



Sobrevivência a falhas para conexões IP sobre WDM em redes ópticas baseadas na topologia em malha

Dayse Gonçalves Correia¹, Wilton Bezerra de Fraga², Glendo de Freitas Guimarães³, Jose Wally Mendonça Menezes⁴

¹Graduanda em Engenharia de Telecomunicações – IFCE. e-mail: daysecorreia@gmail.com

²Doutor em Engenharia de Teleinformática – IFCE. e-mail: wilton.fraga@ifce.edu.br

³Doutor em Engenharia de Teleinformática – IFCE. e-mail: glendofreitas@ifce.edu.br

⁴Doutor em Física – IFCE. e-mail: wally@ifce.edu.br

Resumo: o objetivo deste trabalho é analisar os mecanismos de proteção convencionais, proteção dedicada e proteção compartilhada, na camada referente à multiplexação por divisão de comprimento de onda (WDM), como soluções de provisão para sobrevivência a falhas em redes ópticas com topologia em malha utilizadas no tráfego da tecnologia IP sobre WDM (*Internet Protocol over Wavelength Division Multiplexing*) além de verificar a questão da disponibilidade da rede óptica, mostrando o impacto da conectividade e da reversibilidade na rede referente aos mecanismos empregados. A relevância do tema, esta ainda centrada na crescente demanda e dependência por largura de banda o que tem contribuído para o surgimento de novas tecnologias com promessas e metas de atender satisfatoriamente a demanda da sociedade. Neste contexto, a sobrevivência a falhas em redes ópticas é tema essencial no projeto de manutenção e operação destas redes.

Palavras-chave: IP sobre WDM, redes ópticas, sobrevivência a falhas

1. INTRODUÇÃO

A crescente demanda por largura de banda, capaz de suportar dados, voz e vídeo em aplicações interativas nas redes de telecomunicações, tem contribuído para o surgimento de novas tecnologias cada vez mais extraordinárias, que chegam a todo instante com promessas para atender satisfatoriamente a demanda exigida. Uma das propostas tecnológicas mais investidas para se atingir esta demanda é o IP sobre WDM, que atualmente é capaz de transportar links de até 100Gbps.

Atualmente, a maioria das redes ópticas implantadas utilizam o ATM (*Asynchronous Transfer Mode*) e o SDH (*Synchronous Digital Hierarchy*) como tecnologias de transporte dos dados. Estas tecnologias fundamentam-se em conexões de banda fixa, geralmente estabelecidas de forma manual. Um modelo mais adequado às necessidades das aplicações atuais é o modelo multicamadas IP/GMPLS (*Generalized Multiprotocol Label Switching*) sobre WDM. O WDM é uma tecnologia que permite melhor utilização da banda passante das fibras ópticas. Com esta tecnologia, dentro de uma única fibra consegue-se estabelecer diversos canais ópticos que operam em comprimentos de onda distintos, atingindo taxas de transmissão da ordem de 100 Gbps. Cada canal óptico permite que dados sejam transmitidos utilizando diferentes esquemas de modulação e com taxas distintas uma das outras. Por sua vez, o uso do IP encapsulado no protocolo GMPLS, proporciona o estabelecimento dinâmico destes canais, inserindo o conceito de ASON (*Automatic Switched Optical Network*). A inserção do MPLS (*Multiprotocol Label Switching*), contido no GMPLS, adiciona importantes funcionalidades à rede, pois suas conexões LSP (*Label Switched Path*) possibilitam fornecer engenharia de tráfego, de VPN (*Virtual Private Network*) e de QoS (*Quality of Service*).

Conforme as redes de *backbone* óptico migraram da topologia em anel, comumente implantada em redes de transporte SDH, para a topologia em malha, que objetiva resolver problemas de escalabilidade e de redundância excessiva, as deficiências de implementação de sobrevivência em tal topologia tornaram-se evidentes. A simplicidade nas decisões de envio da



topologia em anel favorece a prática da sobrevivência, pois há apenas duas alternativas para o envio de dados. Entretanto, as redes em malha disponibilizam múltiplos caminhos e precisam de estabelecimento de conexões para transmitir dados da origem ao destino. Então, desde que esta tendência de migração topológica se consolidou, estudos relacionados à sobrevivência em redes em malha como meio de transporte o WDM se desenvolveram visando solucionar tal problema que afeta principalmente a disponibilidade de conexões em redes ópticas. Ligada a esta tendência, há também a consolidação da fabricação de comutadores ópticos. Uma rede contendo comutadores ópticos envia os fluxos de dados sem precisar de conversões óptico-eletrônico, um dos maiores limitantes da taxa de transmissão em redes ópticas. Com isso, a introdução da tecnologia de comutadores ópticos permite uma largura de banda que não era possível anteriormente em conexões ópticas.

A tecnologia WDM, que proporciona a multiplexação de vários canais ópticos em uma única fibra, torna então a rede mais sensível a falhas, pois a interrupção de apenas um cabo óptico interfere na disponibilidade do serviço oferecido por diversas conexões. O quadro piora quando incorpora-se o tráfego de pacotes IP sobre WDM, pois o tempo de recuperação a falhas pode superar a ordem de 100ms, segundo Gerstel. Neste contexto, a sobrevivência a falhas em redes ópticas é essencial no projeto de manutenção e operação destas redes. A sobrevivência a falhas é a capacidade de uma rede não interromper as conexões de seus clientes quando ocorrer uma falha de algum recurso da rede, por exemplo: ruptura de cabo óptico, defeito de placa do equipamento, falta de alimentação da estação, entre outros.

Conforme Lang et al, nas redes ópticas com topologia em malha, os mecanismos que fornecem sobrevivência a falhas são classificados, basicamente, em dois tipos: a proteção, que pré-computam e pré-allocam os recursos para a recuperação; e a restauração, que computam os recursos para a recuperação de forma reativa, isto é, apenas quando ocorre a falha. Aplicando estes mecanismos de sobrevivência a falhas em uma rede IP sobre WDM, as opções de implementações distintas para a sobrevivência aumenta substancialmente, pois agora estes mecanismos podem ser utilizados tanto na camada WDM, oferecendo recuperação nos canais ópticos, como na camada IP, oferecendo a recuperação das conexões GMPLS. Muitos autores afirmam que a introdução desta plataforma de controle torna estas redes robustas, as ASON, e mais indicadas para implementar sobrevivência a falhas. Afirmam também, que este tipo de rede é considerada a próxima geração de redes, denominada de redes NGN (*Network Next Generation*), pois satisfazem os requisitos das aplicações mais exigentes e dinâmicas.

Portanto, a pesquisa na área de IP sobre WDM em relação à sobrevivência de redes ópticas em malha abrange diversos temas que incluem a sobrevivência na camada óptica, na camada IP, análises comparativas entre proteção versus restauração, propostas de mecanismos de recuperação com um modelo multicamadas, entre outros. Este trabalho visa analisar as vantagens e desvantagens dos mecanismos de sobrevivência a falhas de proteção, em redes ópticas IP sobre WDM na topologia em malha utilizando o protocolo de controle e sinalização GMPLS.

2. MATERIAL E MÉTODOS

Muitos dos serviços que funcionam 24 horas não permitem longos períodos de manutenção ou reconfiguração da rede. Portanto, a falha de um enlace óptico pode ocasionar a interrupção de dezenas de canais ópticos e isto pode constituir a perda de uma grande quantidade de dados e a insatisfação de centenas ou milhares de usuários. Segundo Gerstel, em média, a ruptura de cabos 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. Diante desta situação, a pesquisa sobre a questão da sobrevivência a falhas em conexões IP sobre WDM baseado na topologia em malha torna-se crucial para garantir uma boa disponibilidade do serviço em tráfego pela rede óptica, inúmeras teorias e propostas de mecanismos para tal função têm surgido. Algumas propostas visam mais a questão do gerenciamento e controle por software, outros priorizam o hardware, como a pré-alocação de recursos, mas as que vingam na prática é a mescla destas.



De acordo com o Ramaswani, as redes ópticas necessitam implementar mecanismos de recuperação para garantir que falhas de cabos ópticos ou equipamentos sejam recuperadas de maneira rápida e eficiente, atingindo, assim, uma disponibilidade de até 99,999%, 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. As propostas são complexas, pois objetivam a proteção tanto na camada WDM como na camada IP, esta última requer garantias de envio mais criteriosas o que limita a taxa de transmissão, proporcionando estudos de protocolos que dinamizem o processo em tal camada dentro dos parâmetros de QoS adotados na rede, daí o GMPLS. A proteção na camada WDM é mais tranquila, principalmente com o surgimento da tecnologia de chaves ópticas, do ponto de vista que basta associar o enlace a um canal óptico e a rede estar devidamente nivelada, a parte complicada fica para os algoritmos de roteamento e associação de lambda (*Routing and Wavelength Assignment - RWA*).

Atualmente, a maioria das redes ópticas transporta a tecnologia SDH, utilizando anéis ópticos que reservam uma segunda fibra para proteção. Quando ocorre uma falha no canal óptico, a comutação para a fibra reserva se efetua de forma simples e rápida. O tempo de recuperação de falhas nestas redes é da ordem de 50ms, conforme Gerstel. Um dos grandes objetivos nas pesquisas sobre sobrevivência a falhas em redes ópticas IP sobre WDM é chegar em um tempo de recuperação comparável ao da tecnologia SDH. Estas pesquisas visam então a oferta de QoS e, como consequência, a definição do contrato de nível de serviço SLA (*Service Level Agreement*) a ser assinado com o cliente e garantido pela operadora.

Este artigo é embasado em estudos bibliográficos focado nos mecanismos de proteção (*priori*) em redes ópticas trafegando IP sobre WDM, analisando o impacto da conectividade e da reversibilidade da rede, ou seja, sua capacidade de sobrevivência a falhas.

O impacto da conectividade da rede será realizado determinando-se o impacto nos parâmetros de desempenho da rede. 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, conforme Zhang. Já a reversibilidade está relacionada às comutações onde a disponibilidade da rede depende do tempo necessário para realizá-las. Um mecanismo de proteção é dito como reversível se, após a recuperação de um enlace em falha, as conexões afetadas por tal falha voltam ao seu canal original ou primário. Se as comutações forem realizadas em um curto período de tempo, a disponibilidade não será tão afetada. Porém, se as reconfigurações das redes ópticas são lentas, os comutadores totalmente ópticos não apresentam um hardware com tempo de resposta baixo o suficiente, conseqüentemente a comutação entre canais ópticos geralmente ocasiona desordenação na entrega dos pacotes ao destino e também na indisponibilidade do serviço por um período de tempo. Então, em redes onde se pretende garantir um alto índice de disponibilidade, esta comutação de canais deve ser evitada.

Para que as novas redes ópticas com tecnologia IP sobre WDM possuam tempo de recuperação de falhas da ordem de grandeza que o das redes SDH (50ms) os mecanismos de proteção devem ser na camada WDM por serem mais rápidos que os mecanismos de recuperação na camada IP. Por este motivo, este artigo visa estudar mecanismos de recuperação rápidos e, portanto, apenas os mecanismos de proteção na camada WDM são evidenciados.

3. RESULTADOS E DISCUSSÃO

O funcionamento da proteção WDM dedicada 1:1 e compartilhada 1:N em uma rede de topologia em malha é ilustrado na figura 1 e 2, respectivamente. Para comparar estes mecanismos, apresenta-se a questão da conectividade através de uma análise matemática definida por Zhang e a questão da reversibilidade através de um estudo analítico em relação a topologia exemplificada nas ilustrações.

Nas figuras 1 e 2, cada círculo representa um nó da rede, ou seja, um equipamento de rede instalado em uma localidade qualquer e os segmentos que os conectam representam os enlaces da rede, os segmentos contínuos mostram a rota primária e os tracejados mostram a rota



secundária. Através destas figuras, constatam-se de forma simples e didática as diferenças no comportamento de cada mecanismo.

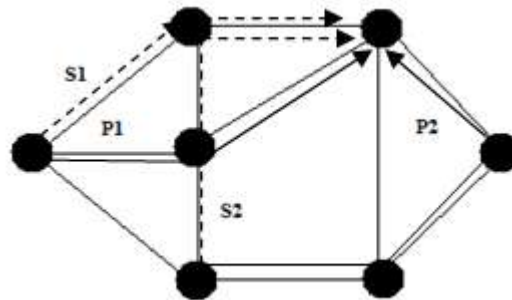


Figura 1 – Proteção 1:1 ou dedicada

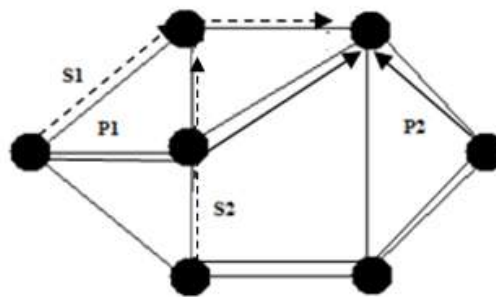


Figura 2 – Proteção 1:N ou compartilhada

O esquema de proteção mais simples é a proteção 1:1, também conhecida proteção dedicada. Nela se estabelece dois canais ópticos disjuntos para cada conexão: um canal óptico primário (P) e um canal óptico secundário (S), canal proteção. Então, no momento em que há uma solicitação 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 estabelecida. Portanto, embora simples, este mecanismo de proteção não é eficiente, pois reserva para proteção muitos recursos da rede ao duplicar os recursos para uma conexão óptica. Conseqüentemente, a metade dos recursos da rede é reservada para proteção e isto ocasiona uma probabilidade de bloqueio excessivamente alta. A probabilidade de bloqueio é um parâmetro que expressa a eficiência de utilização dos recursos da rede. Então, um mecanismo de sobrevivência ineficiente apresenta uma rede com alta probabilidade de bloqueio. Entretanto, atingir maior eficiência da rede aumentando o compartilhamento de recursos de proteção entre conexões traz uma perda na disponibilidade das conexões.

No caso, a proteção 1:N reaproveita os recursos do canal secundário S2 para o canal secundário S1. Para aumentar a eficiência do uso dos recursos da rede, a proteção compartilhada é uma alternativa mais eficiente do que a proteção dedicada. Esta proteção permite que dois ou mais canais de proteção compartilhem lambdas, desde que seus canais primários satisfaçam os requisitos de grupo de risco de falha de enlace, o SRLG (*Shared Risk Link Group*). A SRLG determina que canais de proteção podem compartilhar lambdas em um enlace se os canais primários de cada conexão não pertencerem ao mesmo SRLG, e, portanto, a probabilidade de falharem simultaneamente é muito baixa. Do ponto de vista prático, conexões ópticas α e β



pertencem ao mesmo SRLG quando o conjunto dos enlaces primários de α , $L_\alpha = \{\alpha1, \alpha2, \alpha3\}$ e de β , $L_\beta = \{\beta1, \beta3, \beta4\}$, apresentam pelo menos um enlace em comum. Na figura 3 as linhas tracejadas e pontilhadas representam as conexões α e β , respectivamente. Os conjuntos de grupos enlaces $L_\alpha = \{11, 13, 14\}$ e $L_\beta = \{12, 14\}$ têm em comum o enlace 14, 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.

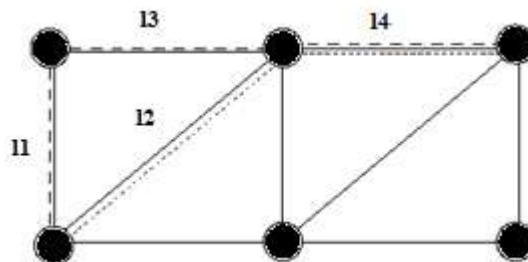


Figura 3 – Grupo de risco de falha de enlace

A proteção 1:1, por sua vez, aloca desnecessariamente um novo lambda. Este comportamento da proteção dedicada ocasiona uma alta probabilidade de bloqueio, pois o estabelecimento das futuras conexões será comprometido devido a menor quantidade de recursos disponíveis.

A probabilidade bloqueio está intimamente relacionada em duas questões triviais para a sobrevivência a falhas, conseqüentemente a disponibilidade do serviço: a conectividade e a reversibilidade. Uma rede de maior conectividade, ou seja, que apresente maior conectividade entre seus nós, permite maior diversidade de rotas e rotas com um menos saltos. Portanto, uma rede de maior conectividade reflete em uma menor probabilidade de bloqueio nas conexões configuradas. Porém, deve-se considerar 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 canais ópticos por nó. Tomando o exemplo das figuras 1 e 2, proteção dedicada tem conectividade de fator 2, pois temos 9 enlaces configurados usando 9 nós $((2 \times 9)/9)$, já na proteção compartilhada tem conectividade de fator 1.78 $((2 \times 8)/9)$, pois ao compartilhar um enlace, a rede fica configurada com 8 enlaces usando os mesmo 9 nós. Ou seja, neste caso, a proteção compartilhada obteve uma conectividade menor.

Em relação à questão da reversibilidade, para mecanismos de proteção dedicados a reversibilidade não é um fator preponderante, pois o canal secundário não é compartilhado. No entanto, nos mecanismos de proteção compartilhada há enlaces dos canais secundários que são compartilhados e isto pode influir no desempenho. A não-reversibilidade prejudica a disponibilidade das conexões, principalmente quando o mecanismo compartilha recursos. Em uma rede que utiliza proteção compartilhada não-reversível, o canal secundário de uma conexão que foi lesada por falhas não é liberado até que a desconexão seja efetuada. Esta ocupação desnecessária de recursos, aliada à ocorrência de uma falha, mesmo que após a recuperação da primeira falha, pode acarretar na indisponibilidade de uma conexão que compartilhava estes recursos da rede, pois enquanto esta conexão não for liberada, as conexões que compartilham recursos com ela não poderão utilizar o canal proteção. Nesta situação, além da desnecessária indisponibilidade do canal secundário, existe ainda a inatividade do canal primário, pois este recurso não é compartilhado. Portanto, a reversibilidade é primordial para proteção do tipo compartilhada, visto que vários enlaces podem utilizar a mesma via como canal secundário.



4. CONCLUSÕES

As redes ópticas IP sobre WDM com topologia em malha é considerado por muitos autores o modelo mais apropriado para as necessidades atuais de demanda de tráfego. Esta opinião é enfatizada neste artigo ao analisar os mecanismos de proteção na camada WDM para provisão de sobrevivência a falhas em redes ópticas. Foram estudados os mecanismos mais utilizados de proteção, dedicada e compartilhada.

Os resultados mostram que a disponibilidade é bastante influenciada pela configuração dos mecanismos de proteção utilizados nos enlaces da rede, ou seja, nas conexões. Quanto maior o número de conexões na rede maior é o impacto de uma falha na disponibilidade. Os exemplos referentes à conectividade foram realizados com a finalidade de comparar o desempenho dos mecanismos de proteção para diferentes níveis de conectividade de rede. Uma conectividade maior permite uma utilização mais eficiente dos enlaces e, portanto, uma menor probabilidade de bloqueio, pois possuem mais caminhos alternativos da origem ao destino e, conseqüentemente, os canais ópticos utilizam uma maior diversidade de enlaces. O mecanismo de proteção dedicada possui maior conectividade, porém requer mais recursos da rede e dependendo do tamanho da rede, do número de nós, pode ser economicamente inviável.

Em relação à reversibilidade, foi mostrado primeiramente que a implementação de mecanismos não-reversíveis reflete num compromisso maior da disponibilidade da rede. A reversibilidade é crucial para mecanismos de proteção compartilhada, pois duas ou mais conexões podem utilizar um mesmo enlace, SLRG, como canal secundário, já as conexões com proteção dedicada são menos impactadas.

REFERÊNCIAS

ABELÉM, A. **Difusão seletiva em inter-redes IP baseadas em redes ópticas**. Tese de doutorado. Departamento de Informática. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2003.

GERSTEL, O. e RAMASWANI, R. *Optical layer survivability: a service perspective*. IEEE Communications Magazine, 2000.

LANG, J. P., RAJAGOPALAN, B., e PAPADIMITRIOU, D. *Generalized Multi-Protocol Label Switching (GMPLS) recovery functional specification*. Internet Draft, 2005.

NORONHA, T. F. D. **Algoritmos para problemas de otimização aplicados a roteamento e atribuição de comprimentos de onda**. PhD thesis. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2009.

PATROCINIO, Z. K. G. **Planejamento de topologia virtual com combinação de tráfegos em redes ópticas multiplexadas por divisão de comprimento de onda**. PhD thesis, Minas Gerais: UFMG, 2005.

PEDRO, J. **Encaminhamento e atribuição de comprimento de onda em redes WDM**. Tese de Mestrado. Lisboa: Instituto Superior Técnico, 2004.

PERROS, H. G. *Connection-oriented networks: SONET/SDH, ATM, MPLS and optical networks*. Reino Unido: John Wiley & Sons Ltd, 2005.

RAMASWANI, R., e SIVARAJAN, K. *Optical networks: a practical perspective*, 2 ed. Morgan Kaufmann Publ., 2002.



RESENDO, L. C. **Contribuições para o projeto de grooming de tráfego sobre redes ópticas WDM.** PhD *thesis*. Espírito Santo: UFES, 2008.

SANTOS, F. A. **Otimização multi-objetivo aplicada à alocação dinâmica de rotas em redes de telecomunicações.** *Master's thesis*. Minas Gerais: UFMG, 2009.

SOARES, A. C. B. e GIOZZA, W. F. **Avaliação de desempenho de algoritmos para alocação dinâmica de comprimentos de onda em redes ópticas transparentes.** Curitiba: Simpósio Brasileiro de Redes de Computadores, 2004.

SOARES A., MARANHÃO J., GIOZZA W. e CUNHA P. ***First load priority: a wavelength converter placement scheme for optical networks with sparse-partial wavelength conversion.*** Curitiba: Simpósio Brasileiro de Redes de Computadores – SBRC, 2006.

SOCIEDADE DA INFORMAÇÃO NO BRASIL, **Infra-estrutura avançada e novos Serviços.** São Paulo: Livro verde, 2000.

ZHANG, J., ZHU, K., ZANG, H., E MUKHERJEE, B. ***A new provisioning framework to provide availability-guaranteed service in WDM mesh networks.*** Vol. 2. In *Proc. IEEE International Conference on Communication* , 2003.