Instituto de Engenharia de Sistemas e Computadores de Coimbra
Institute of Systems Engineering and Computers INESC - Coimbra

Luísa Jorge
Teresa Gomes

Recuperação em redes MPLS
Uma resenha de esquemas de recuperação

No.10 2005

ISSN: 1645-2631

Instituto de Engenharia de Sistemas e Computadores de Coimbra
INESC - Coimbra
Rua Antero de Quental, 199; 3000-033 Coimbra; Portugal
www.inescc.pt

Recuperação em redes MPLS – Uma resenha de esquemas de recuperação

Luísa Jorge[1,3] e Teresa Gomes[2,3]

[1]Escola Superior de Tecnologia e de Gestão do
Instituto Politécnico de Bragança
Campus de St[a] Apolónia, 5301-857 Bragança, Portugal

[2]Departamento de Engenharia Electrotécnica e de Computadores da FCTUC,
Pólo 2 da Univ. Coimbra, 3030-290 Coimbra, Portugal

[3]INESC-Coimbra, Rua Antero de Quental 199,
3000-033 Coimbra, Portugal.

e-mail: ljorge@inescc.pt, teresa@deec.uc.pt,

1 de Julho de 2005

Resumo

Uma rede *MultiProtocol Label Switching* (MPLS) é constituída por recursos que possuem graus de fiabilidade diferentes. Perante falhas nesses recursos, e para fornecer serviços fiáveis aos pedidos solicitados, o MPLS precisa de empregar um conjunto de procedimentos (detecção, notificação e recuperação da falha) para garantir uma protecção apropriada para o tráfego transportado nos diversos *Label Switched Path*s (LSPs).

Numa rede MPLS, quando ocorre uma avaria no LSP primário o esquema de recuperação deve redireccionar o tráfego para um caminho de recuperação que contorne a avaria. São descritos os princípios de recuperação que podem ser usados nas redes MPLS de acordo com o *Request For Comments* (RFC) 3469 de Sharma et al. (2003). De acordo com esse RFC os dois modelos de recuperação básicos usados para redireccionar o tráfego, após uma falha, são a *recuperação por reencaminhamento* e a *protecção por comutação*.

Na protecção por comutação a recuperação é rápida porque o caminho de recuperação é pré-estabelecido. No entanto um dos problemas deste modelo de recuperação é ser incapaz de tratar falhas simultâneas no caminho de trabalho e no caminho de recuperação. Na recuperação por reencaminhamento os recursos são utilizados de uma forma mais eficiente, mas a recuperação é geralmente lenta. Um fornecedor de serviços de rede deve poder aplicar esquemas de recuperação diferentes de acordo com as características de Qualidade de Serviço dos fluxos de tráfego (classes de serviço) que transporta.

Este trabalho começa com uma descrição detalhada dos aspectos relativos à recuperação em redes MPLS. Essa descrição é seguida de uma resenha de diferentes esquemas propostos para recuperação de falhas, começando por modelos de protecção por comutação e seguidamente referindo modelos de recuperação por reencaminhamento. São apresentadas as características mais relevantes do funcionamento de cada um dos esquemas revistos e é analisada a sua aplicabilidade em redes reais. Finalmente é apresentado um resumo comparativo das características dos esquemas anteriormente descritos.

Conteúdo

1 Introdução

Os *routers* de uma rede MPLS são designados por *Label Switching Routers* (LSRs). Um pacote de dados ao entrar numa rede MPLS é classificado, e de acordo com essa classificação é atribuído a uma *Forwarding Equivalence Class* (FEC). Cada FEC é identificada em cada LSR através de uma etiqueta. As redes MPLS usam a técnica conhecida por comutação de etiquetas (*label switching*) para encaminhar os dados através da rede. Num dado *router* todos os pacotes de uma FEC são encaminhados do mesmo modo[1].

Considerando que os LSRs R_u e R_d concordaram em associar a etiqueta L à FEC F, para pacotes enviados de R_u para R_d então, R_u é o LSR a montante (*upstream*), e R_d é o LSR a jusante (*downstream*). O caminho seguido pelos pacotes de uma FEC é designado por *Label Switched Path* (LSP).

Na figura 1 aparecem representados vários pacotes (pertencentes a duas FECs) com as respectivas etiquetas. Na figura são também ilustrados os dois LSPs correspondentes às duas FECs.

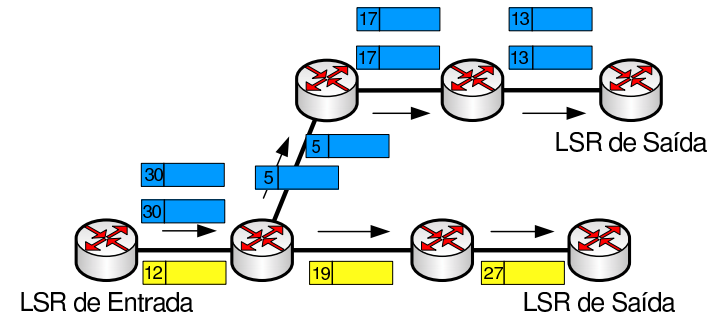

Figura 1: Etiquetas e LSPs.

A recuperação baseada no MPLS refere-se à capacidade de efectuar um restabelecimento rápido e completo do tráfego afectado por uma falha numa rede com MPLS. Nessas redes pretende-se garantir serviços de alta fiabilidade e disponibilidade. Perante falhas, o fornecedor de serviços pretende oferecer uma recuperação rápida e que utilize o mínimo de recursos possíveis. Para tal, têm sido vários os esquemas propostos para oferecer tolerância a falhas em redes MPLS. No entanto, deve ser lembrado que os objectivos propostos são contraditórios. Em geral a eficiência no uso de recursos impede tempos de recuperação pequenos e vice-versa.

Este relatório encontra-se organizado da forma seguinte. Na secção 2 são revistos com algum detalhe aspectos relativos à recuperação de falhas em redes MPLS, e encontra-se dividida em três subsecções. Na primeira vão ser descritos os princípios de recuperação que podem ser usados em redes MPLS, na segunda são mostradas as várias fases dos três ciclos do processo de recuperação do MPLS e por último na terceira vão ser apresentados alguns critérios que podem ser utilizados na comparação de esquemas de recuperação. Na secção 3 são revistos esquemas de recuperação de falhas em redes MPLS, e encontra-se dividida em três subsecções. Na primeira são revistos esquemas que usam o modelo protecção por comutação, na segunda os

[1] São encaminhados no mesmo caminho a menos que seja utilizado encaminhamento multi-caminho (*multi-path*, ver Rosen et al., 2001).

que usam o modelo de recuperação por reencaminhamento, e finalmente na terceira dá-se uma visão conjunta de todos os esquemas revistos salientando as características mais relevantes. Na secção 4 são apresentadas algumas conclusões e sugeridas propostas de trabalho futuro.

2 Recuperação em redes MPLS

As linhas orientadoras relativas à recuperação em redes MPLS foram já objecto de normalização, processo do qual resultou o RFC 3469 (Sharma et al., 2003). A descrição que apresentamos nesta secção segue em geral, esse RFC.

Todas as falhas que podem ocorrer numa rede MPLS são falhas em ramos (o corte de uma fibra ou a falha de um interface de um LSR) ou falhas em nós (a falha no *software*, a falha da alimentação ou uma falha planeada do LSR). Como consequência de uma destas falhas pode resultar a falha de um ou vários LSPs.

Sempre que ocorrer uma falha num LSP o esquema de recuperação deve fazer com que o tráfego seja redireccionando para um caminho que contorne a avaria, de forma que a avaria seja o menos perceptível possível.

O LSP que o tráfego segue antes de ocorrer a falha de um nó ou de um ramo (ou mesmo falhas concorrentes) é designado por **caminho de trabalho**, sendo também frequentes as designações **caminho activo**, **caminho primário** ou mesmo **caminho protegido**. O caminho que o tráfego passa a seguir, após a ocorrência da falha pode ser designado por **caminho de recuperação**, **caminho de *backup***, **caminho alternativo** ou ainda por **caminho de protecção**.

O caminho de recuperação pode ser um **caminho de recuperação equivalente** ou um **caminho de recuperação limitado** conforme os recursos reservados garantam ou não a mesma qualidade de serviço, respectivamente.

De acordo com o RFC Sharma et al. (2003) os dois modelos de recuperação básicos usados para redireccionar o tráfego, após a falha, são **recuperação por reencaminhamento** (*rerounting*) e **protecção por comutação** (*protection switching*).

Estes dois modelos diferem basicamente na altura em que é estabelecido o caminho de recuperação, depois ou antes da falha ser detectada.

Embora os esquemas de recuperação de tráfego sigam, em geral, um dos dois modelos de recuperação, ambos podem ser utilizados simultaneamente.

O mecanismo que faz com que o tráfego seja redireccionado do caminho de trabalho para o caminho de protecção (ou caminhos de recuperação), quando ocorre uma falha, é designado por ***switchover***. O LSR em que é feito o redireccionamento é designado por ***Path Switch LSR* (PSL)**. O PSL pode simplesmente duplicar o tráfego, enviando-o simultaneamente através do caminho de trabalho, e do caminho de recuperação. Por seu lado o LSR que recebe o tráfego do caminho de recuperação e funde esse tráfego de volta para o caminho de trabalho é designado ***Path Merge LSR* (PML)**. Os LSRs que se encontram entre o PSL e o PML, tanto no caminho de trabalho como no caminho de recuperação, são referidos por **LSRs intermédios**.

Além do que foi referido anteriormente, o mecanismo de *switchover*, também designa o processo de transferência do tráfego do caminho de recuperação para um ou mais caminhos de trabalho óptimos. Então, de uma forma mais genérica, o mecanismo de *switchover* designa a operação de redireccionar o tráfego de um dado caminho para um ou mais caminhos alternativos. Por outro lado, o processo de repor o tráfego que seguia um ou mais caminhos de recuperação, de volta no caminho de trabalho original é designado por ***switchback***.

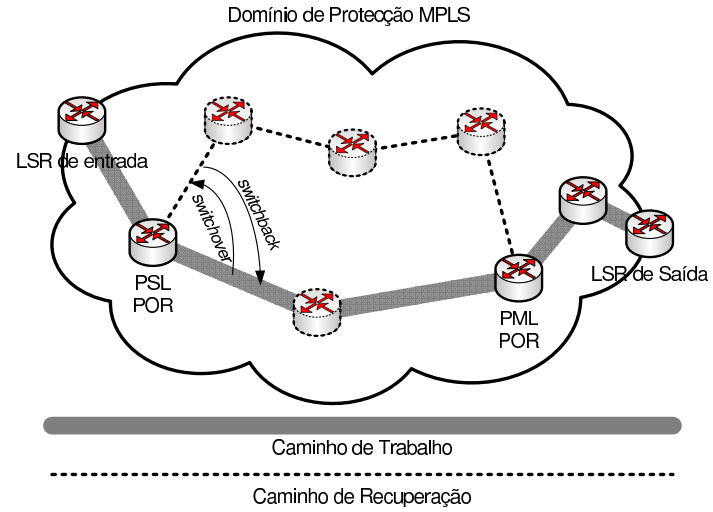

Figura 2: Rede que exemplifica alguns dos conceitos básicos.

A figura 2 ilustra alguns dos conceitos definidos anteriormente. Note que, embora na figura o PSL não seja o LSR de entrada e o PML não seja o LSR de saída, essas situações podem ocorrer. No caso do LSR de saída ser o PML então deve ter como função passar o tráfego aos protocolos das camadas superiores. Na figura aparece ainda a designação ***Point of Repair* (POR)** que é o LSR que faz a recuperação do LSP. O POR pode ser o PSL ou o PML dependendo do esquema de recuperação utilizado, no entanto, o mais comum é ser o PSL.

Se o LSR que detecta a falha num caminho de trabalho não tiver capacidade de fazer a recuperação deve notificar o POR. Para fazer essa notificação utiliza um sinal designado por ***Fault Indication Signal* (FIS)**. Um FIS é enviado por cada LSR intermédio para o seu vizinho a montante ou a jusante[2] até chegar ao POR. Um FIS é transmitido periodicamente pelo LSR/LSRs próximo da falha durante um intervalo de tempo configurável, ou até que o LSR que o transmite receba uma confirmação do seu vizinho.

O LSR que detectou a falha num caminho de trabalho também detectará que a falha foi reparada e quando isso acontecer deve enviar uma notificação para o POR com essa informação. Um sinal que indica que uma falha no caminho de trabalho foi reparada designa-se por ***Fault Recovery Signal* (FRS)**. Tal como acontece com o FIS também o FRS é enviado por cada LSR intermédio para o seu vizinho a montante ou a jusante[2] até chegar ao POR. Um FRS também é transmitido periodicamente pelo LSR/LSRs próximo da falha durante um intervalo de tempo configurável, ou até que o LSR que o transmite receba uma confirmação do seu vizinho.

[2]Se um nó adjacente e a jusante de uma falha envia um FIS/FRS para jusante, tal não implica que o POR (do LSP afectado) esteja necessariamente a jusante da falha.

Geralmente a velocidade de *switchover* está directamente relacionada com a distância entre o ponto em que a falha é detectada e o ponto em que é feita a reparação.

Dependendo da localização do POR, no LSP que necessita ser reparado, assim o âmbito da recuperação pode ser **global** (centralizado) ou **local** (distribuído). Se a recuperação for global então o caminho de recuperação é estabelecido geralmente sempre pelo mesmo LSR do caminho de trabalho enquanto que se a recuperação for local é o LSR do caminho de trabalho que é mais próximo da falha que faz a recuperação.

2.1 Princípios de recuperação

Nesta secção são apresentados alguns dos princípios de recuperação que podem ser combinados para especificar esquemas de recuperação.

2.1.1 Instante em que se estabelece o caminho de recuperação

O caminho de recuperação pode ser estabelecido ao mesmo tempo que o caminho de trabalho ou apenas na altura em que a falha ocorre. Para estabelecer o caminho de recuperação, assim como o caminho de trabalho, deve ser utilizado um protocolo de sinalização que pode ser o protocolo *Resource Reservation Protocol with Traffic Engineering* (RSVP-TE) (RFC 3209 de Awduche et al. (2001)), o protocolo *Constraint-based Routing – Label Distribution Protocol* (CR-LDP) (RFC 3212 de Jamoussi et al. (2002)) ou outro protocolo adequado.

Na protecção por comutação o caminho de recuperação é pré-estabelecido antes da falha ser detectada no caminho de trabalho.

Na recuperação por reencaminhamento o caminho de recuperação é estabelecido, através de sinalização, depois de ter sido detectada uma falha no caminho de trabalho. Aqui o caminho de recuperação pode ser **pré-calculado** ou apenas **calculado quando ocorrer a falha**. Por um lado, os caminhos pré-calculados podem utilizar informação de toda a rede, mas poderão não resolver o problema de falhas múltiplas. Por outro lado, calcular o caminho de recuperação apenas quando a falha ocorrer pode conseguir resolver situações de falhas múltiplas mas à custa do aumento do tempo de recuperação.

Existe ainda uma terceira possibilidade: um LSP é estabelecido e o respectivo caminho de recuperação será seleccionado oportunamente entre LSPs que não foram inicialmente sinalizados com essa finalidade. Nesta situação intermédia, em que o caminho que vai ser utilizado como caminho de recuperação foi previamente estabelecido, mas que não foi estabelecido explicitamente para proteger o caminho de trabalho, diz-se que o caminho de recuperação é **pré-qualificado**.

2.1.2 Instante em que é feita a reserva de recursos

Os recursos que podem ser reservados são por exemplo a largura de banda, os *buffers* e a capacidade de processamento.

Pré-reservados Este tipo de reserva só é utilizado quando o caminho de recuperação é pré-

estabelecido. Neste tipo de reserva os recursos necessários, ao longo de todo o caminho de recuperação, são reservados na altura em que o caminho é estabelecido.

Dependendo da forma como os recursos reservados são usados antes de serem necessários, podem ser considerados os três subtipos seguintes:

- Recursos dedicados - Nesta situação os recursos do caminho de recuperação só podem ser utilizados para transportar o tráfego do caminho de trabalho. A protecção por comutação $1 + 1$ ("um mais um") é um exemplo deste subtipo. Neste tipo de protecção os recursos do caminho de recuperação ficam completamente reservados, e transportam uma cópia do tráfego transportado no caminho de trabalho. Neste subtipo a inteligência está no PML e não no PSL.
- É permitido tráfego extra - É o que acontece quando o caminho de recuperação só transporta o tráfego do caminho de trabalho quando este falha. Nos outros instantes, os recursos reservados podem ser utilizados por tráfego extra de baixa prioridade. Na protecção por comutação designada por $1:1$ ("um por um") mesmo se os recursos do caminho de recuperação forem pré-reservados, estes estão completamente disponíveis para serem utilizados temporariamente por tráfego de baixa prioridade. Só não podem ser utilizados por esse tráfego quando o caminho de recuperação precisa de ser utilizado pelo tráfego do caminho de trabalho devido à falha deste. Nesta situação o tráfego extra tem que ser deslocado para outros caminhos. Desta forma os recursos do caminho de recuperação são utilizados de uma forma mais eficiente. Note no entanto que na protecção por comutação $1:1$ não é obrigatória a existência de reserva.
- Recursos partilhados - São recursos de recuperação que são dedicados para serem utilizados por múltiplos recursos primários assumindo que estes não falham simultaneamente. Um exemplo deste subtipo de reserva é o caso em que há reserva de recursos na protecção por comutação do tipo $1:n$ ou $m:n$ ("m por n"). Note que também na protecção por comutação do tipo $1:n$ ou $m:n$ ("m por n") não é obrigatória a existência de reserva.

Reservados a pedido Aqui os recursos necessários ao estabelecimento do caminho de recuperação só são reservados depois da falha no caminho de trabalho ser detectada e notificada ao POR, mas antes do *switchover*.

2.1.3 Âmbito da recuperação

Topológico

1. Reparação Global

   Na reparação global, o caminho usado na recuperação de qualquer falha (nó ou ramo) do caminho de trabalho (ou segmento do caminho de trabalho) é sinalizado pelo LSR de ingresso do LSP em causa. Por esta razão, é geralmente considerável a distância entre o ponto em que a falha ocorre e o POR.

   Segundo Sharma et al. (2003), neste tipo de recuperação, a notificação da falha precisa ser feita através de um FIS. Se o método utilizado se baseasse na falha do teste de

continuidade do caminho (ver definição na sub-secção 2.1.4) haveria grandes custos em termos de tempos de recuperação, como Marzo et al. (2003) realçaram.

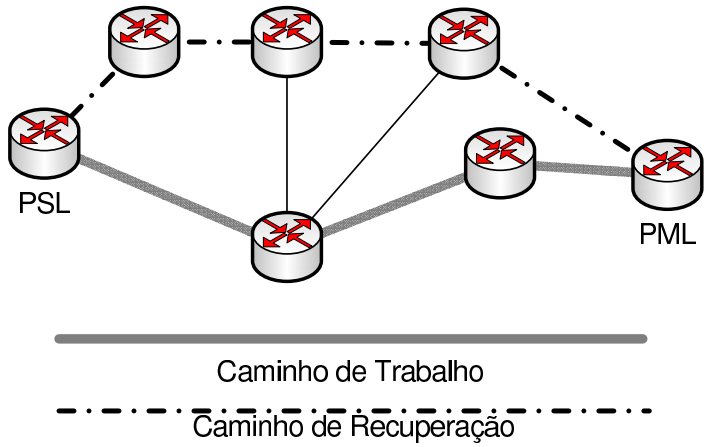

Figura 3: Exemplo do modelo de reparação global.

A figura 3 apresenta uma rede simples formada por 10 LSRs. É exemplificado nessa rede um caminho de trabalho e o caminho de recuperação respectivo. Em condições normais, o tráfego do LSR de entrada para o LSR de saída segue o caminho de trabalho. Quando ocorre uma falha o tráfego é redireccionado para o caminho de recuperação.

Nos esquemas que calculam o caminho de recuperação antes da falha ocorrer, se esse caminho não for completamente disjunto do caminho de trabalho pode acontecer que a avaria ocorra simultaneamente nos dois caminhos (mesmo tratando-se de uma falha isolada) ficando desse modo a recuperação comprometida. Note que o caminho de recuperação nunca consegue proteger contra falhas no LSR de entrada ou saída.

2. Reparação Local

   Na reparação (recuperação) local é o LSR que é imediatamente **a montante** ou **a jusante** à falha, que inicia a recuperação. O caminho de recuperação, estabelecido por esse LSR, é usado na recuperação da falha do ramo adjacente e/ou do nó vizinho do caminho de trabalho.

   Deste modo, neste método de recuperação, a falha é reparada pelo LSR mais próximo, conseguindo assim que o tempo de recuperação seja pequeno. Este tipo de recuperação possui geralmente a vantagem de ter tempos de recuperação menores que o método de reparação global.

   A figura 4 mostra uma rede que também ilustra um caminho de trabalho e um caminho de recuperação, mas agora para o caso da recuperação local. Com o caminho de recuperação representado apenas se consegue recuperar falhas que ocorram no ramo entre o PSL e o PML.

   Neste tipo de recuperação, o caminho de recuperação apenas precisa ser disjunto do caminho de trabalho num ramo particular, no caso de recuperação de ramos, ou num LSR particular, no caso de recuperação de nós.

   Se apenas algumas partes de um LSP devem ser protegidas (por serem menos fiáveis que as restantes), a utilização de protecção local conduz a um menor consumo de recursos

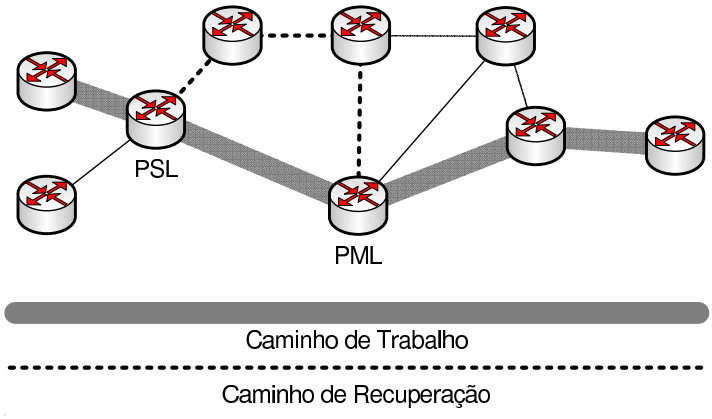

Figura 4: Exemplo do modelo de reparação local.

na rede do que a protecção global. Por outro lado se for utilizado este tipo de recuperação para proteger todo o LSP, ele possui a desvantagem, se for utilizado o modelo de protecção por comutação, da necessidade de configuração de vários caminhos de recuperação, além da provável ineficiência em termos de recursos. Este tipo de recuperação é geralmente ineficiente em termos de utilização de recursos pois o percurso que os pacotes seguem após uma falha é frequentemente mais comprido do que seria necessário (Vasseur et al., 2004; Menth et al., 2004).

É frequente encontrar esquemas de reparação local com o modelo de recuperação por reencaminhamento e de reparação global com protecção por comutação, como por exemplo nos esquemas comparados por Ahn et al. (2002), embora qualquer outra combinação seja possível como pode ser constatado pelo esquemas descritos na secção 3.

3. Reparação Multi-Camada

   Neste tipo de reparação permite-se que várias camadas sejam envolvidas na recuperação.

4. Outros âmbitos de recuperação ainda em termos topológicos

   Embora menos referidos na literatura, métodos que consideram a concatenação de vários domínios de protecção e a reparação com LSR de saída alternativo, têm actualmente grande importância, pois hoje em dia é comum um serviço atravessar várias redes que possivelmente utilizam esquemas de protecção diferentes.

   Com a concatenação de vários domínios de protecção pretende-se oferecer uma recuperação dos serviços extremo a extremo, embora os esquemas de recuperação dos vários domínios funcionem autonomamente. Devem ser utilizados vários pontos de ligação entre domínios para garantir que se o ponto de ligação falhar existem alternativas.

   Na reparação com LSR de saída alternativo o LSR de saída do caminho de recuperação deve ser um *router* que seja aceitável para encaminhar a FEC transportada pelo caminho de trabalho.

Granularidade da recuperação Outro aspecto da recuperação tem a ver com a quantidade de tráfego que precisa ser protegido: parte do tráfego de um caminho, todo o tráfego de um caminho ou o tráfego de um grupo de caminhos.

- Recuperação selectiva do tráfego – Este item diz respeito à possibilidade de proteger apenas uma fracção do tráfego de um caminho individual. Este aspecto é importante pois um mesmo caminho pode transportar classes de tráfego diferentes, que podem ter diferentes necessidades de protecção.

- Agrupamento – Sendo a designação **Grupo de caminhos protegidos** (*Protected Path Group* (PPG)) utilizada para referir um agrupamento lógico de vários caminhos de trabalho que necessitam de protecção, e que são encaminhado da mesma forma entre o PSL e o PML. O princípio de agrupamento é a técnica que corresponde à criação de um PPG, de forma a recuperar simultaneamente os seus múltiplos caminhos.

  Se ocorrer uma falha no PPG, este pode ser protegido como um todo redireccionando o tráfego para um *bypass tunnel*. Um ***bypass tunnel*** é um túnel, utilizado como caminho de recuperação para um PPG, que usa a aproximação do empilhamento de etiquetas (RFC 3031 de Rosen et al. (2001)). Quando os pacotes entram num *bypass tunnel* é-lhes acrescentada uma etiqueta adicional, com base na qual são encaminhados. As etiquetas originais são mantidas inalteradas durante todo o encaminhamento através do *bypass tunnel* para os pacotes poderem ser distinguidos quando saírem dele. A figura 5 apresenta um exemplo de um PPG constituído por três caminhos de trabalho e um *bypass tunnel* para recuperação desse PPG. Os três caminhos de trabalho estão estabelecidos respectivamente entre o LSR A e o LSR X, entre o LSR B e o LSR Y e entre o LSR C e o LSR Z, seguindo cada um os ramos assinalados.

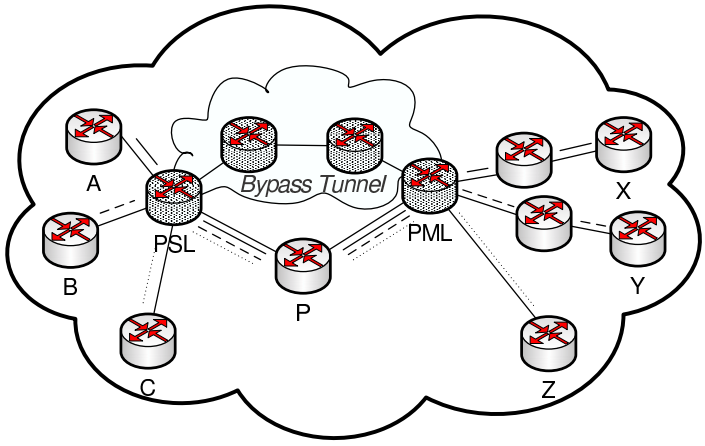

Figura 5: Exemplo de um PPG e de um *bypass tunnel*.

Vamos supor que ocorre a falha do LSR P (figura 5). Nesse caso logo que o PSL detecte a falha, cada um dos caminhos protegidos do PPG será reencaminhado para o *bypass tunnel*. As operações de reencaminhamento efectuadas, em cada pacote, no PSL, consistem em trocar a etiqueta do pacote que chega por uma etiqueta apropriada, depois disso, em empilhar no pacote uma etiqueta adicional correspondente ao *bypass tunnel* e por último em redireccionar o tráfego para a interface de saída correspondente ao *bypass tunnel*. A etiqueta apropriada para utilizar na operação de troca é a etiqueta que é esperada pelo PML para o caminho de trabalho ao qual o pacote pertence. Então o PSL tem que conhecer as três etiquetas que o PML espera para os três caminhos de

trabalho do PPG[3].

Tal como os caminhos de recuperação, os *bypass tunnel* podem ou não ter reserva de recursos suficiente para oferecer a recuperação sem degradação dos serviços.

2.1.4 Detecção da falha

Existe um conjunto de mecanismos que podem ser usados pelo MPLS para detectar as falhas. Assim, o MPLS detecta uma falha porque recebeu uma notificação de uma camada inferior ou da camada IP ou ainda devido à própria operação dos mecanismos baseados no MPLS.

Os dois mecanismos utilizados na detecção de falhas, baseados no MPLS são:

Liveness Message é uma mensagem trocada periodicamente entre dois LSR adjacentes (ver figura 6) que serve como um mecanismo de teste ao ramo. Esta mensagem oferece um teste da integridade das duas direcções do ramo entre os dois LSRs bem como um teste à "vida" de LSRs vizinhos.

Teste de continuidade do caminho é um teste que verifica a integridade e continuidade de um caminho ou de um segmento de caminho.

Os dois mecanismos anteriores podem ser utilizados para detectar falhas num caminho, ou seja detectar situações em que o caminho deixou de ter conectividade. Embora um caminho não tenha perdido a conectividade a sua qualidade pode tornar-se inaceitável, nesta situação diz-se que o caminho sofreu uma degradação. A degradação de caminhos pode também ser detectada através de mecanismos baseados no MPLS tais como mecanismos de monitorização do desempenho do caminho ou de determinação de taxas de erro no caminho ou segmentos do caminho.

Por outro lado, as falha nos ramo são normalmente detectadas por uma camada inferior e notificadas por ela ao MPLS. Embora a detecção de falhas de ramos pelas camadas inferiores dependa da tecnologia utilizada é em geral mais rápida que a detecção oferecida por mecanismos de detecção baseados em *hellos* oferecidos pelos protocolos de encaminhamento (por exemplo pelo *Open Shortest Path First* (OSPF)) e por mecanismos de detecção de falhas baseados apenas no MPLS. Apesar disto, como podem existir falhas que são consideradas falhas em ramos mas que não são falhas detectadas pela camada de ligação[4], os mecanismos de detecção da camada 2 devem ser complementados com mecanismos baseados em *hellos*.

O protocolo RSVP-TE (Awduche et al., 2001) define um protocolo baseado em *hellos*, com funcionamento análogo a qualquer outro mecanismo *hello* oferecido pelos protocolos de encaminhamento, no entanto mais rápido na detecção de falhas.

Qualquer mecanismo baseado em mensagens *hello* possui o problema da escalabilidade. Por um lado, como o processamento das mensagens *hello* não é desprezável, não devem ser utilizadas frequências altas. Por outro lado, o número de vizinhos pode ter que ser limitado. Podem, por vezes, surgir situações em que um *router* vizinho não consiga responder às mensagens *hello*

[3]Assumindo que o espaço de etiquetas é global.

[4]Por exemplo, falhas nos processadores das interfaces dos routers.

porque está demasiado ocupado e isso pode ser interpretado como uma falha, falha que na realidade não ocorreu.

Por vezes os LSRs não conseguem distinguir entre a falha de um ramo e a falha de um LSR vizinho (em ambos os casos a falha detectada é a falha de um ramo). Em Vasseur et al. (2004) são indicadas algumas situações em que é importante distinguir entre a falha de um ramo e a falha de um nó, e é proposta uma solução para conseguir distinguir esses dois tipos de falha.

2.1.5 Notificação da falha

Quando um LSR detecta uma falha (falha de um ramo ou nó) que implica a necessidade de recuperação do caminho, e não possui a capacidade de recuperação deve enviar um sinal, designado por FIS, que faça a notificação da falha ao POR. Um FIS é uma mensagem de controlo que deve ser transmitida com alta prioridade. Um FIS, de acordo com Huang et al. (2002), pode ser enviado como um pacote da camada 2 ou da camada 3, dependendo da forma como a notificação foi configurada no LSR. Os LSRs que recebem um FIS devem determinar para que ramos o propagar. Um exemplo de um FIS é a mensagem "RSVP *Path Error*" do protocolo *Resource Reservation Protocol* (RSVP) (RFC 2205 de Braden et al. (1997)).

Um FIS é enviado por cada LSR intermédio, começando no LSR ou LSRs próximos ao ponto em que ocorreu a falha, para o seu LSR a montante ou a jusante até atingir o POR. Se o FIS tiver que ser transmitido no sentido a montante, é óbvio que isso obriga a que tenha que existir um caminho inverso (não necessariamente ao nível do plano do dados) ao caminho usado na transmissão dos dados. Para estas situações Huang et al. (2002) definem uma estrutura especial em árvore, designada por árvore de notificação inversa - *Reverse Notification Tree* (RNT), para distribuir eficientemente as mensagens de notificação e da reparação da falha desde o ponto em que a falha ocorreu até ao PSL. Pormenores sobre essa estrutura serão apresentados na secção 3.1.2.

A figura 6 apresenta um cenário no qual um dos ramos do caminho de trabalho falhou. A figura mostra o envio da notificação pelo LSR que detectou a falha em direcção ao PSL.

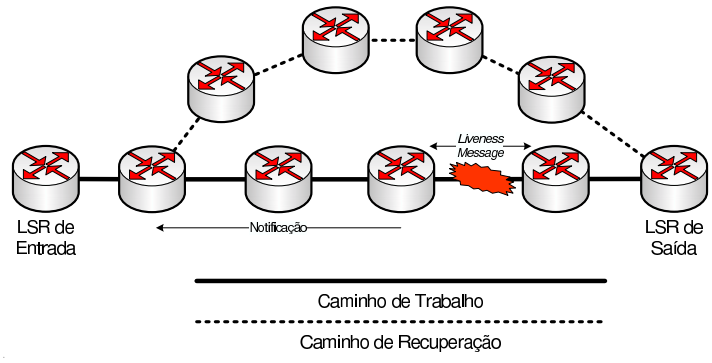

Figura 6: Exemplo de detecção e notificação de falhas.

2.1.6 Operação de *switchover*

É necessário que exista um mecanismo despoletador que redireccione o tráfego quando há a detecção de uma falha ou a recepção de uma notificação de falha. O redireccionamento pode ser automático ou ser a resposta a comandos externos. O redireccionamento é automático quando acontece como o resultado de uma falha detectada no PSL ou da recepção de uma notificação de falha no PSL. O redireccionamento é uma resposta a comandos externos quando é o resultado de comandos externos executados por um operador no POR.

2.1.7 Operações após a recuperação

Quando o tráfego é transportado no caminho de recuperação, deve ser feita uma escolha de entre as seguintes opções:

- manter o tráfego no caminho de recuperação mas passar a designá-lo por caminho de trabalho;
- efectuar uma operação de *switchback* para o caminho de trabalho (como é obvio esta operação só deve ser feita quando a avaria for reparada);
- efectuar uma operação de *switchover* para um caminho de trabalho novo.

Os caminhos de trabalho e de recuperação podem manter-se fixos ou podem ser alterados dinamicamente. Se o caminho de trabalho e de recuperação forem fixos podem surgir os problemas seguintes:

- O tráfego não está protegido entre o instante em que ocorre uma falha no caminho de trabalho (e o tráfego é *switched over* para o caminho de recuperação) e o instante em que ocorre a reparação da falha (e o tráfego é *switched back*).
- Os recursos associados com o caminho de trabalho, mesmo quando não estão a ser utilizados por ele, não são libertados para a rede, isto é mantêm-se reservados.

Segundo o RFC 3469 (Sharma et al., 2003) as operações que podem ser configuradas para serem efectuadas após o *switchover* do caminho de trabalho para o caminho de recuperação são o modo reversivo, o modo não reversivo e a alteração dinâmica dos caminhos.

Modo reversivo Quando a avaria no caminho de trabalho for resolvida o tráfego é automaticamente *switched back* para ele. Assume-se que os recursos do caminho de trabalho não são libertados quando ocorre a falha.

Alteração dinâmica dos caminhos Quando o tráfego foi *switched over* do caminho de trabalho para o caminho de recuperação a associação entre eles pode deixar de existir, uma vez que após a falha o caminho de trabalho pode já não existir de existir. Quando a rede encontrar um estado estável, depois da convergência do encaminhamento, o tráfego pode ser *switched over* para um novo caminho preferido.

Modo não reversivo Neste modo a acção realizada depende do que for mais útil em cada caso. Assim sendo depois do *switchover* do caminho de trabalho para o caminho de recuperação pode acontecer uma das três situações seguintes:

- ser feito o *switchback* para o caminho de trabalho original (após reparação deste);
- continuar a utilizar o caminho de recuperação;
- calcular um novo caminho de trabalho óptimo e redireccionar o tráfego para esse caminho.

2.1.8 Restabelecimento

O restabelecimento MPLS significa o retorno do tráfego ao caminho de trabalho original ou o seu redireccionamento para um novo caminho de trabalho. O restabelecimento é feito pelo PSL após receber uma notificação, através de um FRS, indicando que o caminho já foi reparado. O restabelecimento também pode ser feito pelo PSL após receber uma notificação de que um novo caminho de trabalho está estabelecido.

No modo reversivo o LSR que detecta a falha no caminho de trabalho também detecta o seu restabelecimento. Quando detecta o restabelecimento notifica os LSRs a montante, através de um FRS. Quando o PSL recebe o FRS, repõe o tráfego no caminho de trabalho original.

No modo dinâmico o mecanismo que despoleta o estabelecimento de um novo caminho de trabalho pode notificar o PSL para este efectuar o *switchover*.

Quando o caminho de trabalho é recuperado este pode trocar de funções com o caminho de recuperação. Isto é, o caminho de trabalho passa a ser o de recuperação e vice-versa. Esta solução requer que o caminho de recuperação seja equivalente ao caminho de trabalho e que seja possível transmitir a informação de uma possível falha ao longo do caminho de recuperação em direcção ao PSL. Aqui o restabelecimento não significa precisamente retorno, como definido inicialmente, mas sim troca de funções.

O retorno do tráfego ao caminho original ou o seu redireccionamento para um novo caminho pode ser efectuado usando a técnica *make-before-break*. Esta técnica consiste em sinalizar um novo caminho, capaz de partilhar recursos com o caminho que se pretende reencaminhar. Quando o LSR de ingresso recebe a confirmação do estabelecimento, com sucesso, do novo caminho, o tráfego do caminho original deve ser *switched over* para esse caminho, podendo finalmente ser desligado o caminho original. Desta forma permite-se que o novo caminho possa ter arcos em comum com o caminho original, sem obrigar a dupla captura de largura de banda nesses arcos, o que poderia enviabilizar o redireccionamento.

2.1.9 Resumo de alguns dos princípios de recuperação

A tabela 1 apresenta um resumo de alguns dos princípios de recuperação, nomeadamente o instante em que é estabelecido e calculado o caminho de recuperação e o instante em que é feita a reserva de recursos. Relativamente aos princípios de detecção e notificação da falha, operação de *switchover* e operações após a recuperação, na secção 2.2 faz-se o seu enquadramento.

Modelos de recuperação	**Reencaminhamento**		**Pré-qualificado**	**Protecção por comutação**
Estabelecimento do caminho	quando a falha é detectada		—	pré-estabelecido
Cálculo do caminho	pré-calculado	quando a falha é detectada	escolhido entre LSPs admissíveis	em paralelo ao primário
Reserva de recursos (se houver)	quando a falha é detectada		—	pré-reservados

Tabela 1: Resumo de alguns princípios de recuperação.

2.2 Ciclos do processo de recuperação do MPLS

Sempre que ocorre um determinado acontecimento (por exemplo uma falha) um esquema de recuperação executa uma sequência de fases designada por ciclo. No processo de recuperação do MPLS são definidos os três ciclos seguintes: o ciclo de recuperação do MPLS, o ciclo de reversão do MPLS e o ciclo de reencaminhamento dinâmico. O **ciclo de recuperação** começa quando ocorre uma avaria e termina quando o tráfego é completamente restabelecido no caminho de recuperação. Depois deste ciclo a rede está de novo operacional.

O **ciclo de reversão** aplica-se ao tráfego encaminhado explicitamente que não depende de quaisquer outros protocolos de encaminhamento dinâmico para convergir, é neste ciclo que ocorre a operação de *switchback*, o que acontece quando a falha está completamente reparada. Aparentemente[5] o RFC 3469 não considera a hipótese de utilizar como caminho de *switchover*, um LSP explícito (possivelmente diferente do caminho de trabalho original), que tenha sido re-calculado com base no estado da rede.

Por outro lado o **ciclo de reencaminhamento dinâmico**[6] aplica-se para o tráfego que é encaminhado baseado no encaminhamento *hop-by-hop*, aqui o encaminhamento dinâmico deve determinar um (possivelmente) novo caminho de trabalho re-optimizado depois da ocorrência de uma falha. Se depois dos protocolos de encaminhamento convergirem for determinado que existe um caminho melhor para caminho de trabalho então desencadeia-se este ciclo.

Depois do ciclo de recuperação os caminhos utilizados (caminhos de recuperação) podem não ser tão bons como os caminhos de trabalho. A utilização dos recursos da rede pode ser optimizada se este ciclo for seguido pelo ciclo de reencaminhamento dinâmico. Outra possibilidade é esperar que ocorra a reparação da falha e redireccionar o tráfego do caminho de recuperação de volta para o caminho de trabalho, ou seja, o ciclo de recuperação ser seguido pelo ciclo de reversão. No entanto, existem situações em que o ciclo de recuperação pode não ser seguido por nenhum dos outros dois, é o caso, já referido na secção 2.1.7, em que se decide manter o tráfego no caminho de recuperação que passará a ser designado por caminho de trabalho.

[5] Em (Sharma et al., 2003, pág. 12, secção 2.2.3) é afirmado que o ciclo de reencaminhamento dinâmico poderá "ser sobreposto"ao ciclo de recuperação e/ou ao ciclo de reversão, mas esta possibilidade não parece contemplar a possibilidade do novo caminho de trabalho (LSP explícito), ser diferente do caminho de trabalho (original) recuperado.

[6] O conceito de encaminhamento dinâmico em redes MPLS não se limita ao encaminhamento *hop-by-hop*, contrariamente ao que aqui é sugerido, ao procurar apresentar a definição de *Dynamic Rerouting Cycle Model* tal como ela surge no RFC 3469 Sharma et al. (2003).

Cada um dos ciclos é constituído por vários intervalos de tempo, cada um dos quais será descrito a seguir no ciclo respectivo.

2.2.1 Modelo do ciclo de recuperação do MPLS

Após a ocorrência de uma falha a sucessão de fases seguida pelos diversos esquemas de recuperação é muito semelhante e é designada, como já referido, por ciclo de recuperação. A figura 7 ilustra o modelo do ciclo de recuperação do MPLS.

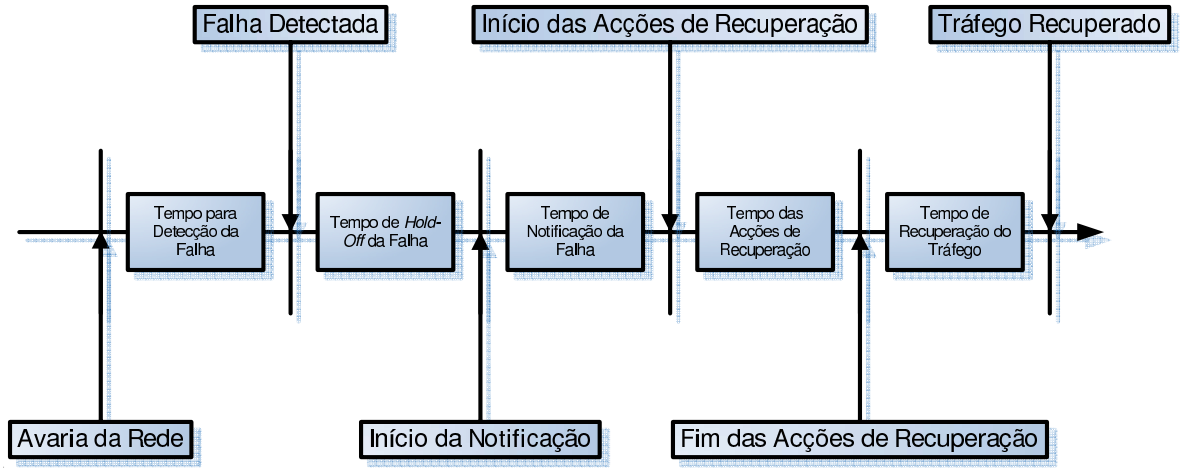

Figura 7: Modelo do ciclo de recuperação do MPLS.

As várias fases do modelo do ciclo de recuperação são definidas a seguir.

Tempo para Detecção da Falha Instante entre a ocorrência de uma avaria na rede e o momento em que a falha é detectada pelos mecanismos de recuperação do MPLS. O valor deste tempo é altamente dependente do mecanismo de detecção usado. Por este motivo a duração deste intervalo pode ser fortemente dependente dos protocolos das camadas inferiores, ou da frequência dos sinais enviados entre os LSRs (*hellos*), etc.

Tempo de *Hold-Off* da Falha Tempo de espera entre a detecção de uma falha e o início da notificação. Este tempo terá grande importância se a estratégia de recuperação envolver várias camadas. Pode ser por exemplo o tempo necessário para permitir aos esquemas das camadas inferiores repararem a falha. Este tempo é configurável administrativamente e pode ser nulo.

Tempo de Notificação da Falha Se a falha ainda existir depois do Tempo de *Hold-Off* da Falha, são enviadas mensagens de notificação (FIS) para os LSRs que serão envolvidos nas acções de recuperação. O Tempo de Notificação da Falha é o tempo entre o instante em que o sinal que indica a falha (FIS) começa a ser emitido pelo LSR que a detectou e o instante em que o POR começa as acções de recuperação. Este tempo depende do esquema de recuperação usado, pode mesmo ser zero (pois a recuperação do tráfego pode ser feita pelo LSR imediatamente a montante à falha).

Tempo das Acções de Recuperação Tempo entre o instante em que o POR inicia as acções de recuperação e o instante em que termina essas acções.

Tempo de Recuperação do Tráfego Tempo entre o a última acção de recuperação e instante em que o tráfego (se existir) é completamente recuperado.

O tempo total da recuperação é obtido somando os valores de todos os tempos anteriores.

2.2.2 Modelo do ciclo de reversão do MPLS

Nos esquemas de recuperação revertivos a operação de *switchback* também segue uma sucessão de fases gerais a qual é designada por ciclo de reversão. A figura 8 ilustra o modelo do ciclo de reversão do MPLS.

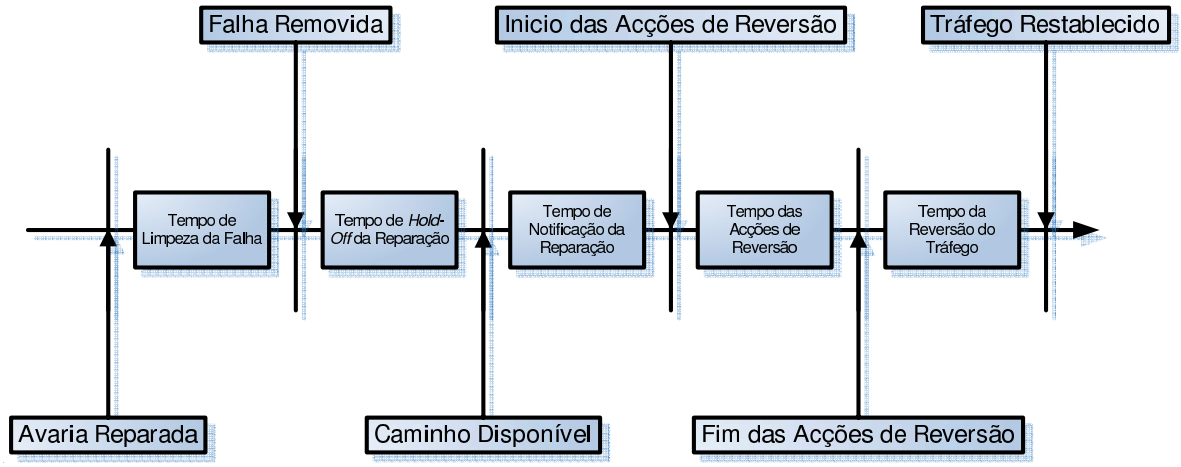

Figura 8: Modelo do ciclo de reversão do MPLS.

Os intervalos de tempo do modelo do ciclo de reversão são definidos a seguir.

Tempo de Limpeza da Falha Instante entre a altura em que a avaria foi reparada e o momento em que os mecanismos baseados no MPLS detectaram que a falha já não existe.

Tempo de *Hold-Off* da Reparação Tempo de espera, que é configurado, entre o instante em que os mecanismos baseados no MPLS detectaram que a falha já não existe e o instante em que estes mecanismos efectivamente iniciam a notificação da reparação da falha. Este tempo pode ser necessário para assegurar que o caminho é estável (que não se trata de uma falha intermitente).

Tempo de Notificação da Reparação Tempo entre o instante em que o FRS começa a ser emitido pelo LSR que inicia a notificação da reparação da falha e o instante em que o LSR responsável pelas acções de reversão as inicia. Este tempo pode ser zero.

Tempo das Acções de Reversão Tempo entre o instante em que o POR inicia as acções de reversão e o instante em que termina essas acções.

Tempo da Reversão do Tráfego Tempo entre o a última acção de reversão e instante em que o tráfego (se existir) é completamente restabelecido no caminho de trabalho.

2.2.3 Modelo do ciclo de reencaminhamento dinâmico

A figura 9 ilustra o modelo do ciclo de reencaminhamento dinâmico.

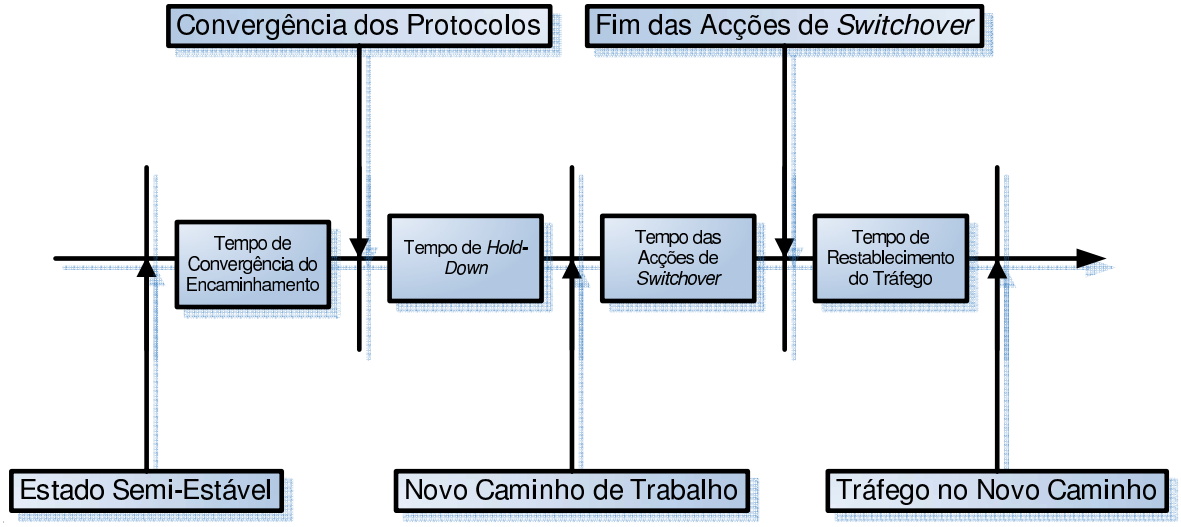

Figura 9: Modelo do ciclo de reencaminhamento dinâmico.

Os intervalos de tempo do modelo do ciclo de reencaminhamento dinâmico são definidos a seguir.

Tempo de Convergência do Encaminhamento É o tempo para os protocolos de encaminhamento convergirem e para a rede alcançar um estado estável.

Tempo de *Hold-Down* (opcional) É um período de tempo durante o qual deve ser utilizado o caminho de recuperação.

Tempo da Acções de *Switchover* Tempo entre a primeira e a última acção de *switchover*.

Tempo de Restabelecimento do Tráfego Tempo entre o a última acção de *switchover* e instante em que o tráfego (se existir) é completamente restabelecido no novo caminho de trabalho.

2.3 Critérios de comparação de esquemas de recuperação

Nesta secção vão ser enumerados alguns critérios que podem ser utilizados na comparação dos esquemas de recuperação baseados no MPLS ainda segundo Sharma et al. (2003).

Tempo da Recuperação É definido como sendo o tempo que demora a activação do *caminho de recuperação* após a falha. Na figura 7 é o tempo total desde o instante em que ocorreu a avaria da rede até ao instante em que tráfego foi completamente recuperado.

Tempo Total da Reposição Tempo necessário até ao restabelecimento permanente do tráfego. Pode ser igual ao anterior se os caminhos trocarem de funções, ou pode ser diferente, se existir necessidade de reversão ou encaminhamento dinâmico.

Vulnerabilidades na inicialização Outro critério que pode ser utilizado na comparação dos esquemas de recuperação é o tempo que o caminho de trabalho ou conjunto de caminhos de trabalho funcionam sem protecção. Exemplos de situações em que esta condição ocorre são o tempo durante o cálculo do caminho de recuperação e o tempo necessário ao estabelecimento do caminho de recuperação.

Capacidade de *Backup* A quantidade da Capacidade de *Backup* necessária quando ocorre uma falha pode diferir de esquema de recuperação para esquema de recuperação.

Latência Cumulativa Os esquemas de recuperação podem aumentar a latência ao tráfego. Por exemplo, um caminho de recuperação pode ter muitos mais nós que o caminho de trabalho.

Qualidade da protecção O grau de garantia de sobrevivência do tráfego é outro factor dependente do esquema de recuperação. A sobrevivência de um pacote pode variar de *sobrevivência relativa* a *sobrevivência absoluta*. Sobrevivência relativa pode (por exemplo) significar que o pacote está num pé de igualdade com outro tráfego. Sobrevivência absoluta pode (por exemplo) significar que o tráfego protegido tem garantias explícitas de sobrevivência.

Reordenação de pacotes Também é dependente do esquema de recuperação a necessidade de reordenação de pacotes que pode ocorrer tanto após a operação de *switchover* como após a operação de *switchback*.

(*Overhead*) associado ao estado A quantidade de informação de *estado* necessária para registar os caminhos de recuperação aumenta à medida que aumenta o número de caminhos de recuperação. No entanto, a quantidade de informação de *estado* necessária por cada esquema de recuperação pode também depender de muitos outros parâmetros, como por exemplo o número, tipo dos itens protegidos e da definição de *Shared Risk Link Group*s (SRLGs).

Perda de pacotes Durante o *switchover* um determinado número de pacotes pode ser perdido. Uma medida do número de pacotes perdidos pode ser obtida através da proporção entre o tempo de recuperação e a velocidade do ramo.

Cobertura Diferentes esquemas de recuperação oferecem diferentes tipos de cobertura de falhas. Para avaliar um esquemas de recuperação em termos de cobertura total devem ser tidas em consideração várias métricas. Algumas dessas métricas são:

- **Tipo de falha** As falhas cobertas podem ser apenas falhas nos ramos, ou falhas nos nós e nos ramos ou também ser considerada a degradação de serviço.

- **Número de falhas simultâneas** É dependente do esquema de recuperação a possibilidade de recuperação de várias falhas que possam ocorrer simultaneamente.
- **Número de caminhos de recuperação** Número de caminhos de recuperação que podem existir por cada falha.
- **Percentagem da cobertura** Percentagem das falhas que podem ser cobertas. Esta percentagem pode ser subdividida em percentagens por tipo de falha.
- O número de caminhos protegidos pode afectar a rapidez com que o conjunto total de caminhos afectados por uma falha podem ser recuperados. A **razão de protecção** é n/N, onde n é o número de caminhos protegidos e N é o número total de caminhos.

Destes critérios de comparação os utilizados mais frequentemente são: o tempo da recuperação, a percentagem de pacotes reordenados, a percentagem de pacotes perdidos e a eficiência em termos de utilização da capacidade de *backup*.

2.4 Os vários significados de recuperação global e local - clarificando a notação

Na recuperação global o objectivo é oferecer protecção para a falha de qualquer nó ou ramo do caminho de trabalho ou seu segmento, como já foi referido. Neste tipo de recuperação é usual o LSR de entrada e o LSR de saída do caminho de trabalho coincidirem com o PSL e com o PML, respectivamente. Um exemplo de uma situação em que tal não se verifica é ilustrado na figura 10, na qual o PSL (origem do tráfego recuperado) não é a origem do tráfego de trabalho. Isso acontece porque apenas o segmento entre o PSL e o PML necessita protecção (Huang et al., 2002; Sharma et al., 2003). Muitos autores omitem o caso em que apenas um segmento do caminho de trabalho necessita de protecção é o caso, por exemplo de Park et al. (2004), Mellah e Mohamed (2003) e Vasseur et al. (2004).

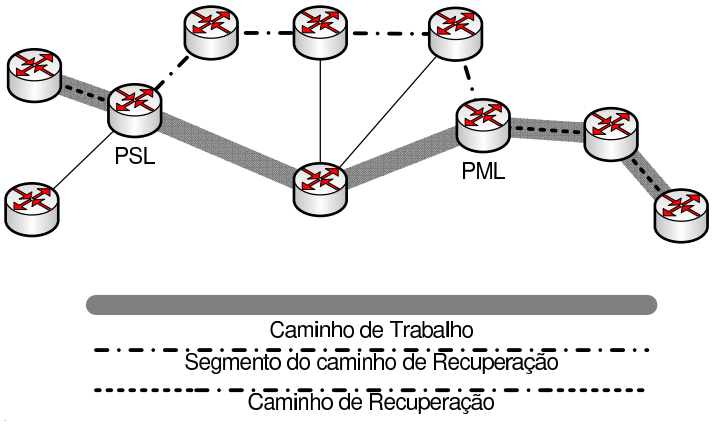

Figura 10: Exemplo do modelo de reparação global.

Consideramos, em sentido lato, que um mecanismo de recuperação é global sempre que a acção de recuperação é desempenhada pelo mesmo par de LSRs (o PSL e o PML), qualquer que seja a localização da falha nesse caminho. Quando o PSL e o PML coincidem com o LSR

de entrada e o LSR de saída, respectivamente, este mecanismo é designado por recuperação extremo a extremo (*end-to-end*).

As definições apresentadas para recuperação global e local (secção 2.1.3) representam apenas dois extremos do conjunto de possibilidades, pois existem muitas situações intermédias, como realçado por Vasseur et al. (2004). Podem apontar-se como exemplos de situações intermédias os esquemas propostos por Hong et al. (2004), Yoon et al. (2001), Haskin e Krishnan (2001). Para abranger as situações intermédias, que consideramos se enquadram no âmbito da recuperação local, vamos alargar esta definição. Vamos considerar como sendo recuperação local toda a recuperação que é feita por um LSR próximo da falha, não obrigatoriamente um dos LSRs adjacentes à falha (porque utilizando um destes LSRs pode não existir um caminho que contorne a falha, ou porque estes LSRs podem não ter capacidade de efectuar a recuperação, ou por qualquer outra razão que os impeça).

Normalmente a recuperação local será tentada pelo LSR a jusante mais próximo da falha no LSP de trabalho. Caso esse LSR não seja bem sucedido, poderá enviar para o nó seguinte a montante a informação necessária para que este tente por sua vez recuperar o LSP afectado. Consideramos que, quando a acção de recuperação é efectuada com sucesso pelo o LSR de entrada, porque nenhum dos outros LSRs a montante da falha o conseguiu (ou seja pelo menos um tentou e falhou), estamos ainda na presença de um mecanismo de recuperação local.

3 Alguns esquemas de recuperação propostos na literatura

Nas descrições seguintes relativas aos esquemas de recuperação apenas são detalhados, para cada um, o aspecto essencial à sua operação. Por exemplo para uns será o algoritmo de encaminhamento (para o caminho de trabalho e de recuperação), para outros será a forma de notificação das falhas, para outros ainda será a distribuição de carga por vários caminhos, etc.

O critério principal utilizado para organizar os esquemas de recuperação foi o modelo de recuperação (protecção por comutação ou reencaminhamento).

3.1 Protecção por comutação

3.1.1 Caminho de protecção inverso ao de trabalho

No documento Haskin e Krishnan (2001) é definido um esquema que estabelece caminhos de recuperação que oferecem protecção contra uma falha isolada (ramo ou nó). A característica essencial do esquema proposto é a forma como é construído o caminho de recuperação. O caminho de recuperação é formado por dois segmentos: o primeiro segmento começa no LSR, do caminho de trabalho, adjacente ao LSR de saída e vai através de todos os LSRs protegidos, na direcção inversa ao caminho de trabalho, até ao LSR de entrada. Alternativamente este segmento pode começar no LSR de saída, sendo em tudo o resto igual ao anterior; o segundo segmento é estabelecido entre o LSR de entrada e o LSR de saída sem partilhar nenhum LSR com o caminho de trabalho, ou seja, é um caminho paralelo ao caminho protegido.

Na figura 11 apresenta-se uma rede simples constituída por 6 LSRs. A figura mostra um caminho primário estabelecido entre o LSR 1 e o LSR 4 (1-2-3-4) e também o correspondente

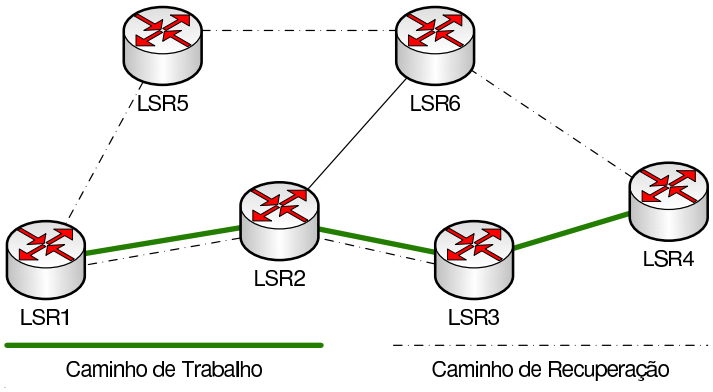

Figura 11: Rede com exemplo de caminhos, de acordo com o esquema de Haskin e Krishnan (2001).

caminho de recuperação completo estabelecido entre o LSR 3 e o LSR 4 (3-2-1-5-6-4).

Quando uma falha é detectada por um LSR o tráfego é redireccionado para o caminho de recuperação já pré-estabelecido. É o LSR que detecta a falha que inverte o tráfego de volta para o LSR de entrada (através do segmento do caminho de recuperação que tem direcção inversa ao caminho primário). Quando o tráfego chega ao LSR de entrada este faz com que ele siga o segundo segmento do caminho de recuperação (segmento do caminho de recuperação que é paralelo ao caminho protegido). Este esquema pode utilizar a protecção $1:1$ ou $1:n$.

Recorrendo de novo à figura 11 e supondo que falha o LSR4 ou o ramo entre o LSR3 e o LSR4, quando o LSR3 detectar essa falha inverte o tráfego para o caminho de recuperação (3-2-1-5-6-4), no entanto, se a falha for por exemplo no LSR2 o caminho de recuperação será apenas (1-5-6-4).

O esquema proposto tem as vantagens de uma recuperação rápida (o caminho de recuperação é pré-estabelecido e o LSR que detecta a falha reencaminha imediatamente os pacotes para o caminho de recuperação) e simultaneamente da minimização da complexidade do cálculo e da sinalização do caminho de recuperação (apenas é calculado um caminho de recuperação para proteger todo o caminho de trabalho). Consequentemente, como a recuperação é rápida é minimizada a perda de pacotes, quando um LSP falha.

Uma das desvantagens do esquema é o aumento da latência no caminho de recuperação face ao caminho de trabalho. A latência pode ser reduzida se o LSR de entrada ao detectar o fluxo de tráfego inverso deixar de enviar o tráfego pelo caminho de trabalho e o passar a enviar logo através do segundo segmento do caminho de recuperação, no entanto, esta opção aumenta possivelmente a necessidade de reordenação de pacotes. Outra desvantagem do esquema é não ser geralmente eficiente em termos de utilização de recursos.

Segundo Haskin e Krishnan (2001) o esquema por eles proposto requereria alguma extensão de sinalização.

3.1.2 Notificação na protecção global do caminho

O esquema proposto por Huang et al. (2002) segue o modelo de protecção por comutação. O esquema protege o caminho de trabalho (ou segmento do caminho de trabalho) de qualquer falha num seu nó ou ramo, como um todo. Quando um LSR detecta uma falha tem que enviar uma mensagem de notificação da falha que deve alcançar o PSL. O objectivo principal do esquema é minimizar o atraso na propagação dessas mensagens de notificação.

O mecanismo proposto define uma estrutura de notificação especial em árvore para distribuir eficientemente e rapidamente a informação da falha e/ou da recuperação. A essa estrutura chamaram árvore de notificação inversa - *Reverse Notification Tree* (RNT). O mecanismo define também um protocolo *Hello* como uma forma de detecção de falhas, mais rápido do que o *Hello* da camada *Internet Protocol* (IP), para falhas que não são detectadas pelas camadas inferiores e que devem ser detectadas e corrigidas na camada MPLS. É definido ainda um protocolo de transporte leve e escalável para o transporte das mensagens de notificação.

O mecanismo proposto consiste portanto em três componentes:

RNT Antes de descrever a estrutura RNT é importante relembrar que o MPLS possui um mecanismo designado por fusão de etiquetas, no qual vários caminhos de trabalho podem convergir para formar uma árvore multiponto-ponto, em que os PSLs são as folhas. Os autores de Huang et al. (2002) chamam a esta fusão de etiquetas, fusão física dos LSPs. E definem fusão virtual dos LSPs quando vários LSPs, que têm origem em diferentes LSRs, partilham um segmento comum para além de algum nó e também um identificador, mas não são fundidos fisicamente.

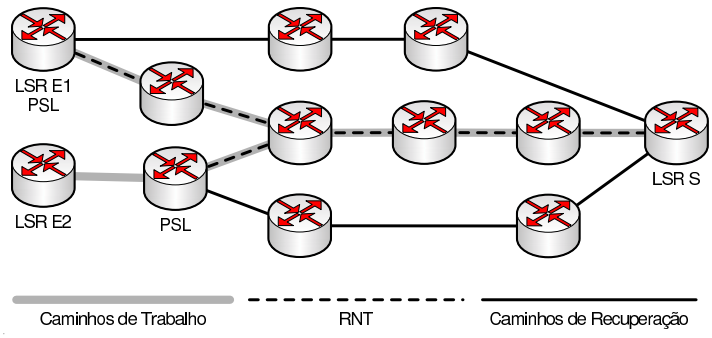

Figura 12: Exemplo de uma RNT.

Quando ocorre fusão física ou virtual dos LSPs o mecanismo de propagação das mensagens de notificação não é simples. Nestas situações eles propõem uma simplificação na sinalização das notificações, através da criação de uma estrutura de notificação inversa (designada por RNT), que é uma arvore ponto-multiponto. A figura 12 apresenta um exemplo de uma RNT numa rede que tem estabelecidos dois caminhos de trabalho e os dois caminhos de recuperação respectivos. A raiz da estrutura RNT é um LSR escolhido de entre os do segmento comum dos LSPs em que há fusão dos caminhos e a estrutura termina nos PSLs. A estrutura RNT define o modo como é feita a propagação das mensagens de notificação e da reparação da falha desde o ponto em que a falha ocorre até ao PSL. Esta estrutura pode ser criada como extensão ao processo de estabelecimento

do LSP. A simplificação na sinalização das notificações consiste em enviar uma única mensagem de notificação nos segmentos partilhados pelos LSPs. Portanto a estrutura RNT possibilita a redução no *overhead* de sinalização associado com a recuperação, ao contrário do que se passa em esquemas que tratam cada LSP independentemente, que necessitam de sinalização por cada LSP. Esta estrutura pode ser implementada na camada 3, na camada 2 ou mesmo na camada 1 para reduzir mais o atraso.

Protocolo *Hello* para detecção de falhas Cada LSR deve ser capaz de detectar certos tipos de falhas. O protocolo *Hello*, semelhante ao protocolo *Hello* do OSPF, deve despoletar a geração do FIS, quando necessário.

Neste protocolo são trocadas mensagens *liveness* periodicamente entre os LSRs vizinhos. Uma mensagem *liveness* transporta o identificador do LSR que a envia e todos os identificadores dos seus vizinhos, descobertos através das mensagens (*liveness*) enviadas pelos vizinhos. Um LSR pode determinar se um ramo bidireccional está a funcionar correctamente se vir a sua própria identificação na mensagem *liveness* enviada pelo LSR no outro extremo do ramo.

Protocolo de transporte leve Os pacotes de notificação são transmitidos periodicamente até que o nó responsável pelo *switchover* seja atingido. Neste protocolo as mensagens não são confirmadas por isso recorre-se a temporizadores. Um temporizador indica o tempo durante o qual são transmitidas as mensagens de notificação. Um outro temporizador serve para determinar o ritmo a que as mensagem de notificação são emitidas. O valor do período deste temporizador não deve ser demasiado grande nem demasiado pequeno de modo a que o atraso na notificação do FIS não aumente muito devido à perda de um FIS e para que não sejam consumidos demasiados recursos, respectivamente. A notificação é efectuada através da propagação do FIS na RNT.

3.1.3 Protecção/recuperação local baseada em túneis

Mellah e Mohamed (2003) propõem um algoritmo de protecção local baseado na utilização de túneis de recuperação, designados por *bypass tunnels* (de acordo com a designação utilizada no RFC 3469 (Sharma et al., 2003)). Os túneis são pré-estabelecidos localmente por cada LSR para contornar a avaria de um ramo. De acordo com o algoritmo proposto, para todos os pacotes que chegam a um LSR, este testa o estado do ramo de saída e efectua a operação normal na etiqueta do pacote. Se verificar que existe falha desse ramo então acrescenta uma nova etiqueta à pilha de etiquetas do pacote (a etiqueta do túnel de recuperação), e o pacote segue o *bypass tunnel* correspondente. Logicamente, nesta situação o pacote sai do LSR por um *interface* diferente daquele que seria utilizado caso não houvesse a avaria do ramo. Se verificar que não existe falha do ramo de saída, o pacote é encaminhado nesse ramo (e sem empilhamento de etiquetas). A figura 13 apresenta um cenário no qual um dos ramos do caminho de trabalho, que se encontra protegido por um *bypass tunnel*, falhou. A figura mostra o empilhamento da etiqueta do *bypass tunnel* nos pacotes dos dois caminhos de trabalho protegidos por ele.

A informação relativa ao estado dos ramos é actualizada periodicamente, nas entradas respectivas da tabela de encaminhamento de etiquetas pelos LSRs adjacentes a esses ramos, e sempre que é detectada uma falha localmente.

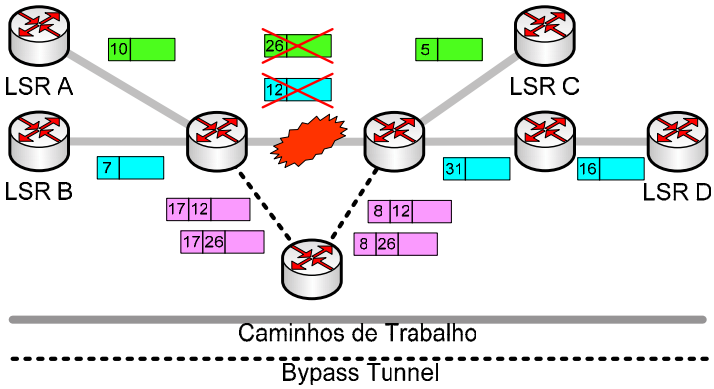

Figura 13: *Bypass tunnel* para protecção de um ramo.

A grande vantagem do esquema proposto são os tempos pequenos de recuperação, pois quando ocorre uma falha não existe a necessidade enviar uma notificação da falha para o LSR de entrada, dado que a recuperação é local, e porque simultaneamente o caminho de protecção é pré-estabelecido. No entanto, o esquema proposto só trata de falhas em ramos. Este método de protecção, focado num dado recurso da rede, não permite seleccionar, entre os LSPs que usam esse recurso, os LSPs a proteger. Em Pan et al. (2005) são propostas extensões de sinalização ao RSVP-TE que tornam essa selecção possível. De notar que o esquema, tal como é proposto em Mellah e Mohamed (2003), apenas funciona correctamente se o espaço de etiquetas for global.

3.1.4 Recuperação utilizando "*p*-cycles"

Kang e Reed (2003) apresentam um trabalho que é dedicado ao problema do encaminhamento nos *bypass tunnels* com largura de banda garantida (o túnel de recuperação deve oferecer largura de banda garantida para todos os caminhos protegidos por ele, em casos de falha isolada). Nesse artigo os autores investigam a utilização de "*p*-cycles" (*preconfigured-cycles*) no encaminhamento desses túneis.

O conceito "*p*-cycle" foi inicialmente proposto para a recuperação em redes de transporte como as redes *Synchronous Optical Network* (SONET) ou as redes *Wavelength Division Multiplexing* (WDM) por Grover e Stamatelakis (1998). Os mesmos autores também estudaram em Stamatelakis e Grover (2000a) a utilização do conceito "*p*-cycle" na recuperação de redes com características do MPLS, mas sem a restrição de largura de banda garantida.

A ideia base do conceito "*p*-cycle" é a pré-configuração da capacidade extra da rede em ciclos, que devem ser criados antes de ocorrer qualquer falha. Com este conceito são recuperadas falhas não apenas no ciclo mas também falhas de ramos que ligam dois pontos não adjacentes do "*p*-cycle" (ramos *straddling*) e neste caso existem dois caminhos de recuperação para cada falha. A figura 14 apresenta um exemplo de um '*p*-cycle" e de ramos *straddling*. A recuperação de ramos *straddling* contribui significativamente para a eficiência dos "*p*-cycles".

Grover e Stamatelakis (1998) apresentam uma formulação para o projecto óptimo dos "*p*-cycle", para a recuperação em redes de transporte SONET ou WDM. Esta formulação divide-

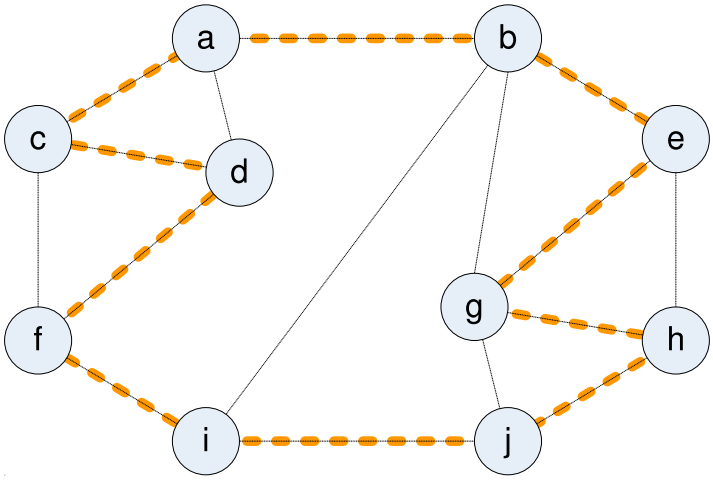

Figura 14: Exemplo de um "p-cycle"e ramos *straddling*.

se em duas fases: a primeira fase consiste em gerar o conjunto de todos os ciclos distintos elementares, até um tamanho limite, para a topologia da rede existente; a segunda fase consiste na resolução de um problema de programação linear inteira que gera um plano óptimo dos "p-cycle" através da escolha do número de cópias de cada ciclo elementar no grafo da rede, para ser configurado como um "p-cycle". Posteriormente os mesmos autores, em Stamatelakis e Grover (2000a), fizeram (segundo Kang e Reed (2003)) a adaptação da formulação original dos "p-cycle" para redes IP/MPLS.

No trabalho apresentado por Kang e Reed (2003) foi adaptada a formulação, para o projecto óptimo dos "p-cycle", proposta em Stamatelakis e Grover (2000a) acrescentando-lhe a protecção com largura de banda garantida. Nessa adaptação foi tida em atenção apenas a protecção contra falhas isoladas de ramos. Como o problema de optimização dos "p-cycle" é NP-*hard* (Stamatelakis e Grover, 2000a), é proposto em Kang e Reed (2003) um método de relaxação que pré-selecciona ciclos candidatos. Este método foi baseado no resultado teórico apresentado por Stamatelakis e Grover (2000b), que indica que "p-cycles" grandes tendem a oferecer maior eficiência em termos de capacidade. Estes resultados foram confirmados, no caso geral, através dos resultados das experiências apresentadas em Kang e Reed (2003). Na primeira experiência apresentada, constataram que para os casos em que tal não se verifica isso é devido a duas razões: 1 - a utilização de ciclos grandes faz com que seja necessário reservar mais capacidade de *backup*, no caso da protecção de ramos sobrecarregados (ramos com muito tráfego de caminhos de trabalho), do que se fossem utilizados ciclos mais pequenos; 2 - a existência de poucos ciclos candidatos grandes, (nomeadamente com uma distribuição não uniforme da carga de trabalho), conduz a uma menor flexibilidade e consequentemente a uma diminuição da eficiência da solução.

Kang e Reed (2003) dizem que o problema do projecto dos "p-cycles" pode ser simplificado considerando apenas como ciclos candidatos os ciclos grandes, que são óptimos no caso da distribuição uniforme da carga na rede. No entanto como constaram que, no caso em que a distribuição de tráfego é não uniforme, existe uma degradação da eficiência causada pelo número limitado de ciclos candidatos, concluíram que alguns ciclos mais pequenos deveriam ser acrescentados. Assim, a heurística, proposta com o objectivo de reduzir a dimensão do

problema, consiste em pré-seleccionar o conjunto dos ciclos maiores e o conjunto dos ciclos mais pequenos. No artigo apresentam resultados de experiências realizadas em várias redes que atestam que a sua heurística é superior a outras consideradas.

Através de várias experiências realizadas, Kang e Reed (2003) também mostram que uma boa distribuição da carga de trabalho pela rede pode melhorar o desempenho dos "p-cycles" em termos de utilização de capacidade.

Algumas considerações finais relativamente à utilização de "p-cycles" na recuperação de redes MPLS:

- A utilização de túneis de recuperação encaminhados utilizando o conceito "p-cycle" possui as mesmas vantagens que foram apresentadas para o esquema da subsecção 3.1.3.
- Uma desvantagem da aplicação do conceito "p-cycle" à recuperação em redes MPLS é a quantidade de túneis que é necessário estabelecer. Para cada "p-cycle" é necessário no mínimo estabelecer tantos túneis quantos o número de ramos do "p-cycle" mais o dobro do número de ramos *straddling* desse "p-cycle".
- Em redes reais de grandes dimensões não podem ser utilizados os ciclos máximos mas apenas os ciclos maiores permitidos, porque em ciclos grandes o sinal pode sofrer uma degradação inaceitável e porque ciclos grandes têm maior probabilidade de falhas múltiplas. Por outro lado, mesmo após a aplicação da heurística apresentada em Kang e Reed (2003), a dimensão do problema pode ainda ser excessiva.
- Para evitar a dependência de um controlo centralizado para o desenvolvimento e manutenção de um estado óptimo de pré-configuração dos "p-cycle", pensamos que haveria vantagem em desenvolver um protocolo distribuído de auto-planeamento que continuamente aproximasse o estado óptimo, à semelhança do que foi proposto para a recuperação em redes de transporte SONET ou WDM por Grover e Stamatelakis (1998).

3.1.5 Recuperação com dois caminhos de protecção por cada nó protector

No esquema proposto em Bartoš e Raman (2001) os caminhos de protecção de todos os LSRs de entrada para cada LSR de saída são calculados simultaneamente, após o que são estabelecidos. O algoritmo de cálculo dos caminhos de protecção (apresentado em Bartoš et al. (2001)) é executado concorrentemente em todos os LSRs de saída, para oferecer protecção completa para todo o domínio de protecção. Como resultado de uma execução do algoritmo obtém-se, em cada LSR de saída, dois caminhos de protecção disjuntos para cada um dos pares LSR de entrada / LSR de saída, em que o LSR de saída é fixo. Esses caminhos de protecção protegem os caminhos de trabalho contra a falha isolada de um ramo qualquer. A localização dos caminhos de protecção, determinados pelo algoritmo, não é influenciada pela localização dos caminhos de trabalho (os quais podem não ser disjuntos com os caminhos que os protegem) o que oferece uma maior flexibilidade ao esquema de protecção. O algoritmo faz a fusão dos caminhos de protecção sempre que possível, diminuindo assim o consumo de recursos.

O algoritmo garante as duas condições seguintes: todo o LSR protector (LSR que pode efectuar recuperação) possui uma ligação, através de dois caminhos de protecção, ao LSR de saída; esses dois caminhos de protecção estão colocados de forma que nenhuma falha de um ramo

causará perda de conectividade entre um LSR protector e o LSR de saída. Isto é, a falha de um ramo não causa a perda de conectividade simultânea em ambos os caminhos de protecção.

A notificação da falha de um ramo, aos LSRs afectados, é feita utilizando um FIS, transmitido pelos LSRs adjacentes ao ramo que falhou e que se propaga através da RNT. Quando os LSRs recebem um FIS, deixam de transmitir tráfego nos caminhos de trabalho em que ocorreu a avaria de um ramo, e redireccionam o tráfego para os caminhos de protecção globais. No entanto, todo o tráfego de caminhos de trabalho com falha num ramo que chegou aos LSRs que são adjacentes ao ramo que falhou, imediatamente depois do ramo falhar e antes da propagação completa do FIS, é redireccionado para os caminhos de protecção que emergem desses LSRs protectores. Desta forma, no esquema proposto, a recuperação é tão rápida como a recuperação local mas a quantidade de recursos necessários é normalmente reduzida relativamente a outros esquemas de recuperação local. O esquema proposto oferece protecção contra a falha de um ramo, mas falhas múltiplas em ramos e falhas em nós não foram consideradas pelo autores.

As medidas consideradas pelos autores para determinar a qualidade de um esquema de protecção foram o comprimento dos caminhos de protecção e o número de caminhos de protecção por ramo. Eles referem que o seu esquema é mais eficiente que outros em termos destes critérios mas não explicitam a forma de cálculo utilizada para obter esses parâmetros.

Embora não seja propriamente um esquema muito simples na construção (sinalização) dos caminhos, parece um esquema interessante, e fácil de implementar sem exigir grandes recursos computacionais. Uma vez que os caminhos de protecção ignoram o caminho de trabalho e a capacidade dos ramos no seu cálculo, a sua aplicabilidade em situações de tráfego elevado (*best effort*) não parece comprovada.

A contagem do número de caminhos Bartoš e Raman (2001) que é preciso estabelecer não é devidamente explicada. Para que essa contagem ficasse clara, seria necessário que tivesse sido explicado o método de sinalização dos LSPs de protecção.

Os LSPs de protecção, são calculados pelo LSR de saída mas têm de ser sinalizados pelo LSR de entrada de cada um deles. Essa dificuldade poderá ser contornável se houver troca de informação entre os LSRs de saída e uma entidade central de gestão da rede que solicite (aos LSRs de entrada) o estabelecimento dos LSPs de protecção calculados em cada LSR de saída.

Os LSPs de protecção poderão ser sinalizados sob a forma de túneis, mas para que as regras de fusão esboçadas em Bartoš e Raman (2001) se apliquem, será necessário que todos esses LSPs pertençam à mesma sessão (considerando fixo o LSR de saída). Bartoš e Raman (2001) dizem que fazem a fusão dos caminhos para diminuir o consumo de recursos. no entanto LSPs explícitos só podem ser fundidos em situações específicas (ver RFC 4090 Pan et al., 2005).

3.1.6 Determinação dos caminhos através da resolução de problemas de programação linear

Em Yetginer e Karasan (2002), os autores estudam um esquema de recuperação com as seguintes características: o caminho de trabalho e o caminho de recuperação são determinados *off-line*, e a recuperação é global, por protecção por comutação e com reserva de largura de banda. No esquema proposto existe a possibilidade de partilha de largura de banda entre

caminhos de protecção que protegem caminhos de trabalho disjuntos nos ramos. Todas as falhas na rede de um único ramo são completamente recuperáveis.

O aspecto central explorado é a forma como são determinados os caminhos. São apresentados algoritmos para quatro abordagens ao processo de determinação dos caminhos de trabalho e dos caminhos de recuperação. Todos os algoritmos para a determinação dos caminhos são formulados como problemas de programação linear inteira.

Os algoritmos das quatro abordagens determinam um conjunto inicial de caminhos e seleccionam dele caminhos de trabalho e de recuperação para todos os pedidos. Considera-se que a procura na rede é conhecida, e que cada pedido de ligação entre dois nós requer uma dada largura de banda. A partir destes pedidos, o conjunto inicial de caminhos é obtido determinando para cada pedido, um conjunto de caminhos disjuntos nos ramos, em que o número de caminhos é maximizado e simultaneamente a largura de banda total utilizada por eles é minimizada.

O primeiro algoritmo começa por seleccionar (de uma vez só) os caminhos de trabalho, de entre os elementos do conjunto previamente determinado. Seguidamente selecciona os caminhos de recuperação. Em ambos os caso o objectivo é que a largura de banda total utilizada na rede seja mínima, isto é, que a capacidade residual total na rede seja máxima. A capacidade residual total é considerada como sendo a soma das capacidades residuais em todos os ramos.

No segundo algoritmo o projecto dos caminhos de trabalho e o projecto dos caminhos de recuperação também é feito em separado. Porém, além de pretenderem que a capacidade residual total na rede seja maximizada também pretendem que a carga seja distribuída pela rede, de modo a evitar que uns ramos possam estar congestionados enquanto outros estão sub utilizados. Para o conseguir maximizam o mínimo das capacidades residuais individuais, considerando todos os ramos.

Os terceiro e o quarto algoritmos, ao contrário dos anteriores, integram o cálculo dos caminhos de trabalho e dos caminhos de recuperação. O terceiro algoritmo tem os mesmos objectivos que o segundo algoritmo diferindo deste apenas na forma integrada como são obtidos os caminhos de trabalho e protecção.

O quarto algoritmo (muito semelhante ao anterior) procura manter com elevada capacidade residual os ramos que estima (com base em dados históricos) que serão os mais utilizados. Para tal atribui a cada ramo um peso inversamente proporcional ao nível de utilização esperada.

Os autores comparam as quatro abordagens em função da sua capacidade de suportar variações nos padrões de tráfego. Para isso observam como é distribuída a capacidade residual pela rede e determinam o número de pedidos adicionais que podem ser transportados, mantendo os caminhos de trabalho existentes inalterados, para cada uma das abordagens.

Concluíram que ao distribuir cuidadosamente a carga de tráfego pelos recursos da rede, a abordagem que integra o projecto dos caminhos de trabalho e recuperação e que faz a distribuição da carga considerando os ramos com pesos adequados, tem um desempenho melhor que as outras abordagens no transporte de tráfego adicional resultante de imprevisões no tráfego.

O esquema proposto, qualquer que seja a abordagem escolhida para seleccionar os caminhos, parece ser dificilmente implementável em redes de dimensão não trivial porque exige a resolução de problemas de programação linear inteira complexos. Como os cálculos são feitos

off-line esta restrição é ligeiramente reduzida, mas ainda assim parece inviável para redes de dimensão média ou superior.

3.1.7 Determinação *on-line* dos caminhos para um novo pedido

No esquema de recuperação proposto por Kodialam e Lakshman (2002), quando surge um pedido de um novo LSP os caminhos (activo e de recuperação) são determinados *on-line*. Se não for possível garantir largura de banda para recuperação (medida de QoS utilizada) o pedido é rejeitado. Caso contrário, o/os caminho/s de recuperação é/são estabelecidos ao mesmo tempo que o caminho activo. Kodialam e Lakshman (2002) descrevem algoritmos de encaminhamento dinâmico para a determinação do caminho activo (CA) e de recuperação (CR). Consideram três situações distintas de informação disponível e designam os três modelos de informação resultantes por: modelo com Nenhuma Informação (NI), modelo com Informação Completa (IC) e modelo com Informação Parcial (IP). No primeiro apenas é conhecida a LB reservada em cada ramo[7] (e a LB residual), no segundo são conhecidos os percursos de todos os CAs e CRs e no último é conhecida a LB total utilizada pelos CAs e a LB total utilizada pelos CRs em cada ramo (apenas é conhecida informação agregada[7] que não depende do número de LSPs estabelecidos). O único modelo com interesse prático é o modelo com IP. Os modelos com NI e com IC[8] podem ser utilizados para obter o limite superior e o limite inferior, respectivamente, de LB necessária ao modelo com IP. Kodialam e Lakshman (2002) apresentam a formulação de algoritmos para a recuperação global (para os três modelos de informação) e em (Kodialam e Lakshman, 2001) apresentam a formulação de um algoritmo para a recuperação local (para o modelo IP). Os algoritmos apenas consideram falhas isoladas de ramos mas podem facilmente ser estendidos para considerar também falhas isoladas de nós.

Designam por partilha inter pedido (*interdemand*) a partilha de caminhos de recuperação entre pedidos cujos LSPs activos não partilham o mesmo ramo (mesmo que os CAs não sejam disjuntos pode ainda ser possível existir partilha). Designam por partilha intra pedido (*intra-demand*) a partilha entre os vários LSPs de recuperação de um mesmo LSP activo (possível apenas na recuperação local). Em cada algoritmo exploram a possibilidade de partilha de largura de banda (LB) dos CR. Essa partilha será tanto maior quanto mais informação, relativa à utilização dos ramos, estiver disponível.

Recuperação global - Algoritmos para selecção do CA e do CR

1. Modelo com Nenhuma Informação

   Neste caso não é possível qualquer partilha de LB. O objectivo é seleccionar os caminhos (activo e de recuperação) que minimizem a largura de banda total usada pelos dois. Para tal deve ser escolhido o par de caminhos disjuntos nos ramos com o menor número de ramos. Este problema é formalizado como um problema standard de fluxo de redes (considerando cada ramo com custo e capacidade unitária). Pode ser resolvido por qualquer algoritmo de fluxo de custo mínimo (por exemplo, pelo algoritmo de Suurballe (Suurballe e Tarjan, 1984) que um algoritmo bastante rápido).

[7] Esta informação pode ser distribuída como resultado de extensões aos protocolos de encaminhamento.

[8] A grande quantidade de informação que precisa de ser enviada faz com que não possa ser aplicado em situações práticas.

2. Modelo com Informação Completa

   Neste caso é possível partilha inter pedido. O problema é formalizado como um problema de programação inteira com restrições quadráticas. A função objectivo minimiza a soma das duas parcelas seguintes: a soma dos custos dos ramos no CA (que é igual à soma das LB usadas pelo CA em cada um dos seus ramos) e a soma dos custos nos ramos no CR (determinados como sendo a LB adicional que é necessária reservar em cada ramos para *backup*).

3. Modelo com Informação Parcial

   Neste caso é possível alguma partilha inter pedido. A formalização (função objectivo e restrições) para este caso é igual ao caso anterior (modelo com IC) mas os custos dos ramos do CR[9], utilizados na função objectivo, são superiores ou iguais aos utilizados no caso anterior. No entanto, como nesta formalização a obtenção de solução é demasiado lenta, para ser utilizada em encaminhamento *on-line*, em redes de dimensão não trivial, apresentam uma heurística para a resolução do problema. Essa heurística consiste num algoritmo que selecciona os caminhos através de um processo iterativo. Em cada iteração são determinados os custos a associar a cada ramo (um para ser utilizado na determinação do CA e outro na determinação dos CR). Depois disso é necessário resolver o problema de encontrar dois caminhos disjuntos nos ramos, óptimos para os custos utilizados (determinados anteriormente). A resolução do problema deve minimizar a soma dos custos dos ramos no CA mais a soma dos custos nos ramos no CR. A solução do processo iterativo será a melhor solução obtida em todas as iterações. No entanto, o problema de encontrar dois caminhos disjuntos nos ramos, óptimos para os dois custos associados a cada ramo é um problema NP-hard. Para obter a solução desse problema apresentam um algoritmo (solução heurística), baseado na resolução simultânea e iterativa de heurísticas para o primal e para o dual, obtendo sucessivos limites inferiores e superiores para o intervalo onde se encontra a solução. Pode-se assim ter alguma confiança que a solução admissível encontrada estará assim numa vizinhança de dimensão arbitrariamente definida do óptimo.

Embora nos modelos com informação parcial e com nenhuma informação, os caminhos de trabalho e de recuperação sejam calculados, no nó origem, sem informação completa (com informação parcial ou com nenhuma informação), é possível, reservar localmente, apenas a LB realmente necessária para recuperação. Para isso, ou seja para fazer reservas exactas de LB de protecção, é necessário que ao sinalizar o CR seja enviado o percurso do CA correspondente (informação que é gerada na sinalização do CA). Quando um CA protegido é redireccionado ou desligado o respectivo CR deve ser suprimido; a mensagem de terminação de um CR deve ser acompanhada da descrição do CA de forma a garantir a gestão correcta (da partilha) da LB de protecção. Essa informação deve ser mantida nos nós do CR, enquanto este estiver estabelecido.

Recuperação local - Algoritmo heurístico para selecção do CA e dos CRs

- Modelo com Informação Parcial

[9]Definidos em (Kodialam e Lakshman, 2002).

O algoritmo principal é uma versão modificada do algoritmo de Dijkstra. O algoritmo determina uma árvore de caminhos mais curtos, com raiz no destino do CA. A árvore pode não incluir todos os nós, pois o algoritmo termina quando o próximo nó a ficar com etiqueta permanente for o nó origem.

Em cada iteração do algoritmo é determinado o caminho de recuperação local de custo mínimo para todos os ramos que saem do nó que passou a estar etiquetado de forma permanente. Para determinar o caminho de recuperação de custo mínimo para contornar a avaria de um ramo (a, b), é invocada uma subrotina que, iterativamente, determina todos os caminhos de recuperação de custo mínimo que contornam a avaria desse ramo, e que terminam num dos vários nós do caminho mais curto desde o nó a até ao nó destino. Para determinar cada um destes caminhos de custo mínimo é invocada uma nova subrotina, que também é uma versão modificada do algoritmo de Dijkstra.

O algoritmo entra em consideração com a partilha intra pedido e também com alguma partilha inter pedido no entanto, aparentemente, não entra em consideração com o custo do CA.

Para ser possível implementar o modelo com IP é necessário que o protocolo de encaminhamento anuncie a Largura de Banda (LB) disponível e a LB reservada para protecção, em cada ramo. No OSPF e *Itermediate System – to – Itermediate System* (IS-IS) já foram propostas extensões, para engenharia de tráfego, que abrangem parte desta informação.

Os algoritmos anteriores calculam e/ou reservam LB de protecção considerando que é possível fazer partilha inter pedido dessa LB. No entanto, actualmente os protocolos de sinalização existentes não permitem a possibilidade de partilha de LB entre LSPs, com caminhos explícitos, pertencentes a sessões diferentes. Os autores não falam acerca dos requisitos de sinalização necessários à implementação da partilha inter pedido de LB de protecção.

Qiao e Xu (2002) propuseram um modelo IP, designado por DPIM (*Distributed Partial Information Management*), para protecção global. Este esquema é semelhante ao proposto em (Kodialam e Lakshman, 2000) (idêntico ao revisto em (Kodialam e Lakshman, 2002)), mas utiliza informação adicional relacionada com a utilização de LB de protecção. Os resultados das simulações com redes com 15 e 70 nós apresentados em (Qiao e Xu, 2002) apontam para um desempenho significativamente superior de DPIM face ao algoritmo proposto para o modelo IP em (Kodialam e Lakshman, 2000).

3.1.8 Recuperação do LSP usando a abordagem baseada em CBR

No esquema de recuperação proposto por Dana et al. (2003) um LSP é recuperado redireccionando o seu tráfego para vários LSPs pré-sinalizados, mas sem reserva de largura de banda.

Por cada caminho de trabalho é pré-estabelecido um conjunto de caminhos de recuperação. Quando ocorre a falha de um LSP protegido o seu fluxo de tráfego será dividido pelos LSPs de recuperação correspondentes. Dana et al. (2003) apresentam uma forma de obter as percentagens de tráfego que deve ser oferecido a cada LSP de recuperação utilizando uma abordagem baseada em *Case-Based Reasoning* (CBR) (Aamodt e Plaza, 1994).

A abordagem baseia-se na informação armazenada numa biblioteca de casos. Essa biblioteca contém um conjunto de casos, por LSP protegido. Cada um destes casos consiste numa

situação possível para o valor da largura de banda requerida pelo caminho protegido, para os valores das larguras de banda disponíveis nos LSP de recuperação correspondentes e também na solução para essa situação (valores admissíveis para as percentagens de tráfego a atribuir a cada LSP de recuperação). Quando ocorre a falha de um caminho (os autores referem que são apenas consideradas falhas isoladas de ramos) é determinada a largura de banda necessária para o LSP que falhou e também a largura de banda disponível em cada LSP de recuperação. Para a situação actual vão ser procuradas situações semelhantes na biblioteca de casos. As soluções encontradas para situações semelhantes são combinadas através de uma técnica de adaptação por composição (Borner, 1994), para obter a solução que será utilizada para resolver o problema actual.

Se o número de casos armazenados for grande, a obtenção de uma solução para o problema quando uma falha ocorre consumirá demasiado tempo devido à dimensão do problema que tem de ser resolvido. E nesses casos uma pesquisa simples de uma solução que satisfaça as restrições poderia ter maior probabilidade de ser encontrada facilmente, principalmente se os espaço de soluções admissíveis for grande.

3.1.9 Distribuição da carga para protecção

O esquema proposto em Kim (2003), tal como o esquema de recuperação anterior, é baseado na possibilidade da carga poder ser distribuída por múltiplos caminhos existentes entre um mesmo par de LSRs de entrada/saída. A distribuição de carga numa rede MPLS, segundo Kim (2003), resulta numa maior utilização de recursos e melhor tolerância a falhas do que os sistemas com caminho único.

No artigo Kim (2003), a autora fez a análise numérica da distribuição de carga para a protecção do caminho em termos da relação entre a utilização de recursos e a fiabilidade do serviço, numa rede MPLS. A análise abrange dois mecanismos: um mecanismos de protecção com partilha total, designado por *Fully Shared Mechanism* (FSM), e um mecanismo de protecção com partilha parcial, designado por *Partially Shared Mechanism* (PSM).

Em ambos os mecanismos, quando é necessário fornecer um serviço, que solicita uma quantidade de largura de banda R, são procurados na rede os recursos disponíveis. Desta pesquisa resultam, para o serviço solicitado, n caminhos disjuntos cada um com largura de banda B (em que $nB \geq R$). Após os caminhos terem sido determinados, devem ser estabelecidos e a sua largura de banda reservada. Quando o tráfego é transmitido, existem mecanismos para detecção, notificação e recuperação de falhas.

Apesar dos caminhos de protecção serem pré-estabelecidos e com uma largura de banda garantida podem ainda ocorrer situações em que a recuperação não seja possível, pois os caminhos de recuperação podem falhar. No artigo a autora define fiabilidade como a "probabilidade de que as situações em que a recuperação não é possível não existam" e a utilização de recursos y, como a "razão entre a quantidade de largura de banda pedida e a quantidade de largura de banda ocupada". A quantidade ocupada é a soma da largura de banda dos caminhos de trabalho e de recuperação.

No mecanismo FSM, ilustrado na figura 15, todos os n caminhos são simultaneamente caminhos de trabalho e caminhos de protecção. Inicialmente o tráfego é dividido pelos n caminhos

sendo atribuída a fracção de tráfego R/n a cada um. Quando um caminho falha é atribuída, a cada um dos outros caminhos, a fracção de tráfego $R/(n-1)$. Se ocorrer a falha de mais do que um caminho, aos caminhos válidos é sempre atribuída a fracção do tráfego pedido dividido igualmente por eles.

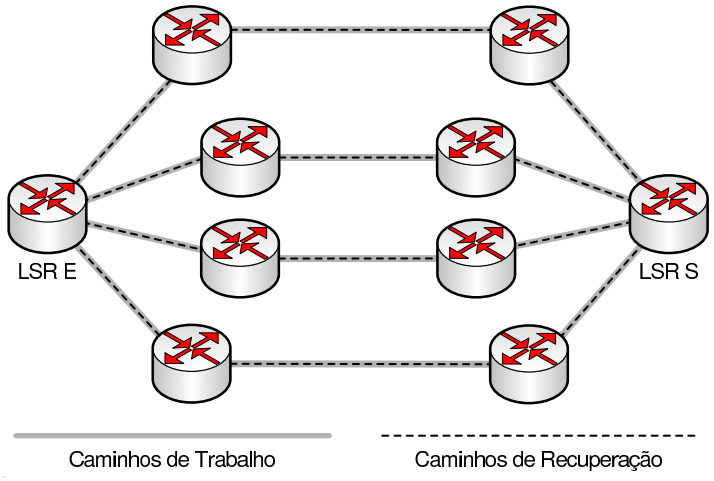

Figura 15: Exemplo do mecanismo FSM.

No mecanismo PSM, ilustrado na figura 16, apenas alguns dos n caminhos são utilizados como caminhos de trabalho, sendo os restantes utilizados como caminhos de protecção. Quando ocorrer a falha de alguns caminhos de trabalho a fracção de tráfego desses caminhos é movida para os caminhos de protecção. Logo que ocorra a recuperação desses caminhos o tráfego que era transportado nos caminhos de recuperação "regressa" aos caminhos de trabalho originais.

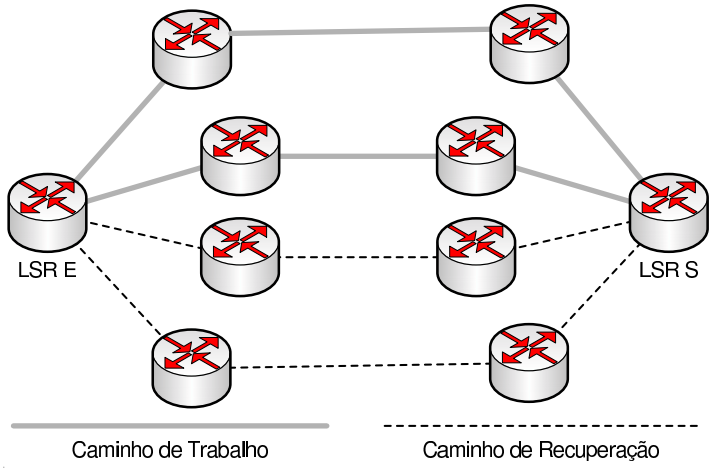

Figura 16: Exemplo do mecanismo PSM.

Através de um estudo comparativo a autora concluiu que, nas condições consideradas (em que todos os caminhos têm a mesma probabilidade de falha), o mecanismo PSM é tão bom como o mecanismo FSM em termos de fiabilidade. No entanto, isto só é válido quando no mecanismo PSM o número de caminhos de protecção for igual a $\lfloor (1-y)n \rfloor$, que é o número máximo de caminhos de protecção possível. Para ambos os mecanismos, apresentou soluções analíticas

que permitem determinar a quantidade de largura de banda B que é necessário reservar de acordo com a largura de banda R e a fiabilidade pedida. No estudo foi considerado que a largura de banda solicitada pelo serviço é igualmente distribuída pelos vários caminhos de trabalho e que em todos os caminhos é reservada a mesma largura de banda. Os mecanismos com essas restrições não são muito realistas.

3.1.10 Protecção extremo-a-extremo com multi-caminho

Menth et al. (2004) apresentam mecanismos de protecção por comutação e que utilizam os recursos de forma eficiente. Os mecanismos de protecção apresentados baseiam-se na utilização de caminhos de protecção extremo-a-extremo, e na utilização de múltiplos caminhos disjuntos pelos quais o tráfego é enviado simultaneamente (multi-caminho – *multi-path*). Pretendem minimizar a largura de banda a afectar aos ramos, dimensionando a rede para um determinado tráfego e optimizando a distribuição de carga através de algoritmos que correm em tempo polinomial (na prática, o encaminhamento e a largura de banda são optimizados simultaneamente).

Os autores propõem dois mecanismos, um dos quais designado por *Self-Protecting Multi-Paths* (SPM), que consiste na utilização de um multi-caminho, no qual é distribuído o tráfego. Se ocorre uma falha num dos caminhos o tráfego é distribuído pelos caminhos de trabalho restantes. O outro mecanismo, designado por protecção do caminho, tem como caminho de trabalho apenas um único caminho simples e um multi-caminho como protecção.

Foram comparadas três variantes do SPM que diferem na forma de distribuir a carga pelo multi-caminho: carga distribuída igualmente por todos os caminhos, factores de distribuição de carga inversamente proporcionais ao comprimento dos caminhos e optimização da distribuição de carga calculada através da resolução de um problema de programação linear para minimizar a capacidade extra requerida pela protecção.

O caminho primário, no mecanismo designado por protecção do caminho, pode ser determinado através da solução dos k caminhos disjuntos mais curtos *k-Disjoint Shortest Paths* (k DSP) ou através de um encaminhamento que minimize o fluxo de tráfego de trânsito em cada nó da rede. Cada uma destas duas possibilidades pode ser conjugada com diferentes formas de determinar os múltiplos caminhos de protecção: os caminhos de protecção podem ser calculados juntamente com um esquema apropriado de distribuição de carga através de resolução de problemas de programação linear; ou podem ser considerados os $k-1$ caminhos disjuntos mais curtos. Neste último caso, as formas de distribuir a carga podem ser as mesmas três utilizadas no SPM.

Estas variantes foram comparadas pelos autores relativamente à capacidade necessária para protecção em cada uma delas. Para tal foram utilizadas diferentes tipos de matrizes de tráfego e várias topologias de rede. Perante estes testes, os autores afirmam que a capacidade extra necessária para oferecer fiabilidade contra todas as falhas isoladas de ramos ou LSRs é apenas uma fracção da requerida pelo reencaminhamento OSPF. Verificaram também que a capacidade extra requerida depende da topologia da rede e em particular do número médio de caminhos disjuntos existentes, mas não da dimensão da rede.

O conceito geral dos mecanismos de protecção propostos (multi-caminhos) é semelhante ao

dos mecanismos propostos por Kim (2003). Menth et al. (2004) aprofundam estes conceitos nomeadamente na área da optimização do encaminhamento e de distribuição equilibrada da carga. A aplicação de algumas das abordagens a redes de grande dimensão parece difícil ou dependente de abordagens heurísticas ainda a desenvolver.

3.1.11 Recuperação rápida (dois esquemas)

Os esquemas de recuperação rápida (genericamente conhecidos por *Fast Reroute* (FRR)) utilizam o modelo protecção por comutação e em que a recuperação é efectuada pelo LSR mais próximo da falha.

Os dois esquemas do FRR são designados por *Facility backup* e *One-to-one backup* e foram normalizados recentemente, tendo sido o processo de normalização conduzido e documentado por Pan et al. (2005).

Os LSPs afectados por uma falha (isolada de um ramo ou nó) são recuperados localmente e os caminhos de protecção são estabelecidos antes de ocorrer a falha. Estas características tornam possível redireccionar o tráfego para os caminhos de protecção em tempos da ordem das dezenas de milisegundos, o que vai de encontro às necessidades das aplicações em tempo real.

É possível aplicar o esquema de recuperação apenas a um subconjunto de LSPs, os LSP sinalizados como a bandeira *local protection desired* activa. Esses LSPs poderão ter protecção com largura de banda garantida, caso a mesma tenha sido solicitada.

O protocolo de sinalização utilizado por estes dois esquemas é o RSVP-TE (RFC 3209 de Awduche et al. (2001)) com um conjunto adicional de extensões especificadas em Pan et al. (2005).

One-to-one backup Neste esquema de recuperação é necessário um caminho de protecção ("Detour LSP") em cada *Point of Local Repair* (PLR)[10] por cada LSP protegido, ou seja, cada LSR do LSP protegido terá que calcular um caminho de protecção com origem nesse nó e destino no LSR de saída desse LSP. A figura 17 apresenta um exemplo que ilustra esta característica do esquema de recuperação. Na figura o caminho de trabalho com origem no LSR1 e destino no LSR4 (1-2-3-4) é protegido com três caminhos de protecção, pois é criado um caminho de protecção em cada PLR . Por exemplo o LSR 1 cria o caminho de protecção seguindo os LSRs 1-5-6-7-4 para proteger o ramo 1-2 e o LSR 2.

Na figura 18 são ilustrados dois caminhos de trabalho seguindo os LSRs 1-2-3-4-5-8 e 9-2-3-4-5-12, respectivamente e dois caminhos de protecção respectivos (caminhos seguindo os LSRs 2-6-7-5-8 e 2-10-11-4-5-12). Repare-se que esses caminhos de protecção apenas protegem o ramo 2-3 e o LSR 3, para proteger outros recursos são necessários outros caminhos de protecção. É visível na figura que neste esquema os caminhos de protecção são criados por caminho de trabalho.

Como pode ser observado na figura 17 e na figura 18 este esquema tem a desvantagem de necessitar de um grande número de caminhos de protecção. Esse número não é apenas função

[10] O RFC (Pan et al., 2005) não utiliza a designação POR utilizando em seu lugar PLR.

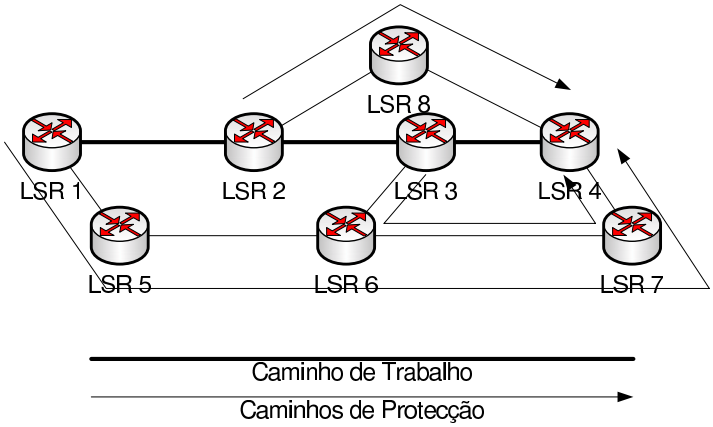

Figura 17: Exemplo com os vários caminhos de protecção de um LSP no *One-to-one backup*.

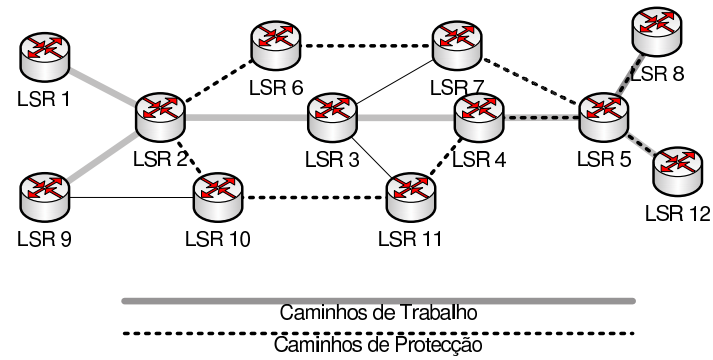

Figura 18: Exemplo de caminhos de protecção no *One-to-one backup*.

do número de caminhos protegidos mas é também função do comprimento desses caminhos (números de LSRs). Para minimizar este aspecto é feita a fusão, quando possível, de vários caminhos de protecção de um LSP protegido, e possivelmente também com o LSP protegido. Pan et al. (2005) definem várias regras para esse efeito. No exemplo da figura 17 o LSR 6 detecta que existem dois LSPs de protecção, para proteger o mesmo caminho de trabalho, e que portanto podem ser fundidos. Neste exemplo, os LSRs nos dois caminhos de protecção entre o LSR 6 e o LSR 4 são os mesmos por isso não existe vantagem em escolher qualquer um dos dois para caminho resultante da fusão, mas no caso de serem diferentes o caminho resultante da fusão seria o caminho de protecção mais curto.

Cada "Detour LSP"pode ser recalculado e actualizado pelo PLR sempre que este achar necessário.

Facility backup Neste esquema é criado um *bypass tunnel* para proteger contra a falha de um ramo ou para proteger contra a falha de um nó. Na figura 19 é configurado um *bypass tunnel* no LSR3 para proteger caminhos de trabalho que vão do LSR3 até ao LSR5 seguindo os ramos LSR3-LSR4 e LSR4-LSR5, contra a falha do ramo LSR3-LSR4 e do LSR4. Para qualquer uma destas falhas o PSL é o LSR3 e o PML é o LSR5.

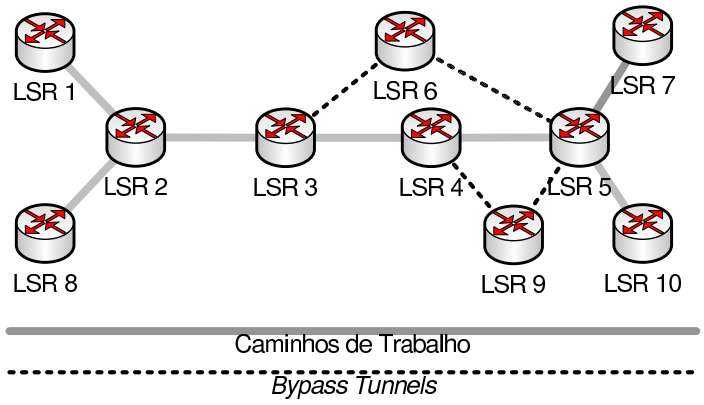

Figura 19: Exemplo de *bypass tunnels* na recuperação *Facility backup*.

No exemplo da figura 19 aparece também representado um segundo *bypass tunnel* do LSR4 ao LSR5 para proteger caminhos de trabalho que utilizem o ramo LSR4-LSR5.

Na figura 19 são apresentados exemplos dos dois tipos de *bypass tunnel* que é possível utilizar neste esquema de protecção, um *bypass tunnel* que protege contra a falha de um LSR (e necessariamente também de um ramo) e outro que protege apenas contra a falha de um ramo.

Este esquema de recuperação possui uma característica, muito importante em termos de escalabilidade: o número de *bypass tunnels* necessários não é uma função do número de caminhos de trabalho. Um *bypass tunnel* pode proteger um conjunto de LSPs que possuam restrições semelhantes em termos do caminho de protecção. Entre dois LSRs, para garantir largura de banda de protecção aos caminhos de trabalho, poderá existir mais do que um *bypass tunnel*, dependendo da forma como são calculados e sinalizados. Por exemplo, o número de *bypass tunnel* entre dois LSRs será elevado se for estabelecido um novo *bypass tunnel* cada vez que é sinalizado um novo LSP protegido.

3.2 Reencaminhamento

3.2.1 Caminho de recuperação pré-calculado

O esquema de recuperação proposto por Yoon et al. (2001) segue o modelo de recuperação por reencaminhamento local do tipo pré-calculado. Apresentam a sua proposta como sendo uma boa escolha quando um operador de rede pretende em simultâneo que o tempo de recuperação seja mínimo e que os recursos do caminho de recuperação sejam utilizados de forma o mais eficiente possível.

O caminho de recuperação é actualizado sempre que o LSR (que o calcula) recebe actualização da informação de estado da rede (utilização dos ramos). Nesse instante o caminho de recuperação calculado será óptimo de acordo com a informação do estado exacto dos recursos da rede. Assumem que as avarias possíveis são apenas falha ou degradação de um ramo e que se limitam a um único domínio de protecção MPLS.

Em cada caminho de trabalho, o LSR de entrada, e todos os LSRs intermédios com capacidade de recuperação pré-calculam um caminho de recuperação para o LSR mais próximo a jusante. Perante uma falha, o LSR que faz a recuperação será o mais próximo a montante desta, se tiver capacidade de recuperação. Se esse LSR não tiver capacidade de recuperação então será necessário enviar um FIS através da RNT[11]. O LSR, que faz a recuperação, estabelecerá o caminho de recuperação, no instante em que detecta a falha ou no instante em que recebe a notificação da falha, utilizado o CR-LDP. Quando o problema no ramo for reparado, o LSR que recebe o FRS liberta o caminho de recuperação e repõe o tráfego no caminho de trabalho original. O diagrama de fluxo apresentado na figura 20 resume o esquema proposto[12].

Em cada LSR com capacidade de recuperação, existe um processo que actualiza os caminho de recuperação, sempre que recebe uma actualização do estado da rede. Como isto implica a necessidade de troca de informação do desempenho da rede é necessário fazer uma extensão ao *Interior Gateway Protocol* (IGP) utilizado (por exemplo ao protocolo OSPF ou ao protocolo IS-IS).

Os autores comparam o esquema que propõem com um esquema semelhante mas em que o caminho de recuperação pré-calculado mantém-se inalterado independentemente do estado de congestão actual da rede. Nos estudos simulacionais realizados concluíram, quando simularam a avaria de um ramo, que o número de pacotes perdidos assim como o número de pacotes que precisam ser ordenados é menor no esquema proposto.

O esquema proposto utiliza os recursos de forma eficiente e o tempo de recuperação é reduzido dado calcular o caminho de recuperação antes da falha ocorrer. No entanto a grande vantagem do esquema proposto relativamente aos esquemas que seguem o modelo de recuperação por reencaminhamento está na actualização constante do caminho de recuperação, tendo em consideração a utilização dos ramos.

[11] Uma vez que os nós intermédios apenas calculam caminhos de recuperação (para um dado LSP) até ao nó adjacente a jusante, sempre que um nó é incapaz de resolver uma situação de falha o FIS será propagado até ao LSR de ingresso.

[12] O fluxograma da figura difere do fluxograma apresentado em Yoon et al. (2001) porque este não traduzia de forma completa o esquema aí proposto.

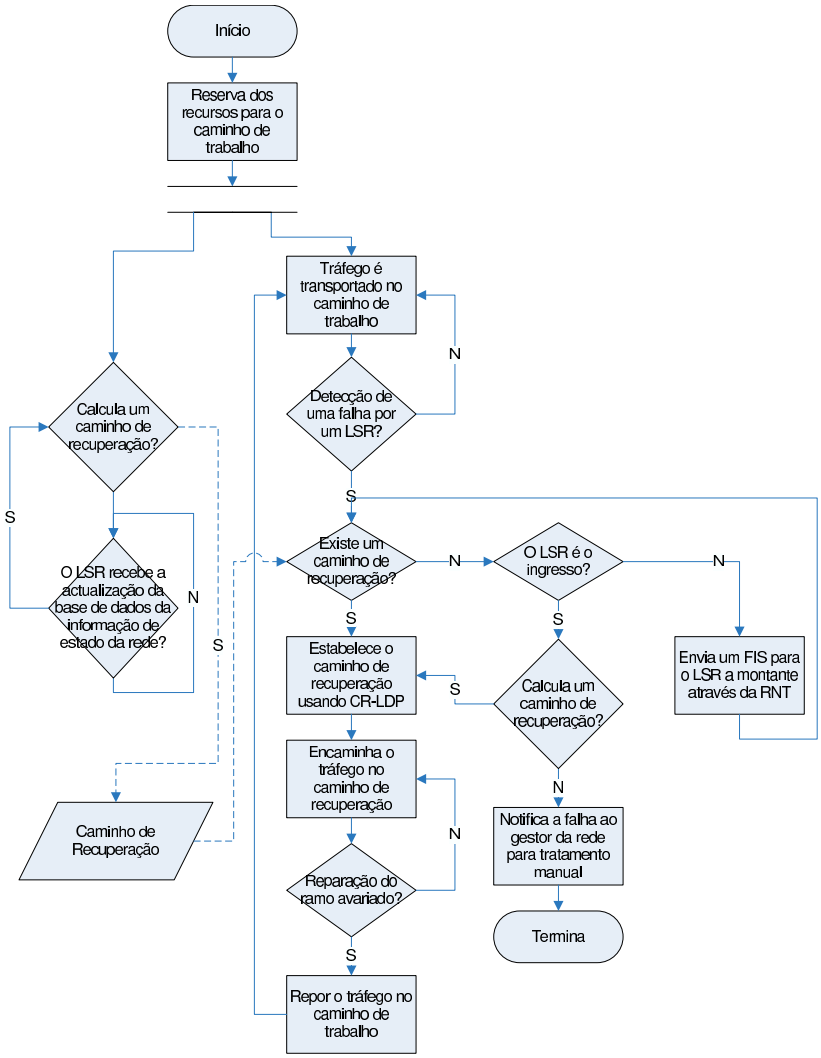

Figura 20: Diagrama de fluxo do esquema proposto por Yoon et al. (2001).

3.2.2 Caminhos de recuperação de menor custo

No esquema de recuperação proposto por Ahn et al. (2002), o caminho de recuperação é determinado e estabelecido, depois da falha ocorrer, pelo LSR a montante que a detectou. Para caminho de recuperação é escolhido aquele que tiver menor custo, de entre todos os caminhos alternativos possíveis. O caminho de recuperação só será utilizado enquanto a falha não for reparada.

No artigo é definido PML-candidato como um LSR do caminho de trabalho que pode ser usado como PML. Através das mensagens de sinalização utilizadas no estabelecimento dos caminhos de trabalho os LSRs podem obter conhecimento dos PML-candidatos. Os caminhos alternativos possíveis para caminhos de recuperação são todos os caminhos entre o LSR a montante que detecta a falha e cada PML-candidato.

A grande vantagem do esquema proposto é a sua eficiência em termos de utilização de recur-

sos pois utiliza o modelo de recuperação por reencaminhamento e escolhe para caminhos de recuperação os de menor custo.

Ahn et al. (2002) explicam como o reencaminhamento local poderia ser feito usando o CR-LDP. Pensamos que este método também é viável usando o RSVP-TE, recorrendo à sinalização proposta em (Gomes et al., 2005).

3.2.3 Recuperação hierárquica

Em Hong et al. (2004) os autores propõem um esquema de recuperação por reencaminhamento, cujos objectivos também são minimizar o tempo gasto na recuperação e maximizar a utilização de recursos da rede.

O esquema de recuperação tenta inicialmente encontrar um caminho alternativo utilizando apenas um número reduzido de LSRs, ou seja, começa com um âmbito da recuperação limitado de forma a minimizar o tempo gasto na recuperação. O âmbito da recuperação é expandido quando não for possível calcular um caminho de recuperação razoável, que contorne a falha, dentro do âmbito anteriormente determinado.

O processo de criação de um caminho de recuperação é um processo iterativo que segue os seguintes passos:

1. Determinação de um grafo pesado, para o qual os autores apresentam um algoritmo. As entradas para esse algoritmo são: o grafo da rede, o local da falha e métricas de tráfego (largura de banda requerida, classe de tráfego e número de "saltos").
2. Determinação de um LSR que possa ser o PSL (pode ser um LSR arbitrário do caminho de trabalho entre o LSR de entrada e o LSR mais próximo a montante que detectou a falha), após o que o âmbito da recuperação fica delimitado.
3. Tentativa para encontrar um caminho alternativo óptimo do PSL até ao LSR de saída do caminho de trabalho, tendo em consideração os requisitos do tráfego do caminho de trabalho. Os autores apresentam também um algoritmo para a selecção dinâmica do caminho alternativo.

Os dois primeiros passos do processo determinam o âmbito da recuperação, dinamicamente, em termos topológicos. De forma a que o âmbito da recuperação comece por ser o mais apertado possível, no passo dois do processo, o PSL seleccionado deve ser o LSR do caminho de trabalho, mais próximo da falha no sentido a montante, que tenha essa possibilidade. Nas iterações seguintes o PSL passa a ser um LSR do caminho de trabalho que se vai aproximando, em cada iteração, do LSR de entrada do caminho de trabalho. Assim, o âmbito da recuperação começa por ser uma pequena sub-rede delimitada pelo LSR de saída e pelo LSR adjacente à falha (a montante), se este LSR puder ser o PSL. Nas próximas iterações o âmbito da recuperação vai sendo expandido dinamicamente em função do local da falha e do estado da rede. O esquema é designado por esquema de recuperação hierárquica devido a este aspecto de expansão gradual do âmbito de recuperação. O âmbito da recuperação pode ser expandido até englobar toda a rede. A figura 21 mostra um exemplo de expansão do âmbito da recuperação. Assume-se que o ramo assinalado falhou. Considerando que não foi possível encontrar um caminho de

recuperação dentro do âmbito de recuperação **A** então o âmbito de recuperação foi expandido. Considerando que também não foi possível encontrar um caminho de recuperação dentro do âmbito de recuperação **B** então o âmbito de recuperação foi novamente expandido. O âmbito de recuperação **C** é a última possibilidade para encontrar um caminho de recuperação pois o LSR responsável pela recuperação coincide com o LSR de entrada.

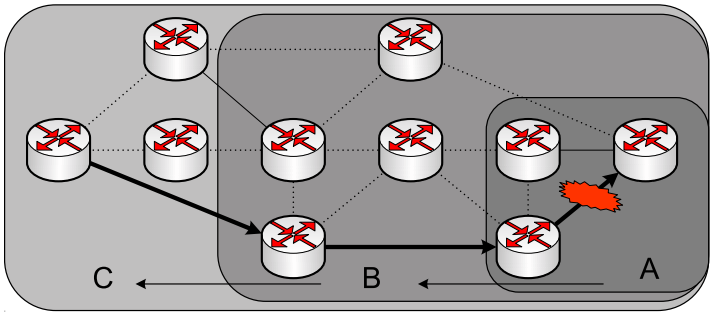

Figura 21: Exemplo de expansão do âmbito da recuperação (adaptada de Hong et al. (2004)).

Antes de uma nova iteração o PSL anteriormente determinado é definido implicitamente como um nó com avaria (*implicit abnormal node*) o que conduz a que o âmbito da recuperação seja extendido. O processo iterativo termina quando o algoritmo conseguir encontrar um caminho alternativo entre o PSL e o LSR de saída. Se o PSL for o LSR de entrada do caminho de trabalho, significa que o âmbito foi expandido até ao limite.

Logicamente quantas mais iterações forem efectuadas mais lenta será a recuperação mas, por outro lado, maior o âmbito da recuperação, o que melhora a utilização dos recursos.

O caminho de recuperação encontrado é estabelecido utilizando um protocolo de sinalização e é libertado quando a avaria for reparada. O esquema proposto abrange a recuperação de ramos ou nós e não tem o problema da falha simultânea do caminho de trabalho e do caminho de recuperação, como acontece nos esquemas de protecção por comutação.

Em geral, a eficiência deste esquema será tanto maior quanto mais limitado for o âmbito da recuperação. De facto, se for preciso aumentar o âmbito diversas vezes, torna-se necessário repetir cálculos e trabalhar com redes de maior complexidade. No entanto, como os próprios autores referem, a escolha de um âmbito muito reduzido levanta problemas de utilização de recursos por ignorar capacidades disponíveis noutras zonas da rede (problemas aumentados pela decisão de efectuar sempre a recuperação entre a falha e o fim do caminho, o que implica concentração de recursos na área da rede próxima do fim do caminho).

No método proposto, quando um PSL não consegue determinar um caminho de recuperação define-se esse PSL como um nó com avaria (*implicit abnormal node*), isto implica a alteração da sinalização para garantir que não é difundida informação errada do estado da rede. Pensamos no entanto que tal não é necessário, desde que um nó ao receber um FIS, com a indicação da localização da falha inferisse que todos os nós intermédios entre si próprio e o nó adjacente à falha não devem ser usados no caminho de recuperação a calcular - isto implica que cada LSR tem de conhecer o caminho total a recuperar.

3.2.4 Protecção dinâmica do caminho

Park et al. (2004) propõem um mecanismo de protecção dinâmica do caminho em redes MPLS que permite recuperar rapidamente a falha num ramo e/ou nó. No esquema proposto, quando um LSR detecta uma falha, ele selecciona um caminho de recuperação apropriado de entre os caminhos de trabalho já estabelecidos. O caminho seleccionado é um caminho que tenha o mesmo destino que o caminho que falhou. Se o LSR, local à falha, encontrar vários caminhos para o esse destino então a escolha é feita seguindo os critérios indicados por Park et al. (2004).

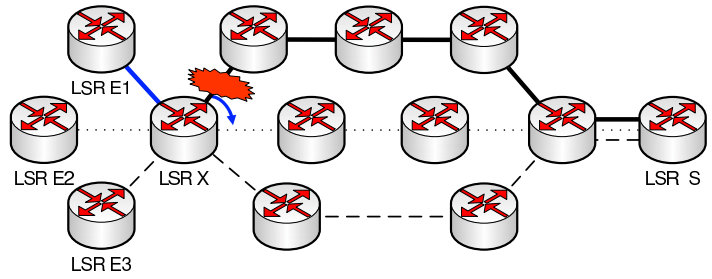

Figura 22: Rede exemplo com três caminhos de trabalho estabelecidos.

A figura 22 apresenta um cenário de falha num dos ramos em um dos três caminho de trabalho estabelecidos. Os LSRs de entrada dos três caminhos de trabalho são respectivamente o LSR E1, o LSR E2 e o LSR E3 e o LSR S é o LSR de saída comum. Considerando que ocorreu a falha indicada na figura, o LSR X ao verificar que possui dois caminhos estabelecidos para o mesmo destino, selecciona um deles e redirecciona o tráfego do caminho que falhou para ele.

Este esquema é rápido porque não requer a sinalização de um novo caminho, mas apenas alterações nas tabelas no LSR que redirecciona o tráfego para um LSP existente. Trata-se de uma forma de implementação do método pré-qualificado. No entanto, pode acontecer que o LSR não possua outro caminho estabelecido para o mesmo destino do caminho que falhou. Nesta situação o LSR estabelece localmente um novo caminho com origem em si e com o destino pretendido. Se o caminho de recuperação falhar, o esquema de protecção selecciona outro caminho de recuperação seguindo o mesmo procedimento utilizado na selecção do caminho de recuperação anterior.

Park et al. (2004) afirmam que o mecanismo não requer extensões aos protocolos de sinalização.

É discutível se o mecanismo poderá ser usado muitas vezes pois o número de caminhos alternativos pré-estabelecidos para o mesmo destino poderá ser reduzido. Outro problema é saber o que é que se faz com o tráfego que utilizava o caminho estabelecido que agora também é caminho de recuperação. Provavelmente se for mantido no mesmo caminho sofrerá uma degradação.

Redireccionamentos sucessivos podem ser utilizados, segundo Park et al. (2004), para lidar com falhas múltiplas. No entanto, esses sucessivos redireccionamentos, poderão dar origem a caminhos com ciclos os quais contribuirão para a degradação do funcionamento da rede.

3.3 Conclusões gerais acerca dos esquemas analisados

A tabela 2 resume, para os esquemas estudados, o modelo de recuperação utilizado e o âmbito da recuperação em termos topológicos.

1º autor do esquema	**modelo de recuperação**	**reparação local/global**
Haskin	protecção por comutação	local
Huang	"	global
Mellah	"	local
Kang	"	local
Bartoš	"	global, transitoriamente faz a recuperação local do tráfego recebido no LSR que detecta a falha
Yetginer	"	global
Kodialam	"	global ou local
Dana	"	global
Kim	"	global
Menth	"	global
Pan (2 esquemas)	"	local
Yoon	reencaminhamento	local
Ahn	"	local
Hong	"	local
Park	pré-qualificado	local

Tabela 2: Âmbito da recuperação em termos topológicos.

No trabalho de Kodialam e Lakshman (2002) são apresentados algoritmos (distintos) para recuperação global ou local, pelo que na tabela 4 é dito que o algoritmo suporta essas duas opções.

Para além dos apresentados na tabela 2, vários outros aspectos estão envolvidos na recuperação. Nesta secção vamos começar por relembrar alguns desses aspectos, e referir para cada um deles (os esquemas apresentados nas subsecções 3.1 e 3.2) os aspectos a que os respectivos autores deram ênfase especial.

A escolha dos **LSRs entre os quais é estabelecido o caminho de recuperação** é uma característica do esquema. Existem esquemas em que o LSR de entrada e o LSR de saída são o PSL e o PML respectivamente (recuperação global e extremo a extremo), noutros esquemas o PSL é o LSR mais próximo da falha a montante e o PML é o LSR mais próximo da falha a jusante (recuperação local). Entre estes dois extremos existem também vários outros esquemas, são exemplo destes os propostos por Ahn et al. (2002) e Hong et al. (2004).

Quando o PSL não é o LSR que detecta a falha, é necessário fazer-lhe chegar uma **mensagem de notificação da falha**. O trabalho por Huang et al. (2002) é centrado neste aspecto.

Como é sabido, nos esquemas de recuperação por reencaminhamento o caminho de recuperação só é estabelecido quando a falha ocorre. No entanto, o **instante do cálculo/actualização do caminho de recuperação** pode ocorrer em diferentes alturas antes da falha, o que fornece a base para o esquema proposto por Yoon et al. (2001).

Uma **recuperação extremamente rápida** foi o objectivo de Pan et al. (2005), ao conjugar o modelo de protecção por comutação com a recuperação local.

Em muitos dos esquemas de recuperação é estabelecido um caminho de recuperação para recuperar uma ou várias falhas do caminho de trabalho. É contudo possível **utilizar vários caminhos de recuperação simultaneamente** com distribuição de carga entre eles. A distribuição de carga pode ocorrer não só em caminhos de recuperação mas também em caminhos de trabalho. Kim (2003), Menth et al. (2004) e Dana et al. (2003) apresentaram propostas com base nesta possibilidade.

Outro aspecto é a utilização de um caminho/caminhos de recuperação por cada caminho de trabalho ou a utilização de **um caminho de recuperação para recuperar simultaneamente vários caminhos de trabalho**. Exemplo de um esquema que utiliza um só caminho para este último objectivo é o proposto por Mellah e Mohamed (2003) e mais recentemente o *Facility backup* (Pan et al., 2005).

Outra preocupação é **determinar o algoritmo de encaminhamento** a utilizar no cálculo dos caminhos de recuperação. Trabalhos focados nesta questão são os de Bartoš e Raman (2001), Yetginer e Karasan (2002) e Kang e Reed (2003), este último dedicado ao caso especial do encaminhamento em *bypass tunnels*. É comum serem apresentados algoritmos que calculam os caminhos de recuperação e de trabalho de forma integrada, como em Yetginer e Karasan (2002) e em Kodialam e Lakshman (2002).

Apresentamos a seguir uma abordagem resumida da forma como cada um dos aspectos anteriores é **tratado** por um dado esquema de recuperação em particular, escolhendo para cada um desses aspectos o esquema que o explorou em detalhe. Os esquemas são apresentados neste resumo geralmente pela mesma ordem que foi utilizada nas subsecções 3.1 e 3.2.

A característica essencial do esquema proposto por Haskin e Krishnan (2001) é a forma como é construído o caminho de recuperação. Este caminho além de um segmento de recuperação global possui também um segmento de recuperação no sentido inverso ao do caminho de trabalho. Este último segmento é utilizado, pelo LSR que detecta a falha, para transmitir de volta para o LSR de entrada os pacotes (que não conseguiu fazer chegar ao destino), conseguindo deste modo reduzir o número de pacotes perdidos. Apesar de neste esquema a recuperação ser global, devido à forma de construção do caminho de recuperação não é necessário enviar uma mensagem de notificação da falha, pois é o LSR que a detecta que faz a sua recuperação.

O objectivo principal do esquema proposto por Huang et al. (2002) é minimizar o atraso na propagação das mensagens de notificação da falha. Para atingir esse objectivo definiram uma estrutura para o envio das mensagens de notificação rápida e eficiente, um mecanismo de transporte leve para essas mensagens de notificação e um mecanismo para detecção de falhas.

O esquema de recuperação de Mellah e Mohamed (2003) utiliza um algoritmo de protecção local baseado na utilização de *bypass tunnels* pré-estabelecidos localmente por cada LSR para contornar a avaria de um ramo. O trabalho apresentado por Kang e Reed (2003) também se baseia na utilização de *bypass tunnels*, mas estes autores focam o seu estudo no problema do encaminhamento nesses túneis e apresentam uma resolução recorrendo à utilização de "*p*-cycles". Um dos esquemas de protecção, já normalizado em Pan et al. (2005), também é baseado na utilização de *bypass tunnels* mas ao contrário dos anteriores, em que os *bypass tunnels* só permitem a recuperação de ramos, aqui os *bypass tunnels* também permitem a recuperação de falhas em LSRs. Além deste esquema de *Fast Reroute*, é também apresentado em Pan et al. (2005) um outro em que são estabelecidos caminhos de recuperação por cada

caminho de trabalho.

O esquema proposto em Bartoš e Raman (2001) é também um esquema de protecção por comutação que utiliza recuperação global, mas que possui a particularidade de conseguir recuperar localmente o tráfego temporário que é recebido no LSR que detecta a falha, enquanto esse tráfego não for *switched over* para o caminho de protecção global. O realce do esquema vai para o algoritmo que propuseram para calcular os caminhos de protecção, que determina dois caminhos de protecção por cada LSR que oferece recuperação. Os dois caminhos de protecção são posicionados de forma que a falha de um ramo não causa a perda de conectividade simultânea em ambos. O algoritmo possui a vantagem da determinação os caminhos de protecção sem considerar a localização dos caminhos de trabalho. Esta característica do algoritmo permite a possibilidade de partilha de ramos entre caminhos de protecção e caminhos de trabalho, mas devido à forma como os dois caminhos de protecção são construidos é garantido que não existem situações em que a recuperação não seja possível.

O aspecto central explorado por Yetginer e Karasan (2002) é a forma como são determinados os caminhos. Os autores apresentam algoritmos para quatro abordagens para o processo de determinação *off-line* dos caminhos de trabalho e dos caminhos de recuperação, que vão desde a determinação dos caminhos separadamente até à integração do cálculo dos caminhos de trabalho e de recuperação. Todos os algoritmos para a determinação dos caminhos são formulados como problemas de programação linear inteira. Outra proposta de algoritmos para o cálculo dos caminhos de trabalho e de recuperação foi apresentada por Kodialam e Lakshman (2002). Mas, enquanto que em Yetginer e Karasan (2002) o cálculo é feito *off-line* para todos os pedidos, em Kodialam e Lakshman (2002) o cálculo é feito *on-line* pedido a pedido.

Foram revistos três esquemas (Dana et al., 2003; Kim, 2003; Menth et al., 2004) baseados na possibilidade da distribuição dos pacotes de um fluxo de tráfego por vários caminhos existentes entre um par de LSRs de entrada/saída. Em Kim (2003) e Menth et al. (2004) são apresentados dois mecanismos de distribuição de carga em cada, um dos quais é comum a ambos e consiste na utilização de múltiplos caminhos que são simultaneamente caminhos de trabalho e caminhos de protecção[13]. Nesse mecanismo em situações normais o tráfego é distribuído igualmente pelos vários caminhos estabelecidos. Quando um ou vários caminhos falham, o tráfego afectado é distribuído igualmente pelos caminhos válidos remanescentes. No outro mecanismo apresentado por Kim (2003) alguns caminhos do conjunto total são utilizados apenas como caminhos de trabalho e os restantes são utilizados apenas como caminhos de protecção. Neste mecanismo quando ocorrer a falha de alguns caminhos de trabalho a fracção de tráfego desses caminhos é movida para os caminhos de protecção. O caso particular em que é utilizado apenas um caminho de trabalho e vários caminhos de protecção corresponde ao segundo mecanismo apresentado por Menth et al. (2004). Para estas situações, ou seja, quando por cada caminho de trabalho é pré-estabelecido um conjunto de caminhos de protecção, Dana et al. (2003) apresentam um modo de obter as percentagens de tráfego que deve ser oferecido a cada LSP de protecção utilizando uma abordagem baseada em CBR (Aamodt e Plaza, 1994).

Yoon et al. (2001) propuseram um esquema de recuperação por reencaminhamento que minimiza o tempo de recuperação e aparentemente com boa taxa de sucesso. O factor de decisão é o instante em que se deve determinar o caminho de recuperação. Para conseguir o primeiro

[13] A semelhança reduz-se apenas a esta forma de utilização dos caminhos!

1° autor do esquema	LSR que faz a recuperação	Orientação	Falhas consideradas	Aspecto essencial
Haskin	LSR que detecta a falha	Caminho	Isoladas de ramos ou nós	Forma de construção do caminho de recuperação (constituído por 2 segmentos)
Huang	LSR de entrada do segmento a recuperar	Caminho	Isolada de nós ou ramos	Notificação e detecção da falha
Mellah	LSR que detecta a falha	Recurso	Isoladas de ramos	Utilização de *bypass tunnels*
Kang	LSR que detecta a falha	Recurso	Isoladas de ramos	Encaminhamento dos *bypass tunnels*
Bartoš	É o LSR de entrada mas inicialmente é o LSR que detecta a falha	Recurso /Caminho	Isoladas de ramos	Algoritmo de cálculo do caminho de recuperação
Yetginer	LSR de entrada	Caminho	Isoladas de ramos	Algoritmos de cálculo *off-line* dos caminhos de trabalho e de recuperação
Kodialam	LSR de entrada ou LSR que detecta a falha	Caminho	Isoladas de ramos ou nós	Algoritmos de cálculo *on-line* dos caminhos de trabalho e de recuperação
Dana	LSR de entrada	Caminho	Isoladas de ramos	Distribuição de carga
Kim	LSR de entrada	Caminho	Caminhos	Distribuição de carga
Menth	LSR de entrada	Caminho	Isoladas de ramos ou nós	Distribuição de carga
Pan	LSR que detecta a falha	Recurso	Isoladas de ramos ou nós	Recuperação rápida – Utilização de *bypass tunnels*
Pan	LSR que detecta a falha	Caminho	Isoladas de ramos ou nós	Recuperação rápida – Utilização de *detours*

Tabela 3: Protecção por Comutação.

objectivo o caminho de recuperação deve ser pré-calculado, mas para o segundo é necessário que o caminho de recuperação seja óptimo de acordo com o estado da rede na altura que a falha ocorre. Portanto, o esquema que propuseram, pré-calcula o caminho de recuperação e actualiza-o sempre que obtém actualização da informação do estado da rede.

Nos esquemas de recuperação propostos por Ahn et al. (2002) e Hong et al. (2004), o aspecto mais relevante é a escolha dos LSRs entre os quais deve ser estabelecido o caminho de recuperação, quando ocorrer uma falha. Ahn et al. (2002) escolheram sempre para PSL o LSR mais próximo a montante que detectou a falha mas, para PML permitem que seja usado qualquer LSR entre o LSR mais próximo da falha a jusante e o LSR de saída, e escolhem aquele LSR que permita obter o caminho de recuperação de menor custo. Por outro lado, Hong et al. (2004) escolheram para PML sempre o LSR de saída do caminho de trabalho. Para PSL começam por escolher o LSR a montante mais próximo da falha, e vão-se afastando da falha em direcção ao LSR de entrada até encontrar um caminho de recuperação que contorne a falha.

As tabelas 3 e 4 apresentam um resumo das características dos esquemas de recuperação descritos.

Como sumário final podemos dizer que a grande maioria dos esquemas de recuperação propostos utilizam o modelo de protecção por comutação (considerando apenas os esquemas analisados) e portanto a grande maioria dos esquemas de recuperação apenas se propõem recuperar

1° autor do esquema	Modelo de recuperação	LSR que faz a recuperação	Orientação	Aspecto essencial
Yoon	Reencaminhamento	Pode ser o LSR que detecta a falha ou o LSR de entrada, depende da situação encontrada	Caminho	Manter o caminho de recuperação óptimo pré-calculado
Ahn	Reencaminhamento	LSR que detecta a falha	Caminho	Forma de determinar o caminho de recuperação
Hong	Reencaminhamento	Pode ser qualquer LSR entre o LSR que detecta a falha e o LSR de entrada, depende da situação encontrada	Caminho	Forma de determinar o caminho de recuperação
Park	Pré-qualificado	LSR que detecta a falha	Caminho	Como escolher o caminho a utilizar na recuperação

Tabela 4: Recuperação por Reencaminhamento (e pré-qualificado).

de falhas isoladas. Para os esquemas que utilizam o modelo de recuperação por reencaminhamento estamos perante situações diversas. O esquema proposto por Yoon et al. (2001), uma vez que faz uso de caminhos pré-calculados para a recuperação, pode ter problemas no caso de falhas múltiplas. Já Ahn et al. (2002) consideram que o seu esquema recupera de falhas múltiplas uma vez que se trata de um esquema de recuperação por reencaminhamento em que o caminho de recuperação não está pré-calculado; e Hong et al. (2004) tratam explicitamente com a possibilidade de haver falhas múltiplas simultâneas. Park et al. (2004) afirmam que o seu esquema pode ser aplicado a redes sujeitas a falhas múltiplas. Tal só será possível se, existindo vários caminhos alternativos para o destino a partir do LSR que detectou a falha, algum destes não tiver falhado. Nos esquemas analisados, o LSR que faz a recuperação é sempre o PSL e nunca o PML, por conseguinte quando nas tabelas se diz que a recuperação é feita pelo LSR que detecta a falha, deve subentender-se o LSR a montante da falha. A recuperação é classificada como **orientada ao recurso** (ramo ou LSR) se tentar a recuperação de cada recurso da rede, independentemente dos caminhos de trabalho estabelecidos, ou **orientada ao caminho**, se tentar explicitamente recuperar o caminho de trabalho. No caso do esquema de Bartoš e Raman (2001) consideramos que a falha é orientada ao recurso/caminho[14] uma vez que recupera localmente o tráfego temporário que é recebido no LSR que detecta a falha e posteriormente usa caminhos de protecção global. Dos esquemas apresentados três são orientados ao recurso (dos quais dois são apenas orientados ao ramo), 12 esquemas são orientados ao caminho e um é orientado simultaneamente ao recurso e ao caminho.

Ao longo desta revisão foi chamada a atenção para o facto de alguns destes esquemas requererem extensões de sinalização, as quais nem sempre são referidas pelos respectivos autores.

A grande maioria dos autores dos esquemas de recuperação apenas apresentam a preocupação de recuperar falhas isoladas de ramos ou de ramos e nós. Embora os autores apresentem justificação para tal, estas justificações não tomam em consideração o facto de muitas redes poderem ser organizadas através de SRLGs, o que implica que falhas múltiplas podem ser bastante prováveis. No entanto, nos esquemas em que a recuperação é global mas as falhas múltiplas que ocorram se confinem aos recursos de um mesmo caminho de trabalho, também será possível, em princípio, a sua recuperação.

[14]No entanto, gostariamos de chamar a atenção para o facto deste esquema ao proteger um caminho está na realidade a proteger todos os caminhos entre um dado LSR de entrada e um dado LSR de saída.

4 Conclusões e Trabalho Futuro

Foram revistas as técnicas relativas à recuperação que podem ser usadas nas redes MPLS bem como propostas de esquemas de recuperação do tipo protecção por comutação e do tipo recuperação por reencaminhamento. Além de apresentar as características mais relevantes do funcionamento destes esquemas foram ainda tecidas algumas considerações acerca da sua aplicabilidade em redes reais. Finalmente foi apresentada uma resenha comparativa das suas características mais relevantes.

O estudo da possibilidade de utilização de diversos esquemas de recuperação simultaneamente, utilizando critérios de escolha do esquema em cada instante (por exemplo os tipos de serviços pedidos e o estado da rede) tendo em vista a conjugação das suas melhores características, é uma área a explorar. Assim poderá surgir uma proposta de recuperação que por um lado tire partido da articulação entre esquemas (conhecidos) e por outro incorpore alguma(s) variante(s) de esquemas descritos na literatura.

Referências

A. Aamodt e E. Plaza. Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI Communications*, 7(1):39–59, 1994.

G. Ahn, J. Jang, e W. Chun. An efficient rerouting scheme for MPLS-based recovery and its performance evaluation. *Telecommunication Systems*, páginas 481–495, 2002.

D. Awduche, L. berger, D. Gan, T. Li, V. Srinivasan, e G. Swallow. RSVP-TE: Extensions to RSVP for LSP tunnels. IETF RFC 3209, December 2001.

R. Bartoš e M. Raman. A heuristic approach to service restoration in MPLS networks. In *IEEE International Conference on Communications, ICC 2001*, volume 1, páginas 117–121, June 2001.

R. Bartoš, M. Raman, e A. Gandhi. New approaches to service restoration in MPLS-based networks. In *International Conference on Trends in Communications, EUROCON'2001*, volume 1, páginas 58–61, July 2001.

K. Borner. Structural similarity as a guidance in case-based design. In *Topics in Case-Based Reasoning - EWCBR*, páginas 197–208, 1994.

R. Braden, L. Zhang, S. Berson, S. Herzog, e S. Jamin. Resource reservation protocol (RSVP) – version 1 functional specification. IETF RFC 2205, September 1997.

A. Dana, A. K. Zadeh, K. Badie, M. E. Kalantari, e N. Reyhani. LSP restoration in MPLS network using case-based reasoning approach. In *Proceedings of ICCT2003*, páginas 462–468, 2003.

T. Gomes, P. Nunes, e L. Jorge. Explorando a recuperação de redes baseada em mecanismos do MPLS. Technical Report 11, INESC - Coimbra, Coimbra, Portugal, July 2005.

W. D. Grover e D. Stamatelakis. Cycle-oriented distributed preconfiguration: Ring-like speed with mesh-like capacity for self-planning network restoration. In *Proceedings of IEEE ICC'98*, páginas 537–543, Atlanta, Georgia, June 1998.

D. Haskin e R. Krishnan. A method for setting an alternative label switched paths to handle fast reroute. IETF Draft, April 2001.

D.-K. Hong, C. S. Hong, e Dongsik-Yun. A hierarchical restoration scheme with dynamic adjustment of restoration scope in an MPLS network. In *Network Operations and Management Symposium*, páginas 191–204, April 2004.

C. Huang, V. Sharma, K. Owens, e S. Makam. Building reliable MPLS networks using a path protection mechanism. *IEEE Communications Magazine*, páginas 156 – 162, March 2002.

B. Jamoussi, L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, M. Girish, E. Gray, J. Heinanen, T. Kilty, e A. Mallis. Constraint-based LSP setup using LDP. IETF RFC 3212, January 2002.

J. Kang e M. J. Reed. Bandwith protection in MPLS networks using p-cycle structure. In *Design of Reliable Communication Networks (DRCN) 2003*, páginas 356–362, Banff, Alberta, Canada, October 2003.

S.-Y. Kim. Effect of load distribution in path protection of MPLS. *International Journal of Communication Systems*, 16(4):321–335, February 2003.

M. Kodialam e T. V. Lakshman. Dynamic routing of bandwidth guaranteed tunnels with restoration. In *IEEE INFOCOM 2000*, páginas 902–911, 2000.

M. Kodialam e T. V. Lakshman. Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information. In *Proceedings of IEEE INFOCOM 2001*, páginas 376–385, April 2001.

M. Kodialam e T. V. Lakshman. Restorable dynamic quality of service routing. *IEEE Communications Magazine*, páginas 72–81, June 2002.

J. L. Marzo, E. Calle, C. Scoglio, e T. Anjali. QoS online routing and MPLS multilevel protection: A survey. *IEEE Communications Magazine*, páginas 126–132, October 2003.

H. Mellah e A. F. Mohamed. Local path protection/restoration in MPLS-based networks. In *The* 9^{th} *Asia-Pacific Conference on Communications - APCC 2003*, volume 2, páginas 620–622, September 2003.

M. Menth, J. Milbrandt, e A. Reifert. End-to-end protection switching mechanisms for MPLS networks. Technical Report 320, University of Wurzburg, Institute of Computer Science, February 2004.

P. Pan, G. Swallow, e A. A. (Eds.). Fast reroute extensions to RSVP-TE for LSP tunnels. IETF RFC 4090, May 2005.

P.-K. Park, H.-S. Yoon, S. C. Kim, J. Park, e S. Yang. Design of a dynamic path protection mechanism in MPLS networks. In *The* 6^{th} *International Conference on Advanced Communication Technology*, volume 2, páginas 857–861, 2004.

C. Qiao e D. Xu. Distributed partial information management (DPIM) schemes for survivable networks - part I. In *Proceedings of IEEE INFOCOM 2002*, páginas 302 –311, 2002.

E. Rosen, A. Viswanathan, e R. Callon. Multiprotocol label switching architecture. IETF RFC 3031, January 2001.

V. Sharma, F. Hellstrand, B. Mack-Crane, S. Makam, K. Owens, C. Huang, J. Weil, B. Cain, L. Anderson, B. Jamoussi, A. Chiu, e S. Civanlar. Framework for multi-protocol label switching (MPLS)-based recovery. IETF RFC 3469, February 2003.

D. Stamatelakis e W. D. Grover. IP layer restoration and network planning based on virtual protection cycles. *IEEE Journal on Selected Areas in Communications*, 18(10):1938–1949, October 2000a.

D. Stamatelakis e W. D. Grover. Theoretical underpinnings for the efficiency of restorable networks using preconfigured cycles ("p-cycles"). *IEEE Transactions on Communications*, 48(8):1262–1265, August 2000b.

J. W. Suurballe e R. E. Tarjan. A quick method for finding shortest pairs of disjoint paths. *Networks*, 14(2):325–336, 1984.

J.-P. Vasseur, M. Pickavet, e P. Demeester. *NETWORK RECOVERY - Protection and restoration of optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann, 2004.

E. Yetginer e E. Karasan. Robust path design algorithms for traffic engineering with restoration in MPLS networks. In *Proceedings of the Seventh International Symposium on Computer and Communications - ISCC 2002*, páginas 933–938, 2002.

S. Yoon, H. Lee, D. Choi, Y. Kim, G. Lee, e M. Lee. An efficient recovery mechanism for MPLS–based protection LSP. In *Joint 4^{th} IEEE International Conference on ATM (ICATM 2001)*, páginas 75–79, Seoul, Korea, April 2001.

A Acrónimos

CBR *Case-Based Reasoning*

CR-LDP *Constraint-based Routing – Label Distribution Protocol*

k **DSP** *k-Disjoint Shortest Paths*

FRR *Fast Reroute*

FEC *Forwarding Equivalence Class*

FIS *Fault Indication Signal*

FRS *Fault Recovery Signal*

FSM *Fully Shared Mechanism*

IGP *Interior Gateway Protocol*

IP *Internet Protocol*

IS-IS *Itermediate System – to – Itermediate System*

LB Largura de Banda

LDP *Label Distribution Protocol*

LSP *Label Switched Path*

LSR *Label Switching Router*

MPLS *MultiProtocol Label Switching*

OSPF *Open Shortest Path First*

PLR *Point of Local Repair*

PML *Path Merge LSR*

POR *Point of Repair*

PPG *Protected Path Group*

PSL *Path Switch LSR*

PSM *Partially Shared Mechanism*

RFC *Request For Comments*

RNT *Reverse Notification Tree*

RSVP *Resource Reservation Protocol*

RSVP-TE *Resource Reservation Protocol with Traffic Engineering*–Neste trabalho chamamos protocolo RSVP-TE à conjugação do protocolo RSVP (Braden et al., 1997) com as extensões RSVP-TE (Awduche et al., 2001)

SONET *Synchronous Optical Network*

SPM *Self-Protecting Multi-Paths*

SRLG *Shared Risk Link Group*

WDM *Wavelength Division Multiplexing*