-LDP ou RSVP-TE podem ser utilizados. Considerando a grande importância que a sobrevivência a falhas requisita cada vez mais, o módulo PRM tem por objetivo garantir a tolerância a falhas destas redes. O objetivo do módulo MM é receber as mensagens para o nó e, trabalhando em conjunto com os outros módulos, processar as requisições. Com estes módulos, uma rede WDM que apresente estes módulos de controle pode ser extendida para um conceito de tecnologia de camadas de redes que oferece inteligência necessária para que esta rede óptica se torne flexível, escalável e resiliente.

Como este trabalho é focado no módulo de proteção e restauração, este módulo é mais extensamente abordado a seguir. No momento que uma requisição de conexão é recebida pelo módulo principal ela é transferida para o módulo PRM de proteção e restauração. Em seguida, o módulo PRM invoca o módulo RMM para processar os algoritmos de roteamento e alocação de lambda. Para cada rota, ou caminho, computado, uma mensagem de sinalização é construída e o módulo CM é invocado pelo PRM para sinalização e esta-

belecimento de canal óptico. Se o cliente requisitar proteção, o canal secundário também será requisitado neste instante. Neste momento, o PRM é responsável por lidar com as mensagens assíncronas (como ACKs e NACKs). Caso ambos os canais primário e secundário sejam estabelecidos com sucesso, o módulo CM envia uma mensagem de sucesso no estabelecimento da conexão. Caso contrário, o módulo CM envia uma mensagem de falha no estabelecimento de conexões. O PRM também é responsável por detectar falhas e iniciar procedimentos de proteção e restauração de falhas. Após a detecção da falha, que pode ser detectada através de diversos mecanismos, o nó envia em difusão um FIS (*Failure Information Signal*) até que todos os nós que utilizem o recurso falho sejam alcançados. Ao receber o FIS, o nó afetado verifica os atributos de qualidade de serviço daquela conexão óptica e aciona o seu canal secundário, se for o caso.

No Capítulo 3, a recuperação em redes WDM é abordada mais detalhadamente. As vantagens e desvantagens da escolha de proteção ou de restauração são apresentadas. Também são discutidas as características da camada óptica e da camada IP que mais se adequam a cada mecanismo de sobrevivência, seja este de proteção ou de restauração.

Capítulo 3

Sobrevivência a Falhas

MUITOS dos serviços que funcionam 24 horas por dia não permitem longos períodos de manutenção ou reconfiguração da rede. Neste contexto, a falha de um enlace óptico pode causar a interrupção de dezenas de canais ópticos e isto pode significar a perda de uma enorme quantidade de dados e a insatisfação de milhares de usuários. Em média, a quebra de fibras ópticas ocorre entre 4 e 7 vezes ao ano por cada 1600 km de extensão e o tempo médio de recuperação destas falhas é de 12 horas [5, 17, 59]. Portanto, as redes ópticas transparentes precisam implementar mecanismos de recuperação para garantir que falhas de fibras ópticas ou equipamentos sejam recuperadas de maneira rápida e eficiente, atingindo, assim, uma disponibilidade de até 99,999% [5, 43], que é requisitada por aplicações mais exigentes. Esta capacidade da rede de permanecer operacional, mesmo quando ocorre uma falha de algum componente da rede, é conhecida como sobrevivência a falhas.

Neste capítulo, diversas abordagens de implementação de sobrevivência a falhas em redes ópticas são apresentadas e as vantagens e desvantagens de cada uma são analisadas. Também é justificada a escolha da camada óptica usada nesta tese para implementação da sobrevivência. Além disso, o conceito de conectividade da rede e de reversibilidade dos mecanismos de proteção são apresentados. As vantagens e desvantagens da implementação de uma rede de maior conectividade e os possíveis impactos positivos e negativos da implementação de mecanismos não-reversíveis também são discutidos.

3.1 Parâmetros de Desempenho das Redes Ópticas

Com o desenvolvimento das técnicas de operação e gerenciamento de redes ópticas transparentes, as pesquisas tendem a abordar o problema de desempenho das redes pela perspectiva da oferta de serviço [19, 43]. Assim, o foco das pesquisas passa a ser a oferta de Qualidade de Serviço (QoS) e, como conseqüência, a definição do contrato de nível de serviço (*Service Level Agreement* - SLA) a ser assinado com o cliente e garantido pela operadora. Portanto, a definição dos parâmetros de qualidade de serviço e a especificação dos seus valores são fundamentais. Esta seção introduz alguns dos principais parâmetros de desempenho das redes ópticas transparentes que são utilizados neste trabalho.

Confiabilidade

A confiabilidade de uma conexão é a probabilidade de uma conexão operar ininterruptamente, ou seja sem falhas, por um período de tempo. A confiabilidade está associada ao tempo médio entre falhas (*Mean Time Between Failures* - MTBF) que o sistema apresenta.

Disponibilidade

A disponibilidade da conexão, ou simplesmente disponibilidade, é definida como a probabilidade da conexão estar operacional. Ao contrário da confiabilidade, a disponibilidade leva em conta o tempo que uma falha deixou a conexão inativa. Portanto, o tempo que se gasta em recuperar uma falha da conexão é levado em consideração. A confiabilidade está relacionada ao número de interrupções que sofre uma conexão em um período de tempo e a disponibilidade está também relacionada à percentagem de tempo que a conexão ficou interrompida. A disponibilidade pode ser computada analiticamente levando-se em conta o tempo médio entre falhas e a taxa de recuperação de falhas. É importante ressaltar que como o tempo de recuperação de falha de uma conexão é computado no cálculo da disponibilidade, a política de operação e o mecanismo de proteção de conexão utilizado passam a influir diretamente na disponibilidade. Zhang *et al.* [17, 60] apresentam um estudo analítico da disponibilidade de conexões em redes WDM em ma-

lha. A Figura 3.1 ilustra a disponibilidade de uma conexão, onde C é o início da conexão, D (desconexão) é o término da conexão, F é uma falha e R é a recuperação da falha. O intervalo hachurado representa o período de tempo que a conexão esteve indisponível.

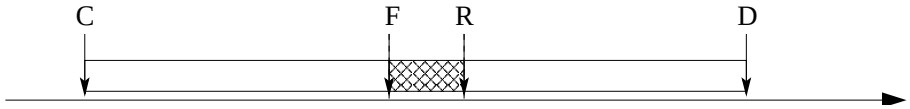


Figura 3.1: A disponibilidade de conexão. Eventos de conexão (C), de desconexão (D), de falha (F) e de recuperação (R).

Probabilidade de Bloqueio

A probabilidade de bloqueio de conexão é a probabilidade de um pedido de conexão não ser atendido por falta de recursos da rede. A probabilidade de bloqueio é um parâmetro que pode ser utilizado para medir a eficiência de utilização da rede. Embora a probabilidade de bloqueio seja uma métrica que geralmente não está presente nos contratos de SLA, ela é de grande interesse para as operadoras de redes uma vez que quanto menor a probabilidade de bloqueio maior é o número de clientes que podem ser atendidos com a mesma quantidade de recursos.

De uma forma simplificada, os usuários requerem contratos de nível de serviço com alta confiabilidade e, principalmente, com alta disponibilidade. Por sua vez, as operadoras para garantirem a alta disponibilidade procuram fornecer redundâncias e caminhos alternativos, ou secundários, que são usados durante as falhas que ocorrem nos caminhos primários. O fato de disponibilizar caminhos secundários implica a reserva de recursos adicionais e, conseqüentemente, o provimento simultâneo de um número menor de conexões e, portanto, uma menor eficiência da rede. Assim, o planejamento da sobrevivência da rede óptica deve levar em conta os recursos extras que são necessários para garantir disponibilidade de conexão ao mesmo tempo em que deve garantir uma alta eficiência da rede, de forma a minimizar a probabilidade de bloqueio de conexão. Logo, a sobrevivência deve levar em consideração o mecanismo de recuperação de falhas e a topologia da rede.

3.2 Sobrevivência em Redes IP-sobre-WDM

De acordo com Manie *et al.* em [61], Papadimitriou *et al.* em [62] e Lang*et al.* em [63], em redes ópticas em malha os mecanismos de sobrevivência a falhas são classificados, basicamente, em dois tipos: proteção e restauração. Os mecanismos de proteção pré-computam e pré-alocam os recursos de recuperação. A pré-alocação de recursos de proteção significa reservar recursos que serão utilizados apenas quando ocorrer uma falha. A reserva de recursos de proteção torna a rede menos eficiente e aumenta a probabilidade de bloqueio de conexão uma vez que os recursos reservados não podem ser utilizados para atender novos pedidos de conexão. Quando ocorre uma falha, as conexões são comutadas do canal primário para o canal secundário, ou de proteção. Já os mecanismos de restauração computam os recursos de recuperação de maneira reativa, ou seja, apenas quando ocorre uma falha. O canal óptico de recuperação será estabelecido somente quando a falha de um enlace afetar o canal primário. A alocação de recursos para recuperar a falha é feita apenas após a falha. Por isso, os mecanismos de restauração utilizam os recursos de maneira mais eficiente do que os mecanismos de proteção. Em contrapartida, apesar do uso ineficiente da rede, os mecanismos de proteção oferecem um tempo de recuperação menor que os mecanismos de restauração. O tempo de recuperação da restauração é maior, pois há a necessidade da reconfiguração da rede, da alocação dos recursos por caminhos alternativos e da comutação do canal primário para o canal de proteção, ou canal secundário. Esta tese aborda apenas os mecanismos de proteção e, como conseqüência, enfoca o estudo da pré-alocação dos recursos necessários para os caminhos alternativos ou secundários e seus efeitos.

A sobrevivência em redes IP-sobre-WDM pode ser implementada tanto na camada WDM quanto na camada IP. A proteção na camada WDM consiste em proteger cada canal óptico por um outro canal óptico, chamado de canal óptico de proteção. A proteção na camada IP, por sua vez, consiste em proteger cada caminho comutado por rótulo (*Label Switched Path* - LSP) por um outro LSP de proteção, ou secundário. A detecção de uma falha pela camada WDM é imediata e o procedimento de restauração se resume em comutar o canal óptico primário que falhou para o canal óptico de proteção. Por outro lado, a camada IP não tem acesso à camada física e isto dificulta a detecção de falhas. Como

o mecanismo de proteção IP não tem acesso aos sensores e receptores ópticos que detectam a interrupção da portadora óptica, é necessário enviar periodicamente mensagens de HELLO para detecção de falhas. Para diminuir o tempo de detecção de falhas de um mecanismo de proteção na camada IP, Zheng *et al.* [23] e Kodialam *et al.* [30] propuseram um mecanismo integrado, que permite que a camada WDM sinalize o evento de falha para a camada IP. Embora a sinalização da falha seja mais rápida, o processo de recuperação na camada IP envolve procedimentos de comutação dos LSPs primários para os LSPs de proteção e estes procedimentos podem acarretar uma grande sobrecarga computacional uma vez que um único canal óptico pode transportar até milhares de LSPs. Portanto, a proteção na camada WDM sempre proporciona um tempo de restauração menor que a proteção na camada IP.

A proteção na camada IP é mais flexível e pode resultar em uma maior eficiência da rede na utilização dos recursos. A granularidade de um LSP é diferente de um canal óptico e LSPs primários e de recuperação podem coexistir em um mesmo canal óptico, tornando a proteção nesta camada mais eficiente. A proteção na camada WDM requer um maior isolamento entre recursos primários e de proteção, pois quando um canal óptico de proteção é reservado, os enlaces que este canal ocupa não mais estarão disponíveis. Esta diferença de comportamento é ilustrada pelas Figuras 3.2 e 3.3.

O mecanismo de proteção na camada WDM pode ser aplicado em um enlace do canal óptico, em um segmento do canal óptico, que é conhecido como sub-canal, composto por um ou mais enlaces, ou no canal óptico composto de todos os enlaces da origem até o destino. Na proteção de canal, apresentada na Figura 3.4, um canal secundário com enlaces e nós totalmente disjuntos conecta a origem ao destino. O tráfego é redirecionado, na origem, para o canal secundário, logo que uma falha é detectada em um dos enlaces do canal primário. Deve ser observado que a informação de falha em um dos enlaces deve percorrer o canal até a origem para que a comutação do canal primário para o de proteção seja efetuada. A proteção de enlace, apresentada na Figura 3.5, é a que apresenta o menor tempo de recuperação uma vez que a detecção da falha é imediata. No entanto, é seguramente a mais ineficiente em termos de recursos, pois se serve de diversos enlaces (no mínimo dois) para proteger cada enlace do canal primário da rede. A proteção de sub-canal óptico, apresentada na Figura 3.6, possui alguns nós comuns no canal primário

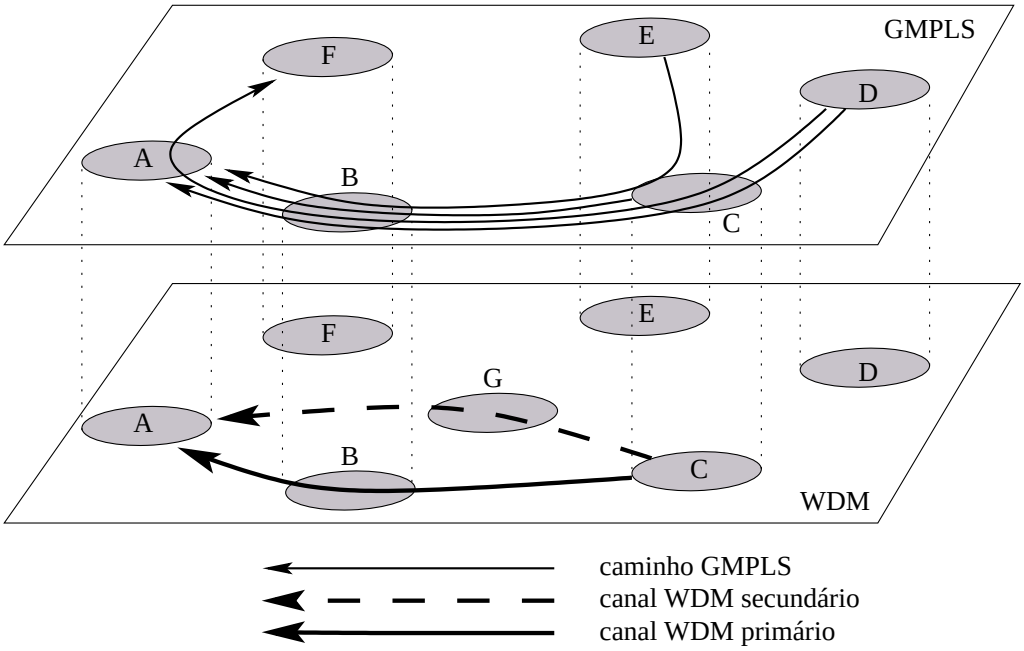


Figura 3.2: Proteção na camada WDM do canal óptico C-A: canal primário C-B-A e canal secundário C-G-A.

e no canal secundário. Há uma proteção por segmento do canal óptico sendo uma solução de compromisso em relação as duas proteções anteriormente descritas. Este tipo de proteção, apresentado por Ou *et al.* [27] e Zang *et al.* [28], proporciona tempos de restauração menores que a proteção de canal, pois a sinalização da falha não necessita percorrer todo o canal óptico para iniciar os procedimentos de recuperação. Em contrapartida, este mecanismo é menos eficiente que a proteção de canal no que se refere a utilização de recursos. Independente da camada em que o mecanismo de proteção é implementado, o conceito de segmentação de canal é válido, portanto a segmentação pode ser implementada tanto na camada WDM quanto na camada IP/GMPLS. Assim, um mecanismo de proteção na camada IP/GMPLS também pode ter seus caminhos segmentados de maneira semelhante.

Atualmente, a maioria das redes ópticas atuais é do tipo SONET, que utiliza anéis ópticos que reservam uma segunda fibra para proteção. Quando ocorre uma falha no canal óptico, a comutação para a fibra de proteção se efetua de maneira simples e rápida. O tempo de recuperação de falhas nestas redes é da ordem de 50 ms. Para que as novas redes com tecnologia WDM possuam tempo de recuperação de falhas da ordem de grandeza que o das redes SONETs, os mecanismos de proteção devem ser na camada WDM por serem

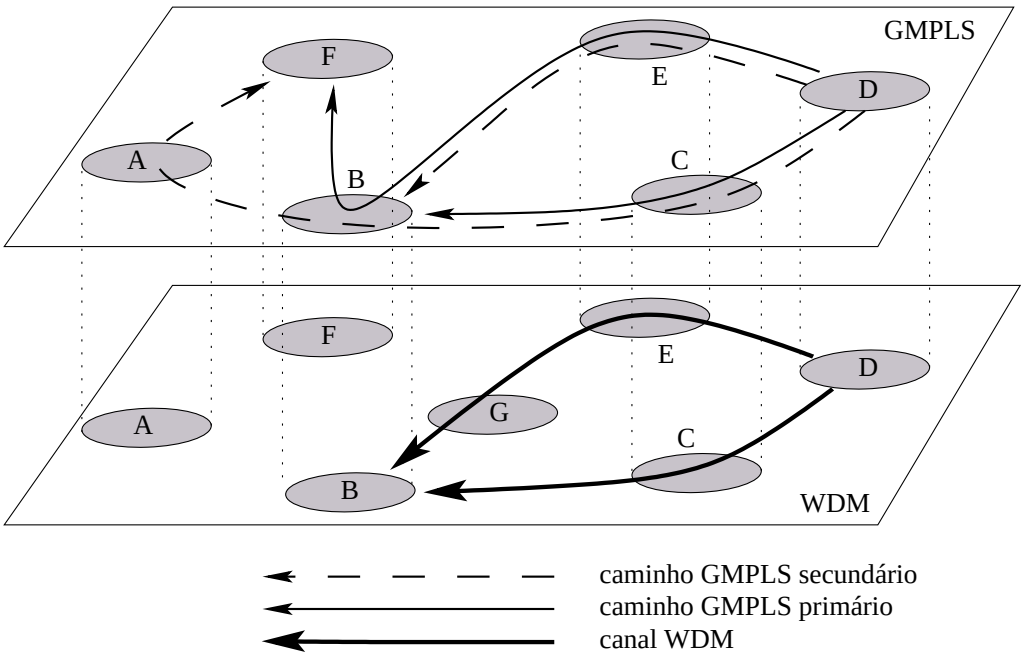


Figura 3.3: Proteção na camada IP dos caminhos D-B e D-F.

mais rápidos que os mecanismos de recuperação na camada IP. Por este motivo, esta tese visa estudar mecanismos de recuperação rápidos e, portanto, apenas os mecanismos de proteção na camada WDM são estudados.

3.2.1 A Proteção WDM 1:1 e 1:N

O mecanismo de proteção mais simples é a proteção `1:1`, também denominada nesta tese de dedicada. A proteção `1:1` estabelece dois canais ópticos disjuntos para cada conexão: um canal óptico primário e um canal óptico secundário ou de proteção. Assim, no momento em que há uma requisição de conexão, se um dos canais, o primário ou o de proteção, não puder ser estabelecido, ocorre um bloqueio de conexão e a conexão não é efetuada. Portanto, embora simples, o mecanismo de proteção `1:1` é ineficiente, pois reserva para proteção muitos recursos da rede ao duplicar os recursos necessários para uma conexão óptica. Conseqüentemente, a metade dos recursos da rede é reservada para proteção e isto acarreta uma probabilidade de bloqueio excessivamente alta.

Para aumentar a eficiência do uso dos recursos da rede, a proteção compartilhada, ou `1:N`, é uma alternativa mais eficiente à proteção `1:1`. Esta proteção permite que dois

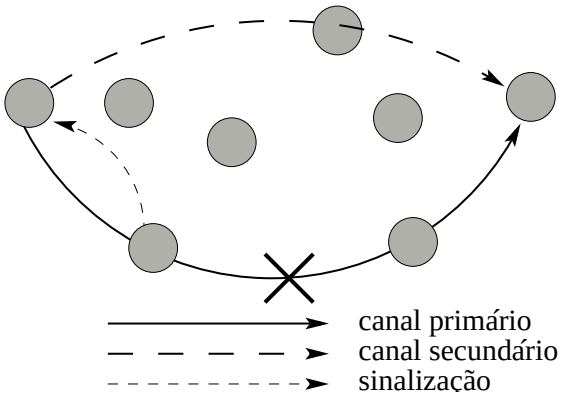


Figura 3.4: Proteção na camada WDM de canal óptico

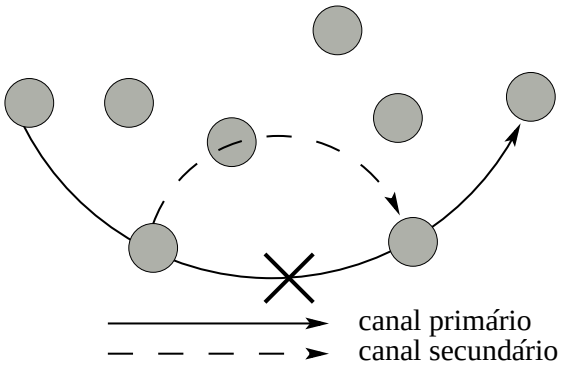


Figura 3.5: Proteção na camada WDM de enlace.

ou mais (N) canais de proteção compartilhem lambdas, desde que seus canais primários satisfaçam as restrições de grupo de risco de falha de enlace (*Shared Risk Link Group* - SRLG). A restrição SRLG define que canais de proteção podem compartilhar lambdas em um enlace se os canais primários de cada conexão não pertencerem ao mesmo grupo de risco de falha de enlace, e, portanto, a probabilidade de falharem simultaneamente é muito baixa. Em termos práticos, as conexões ópticas Ω e Ψ pertencem ao mesmo SRLG quando o conjunto dos enlaces primários de Ω, $L_\Omega = \{\omega_1, \omega_2, \omega_3\}$ e de Ψ, $L_\Psi = \{\psi_1, \psi_3, \psi_4\}$, apresentam pelo menos um enlace em comum. Na Figura 3.7 as linhas tracejadas e pontilhadas representam as conexões Ω e Ψ, respectivamente. Os conjuntos de grupos enlaces $L_\Omega = \{l_1, l_3, l_4\}$ e $L_\Psi = \{l_2, l_4\}$ têm em comum o enlace l_4, e, portanto, pertencem ao mesmo SRLG, não podendo compartilhar recursos de proteção. A utilização desta regra no compartilhamento de recursos aumenta a eficiência sem afetar, de maneira perceptível, a disponibilidade das conexões.

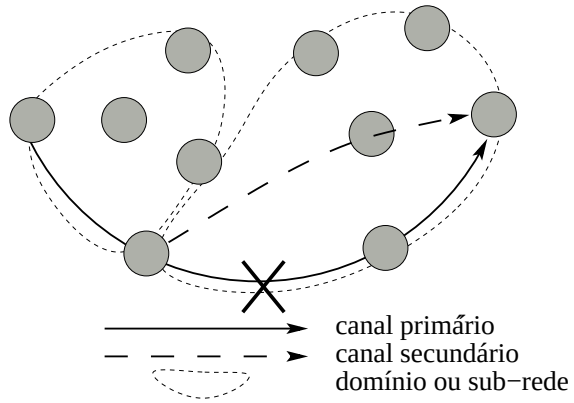


Figura 3.6: Proteção na camada WDM de sub-canal óptico.

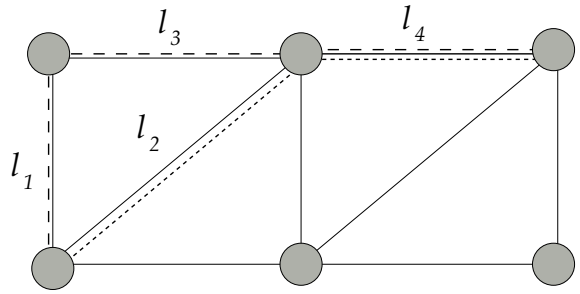
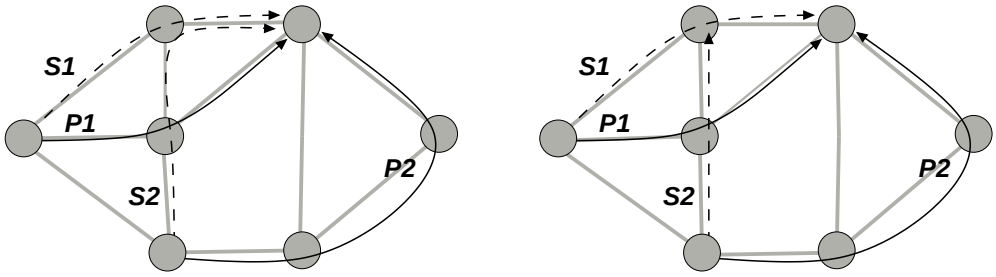


Figura 3.7: Grupo de risco de falha de enlace.

O funcionamento da proteção WDM dedicada `1:1` e compartilhada `1:N` é ilustrado na Figura 3.8(a) e 3.8(b). Através da figura, constata-se as diferenças no comportamento de cada mecanismo. A proteção `1:N` reaproveita os recursos do canal secundário $S2$ para o canal secundário $S1$. A proteção `1:1`, por sua vez, aloca "desnecessariamente" um novo lambda. Este comportamento da proteção `1:1` acarreta em uma alta probabilidade de bloqueio, pois o estabelecimento das futuras conexões será comprometido devido a menor quantidade de recursos disponíveis.

3.3 O Mecanismo Proposto

Apesar da proteção `1:N` apresentar melhor desempenho que a proteção `1:1`, um relaxamento dos critérios verificados no estabelecimento de conexões pode acarretar em uma maior eficiência e, conseqüentemente, em uma menor probabilidade de bloqueio de



(a) Proteção 1:1 ou dedicada.

(b) Proteção 1:N ou compartilhada.

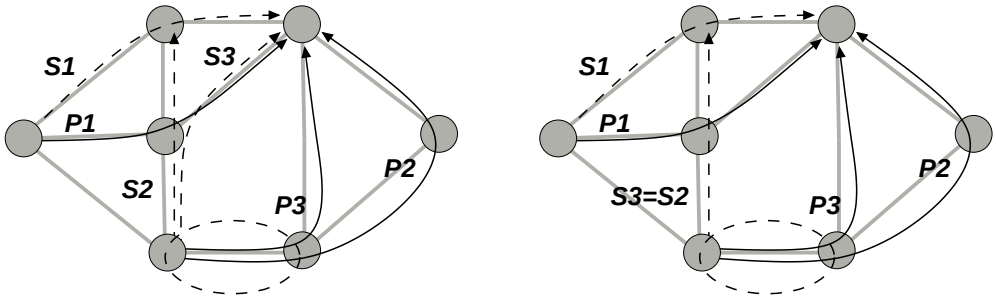
Figura 3.8: Mecanismos de proteção na camada WDM.

conexões.

O mecanismo proposto, chamado mecanismo compartilhado com relaxação de risco, foi desenvolvido para reduzir a probabilidade de bloqueio. Esta redução é obtida aumentando a possibilidade de compartilhamento entre os canais de proteção. Assim, propõe-se um relaxamento das regras que permite o compartilhamento ao permitir que uma determinada percentagem, α, de enlaces que pertençam a um mesmo grupo de risco sejam compartilhados. Portanto, para satisfazer as necessidades do novo mecanismo, as regras de restrição SRLG (grupo de risco de enlaces) são modificadas tornando-se mais permissivas. Com esta nova regra, os canais de proteção podem compartilhar recursos de proteção entre si mesmo que tenham enlaces primários em comum, desde que o número destes enlaces em comum seja menor que uma determinada percentagem. Esta percentagem é denominada de fator de relaxação de risco. O operador da rede determina o parâmetro de desempenho da rede que é favorecido através do fator de relaxação de risco. Se a disponibilidade for prioritária, o fator de relaxação de risco deve ser mínimo. No caso limite, com este fator zerado, o desempenho do mecanismo proposto é igual ao do mecanismo SRLG. Se a probabilidade de bloqueio for prioritária, o fator de relaxação de risco deve ser alto podendo atingir seu valor máximo igual a 1. As modificações implementadas no mecanismo de proteção `1:N` acarretam no detrimento da disponibilidade, e portanto, é necessário ponderar o compromisso entre a probabilidade de bloqueio e a disponibilidade das conexões.

O fator de relaxação de risco representa uma relação entre os canais primários de duas conexões ópticas e apresenta um comportamento bidirecional. Na Figura 3.9(b),

o fator de relaxação de risco do canal primário $P2$ em relação a $P3$ é $0,33$, pois $P2$ utiliza três enlaces primários e tem um enlace em comum com o canal $P3$, enquanto o fator de relaxação de risco de $P3$ para $P2$ é de 0,50, pois o canal $P3$ utiliza somente dois enlaces da rede. Como o fator de relaxação de risco também busca um critério de decisão de compartilhamento que não implique em injustiças, este índice apresenta um comportamento bidirecional. Desta maneira o fator de maior valor é utilizado, não permitindo, assim, que uma conexão com muitos saltos seja favorecida em detrimento de uma conexão com poucos saltos.



(a) Proteção compartilhada.

(b) Proteção compartilhada com relaxação de risco

Figura 3.9: Mecanismos de proteção na camada WDM.

A Figura 3.9 ilustra como o mecanismo proposto, a proteção compartilhada com relaxação de risco, se diferencia do mecanismo `1:N` SRLG. O funcionamento da proteção SRLG é apresentado na Figura 3.9(a). As conexões ópticas dos canais primários $P2$ e $P3$ não compartilhariam o canal secundário $S2$ se a proteção `1:N` SRLG estiver implementada, pois estas conexões compartilham um enlace primário. Visando um maior compartilhamento na rede, o mecanismo proposto, apresentado na Figura 3.9(b), configurado com um fator de relaxação de risco de 0,33, permite que a conexão 2 compartilhe o canal secundário $S2$ com a conexão 3. Desta maneira, os recursos alocados diminuem e, conseqüentemente, a probabilidade de bloqueio de conexões. A contrapartida deste mecanismo é a menor disponibilidade das conexões, pois o canal secundário pode estar indisponível para uma das conexões, se o enlace compartilhado entre os canais primários $P2$ ou $P3$ for interrompido.

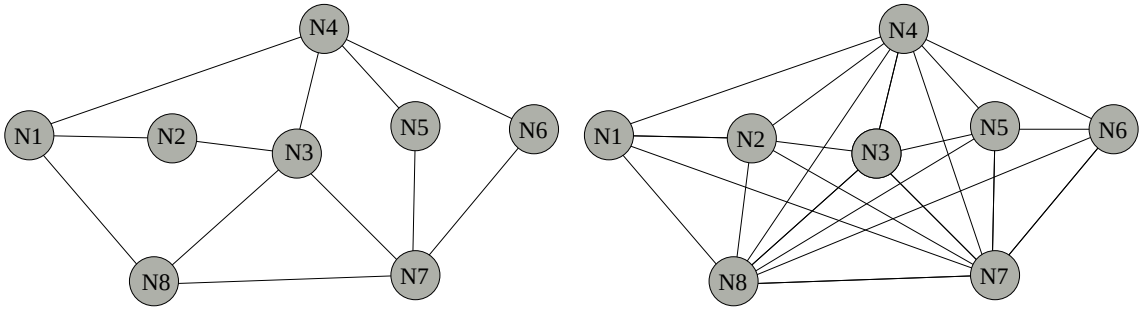
A probabilidade de bloqueio é um parâmetro que representa a eficiência de utilização

dos recursos da rede. Como já dito anteriormente, um mecanismo de sobrevivência ineficiente acarreta em uma rede com alta probabilidade de bloqueio. Por outro lado, buscar maior eficiência da rede aumentando o compartilhamento de recursos de proteção entre conexões acarreta em perda na disponibilidade das conexões. Este compromisso entre a disponibilidade e a probabilidade de bloqueio, quando o compartilhamento de recursos da rede é intensificado, é muito estudado, mas até o presente momento nunca foi quantificado. Com a utilização do mecanismo proposto, adiciona-se a esta análise de desempenho uma nova variável, o fator de relaxação de risco. Variando este fator é possível verificar o impacto na disponibilidade de conexões e na probabilidade de bloqueio. Esta quantização da perda na disponibilidade e do ganho na eficiência, ou vice-versa, é muito importante para adequar a rede aos requisitos de projeto. Estes requisitos têm origem na combinação das necessidades de QoS do cliente com os interesses econômicos do operador da rede, como previsão de custo e manutenção da rede.

3.4 A Conectividade da Rede

O desempenho das redes ópticas transparentes não depende exclusivamente do comportamento do mecanismo de sobrevivência implementado. Algumas características da rede também afetam o seu desempenho. Duas destas características são a topologia da rede óptica, mais especificamente a conectividade de seus nós, e a demanda de tráfego. A demanda de tráfego não está sob o controle direto do operador da rede, e, portanto, não é abordada neste trabalho. Em vista disso, um estudo sobre o impacto da conectividade da rede será realizado, visando determinar o impacto nos parâmetros de desempenho da rede.

A análise do impacto da conectividade no desempenho da rede é essencial para avaliar a implementação de mecanismos de sobrevivência a falhas. A maioria dos trabalhos de sobrevivência a falhas apresenta soluções para topologias de redes pré-existentes. Estas análises supõem uma topologia com um grau de conectividade da rede previamente definido, o que não apresenta valia para uma rede ainda em fase de planejamento e de projeto. Para auxiliar o planejamento e o projeto das redes ópticas transparentes é necessário ana-



(a) Rede de conectividade 3. (b) Rede de maior conectividade $5,5$.

Figura 3.10: Topologia e conectividade da rede.

lisar o impacto da conectividade da rede na eficiência dos mecanismos de sobrevivência a falhas.

A conectividade da rede, também chamada de grau de conectividade, é definida como $2m/n$, onde m é o número de enlaces da rede e n é o número de nós. As Figuras 3.10(a) e 3.10(b) apresentam uma rede com conectividade $24/8 = 3$ e uma rede com conectividade $44/8 = 5,5$, respectivamente. Como pode ser verificado na Figura 3.10, uma rede de maior conectivadade, ou seja, que apresente maior conectividade entre seus nós, possibilita uma maior variedade de rotas e rotas com um menor número de saltos. Assim, a rede de maior conectividade utiliza os recursos de maneira mais eficiente, refletindo em uma menor probabilidade de bloqueio de conexões futuras. Deve-se considerar, porém, que as comparações de conectividade necessitam realizar os testes de desempenho para topologias de rede que apresentam a mesma quantidade de recursos, ou seja, a mesma quantidade de lambdas por nó. Isto significa que uma rede de maior conectividade, que tem o dobro de número de enlaces que uma rede de menor conectividade, deve possuir a metade do número de lambdas em seus enlaces. Desta maneira, a proporção de lambdas por nó é mantida, e, como cada nó tem a mesma quantidade de recursos para criar as conexões, a comparação entre as topologias de conectividade diferente é justa e não favorece a rede que apresenta maior número de lambdas por nó.

3.5 A Reversibilidade dos Mecanismos de Proteção

Uma característica que diferencia a operação dos mecanismos de proteção e que, conseqüentemente, influi no desempenho da rede é a reversibilidade. Para mecanismos de proteção dedicados (tipo `1:1`) a reversibilidade não é um fator preponderante, pois o canal secundário não é compartilhado. No entanto, nos mecanismos de proteção compartilhada (tipo `1:N`) há enlaces dos canais secundários que são compartilhados e isto pode influir no desempenho.

Um mecanismo de proteção é classificado como reversível se, após a recuperação de um enlace falho, as conexões afetadas pela falha voltam ao seu canal primário. Um mecanismo de proteção não-reversível, por sua vez, não reverte para o canal primário as conexões afetadas por uma falha após a recuperação do enlace falho. Uma seqüência de eventos de um mecanismo reversível e de um não-reversível são apresentadas nas Figuras 3.11 e 3.12, respectivamente. Estas figuras apresentam os instantes de tempo tempo de ocorrência de eventos de conexão (C), falha (F), recuperação de falha (R) e desconexão (D). São ilustrados os comportamentos das duas conexões ópticas C1 e C2 que comutam do canal primário para o canal secundário (S), que é compartilhado ou inclui recursos compartilhados. A vantagem da não-reversibilidade é a redução da quantidade de comutações entre o canal primário e o canal secundário que são efetuadas para oferecer sobrevivência às possíveis falhas das fibras ópticas e outros componentes da rede. Analisando as Figuras 3.11 e 3.12 verifica-se que o mecanismo não-reversível utiliza somente duas comutações de canal, enquanto o mecanismo reversível utiliza quatro comutações. O efeito das comutações na disponibilidade depende do tempo necessário para realizar as comutações. Caso as comutações sejam realizadas em um curto período de tempo, a disponibilidade não é muito afetada. No entanto, as reconfigurações das redes ópticas são, em geral, lentas, pois os comutadores totalmente ópticos não apresentam um hardware com tempo de resposta baixo o suficiente. Como conseqüência, a comutação entre canais ópticos usualmente acarreta na desordenação na entrega de pacotes ao destino e até na indisponibilidade do serviço por um período de tempo. Portanto, em redes nas quais que se pretende garantir alto índice de disponibilidade, esta comutação de canais deve ser evitada.

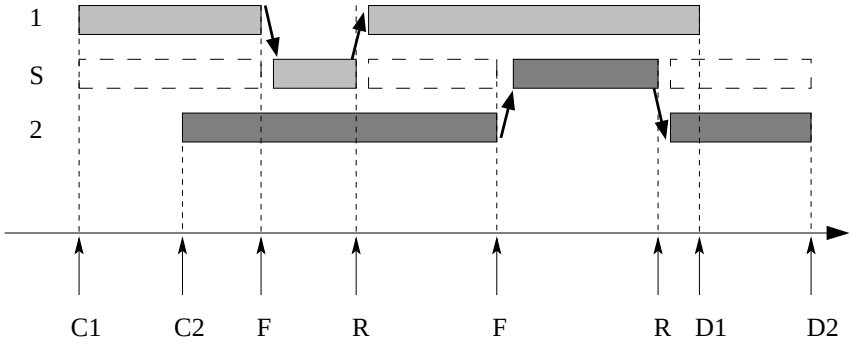


Figura 3.11: Mecanismo de proteção reversível.

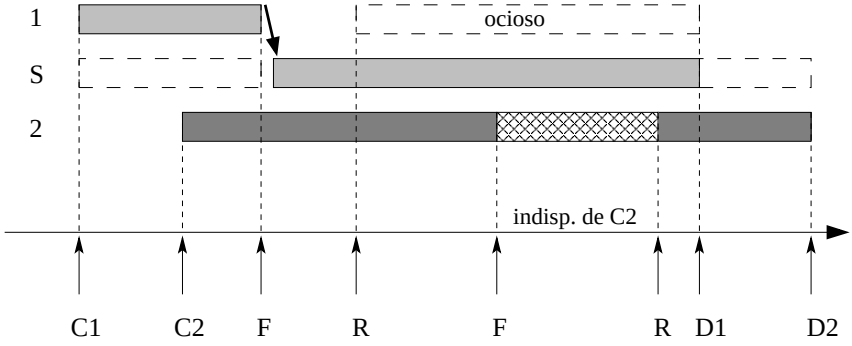


Figura 3.12: Mecanismo de proteção não-reversível.

A não-reversibilidade dos mecanismos de proteção influi em alguns parâmetros de desempenho. A probabilidade de bloqueio não é afetada. Já a disponibilidade das conexões pode ser prejudicada, se o mecanismo de proteção compartilhar recursos, ou pode ser beneficiada, se o tempo de permanência da conexão for pequeno o suficiente. Em uma rede que utiliza proteção `1:N` não-reversível, o canal secundário de uma conexão que foi afetada por falhas não é liberado até que a desconexão seja efetuada. Esta ocupação desnecessária de recursos de proteção, aliada à ocorrência de uma falha, mesmo que após a recuperação da primeira falha, pode acarretar na indisponibilidade de uma conexão óptica que compartilhava estes recursos de proteção, como é apresentado na Figura 3.12. Enquanto esta conexão não for liberada, as conexões que compartilham recursos com ela não poderão requisitar o canal secundário. Nesta situação, além da desnecessária indisponibilidade do canal secundário, existe ainda a ociosidade do canal primário, pois este recurso não é compartilhado.

Se esta ineficiência no uso dos recursos de proteção afeta negativamente a disponi-

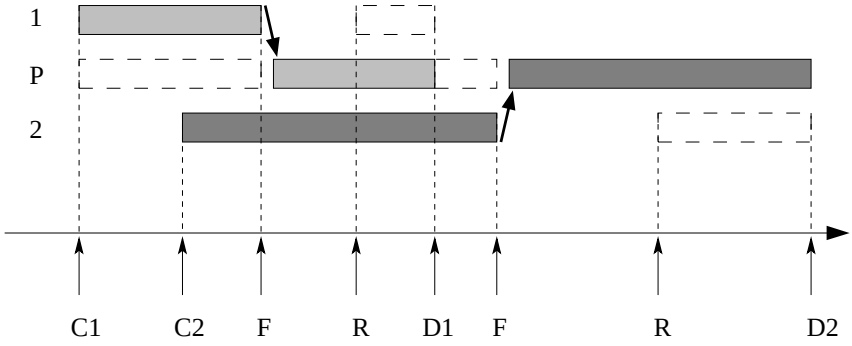


Figura 3.13: Efeito de um menor tempo de duração de conexão.

bilidade, por outro lado, a não-reversibilidade também afeta positivamente, dependendo do tempo médio de duração da conexão e do período de necessário à reconfiguração dos comutadores ópticos da rede. Se o tempo médio de duração de conexão for pequeno o suficiente, a conexão que ocupa o canal secundário desnecessariamente pode efetuar a desconexão e liberar os recursos compartilhados antes que outra conexão os requisite, como a Figura 3.13 ilustra. Assim, o impacto negativo na disponibilidade será, na média, atenuado e a resultante do desempenho geral da rede pode ser majoritariamente positiva. Esta tese estuda este compromisso entre as vantagens e as desvantagens da não-reversibilidade para determinar a viabilidade da implementação de mecanismos não-reversíveis em redes ópticas transparentes.

Capítulo 4

Resultados de Simulação

NESTE capítulo, são apresentados os principais resultados de simulações obtidos, as características da arquitetura do simulador desenvolvido e os detalhes referentes ao ambiente de simulação. O objetivo das simulações é analisar o desempenho de redes que empregam mecanismos de proteção e comparar os mecanismos convencionais com o mecanismo proposto. A avaliação considera aspectos dos mecanismos de proteção referentes a disponibilidade, probabilidade de bloqueio de conexões e também estuda o comportamento destes mecanismos considerando a conectividade da rede e a não-reversibilidade. Estes aspectos de desempenho proporcionam ao operador da rede uma visão sistêmica do impacto dos mecanismos de sobrevivência no desempenho geral da rede óptica.

As simulações, que estão divididas em três partes, foram realizadas em um simulador desenvolvido em C++ especificamente para estas análises. A primeira parte apresenta os resultados referentes ao novo mecanismo proposto. Este mecanismo proposto foi desenvolvido para proporcionar ao operador da rede priorizar a disponibilidade de conexões ou a probabilidade de bloqueio, gerenciando esta relação de compromisso entre estes dois parâmetros. A segunda parte apresenta uma análise sobre a relação entre a conectividade e a probabilidade de bloqueio em redes ópticas. A terceira parte apresenta uma análise sobre a reversibilidade dos mecanismos de proteção, e quais implicações para a rede que um mecanismo de sobrevivência não-reversível pode acarretar.

4.1 Ambiente de Simulação

O simulador, desenvolvido em C++ e orientado a objetos, é dirigido a eventos discretos e se baseia em um escalonador de eventos de conexão, de desconexão, de falha de enlace e de recuperação de falhas. É através da execução das rotinas destes quatro tipos de eventos (conexão, desconexão, falha e recuperação) que o escalonador simula o funcionamento de uma rede óptica com requisição dinâmica de conexões. Inicialmente, antes do escalonamento de eventos ser executado, os parâmetros iniciais são passados para o simulador. Estes parâmetros são: a topologia da rede, o tipo de mecanismo de proteção a ser simulado, a taxa de falha de enlace, a taxa de recuperação de falha, a taxa de conexão e a taxa de desconexão. A simulação é executada e após o seu término, as métricas de desempenho calculadas pelo simulador são apresentadas.

A simulação de redes ópticas transparentes pode ser realizada levando-se em conta uma demanda de conexões estática, onde existe uma matriz de tráfego estática definida antes da simulação e que não varia ao longo da execução, ou levando-se em conta uma demanda de conexões dinâmica, que escolhe aleatoriamente os pares de endereços de origem e destino de uma conexão, o tempo de início da conexão e o período de duração da conexão. O simulador implementado considera um modelo de requisição de conexão dinâmico.

O objetivo das simulações é avaliar o desempenho dos mecanismos de proteção em uma rede óptica. Assim, a cada requisição de conexão o algoritmo de roteamento busca um canal primário e outro secundário, também chamado de proteção. Caso a rede consiga prover os dois canais, a conexão é efetuada e, caso contrário, a conexão não é efetuada, pois ocorreu uma situação de bloqueio de conexão.

O simulador de eventos desenvolvido utiliza um escalonador de eventos, apresentado na Figura 4.1, que contém uma fila de eventos ordenados pelo campo tempo. Outros dois importantes objetos integrantes do escalonador são a matriz de topologia, que representa o grafo da rede simulada, e a lista de conexões ativas, que contém as conexões ativas e os respectivos recursos utilizados. A matriz de topologia consiste em um vetor de listas encadeadas de objetos que representam um enlace unidirecional. Esta estrutura de dados,

que representa o grafo da rede, é chamada de lista de adjacência. O primeiro elemento do vetor é a lista dos enlaces que partem do nó N1. O segundo elemento é referente ao nó N2, o terceiro ao nó N3 e assim por diante. No exemplo da Figura 4.1, o nó N1 tem um enlace com os nós N2, N3, N6 e N7. O nó N2 tem enlaces com os nós N1 e N4. E o nó N3 com os nós N1, N4 e N5. Cada objeto, que representa um enlace óptico neste vetor de listas, é composto de campos que indicam o estado do enlace, indicando se ativo ou falho, e o identificador das conexões que utilizam os lambdas deste enlace. O armazenamento destas informações é necessário para os procedimentos de reserva de recursos no estabelecimento de conexões e para gerenciar as conexões afetadas por falhas de enlaces.

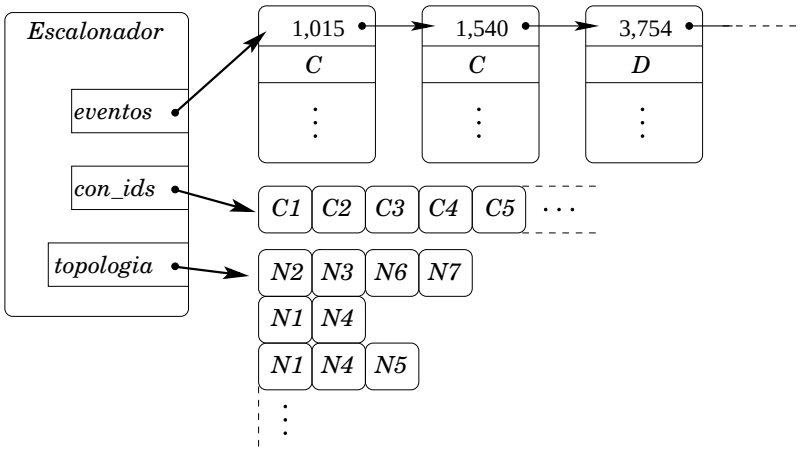


Figura 4.1: O escalonador e a fila de eventos

Na execução da simulação, o processamento de um evento implica a busca e a retirada do evento da fila de eventos e na execução da rotina associada ao tipo do evento. Esta rotina do evento utiliza as variáveis presentes no objeto do evento a executar. Cada objeto de evento contém as seguintes variáveis: o tempo, que determina o instante em que o evento deve ser executado; o tipo de evento, que define o evento descrito por este objeto e a rotina a ser executada; o endereço de origem e de destino, que define os nós da rede utilizados pelo o evento de conexão; o enlace, que define o enlace óptico afetado pelos eventos de falha e de recuperação; e o identificador de conexão, que define a conexão que será liberada pelo evento de desconexão. As duas primeiras variáveis (tempo e tipo) são comuns a todos os eventos. O endereço dos nós é utilizado somente no evento de conexão. O enlace é utilizado somente pelos eventos de falha e recuperação. O identificador de

conexão é utilizado somente pelo evento de desconexão. O identificador de conexão é definido pelo evento de conexão e é armazenado em uma lista que contém as conexões estabelecidas através da rede. No evento de desconexão as informações contidas nesta lista de conexões, como os enlaces utilizados, por exemplo, são utilizadas para liberar os recursos da conexão.

No evento de requisição de conexão, as duas rotas, o canal primário e secundário, são computadas pelo algoritmo de roteamento e, caso existam as duas rotas, a conexão é estabelecida e os enlaces ópticos são reservados. Após o estabelecimento ter sido efetuado, é realizada a inserção do evento de desconexão na fila de eventos do escalonador. Este processo de inserção de evento é chamado de escalonamento. Após o escalonamento do evento de desconexão, a rotina verifica o contador de tentativas de conexão, que é o critério de parada, para determinar se deve ou não escalonar o próximo evento de conexão. O escalonamento do evento de desconexão necessita, além do identificador de conexão, do tempo de duração desta conexão. Para obter esta variável, o instante de tempo de desconexão, é sorteada uma variável aleatória (V.A.) exponencial com a taxa de requisição de desconexão, que foi passada para o escalonador no início da simulação. De maneira semelhante, para escalonar o próximo evento de conexão a rotina necessita do tempo da conexão e do par de endereços de origem e de destino. Para obter o par de endereços, são sorteadas duas variáveis aleatórias uniformemente distribuídas que determinam o par origem-destino da conexão. Estas funções são implementadas obedecendo a restrição de não resultar em endereços iguais. Em seguida, para obter o tempo da próxima conexão, é sorteada uma V.A. exponencial com a taxa de requisição de conexão. Esta V.A. é adicionada ao tempo do evento atual e o objeto do evento de próxima conexão é escalonado na fila de eventos.

Em uma rede de tráfego dinâmico, a carga de tráfego é determinada pela razão da taxa da V.A. de conexão sobre a taxa da V.A. de desconexão. Neste trabalho, esta carga é medida em Erlangs por nó. Em uma rede com 10 nós, a carga na rede será de 20 Erlangs se a rede estiver sob uma carga de 2 Erlangs por nó. Em uma simulação que utiliza uma taxa de conexão duas vezes maior que taxa de desconexão, a carga aplicada na rede é de 2 Erlangs por nó. Isto significa que em média cada nó da rede tem duas conexões estabelecidas durante uma simulação. Isto, porém, não impede que em algum momento

um nó apresente um número de conexões estabelecidas diferente de dois.

O estabelecimento de uma conexão óptica é efetuado ao executar três procedimentos: a ponderação dos pesos dos enlaces, a execução do algoritmo de descoberta de rota e a reserva de lambda nos enlaces. Estes três procedimentos são executados seqüencialmente em duas rodadas. A primeira rodada estabelece o canal primário e a segunda estabelece o canal de proteção. Se um dos canais ópticos, o primário ou o secundário, não for estabelecido, a conexão é bloqueada, e os recursos que eventualmente foram reservados são liberados. O procedimento de ponderação associa a cada enlace da rede o peso utilizado pelo algoritmo de descoberta de rota. Se um enlace estiver falho ou se todos os seus lambdas estiverem ocupados, o peso será infinito indicando que este enlace está indisponível. Desta maneira o algoritmo de roteamento é forçado a não utilizar este enlace. O procedimento de descoberta de rota executa o algoritmo de roteamento. O algoritmo usado pelo simulador é o de caminho mais curto primeiro (*shortest path first*) proposto por *Dijkstra*. Por fim, o procedimento de reserva aloca o lambda que deve ser utilizado em cada enlace da rota calculada. Neste procedimento, os diversos algoritmos de alocação de lambda, que são extensamente abordados na literatura, não são considerados aqui, pois este trabalho supõe uma rede com conversão total de lambda. Após o algoritmo de roteamento escolher o caminho primário na primeira rodada, alguns parâmetros são ajustados para que o algoritmo possa escolher o caminho secundário ou de proteção. Os ajustes dependem do mecanismo de proteção que está sendo avaliado. No caso do mecanismo de proteção dedicado (tipo `1:1`) convencional os canais primários e secundários devem ser disjuntos e isto implica em rotas disjuntas. Assim, ao final da primeira rodada, são escalados para infinito os enlaces que foram utilizados pelo canal primário e, desta forma, o algoritmo que computa a melhor rota é forçado a descartar os enlaces utilizados pelo canal primário. O terceiro procedimento do estabelecimento de conexão é a reserva de recursos que no caso dos mecanismos de proteção compartilhados (tipo `1:N`) deve verificar a possibilidade de compartilhar lambdas seguindo as restrições de cada mecanismo. Assim, no mecanismo de proteção compartilhado convencional aceita-se o compartilhamento de enlaces que não pertençam ao grupo de risco de falha de enlace. No mecanismo proposto, esta restrição é relaxada e aceita-se o compartilhamento de uma percentagem α de enlaces que pertençam ao grupo de risco de falha de enlace.

A rotina de tratamento do evento de falha de enlace verifica o canal de proteção das conexões dependentes do enlace que falhou. Se o canal de proteção está disponível, a conexão comuta para este. Esta conexão não sofre, portanto, alterações na sua disponibilidade. Porém, a conexão que não tiver o canal de proteção disponível tem seu serviço interrompido e indisponível. Esta indisponibilidade da conexão permanece até o evento de recuperação. O tempo desta falha é armazenado na conexão para que após a recuperação ou desconexão a disponibilidade da conexão seja computada.

Nas rodadas de simulação, o critério de parada utilizado não é baseado no tempo simulado, mas no número de tentativas, ou requisições, de conexão. Vale ressaltar que são contabilizadas as requisições de conexão e não apenas as conexões estabelecidas com sucesso. Um número muito grande de requisições de conexão é escolhido de maneira que o efeito transitório inicial seja desprezível e o regime permanente de operação da rede predomine. Cada rodada apresenta uma média de 100.000 conexões por nó. Em uma rede com requisição de conexão em média a cada duas horas, isto equivale a alguns anos de operação da rede e a centenas de eventos de falhas de enlaces. As rodadas de simulação são repetidas até alcançar 95% de confiabilidade para os intervalos de confiança apresentados nos gráficos.

Todas as simulações utilizam os valores de parâmetros descritos a seguir, como apresentado por Zhang *et al.* em [17], exceto quando especificado diferentemente. A chegada de requisição de conexão segue a distribuição de Poisson com 2 horas de média. O tempo médio de duração de cada conexão segue a distribuição exponencial e o tempo médio de desconexão depende da carga de tráfego aplicada na rede. O par origem-destino das conexões é sorteado aleatoriamente entre todos os nós da rede. O evento de falha de um enlace segue a distribuição exponencial com média de 50 dias e o tempo de restauração da falha é exponencial com média de 12 horas.

Após cada rodada de simulação, a probabilidade de bloqueio e a disponibilidade das conexões são computadas. O cálculo da probabilidade de bloqueio é realizado com base em dois contadores. O primeiro contador é o número de requisições de conexões, que é incrementado a cada requisição de conexão, independente do sucesso ou insucesso do estabelecimento. O segundo contador é o número de conexões bloqueadas que é incre-

mentado quando a conexão não é estabelecida com sucesso, independente do motivo para o bloqueio da conexão, que pode ser por excesso de tráfego ou por falha de enlaces. O cálculo da disponibilidade das conexões é realizado com base no tempo que o serviço permanece disponível e no tempo de duração total da conexão. A disponibilidade é um valor adimensional que varia de 0 a 1. Este valor é a razão do tempo disponível da conexão com tempo de duração total da conexão. Através destes dois parâmetros, o desempenho da rede é comparado para os diferentes mecanismos de proteção e diferentes topologias de rede.

4.2 Resultados

Os resultados das simulações são analisados em três seções. Na Seção 4.2.1, são apresentados os resultados referentes ao novo mecanismo de proteção em redes ópticas transparentes. Na Seção 4.2.2 são apresentados os resultados referentes à conectividade da rede. E, finalmente, na Seção 4.2.3 são apresentados os resultados referentes à não-reversibilidade dos mecanismos de proteção.

Em todas as simulações as redes foram simuladas com quatro lambdas em cada fibra óptica. Esta quantidade de lambdas foi utilizada pois os principais produtos comercialmente disponíveis no mercado são implementados para operar com quantidades semelhantes a esta. Ademais, os resultados obtidos não são dependentes da quantidade de recursos por fibra, portanto, um aumento na quantidade destes recursos implica, necessariamente, em um aumento da carga média aplicada na rede, para se obter os mesmos resultados. A carga aplicada na rede foi escolhida de maneira que os valores obtidos de probabildade de bloqueio e disponibilidade de conexões fosse semelhante aos valores encontrados nos trabalhos relacionados. Esta comparação é teste de sanidade para o simulador e para a implementação dos mecanismos de proteção. Além dos resultados do simulador terem sido comparados com os resultados de alguns trabalhos que abordam este mesmo problema das redes ópticas, também foram realizados testes de exaustão computacional e testes de caso que são críticos ao funcionamento dos algoritmos de decisão de compartilhamento de recursos secundários dos mecanismos de proteção. Por

fim, os testes de homologação funcional do mecanismo proposto incluem a comparação dos resultados obtidos do mecanismo proposto com $\alpha = 0$ com os resultados obtidos do mecanismo convencional `1:N`. A comparação mostrou, como esperado, que as duas simulações apresentam resultados idênticos.

4.2.1 O Mecanismo Proposto Compartilhado com Relaxação de Risco

Nas simulações do mecanismo de proteção compartilhado com relaxação de risco são utilizadas duas topologias de rede. A primeira rede, ilustrada na Figura 4.2, consiste em 6 nós interconectados por 9 enlaces. Esta é referida nesta tese como rede 6N9E. A segunda rede é a NSFNet, a rede de pesquisa dos Estados Unidos, ilustrada na Figura 4.3, com 16 nós e 23 enlaces, como apresentada por Wang *et al.* em [21]. Esta rede é referida nesta tese como NSFNet-16N23E. Nesta topologia, os números apresentados ao lado dos enlaces são os pesos dos enlaces utilizados no algoritmo de roteamento. Para a rede 6N9E, os pesos são sempre 1.

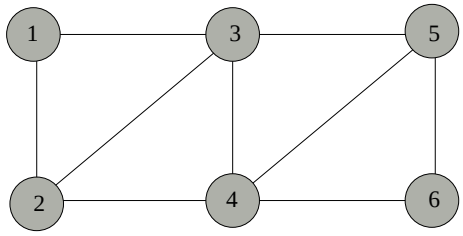


Figura 4.2: Rede 6N9E.

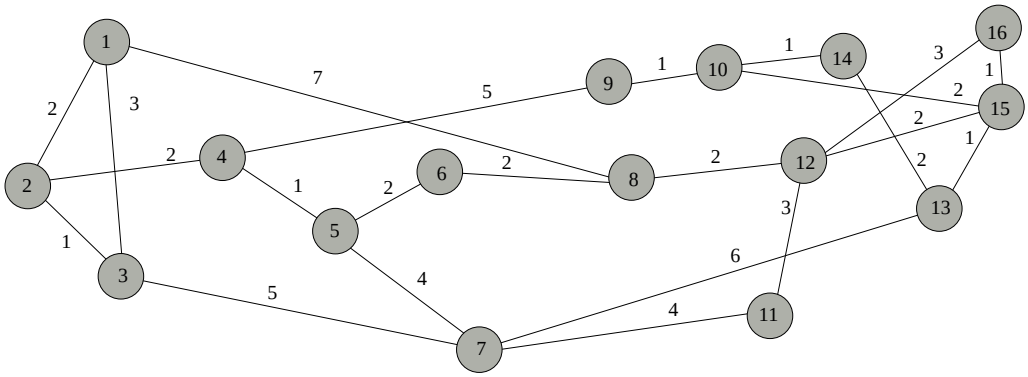


Figura 4.3: Rede NSFNet-16N23E.

Foram realizadas simulações com a finalidade de comparar o desempenho do meca-

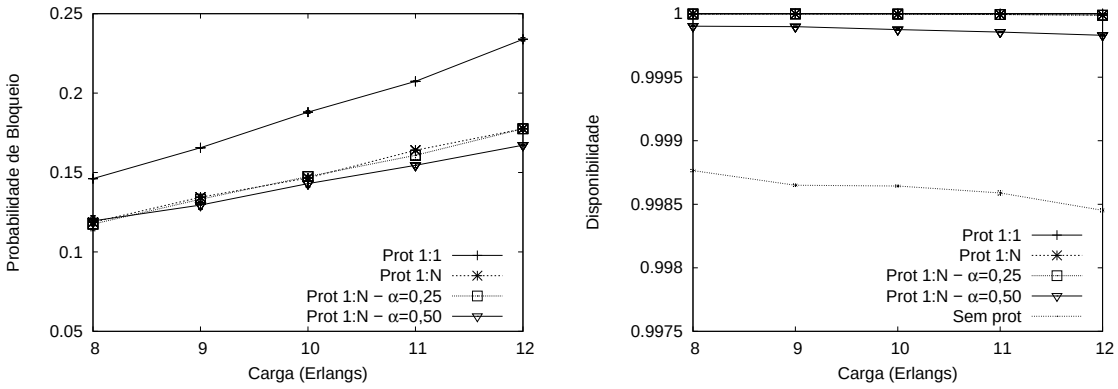
nismo proposto com os mecanismos convencionais. As Figuras 4.4(a) e 4.4(b) mostram como o aumento da carga na rede afeta a probabilidade de bloqueio e a disponibilidade das conexões para a Rede 6N9E. As figuras ilustram o comportamento da rede com: nenhuma proteção; a proteção `1:1`; a proteção `1:N`; e a proteção compartilhada (`1:N`) com relaxação de risco com os fatores de relaxação de risco de 0,25 e 0,5. A probabilidade de bloqueio da rede sem proteção é da ordem de 10^{-5} e por isso não é apresentada no gráfico da Figura 4.4(a). Em contrapartida a esta baixa probabilidade de bloqueio, a rede sem proteção apresenta uma disponibilidade que fica entre 99,8% a 99,9%. Este desempenho não é satisfatório para uma rede óptica transparente que pretende garantir 99,999% de disponibilidade.

Visando garantir esta alta disponibilidade, os mecanismos de proteção `1:1` e `1:N` foram testados. O primeiro mecanismo garante uma disponibilidade superior a 99,999%, como é verificado na Figura 4.4(b). Para isto, estabelece para cada conexão dois canais ópticos, um canal primário e outro de proteção. Porém, analisando a Figura 4.4(a), constata-se que a proteção dedicada `1:1` apresenta uma probabilidade de bloqueio até 50% maior que outros mecanismos de proteção. O mecanismo `1:N` atinge este valor de 99,999% de disponibilidade, sem prejudicar a eficiência da rede, e, por isso, obtém uma probabilidade de bloqueio de 20 a 30% menor que a proteção `1:1`. O mecanismo proposto foi desenvolvido com o objetivo de alcançar uma eficiência maior que a proteção compartilhada `1:N`. Como já dito, isto não é possível sem o prejuízo da disponibilidade das conexões e uma relação de compromisso entre estes dois parâmetros deve ser ponderada.

Esta parte das simulações se propõe a quantizar este compromisso entre o ganho de eficiência, medido pela probabilidade de bloqueio, e a perda de disponibilidade. Pode-se constatar pelos gráficos das Figuras 4.4(a) e 4.4(b) que, para a rede com uma carga de 12 Erlangs e com o mecanismo proposto com fator de relaxação de risco de 0,5, um ganho de 5,6% (de $17,7$ para $16,7$) na probabilidade de bloqueio acarreta em uma perda de 0,016% ($99,9989$ para $99,9829$) na disponibilidade. Porém, esta comparação é tendenciosa, pois as comparações não devem ser realizadas considerando os valores absolutos dos parâmetros. Se as comparações forem realizadas relativas ao ganho comparado à rede sem proteção, o efeito da perda da disponibilidade será mais realista. Neste caso, como a

disponibilidade da rede sem proteção para esta carga é $99,8452$, a perda relativa na disponibilidade é 10,4%. As aplicações e as discussões desta relação de compromisso são abordadas mais adiante nesta seção.

Os gráficos das Figuras 4.5(a) e 4.5(b) apresentam o comportamento da probabilidade de bloqueio e da disponibilidade para a rede NSFNet-16N23E. Vale ressaltar que, salvo algumas pequenas discrepâncias relacionadas à aleatoriedade da simulação, os resultados obtidos nas Redes 6N9E e NSFNet-16N23E apresentam comportamento equivalente. Portanto, as conclusões e comparações realizadas para a Rede 6N9E são válidas para a Rede NSFNet-16N23E.



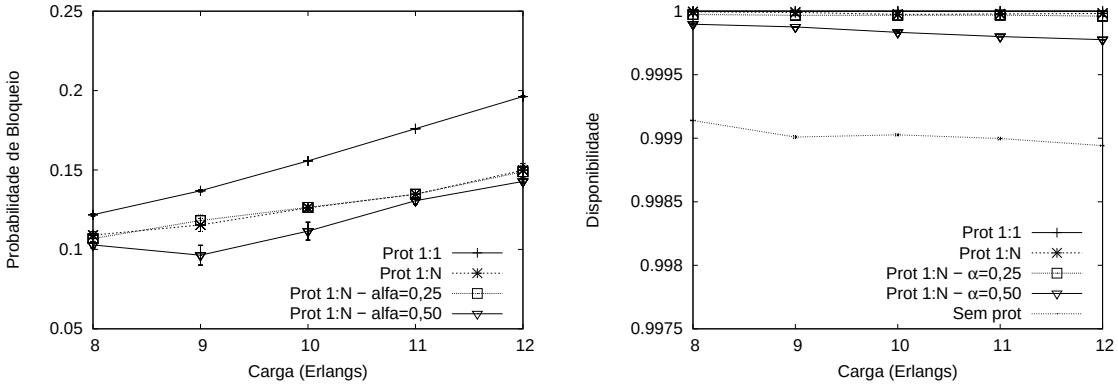
(a) Probabilidade de bloqueio da rede 6N9E.

(b) Disponibilidade de conexões da rede 6N9E.

Figura 4.4: Resultados de simulação para a rede 6N9E.

Em ambas as redes, a probabilidade de bloqueio na configuração sem proteção é menor que a probabilidade de bloqueio da implementação de qualquer mecanismo de proteção, o que é esperado. Porém, a disponibilidade das conexões para as redes configuradas sem proteção apresenta os menores resultados, o que também é esperado mas não é desejado. Já a proteção `1:1`, apesar de apresentar a melhor disponibilidade dentre os mecanismos de proteção, apresenta a pior probabilidade de bloqueio em qualquer cenário, pois este mecanismo utiliza os recursos da rede de maneira ineficiente.

Note que para todos os mecanismos de proteção, a Rede NSFNet-16N23E apresenta menor probabilidade de bloqueio que a Rede 6N9E. À primeira vista este comportamento parece óbvio, pois uma rede maior significa mais recursos, e, conseqüentemente, uma



(a) Probabilidade de bloqueio da rede NSFNet-16N23E.

(b) Disponibilidade de conexões da rede NSFNet-16N23E.

Figura 4.5: Resultados de simulação para a rede NSFNet-16N23E.

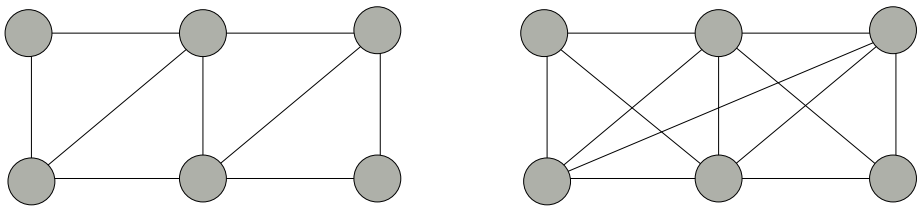
melhor acomodação das conexões na rede para uma mesma carga. Porém, este não é o caso. A Rede NSFNet-16N23E não apresenta mais recursos por nó que a Rede 6N9E. Em ambas, o fator de utilização da rede é o mesmo, ou seja, a razão de carga por recursos é igual. O motivo deste desempenho superior da Rede NSFNet-16N23E é a maior distribuição das requisições de conexões pelos enlaces. O maior número de opções possibilita que o algoritmo de descoberta de rotas evite mais facilmente áreas de deficiências de recursos da rede. Na prática, estas deficiências podem ser ocasionadas por motivos variados, como rajadas inesperadas de conexões entre dois nós adjacentes ou falhas de enlaces.

Teoricamente, a disponibilidade é afetada somente pela taxa de falha dos equipamentos da rede, pelo tempo médio de recuperação das falhas e pelo mecanismo de proteção que a rede implementa. O que as simulações mostram, porém, é uma diminuição da disponibilidade das conexões conforme aumenta a carga da rede. O valor da disponibilidade, que calculado ao fim das simulações, é o valor médio correspondente a todas as conexões estabelecidas com sucesso. Portanto, uma conclusão precipatada seria a de que uma disponibilidade menor implica períodos maiores de indisponibilidade de cada conexão. Na verdade, o que ocorre não é um maior número de conexões afetadas por uma falha e, portanto, influenciando negativamente, com maior peso, a disponibilidade de todas as conexões da rede. Em uma rede com pouca carga, a probabilidade de nenhuma conexão ser afetada pela falha é alta. No entanto, em uma rede com muita carga, alta será

a probabilidade de uma falha afetar muitas conexões.

Analisando a probabilidade de bloqueio nas Figuras 4.4(a) e 4.5(a), verifica-se que a proteção compartilhada (`1:N`) com fator de relaxação de risco de 0,5 apresenta um desempenho superior aos outros mecanismos, inclusive à proteção compartilhada (`1:N`) com fator de relaxação de risco de 0,25. Devido à disputa de recursos no mecanismo de proteção compartilhada (`1:N`) com fator de relaxação de risco, aumentar o fator de risco acarreta na diminuição da probabilidade de bloqueio, mas também implica na diminuição da disponibilidade. Esta flexibilidade permite que o ajuste do compartilhamento esteja de acordo com as necessidades da rede e proporcione um compromisso entre a probabilidade de bloqueio e a disponibilidade de conexões. Um maior compartilhamento acarreta uma menor probabilidade de bloqueio e, conseqüentemente, o operador pode alocar mais usuários sem que para isso sejam necessárias modificações na infra-estrutura de rede. Um menor compartilhamento acarreta, por sua vez, em maior disponibilidade, proporcionando ao operador a oportunidade de oferecer para seus usuários um serviço de conectividade mais confiável, com maior disponibilidade. Esta variável permite que o operador determine qual parâmetro deve ser priorizado, ponderando suas necessidades e as especificações do serviço contratado pelo cliente através das SLAs.

4.2.2 A Conectividade da Rede



(a) Rede 9E: Topologia de menor conectividade.

(b) Rede 12E: Topologia de maior conectividade.

Figura 4.6: Topologias de redes com diferentes conectividades.

Nas simulações de conectividade são utilizadas duas topologias de rede, ambas com o mesmo número de nós mas com o número de enlaces diferentes. A Rede 9E de menor

conectividade, ilustrada na Figura 4.6(a), consiste em 6 nós interconectados por 9 enlaces com 4 lambdas em cada enlace. A Rede 12E de maior conectividade, ilustrada na Figura 4.6(b), é semelhante à primeira, porém apresenta 12 enlaces com 3 lambdas cada. Estas topologias, apesar de terem a proporção de enlaces por nó diferente, apresentam a mesma proporção de recursos por nó. Para isso, basta reduzir o número de lambdas por enlace na mesma proporção que o número de enlaces por nó for aumentada. Desta forma a quantidade de lambdas na rede é sempre a mesma. Pode-se constatar que, como as duas topologias da Figura 4.6 mantêm o produto $enlaces \times lambdas$ destas topologias, $9 \times 4 = 36$ e $12 \times 3 = 36$, a relação entre recursos da rede e o número de nós também se mantém.

Vale ressaltar que não foi possível realizar as simulações de conectividade para mais de duas topologias diferentes. Isto se deve, unicamente, a uma característica do grafo das redes. O requisito de manter o produto de $enlaces \times lambdas$ fixo em 36 restringe as combinações de $enlaces \times lambdas$ para os pares: 2×18, 3×12, 4×9 e 5×6. Filtrando estes pares, à faixa de número mínimo e máximo de enlaces que esta rede comporta, que é de 6 (n) a 15 ($n(n-1)/2$), as combinações se restringem a 3×12, 4×9 e 5×6. Como a rede apresenta seis nós, esta não pode ser composta de somente seis enlaces, pois resultaria em uma rede em anel e, portanto, não estaria no escopo deste trabalho. Assim, restam somente os dois primeiros pares de combinações $enlace \times lambdas$, 3×12 e 4×9.

As simulações foram realizadas com a finalidade de comparar o desempenho dos mecanismos de proteção para diferentes conectividades de rede. As Figuras 4.7 e 4.8 mostram como o aumento da carga na rede afeta a probabilidade de bloqueio e a disponibilidade das conexões para ambas as redes da Figura 4.6. As figuras ilustram o comportamento das redes com a proteção `1:1` e com a proteção compartilhada (`1:N`) com fator de relaxação de risco de 0,5. Como se pode observar, a resposta da rede depende de sua conectividade. Uma conectividade maior acarreta em uma utilização mais eficiente dos enlaces e, portanto, em uma probabilidade de bloqueio menor. Para uma rede com uma conectividade menor, a utilização dos recursos é menos eficiente, pois os canais ópticos utilizam mais enlaces. Isto acarreta em uma maior probabilidade de bloqueio, pois mais lambdas são necessários para o estabelecimento de uma conexão.

Na Figura 4.7 observa-se que a probabilidade de bloqueio da Rede 12E é até 75% menor que a da Rede 9E, para ambas com baixa carga. Esta comparação em alta carga apresenta uma redução de aproximadamente 50% da probabilidade de bloqueio. Com relação à disponibilidade de conexões, observa-se uma melhora para a rede de maior conectividade, como mostra a Figura 4.8. O impacto na disponibilidade geral da rede melhora de 99,9% para 99,999%. Isto ocorre porque na rede de maior conectividade a falha de um enlace acarreta na interrupção de menos conexões.

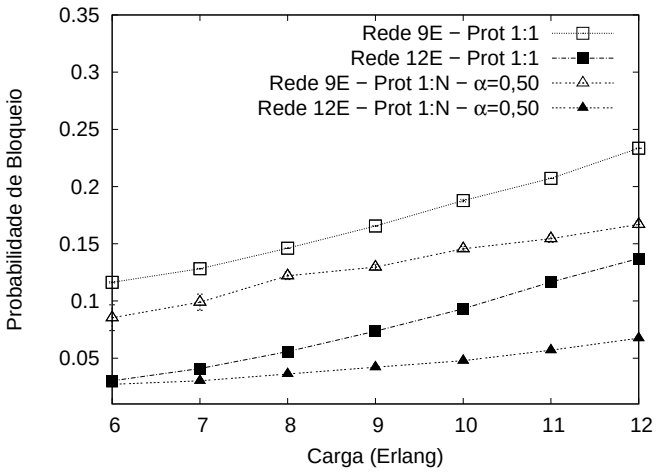


Figura 4.7: Probabilidade de bloqueio para as redes de menor e maior conectividade.

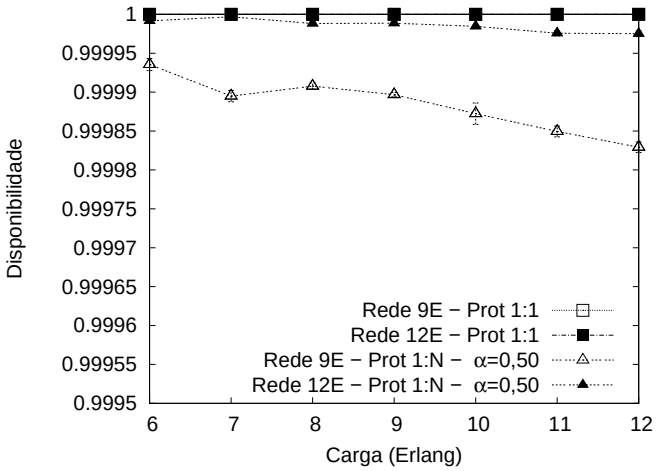


Figura 4.8: Disponibilidade para as redes de menor e maior conectividade.

4.2.3 A Reversibilidade dos Mecanismos de Proteção

Como foi explicado no capítulo anterior, a reversibilidade não afeta a disponibilidade de uma rede que emprega um mecanismo de proteção `1:1`, pois a reversão consiste em comutar do canal de proteção para o canal primário que possuem os mesmos recursos. No entanto, na proteção compartilhada alguns canais de proteção estão compartilhados e, portanto, a não reversão pode afetar o desempenho da rede. As simulações de reversibilidade utilizam a rede NSFNet, com 16 nós e 23 enlaces, ilustrada na Figura 4.3.

Em relação as simulações de reversibilidade, as simulações realizadas utilizando os mesmos parâmetros das simulações anteriores não resultaram em diferenças significativas entre o desempenho dos mecanismos reversíveis e não-reversíveis. Após análise, constatou-se que este comportamento era conseqüência da razão entre a taxa de falha e a taxa de desconexão. A relação entre os valores de taxa de falha e o tempo médio de duração da conexão é determinante no desempenho do mecanismo de proteção não-reversível. Os parâmetros utilizados nas simulações anteriores são desfavoráveis para a avaliação de mecanismos não-reversíveis. As conexões de pequena duração acarretam maior dinamicidade na rede, ou seja, maior freqüência com que as conexões são estabelecidas e liberadas. Desta maneira, em uma rede com mecanismo de proteção não-reversível implementado, que tem seus canais de proteção liberados mais rapidamente, o impacto negativo da não-reversibilidade é amenizado. Da mesma maneira, uma rede que apresenta uma ocorrência de falhas de freqüência baixa, também ameniza o impacto da não-reversibilidade, pois a probabilidade de uma conexão óptica liberar os recursos antes que outra falha ocorra é grande.

Os mecanismos não-reversíveis são adequados para ambientes de simulação onde as falhas são mais freqüentes que o normal ou o tempo de duração da conexão é maior que o usual. Com a tendência atual de convergência das tecnologias de telecomunicações, o aumento de duração da conexão é uma realidade. Como o objetivo da análise desta seção é estudar o impacto dos mecanismos não-reversíveis na disponibilidade das conexões, o ambiente de simulação foi modificado para um ambiente que evidencie as diferenças de desempenho entre os mecanismos reversíveis e não-reversíveis. Este ambiente de simulação, que busca determinar o impacto da variação da taxa de falha de enlaces na dispo-

nibilidade, tem a média da V.A. exponencial de falha reduzida para 5 dias, ao invés dos 50 dias utilizados anteriormente. A redução do tempo médio de falha acarretaria em uma probabilidade de falha menor se a taxa de recuperação não for alterada. Portanto, para que esta probabilidade permaneça inalterada, o tempo médio de recuperação, também é reduzido pela mesma proporção para 1,2 horas. Como conseqüência, os enlaces falham com maior freqüência, porém, são recuperados mais rapidamente, mantendo a proporção de tempo que permanecem operacionais. Vale notar que o mesmo comportamento seria obtido se a taxa de desconexão fosse reduzida, aumentando o tempo médio de duração das conexões. Na verdade, para as análises comparativas da disponibilidade de conexões, o efeito de duplicar o tempo médio entre conexões é o mesmo que reduzir à metade o tempo médio entre falhas. Este comportamento é ilustrado pelas Figuras 4.9 e 4.10.

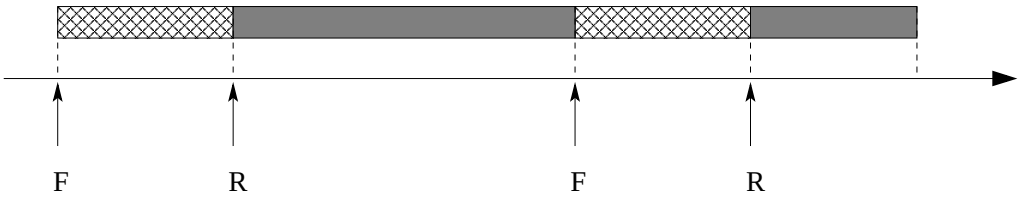


Figura 4.9: Taxas menores de falha e de recuperação.

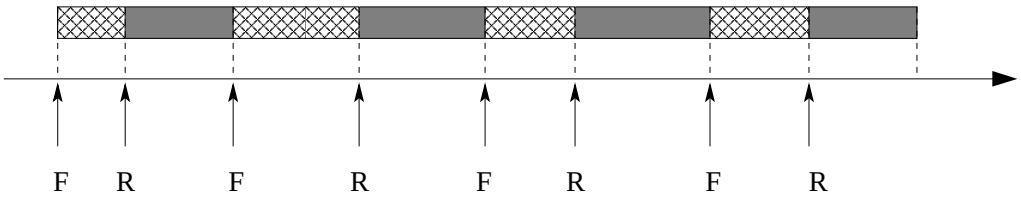


Figura 4.10: Taxas maiores de falha e de recuperação.

Foram realizadas simulações com a finalidade de comparar o impacto dos mecanismos não-reversíveis no desempenho da rede. As Figuras 4.11 e 4.12 mostram como o aumento da carga na rede afeta a disponibilidade das conexões e o número de conversões realizadas entre os canais de uma conexão. Quando os mecanismos não-reversíveis são implementados, a disponibilidade é degradada em até 9% relativo ao ganho da rede sem proteção (de $99,9986$ para $99,9847$), porém a quantidade de comutações entre canais ópticos é reduzida em aproximadamente 50%, o que ameniza o detrimento da disponibilidade. Vale ressaltar que os cálculos de simulação que resultam na disponibilidade não computam o tempo de comutação entre os canais ópticos, que é considerado zero. O simulador foi

implementado propositalmente desta maneira, para que fosse possível a análise individual de cada fator que influencia a disponibilidade de conexões. No caso, o gráfico de disponibilidade da Figura 4.11 representa a disponibilidade de conexões desconsiderando o impacto referente ao tempo de comutação do canal primário para o canal de proteção e vice-versa. O impacto da comutação entre canais ópticos na disponibilidade deve ser analisado através dos gráficos de comutações entre canais na Figura 4.12.

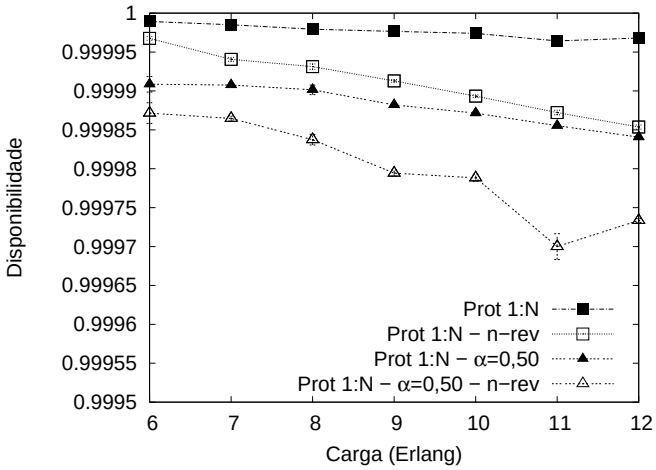


Figura 4.11: Disponibilidade de conexões.

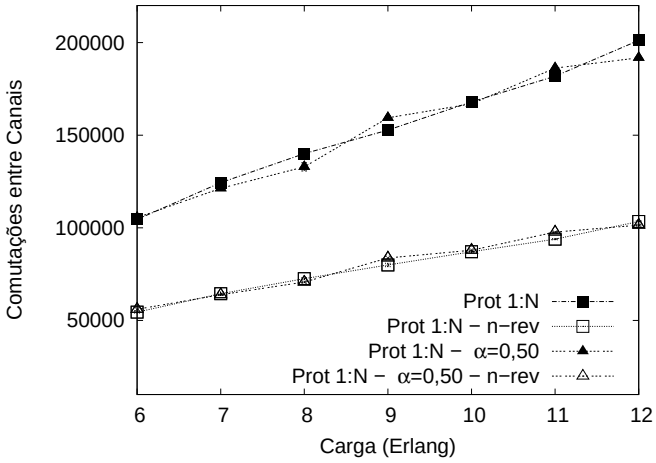


Figura 4.12: Comutações entre canais ópticos.

Capítulo 5

Conclusões

O MODELO de redes IP-sobre-WDM (*Internet Protocol over Wavelength Division Multiplexing*) é considerado o modelo mais apropriado para as necessidades atuais das redes ópticas transparentes. O conjunto de protocolos GMPLS (*Generalized Multi-protocol Label Switching*) provê funcionalidades que facilitam o gerenciamento e operação destas redes. As facilidades oferecidas pelo protocolo GMPLS para estabelecer um canal óptico, o grande número e a diversidade de aplicações existentes, a dinamicidade do comportamento das conexões e a confiabilidade requerida das redes oferecem o ambiente propício para que as pesquisas de sobrevivência a falhas em redes ópticas em malha IP-sobre-WDM avancem.

Este trabalho aborda o problema de provisão de sobrevivência a falhas em redes ópticas transparentes e foca os mecanismos de proteção na camada WDM de forma a obter reduzidos tempos de recuperações de falhas. São estudados mecanismos convencionais de proteção e um novo mecanismo é proposto. O desempenho dos mecanismos é avaliado através de um simulador próprio desenvolvido em C++. A principal característica deste simulador consiste em ser um escalonador de eventos que apresenta uma estrutura de dados simples, o tornando bastante versátil e eficiente.

O mecanismo proposto implementa uma proteção de conexão compartilhada (tipo `1:N`) onde se introduz um parâmetro de suavização da restrição do compartilhamento de enlaces de proteção que pertençam ao mesmo grupo de risco de falha de enlace (*Shared*

Risk Link Group -SRLG) que o canal primário da conexão. Ao se permitir esta flexibilização do uso de determinados enlaces é possível atender mais requisições de conexão e, conseqüentemente, aumentar a eficiência da rede. Por outro lado, a disponibilidade de conexões da rede fica mais vulnerável, podendo ser prejudicado. Este trabalho procura avaliar as vantagens e desvantagens de se permitir esta flexibilização ressaltando o compromisso entre o ganho de eficiência da rede e a perda de disponibilidade de conexões. É importante ressaltar que o uso do parâmetro de flexibilização permite ao operador da rede estimar a quantidade de conexões adicionais que a rede pode atender e o risco que pode advir deste fato por não atender a disponibilidade de conexão definida no contrato de nível de serviço (SLA). Desta forma, o nível de compartilhamento poder ser ajustado de acordo com a necessidade do operador da rede. Também deve ser ressaltado que o uso do simulador é uma poderosa ferramenta para planejamento de expansões das redes. É possível verificar o quanto é mais efetivo aumentar a capacidade (número de lambdas, por exemplo) dos enlaces existentes ou criar um novo enlace na rede.

Os resultados de simulação mostram que, em alguns casos, a probabilidade de bloqueio apresenta um ganho de até 5,6%, enquanto acarreta em uma perda de 0,016% da disponibilidade das conexões. Esta percentagem de perda da disponibilidade em valores absolutos é equivalente a 10,4% de perda relativa à rede sem proteção.

Os resultados mostram que a disponibilidade é influenciada pela carga de tráfego aplicada à rede. Este comportamento pode ser explicado pelo número de conexões afetadas por uma falha quando a rede apresenta carga alta e quando a rede apresenta carga baixa. Quanto maior o número de conexões na rede maior é o impacto de uma falha na disponibilidade.

As simulações referentes à conectividade foram realizadas com a finalidade de comparar o desempenho dos mecanismos de proteção para diferentes níveis de conectividade de rede. Uma conectividade maior acarreta em uma utilização mais eficiente dos enlaces e, portanto, uma menor probabilidade de bloqueio, pois existem mais opções de caminhos da origem para o destino e, conseqüentemente, os canais ópticos utilizam uma maior diversidade de enlaces. As simulações apresentam resultados que mostram um exemplo onde a probabilidade de bloqueio de uma rede de maior conectividade chega a ser até

75% menor que a de uma rede de menor conectividade. Com relação à disponibilidade de conexões, observa-se que, nos cenários simulados, a rede de maior conectividade pode apresentar uma melhora na disponibilidade das conexões de 99,9% para 99,999%.

Em relação à não-reversibilidade foram realizadas simulações com a finalidade de comparar o impacto dos mecanismos reversíveis e não-reversíveis no desempenho da rede. As simulações mostraram que a não-reversibilidade apresenta mudanças no desempenho da rede somente se a razão entre o tempo médio de duração de conexão e o tempo médio entre falhas (*Mean Time Between Failures* - MTBF) for maior que a encontrada atualmente, que não está fora da realidade de um futuro breve, visto a tendência das aplicações da Internet permanecerem *on line* por períodos cada vez maiores. Neste cenário, quando a não-reversibilidade dos mecanismos é implementada, as simulações mostram que a disponibilidade é degradada de 9%, mas em contrapartida o número de comutações das conexões entre seus canais ópticos é reduzido a 50%. Portanto, a implementação de mecanismos não-reversíveis acarreta em um compromisso entre a disponibilidade de conexões e a comutação entre canais ópticos que deve ser ponderado. Esta ponderação deve ser realizada levando-se em conta o tempo de comutação entre canais, que depende da tecnologia dos comutadores ópticos. Este tempo determina se o impacto da redução do número de comutações é predominante sobre o impacto da perda da disponibilidade de conexões e, portanto, define se o mecanismo não reversível é adequado para a rede analisada.

Como trabalhos futuros pretende-se obter expressões analíticas que descrevam o comportamento da probabilidade de bloqueio e da disponibilidade. Um outro ponto que merece maior investigação é estender as simulações sobre reversibilidade para analisar o impacto do tempo de duração de conexão e da taxa de falha no desempenho da rede com os mecanismos não-reversíveis. Com este estudo é possível descobrir o ponto ótimo do compromisso entre número de comutações e a disponibilidade. Por fim, o simulador poderia ser aperfeiçoado inserindo o custo como variável. Assim, ao usá-lo como ferramenta de planejamento de redes, poderia se determinar o custo e os benefícios de se aumentar a capacidade de um ou mais enlaces já existentes e comparar esta solução com a possibilidade de criação de um ou mais novos enlaces entre dois nós da rede.

Referências Bibliográficas

[1] LIANG, L., SUN, Z., E CRUICKSHANK, H. Relative QoS optimization for multi-party online gaming in diffserv networks. *IEEE Communications Magazine 43*, 5 (maio de 2005), 75–83.

[2] MATHY, L., EDWARDS, C., E D.HUTCHISON. The Internet: a global telecommunications solution? *IEEE Network 14*, 4 (julho de 2000), 46–74.

[3] MAESSCHALCK, S. D., COLLE, D., GROEBBENS, A., DEVELDER, C., E LAGASSE, A. L. P. Intelligent optical networking for multilayer survivability. *IEEE Communications Magazine 40*, 1 (janeiro de 2002), 42–49.

[4] VASSEUR, J.-P., PICKAVET, M., E DEMEESTER, P. *Network Recorver: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*, primeira ed. Morgan Kaufmann Publ., 2004.

[5] RAMASWANI, R., E SIVARAJAN, K. *Optical Networks: A Pratical Perspective*, segunda ed. Morgan Kaufmann Publ., 2002.

[6] MANNIE, E. Generalized Multi-Protocol Label Switching (GMPLS) Architecture. *Internet RFC 3945* (outubro de 2004). Proposed Standard.

[7] BANERJEE, A., DRAKE, L., LANG, L., TURNER, B., AWDUCHE, D., BERGER, L., KOMPELLA, K., E REKHTER, Y. Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques. *IEEE Communications Magazine 39*, 7 (junho de 2001), 144–151.

[8] BANERJEE, A., DRAKE, J., LANG, J., TURNER, B., KOMPELLA, K., E REKHTER, Y. Generalized multiprotocol label switching: an overview of routing and ma-

nagement enhancements. *IEEE Communications Magazine 39*, 1 (janeiro de 2001), 144–150.

[9] ROSEN, E., VISWANATHAN, A., E CALLON, R. Multiprotocol Label Switching Architecture. *Internet RFC 3031* (janeiro de 2001).

[10] AWDUCHE, D., E REKHTER, Y. Multiprotocol lambda switching: combining MPLS traffic engineering control with optical crossconnects. *IEEE Communications Magazine 39*, 3 (março de 2001), 111–116.

[11] AUKIA, P., KODIALAM, M., KOPPOL, P., LAKSHMAN, T., SARIN, H., E SUTER, B. RATES: a server for MPLS traffic engineering. *IEEE Network 14*, 2 (março de 2000), 34–41.

[12] VENKATESWARAN, R. Virtual private networks. *IEEE Potentials 20*, 1 (2001), 11–15.

[13] KAHEEL, A., KHATTAB, T., MOHAMED, A., E ALNUWEIRI, H. Quality-of-service mechanisms in IP-over-WDM networks. *IEEE Communications Magazine 40*, 12 (dezembro de 2002), 38–43.

[14] SARADHI, C., GURUSARNY, M., E LUYING, Z. Differentiated QoS for survivable WDM optical networks. *IEEE Communications Magazine 42*, 5 (maio de 2004), S8–14.

[15] RAMAMURTHY, S., E MUKHERJEE, B. Survivable WDM Mesh Networks. Part I - Protection. In *Proc. IEEE INFOCOM* (março de 1999), pag. 744–751.

[16] RAMAMURTHY, S., E MUKHERJEE, B. Survivable WDM Mesh Networks. II. Restoration. In *Proc. IEEE Internation Conference on Communication* (junho de 1999), pag. 2023–2030.

[17] ZHANG, J., E MUKHERJEE, B. A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges. *IEEE Network 18*, 2 (abril de 2004), 41–48.

[18] MOHAN, G., E MURTHY, C. S. R. Lightpath Restoration in WDM Optical Networks. *IEEE Network 14*, 6 (2000), 24–32.

[19] GERSTEL, O., E RAMASWANI, R. Optical Layer Survivability: A Service Perspective. *IEEE Communications Magazine 38*, 3 (março de 2000), 104–113.

[20] GERSTEL, O., E RAMASWANI, R. Optical Layer Survivability - An Implementation Perspective. *IEEE JSAC 18*, 10 (outubro de 2000), 1885–1899.

[21] WANG, J., SAHASRABUDDHE, L., E MUKHERJEE, B. Path vs. Sub-Path vs. Link Restoration for Fault Management in IP-over-WDM Networks. *IEEE Communications Magazine 40*, 11 (novembro de 2002), 80–87.

[22] KODIALAM, M., E LAKSHMAN, T. Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks. In *Proc. IEEE INFOCOM* (abril de 2001), pag. 358–366.

[23] ZHENG, Q., E MOHAN, G. Protection Approaches for Dynamic Traffic in IP/MPLS-over-WDM Networks. *IEEE Communications Magazine 41*, 5 (maio de 2003), S24–29.

[24] YE, Y., ASSI, C., DIXIT, S., E ALI, M. A simple dynamic integrated provisioning/protection scheme in IP over WDM networks. *IEEE Communications Magazine 39*, 11 (novembro de 2001), 174–182.

[25] HUANG, C., SHARMA, V., OWENS, K., E MAKAM, S. Building reliable MPLS networks using a path protection mechanism. *IEEE Communications Magazine 40*, 3 (março de 2002), 156–162.

[26] SAHASRABUDDHE, L., RAMAMURTHY, S., E MUKHERJEE, B. Fault Management in IP-over-WDM Networks: WDM Protection vs. IP Restoration. *IEEE JSAC 20*, 1 (janeiro de 2002), 21–33.

[27] OU, C., ZHANG, H., E BMUKHERJEE. Sub-Path Protection for Scalability and Fast Recovery in Optical WDM Mesh Network. In *Proc. OFC* (março de 2002), pag. 495–496.

[28] ZHANG, J. Service Provision to Provide Per-Connetion-Based Availability Guarantee in WDM Mesh Network. In *Proc. OFC* (março de 2003), pag. 622–624.

[29] COLLE, D., MAESSCHALCK, S., DEVELDER, C., HEUVEN, P., GROEBBENS, A., CHEYNS, J., LIEVENS, I., PICKAVET, M., LAGASSE, P., E DEMEESTER, P. Data-Centric Optical Networks and Their Survivability. *IEEE JSAC 20*, 1 (janeiro de 2002), 100–09.

[30] KODIALAM, M., E LAKSHMAN, T. Dynamic routing of bandwidth guaranteed tunnels with restoration. In *Proc. IEEE INFOCOM* (março de 2000), pag. 902–911.

[31] MODARRESSI, A., E MOHAN, S. Control and management in next-generation networks: challenges and opportunities. *IEEE Communications Magazine 38*, 10 (outubro de 2000), 94–102.

[32] COCHENNEC, J. Activities on next-generation networks under Global Information Infrastructure in ITU-T. *IEEE Communications Magazine 40*, 7 (julho de 2002), 98–101.

[33] ALI, M. Shareability in optical networks: beyond bandwidth optimization. *IEEE Communications Magazine 42*, 2 (fevereiro de 2004), S11–15.

[34] BICUDO, M. D. D., M.MORAES, I., LAUFER, R. P., CUNHA, D. O., VELLOSO, P. B., E DUARTE, O. C. M. B. Protection and Minimal Interference in WDM Mesh Networks. In *12th International Conference on Telecommunications - ICT'2005, Cidade do Cabo, Africa do Sul* (2005).

[35] BICUDO, M. D. D., E DUARTE, O. C. M. B. Um Mecanismo de Proteção em Redes WDM em Malha. In *X Workshop de Gerência e Operação de Redes e Serviços - WGRS2005, Fortaleza, Brasil* (2005).

[36] SGI. *SGI - STL: Standard Template Library*. http://www.sgi.com/tech/stl/, 2005.

[37] AUSTERN, M. H. *Generic Programming and the STL: Using and Extending the C++ Standard Template Library*, primeira ed. Addison-Wesley Professional, 1998.

[38] EL-BAWAB, T., E JONG-DUG, S. Optical packet switching in core networks: between vision and reality. *IEEE Communications Magazine 40*, 9 (setembro de 2002), 60–65.

[39] RENAUD, M., MASETTI, F., GUILLEMOT, C., E BOSTICA, B. Network and system concepts for optical packet switching. *IEEE Communications Magazine 35*, 4 (setembro de 1997), 96–102.

[40] THEOPHILOPOULOS, G., KALYVAS, M., YIANNOPOULOS, K., VLACHOS, K., VARVARIGOS, E., E AVRAMOPOULOS, H. An alternative implementation perspective for the scheduling switch architecture. *IEEE Journal of Lightwave Technology 23*, 2 (fevereiro de 2005), 732–739.

[41] SHANKARANARAYANAN, N. Wavelength-routed optical networks. In *Conference Proceedings. IEEE Lasers and Electro-Optics Society Annual Meeting, 1994. LEOS '94* (outubro de 1994), pag. 107.

[42] BANERJEE, D., E MUKHERJEE, B. Wavelength-routed optical networks: linear formulation, resource budgeting tradeoffs, and a reconfiguration study. *IEEE/ACM Transactions on Networking 8*, 5 (outubro de 2000), 598–607.

[43] FAWAZ, W., AUDOUIN, B., BERDE, B., VIGOUREUX, M., DU-POND, M., E PUJOLLE, G. Service Level Agreement and Provisioning in Optical Networks. *IEEE Communications Magazine 42*, 1 (janeiro de 2004), 36–42.

[44] RAJAGOPALAN, B., LUCIANI, J., E AWDUCHE, D. IP over Optical Networks: A Framework. *Internet RFC 3717* (março de 2004). INFORMATIONAL.

[45] GREEN, P. Progress in optical networking. *IEEE Communications Magazine 39*, 1 (janeiro de 2001), 54–61.

[46] RAMAMURTHY, S., E MUKHERJEE, B. Fixed-alternate routing and wavelength conversion in wavelength-routed optical networks. In *IEEE GLOBECOM 98* (novembro de 1998), pag. 2295–2302.

[47] CHU, X., LI, B., E CHLAMTAC, I. Wavelength converter placement under different RWA algorithms in wavelength-routed all-optical networks. *IEEE Transactions on Communitacions 51*, 4 (abril de 2003), 607–617.

[48] AL-FUQAHA, A., CHAUDHRY, G., GUIZANI, M., E LABRADOR, M. Routing framework for all-optical DWDM metro and long-haul transport networks with sparse

wavelength conversion capabilities. *IEEE JSAC 22*, 8 (outubro de 2004), 1443–1459.

[49] CHU, X., LI, B., E CHLAMTAC, I. Wavelength converter placement under different RWA algorithms in wavelength-routed all-optical networks. *IEEE/ACM Transactions on Networking 51*, 4 (abril de 2004), 607–617.

[50] CHU, X., LIU, J., E ZHANG, Z. Analysis of sparse-partial wavelength conversion in wavelength-routed WDM networks. In *Proc. IEEE INFOCOM* (março de 2004), pag. 1363–1371.

[51] SHIRAGAKI, T., HENMI, N., KATO, T., FUJIWARA, M., SHIOZAWA, M. M. T., E SUZUKI, S. Optical cross-connect system incorporated with newly developed operation and management system. *IEEE JSAC 16*, 7 (setembro de 1998), 1179–1189.

[52] CAO, X., ANAND, V., E QIAO, C. Multilayer versus single-layer optical cross-connect architectures for waveband switching. In *Proc. IEEE INFOCOM* (março de 2004), pag. 2295–2302.

[53] CAO, X., ANAND, V., E QIAO, C. Waveband switching in optical networks. *IEEE Communications Magazine 41*, 4 (abril de 2003), 105–112.

[54] HARAI, H., MURATA, M., E MIYAHARA, H. Performance analysis of wavelength assignment policies in all-optical networks with limited-range wavelength conversion. *IEEE JSAC 16*, 7 (setembro de 1998), 1051–1060.

[55] OZDAGLAR, A., E BERTSEKAS, D. Routing and wavelength assignment in optical networks. *IEEE/ACM Transactions on Networking 11*, 2 (abril de 2003), 259–272.

[56] SAAD, M., E LUO, Z.-Q. On the routing and wavelength assignment in multifiber WDM networks. *IEEE JSAC 22*, 9 (setembro de 2004), 1708–1717.

[57] YOO, Y., AHN, S., E KIM, C. S. Adaptive routing considering the number of available wavelengths in WDM networks. *IEEE JSAC 21*, 8 (outubro de 2003), 1263–1273.

[58] XIN, C., YE, Y., WANG, T., E DIXIT, S. On an IP-Centric Optical Control Plane. *IEEE Communications Magazine 39*, 9 (novembro de 2001), 88–93.

[59] TO, M., E NEUSY, P. Unavailability Analysis of Long-Haul Networks . *IEEE JSAC 12* (janeiro de 1994), 100–09.

[60] ZHANG, J., ZHU, K., ZANG, H., E MUKHERJEE, B. A new provisioning framework to provide availability-guaranteed service in WDM mesh networks. In *Proc. IEEE Internation Conference on Communication* (maio de 2003), vol. 2, pag. 1484–1488.

[61] MANNIE, E., E PAPADIMITRIOU, D. Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS). *Internet Draft* (abril de 2005). INFORMATIONAL.

[62] PAPADIMITRIOU, D., E MANNIE, E. Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration). *Internt Draft* (abril de 2005). INFORMATIONAL.

[63] LANG, J. P., RAJAGOPALAN, B., E PAPADIMITRIOU, D. Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification. *Internet Draft* (abril de 2005). INFORMATIONAL.