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

Teresa Gomes
Pedro Nunes
Luísa Jorge

Explorando a recuperação de redes baseada em mecanismos do MPLS

No.11 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

Explorando a recuperação de redes baseada em mecanismos do MPLS

Teresa Gomes[1,2], Pedro Nunes[3] e Luísa Jorge[2,4]

[1]Departamento de Engenharia Electrotécnica,
Pólo II da Universidade de Coimbra,
Pinhal de Marrocos, 3030-290 COIMBRA. Portugal.

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

[3] Siemens, Systems Engineering - Carrier Networks
Ed. 1, Piso 1, Siemens SA
Rua Irmãos Siemens, 1 2720-093 AMADORA. Portugal.

[4] Escola Superior de Tecnologia e Gestão do
Instituto Politécnico de Bragança
Campus de St^{a} Apolónia, 5301-857 BRAGANÇA. Portugal.

e-mail: teresa@deec.uc.pt, pedro.nunes@siemens.com, ljorge@inescc.pt

15 de Julho de 2005

Resumo

As redes de dados, nomeadamente as redes baseadas em IP têm visto o seu tráfego aumentar de forma significativa nos últimos anos. Simultaneamente essas redes têm sido confrontadas com a necessidade de fornecer serviços com diferentes garantias de QoS. Os mecanismos de rede IP, baseados apenas no destino do tráfego, tendem a utilizar de forma pouco eficiente os recursos da rede. Por outro lado têm grande dificuldade em garantir graus de serviço diferenciados, pelo que em geral recorrem ao sobre-dimensionamento das redes.

As redes MPLS procuram garantir uma melhor utilização dos recursos da rede e simultâneamente garantir qualidade de serviço diferenciado, conforme o solicitado pelos diferentes serviços. Nesse contexto é importante garantir que quando há falhas na rede alguns serviços não são afectados e que os efeitos sobre os restantes serão minimizados tanto quanto possível. Um mecanismo designado por FRR, recentemente estabilizado na forma no RFC 4090, garante a recuperação de LSPs na gama das dezenas de milisegundos, utilizando LSPs de recuperação pré-estabelecidos. Relativamente a mecanismos de recuperação por re-encaminhamento (local) não há nenhuma normalização proposta.

Serão aqui analisadas as possibilidades de recuperação por re-encaminhamento sem extensão do RSVP-TE, concluindo-se que a mesma só é viável em situações particulares. Será seguidamente apresentada uma proposta de extensão do RSVP-TE de forma a suportar re-encaminhamento local de forma eficiente.

Relativamente aos mecanismos de protecção por comutação, embora o FRR suporte partilha de largura de banda entre um LSP protegido e os respectivos LSPs de protecção, não está ainda normalizado nenhum esquema que permita a implementação de partilha de largura de banda utilizada por LSPs de protecção de LSP protegidos diferentes. Será aqui proposto um esquema que permite a sua implementação sem extensão do RSVP-TE (embora exija que os LSRs capazes de o implementar, possuam mecanismos de controlo das reservas mais elaborados).

Será ainda proposto um mecanismo de protecção extremo-a-extremo (com extensão do RSVP-TE) que permite a partilha de LB entre LSPs de protecção de LSPs activos disjuntos.

Conteúdo

1 Introdução

As redes de dados, nomeadamente as redes baseadas em IP têm visto o seu tráfego aumentar de forma significativa nos últimos anos. A oferta de serviços como VoIP (*Voice over-Internet Protocol*) que possui requisitos estritos quanto ao atraso, implicou a necessidade de garantir um tratamento diferenciado para este tipo de serviços face às necessidades do serviço *best-effort*, tradicionalmente oferecido pelas redes IP. Os mecanismos de rede IP, baseados apenas no destino do tráfego, tendem a utilizar de forma pouco eficiente os recursos da rede; por outro lado têm grande dificuldade em garantir graus de serviço diferenciados, pelo que em geral recorrem ao sobre-dimensionamento das redes.

As redes MPLS (*Multiprotocol Label Switching*) procuram garantir uma melhor utilização dos recursos da rede e simultâneamente garantir qualidade de serviço diferenciada, conforme o solicitada pelos diferentes serviços. As redes MPLS procuram explorar a rapidez dos mecanismos da rede IP, conjugando-a com o controlo de fluxo de tráfego, conseguido introduzindo mecanismos orientados à ligação, cuja eficácia já foi comprovada nas redes de comutação de circuitos e nas redes ATM (*Asynchronous Transfer Mode*) [HHS94]. Este controlo conjugado com mecanismos de CAC (*Call Admission Control*) do DiffServ (*Differentiated Services*) permitem garantir por um lado tratamento diferenciado dos serviços e por outro uma distribuição uniforme da carga na rede (ou seja uma boa utilização dos recursos da rede).

Entre as medidas relevantes da qualidade de serviço está a disponibilidade desse mesmo serviço. Nesse contexto é importante garantir que quando há falhas na rede alguns serviços não são afectados (os serviços *gold*) e que os efeitos sobre os restantes serão minimizados tanto quanto possível. O RFC 3469 [SHMC$^+$03] define o enquadramento da recuperação de falhas baseada no MPLS. São aí apresentados dois modelos básicos de recuperação de um LSP: protecção por comutação (*protection switching*) e re-encaminhamento (*rerouting*). Na protecção por comutação um caminho, ou um segmento de um caminho, é pré-estabelecido; se ocorrer uma falha que afecte o LSP protegido o seu tráfego será redireccionado (*switched-over*) para o caminho de protecção; a recuperação por re-encaminhamento consiste no estabelecimento, *usando sinalização*, de um novo caminho ou segmento de um caminho após a ocorrência de uma falha, para o qual o tráfego será em seguida redireccionado. Devido à necessidade de inter-funcionamento de equipamentos produzidos por fabricantes diferentes, surgiu a necessidade de normalização do mecanismo designado por FRR (*Fast ReRoute*), o qual consiste numa recuperação rápida de um LSP (o LSP protegido) recorrendo a LSPs de protecção pré-estabelecidos. O IETF elaborou recentemente o RFC 4090 [PSA05], o qual garante a recuperação de LSPs (em cenários de falha isolada no domínio MPLS) na gama das dezenas de milisegundos.

Um dos inconvenientes do FRR, com protecção de largura de banda (LB) do LSP protegido é a necessidade de reservar LB que só será utilizada em situações de avaria. Embora o FRR suporte partilha de LB entre um LSP protegido e os respectivos LSPs de protecção (os *Detours*), não está ainda normalizado nenhum esquema que permita a implementação da partilha da LB utilizada por LSPs de protecção de LSPs protegidos diferentes. Será aqui proposto um esquema que permite a sua implementação sem extensão do RSVP-TE (embora exija que os LSRs (*Label Switch Router*) capazes de o implementar, possuam mecanismos de controlo das reservas mais elaborados).

A recuperação por re-encaminhamento recebeu muito menos atenção (que a protecção por comutação utilizada no FRR) devido à sua lentidão (potencial) face aos mecanismos de protecção, pelo que não existe nenhuma normalização proposta para a implementação de re-encaminhamento (local). Este mecanismo apresenta no entanto as seguintes vantagens: não consome recursos antes da ocorrência de uma falha e permite a recuperação em cenários de falha não isolada no domínio MPLS (por exemplo no caso de ocorrer um corte de cabos numa conduta, este acidente aparecerá no domínio MPLS como um conjunto de falhas simultâneas). Relativamente à lentidão potencial do mecanismo de recuperação por re-encaminhamento considera-se que este pode ser fortemente mitigado se forem utilizados mecanismos de re-encaminhamento local, como se mostrará na secção 5.

Seguidamente, na sub-secção 1.1 serão apresentados alguns conceitos propostos no RFC 3469 [SHMC+03] e RFC 4090 [PSA05]. Na secção 1.2, são revistos os mecanismos previstos no RSVP-TE para partilha de LB intra-LSP (ou seja entre um LSP protegido e os LSPs que o protegem) e o método de re-encaminhamento usando *make-before-break*, uma vez que os mesmos são relevantes para analisar as possibilidades de estabelecimento de LSPs de recuperação em métodos de recuperação por re-encaminhamento. Na sub-secção 1.3 é explicado como são assinalados os erros numa rede IP/MPLS. Finalmente na sub-secção 1.4 é apresentada a organização restante deste relatório.

1.1 Breve revisão de algumas definições no RFC 3469 e RFC 4090

Em MPLS designa-se por caminho de trabalho, activo ou primário, como sendo o caminho que transporta o tráfego e designa-se por caminho de recuperação, protecção, alternativo ou de *backup* ao caminho usado para transportar o tráfego após a ocorrência de uma avaria que afectou o LSP activo [SHMC+03, pág. 14].

Consoante o papel desempenhado por um LSR na operação de recuperação estes recebem diferentes designações [SHMC+03, pág. 15]:

PSL (*Path Switch LSR*): um LSR responsável por comutar ou replicar o tráfego entre o caminho activo e o caminho de recuperação.

PML (*Path Merge LSR*): Um LSR que é responsável por receber o tráfego do caminho de recuperação, e funde esse tráfego de volta para o caminho activo ou, caso seja o destino desse tráfego, o passa aos protocolos de nível superior.

POR (*Point of Repair*): Um LSR configurado para efectuar uma recuperação baseada em mecanismos do MPLS. O POR poderá ser o PSL ou o PML.

(*Intermediate LSR*): Um LSR, do caminho activo ou de protecção, que não é um PSL nem um PML. Será designado por LSR intermédio.

Um POR será um PML, por exemplo em sistemas de protecção 1+1. Um POR será um PSL, quando efectua a operação de redireccionamento do tráfego do LSP protegido para o LSP de protecção, após a detecção de uma falha.

Iremos designar por LSR de trânsito de um LSP activo, qualquer LSR no seu caminho que não seja nem o LER de ingresso nem o LER de egresso.

No RFC 3469, um caminho activo poderá ser:

> "a hop-by-hop routed path, a trunk, a link, an LSP, or a part of a multipoint-to-point LSP."

Na recomendação Y.1720 da ITU-T [ITU03] surgem definições semelhantes às propostas para PSL e PML no RFC 3469, mas em que o caminho é agora apenas um LSP.

No RFC 4090 [PSA05] aparecem as seguintes definições:

MP (*Merge Point*): O LSR onde um ou mais LSPs de protecção se juntam ao LSP protegido, a jusante da falha potencial.

DMP (*Detour Merge Point*): O LSR onde múltiplos *Detours* (LSPs de protecção) convergem e apenas um deles é sinalizado desse LSR em diante.

PLR (*Point of Local Repair*): O LSR origem de um LSP de protecção, seja ele um *Detour* ou um túnel de protecção (n:1).

É ainda definido um túnel de *bypass* (*bypass tunnel*), como um caminho que permite proteger um conjunto de caminhos activos usando a técnica de empilhamento de etiquetas [RTF+01]. Neste caso esses caminhos devem todos possuir o mesmo PSL e PML.

A recuperação pode ser local ou global. Na recuperação global, também designada por recuperação extremo-a-extremo, o caminho de recuperação deverá proteger todo o caminho activo. O PSL será sempre o LER (*Edge* LSR) de ingresso do LSP. No caso da reparação local, o LSR imediatamente a montante (*upstream*) do local onde ocorreu a falha deverá iniciar a operação de recuperação e deverá ser o PSL.

Em [PSA05] o caminho activo para o qual foi solicitada protecção (de nó ou arco) é designado por caminho protegido. No caso de um LSP cujo mecanismo de recuperação é o re-encaminhamento (também designado por protecção dinâmica) não parece correcto usar essa designação (ou seja designar por caminho protegido o caminho activo) pois o caminho activo só fica efectivamente protegido depois de efectuada a acção de recuperação (cujo sucesso não é garantido, mesmo em cenário de avaria isolada).

No caso do re-encaminhamento local o POR é o LSR que recupera o LSP em falha e é também o LSR que faz o *switch over* do tráfego do LSP activo para o LSP de recuperação, ou seja, neste caso o POR é sempre o PSL. Neste contexto será indiferente falar-se no POR ou no PSL, dando-se preferência a esta última designação.

Algumas vezes é difícil distinguir quando se está a falar do LSP activo, do LSP que resulta de uma acção de recuperação ou de protecção e do LSP que foi usado para conseguir essa recuperação. Assim, no caso do re-encaminhamento local, falar-se-á no LSP de recuperação como o LSP que é criado desde o PSL até ao PML e no LSP recuperado como o LSP que resultou dessa acção de recuperação (cujo caminho se inicia no LER de ingresso e termina no LER de egresso). Quando o PSL é o LSR de ingresso do LSP activo, o "LSP recuperado" é constituído por dois segmentos: o primeiro desde o LSR de ingresso até ao PML e o segundo desde o PML até ao LSR de egresso; se o PML for o LSR de egresso, então o LSP recuperado coincide com o LSP de recuperação. Geralmente o LSP recuperado será constituído por três

segmentos: o primeiro que vai desde o LSR de ingresso do LSP activo até ao PSL; o segundo, que coincide com o LSP de recuperação, vai do PSL até ao PML; e o terceiro que vai do PML até ao LER de egresso e que coincide com o segmento do LSP activo desde o PML até ao LER de egresso. Quando o PML não coincide com o LER de egresso do LSP activo, o segmento final será sempre referido como pertencendo ao LSP activo (e não ao LSP de recuperação) – isto significa que a operação de fusão feita pelo PML entre o LSP activo e de recuperação (calculado desde o PSL até ao LER de egresso) resulta sempre no LSP activo que se está a recuperar.

Não será aqui analisado o re-encaminhamento global como forma de recuperação, pois este já existe por omissão no MPLS. Corresponde a fazer um re-encaminhamento porque o estado da rede se alterou. Será em geral desencadeado quando a mensagem de aviso de erro num LSP chega ao seu LER de ingresso.

Uma descrição detalhada do RFC 3469 [SHMC+03] encontra-se em [JG05].

1.2 Partilha de LB e re-encaminhamento usando o RSVP-TE

O RSVP [BZB+97] faz por omissão a fusão de estados RSVP que sejam identificados como pertencendo à mesma sessão. O significado de sessão no RSVP e no RSVP-TE é diferente [AHX01, pág. 3]:

> "In the RSVP-TE specification, however, a session is implicitly defined as the set of packets that are assigned the same MPLS label value at the originating node of the LSP-tunnel."

Em [PSA05, pag. 18] diz-se que os campos relevantes (numa mensagem *Path*) que identificam um túnel LSP são cinco, dos quais três no objecto `SESSION`:

- `IPv4 (or IPv6) tunnel end point address`
- `Tunnel ID`
- `Extended Tunnel ID`

e dois no objecto `SENDER_TEMPLATE`:

- `IPv4 (or IPv6) tunnel sender address`
- `LSP ID`

e ainda que

> "A backup LSP is considered to be part of the same session as its protected LSP; therefore these three cannot be varied."

em que o *three* se refere aos três elementos anteriores do objecto `SESSION`.

No FRR são propostas duas formas de sinalizar *Detours* [PSA05]: *Path-Specific* e *Sender Template-Specific*, cujas características principais se passa a descrever. No método *Path-Specific*, a mensagem *Path* inicial de um *Detour*, contém os cinco campos anteriores (contidos na mensagem *Path* do LSP activo) inalterados, sendo-lhe acrescentado o objecto `DETOUR` – o LSP protegido e um *Detour* correspondente são distinguidos porque o primeiro contém um objecto `FAST_REROUTE` e/ou a bandeira *Local protection requested* activa no objecto `SESSION_ATTRIBUTE`. No método *Sender Template-Specific* o `IPv4 (or IPv6) tunnel sender address` é modificado e passa a conter o endereço do PLR (se este for o LER de ingresso do LSP este deve escolher um endereço IP diferente do presente no objecto `SENDER_TEMPLATE` do LSP activo).

A partilha de LB entre o LSP protegido e os *Detours* (que o protegem) sinalizados usando o método *Path-Specific*, é feita automaticamente pelo RSVP-TE pois são considerados como pertencendo à mesma sessão (o quinteto anterior não foi modificado).

A partilha de LB entre o LSP protegido e os *Detours* (que o protegem) sinalizados usando o método *Sender Template-Specific*, só será feita automaticamente pelo RSVP-TE, se o LSP original (e os *Detours*) tiverem sido sinalizados usando o estilo SE (*Shared Explicit*): para que sejam vistos como *senders* diferentes da mesma sessão RSVP que podem partilhar uma mesma reserva.

Em [ABG+01, pág. 10-13] fica explícito que dois LSPs com o mesmo ERO (a partir de um dado LSR), que usem o estilo SE poderão partilhar recursos entre si, desde que tenham o mesmo objecto `SESSION`.

O mecanismo *make-before-break* baseia-se em considerar que um LSP pode partilhar LB consigo próprio, modificando o seu `LSP ID` (mantendo os restantes campos inalterados) desde que seja sinalizado com o estilo SE [ABG+01, pág. 12-13 e 42]. A descrição da utilização dessa técnica para fazer o re-encaminhamento suave de um LSP ou um aumento da LB reservada por este encontra-se em [ABG+01, pág. 13].

As formas atrás descritas de partilhar LB usando o RSVP-TE não contemplam a possibilidade de partilha entre LSPs de sessões RSVT-TE diferentes!

1.3 Indicação de falha numa rede IP/MPLS

Segundo [VPD04, pág. 310-1] a indicação de uma falha (FIS - *Fault Signal Indication*) num arco e/ou num nó numa rede IP/MPLS será feita através de uma actualização do IGP (*Interior Gateway Protocol*) e de uma mensagem *Path Error* do RSVP, gerados de forma independente.

No caso do IGP os nós que detectam uma falha gerarão uma actualização do LSA (*Link State Advertisement*). A recepção pelo LER de ingresso de um LSP de uma mensagem de *Path Error* irá em geral desencadear a re-optimização do LSP em causa.

Em [ABG+01] é apresentada a extensão do RSVP ao protocolo *Hello* o qual permite a um nó detectar se outro nó vizinho está ou não acessível. Esta extensão tem como objectivo permitir detectar falhas de nós quando a notificação de falhas na *link layer* não está disponível ou quando os mecanismos fornecidos por essa camada são demasiados lentos para a detecção

atempada da avaria de um nó.

Um LSR com FRR, ao detectar a falha de um LSP protegido, por avaria de um link ou nó adjacente que faz parte do caminho desse LSP, desvia o respectivo tráfego para o *Detour* previamente sinalizado ou para o túnel de *bypass* previamente escolhido pelo PLR. Seguidamente e caso se tenha efectuado uma recuperação com sucesso, o PLR deverá activar a bandeira *Local protection in use* no objecto `RRO` (caso o possua) do LPS protegido [PSA05, pág. 26]. O PLR deverá enviar uma mensagem *Path Error* indicando que o LSP foi reparado localmente, para o que enviará o código *Notify* (código de erro = 25) e um valor do campo de erro cujo significado é *Tunnel locally repaired* [ABG+01, pág. 57] e [PSA05, pág. 27].

O LER de ingresso, de um LSP recuperado usando FRR ou recuperado por re-encaminhado local, poderá optar por solicitar informação acerca do novo caminho enviando uma mensagem *Path* com um objecto RRO (*Record Route Object*) [ABG+01, pág. 35], antes de proceder ao re-encaminhamento de optimização.

1.4 Organização deste texto

Este relatório encontra-se organizado da seguinte forma. Na secção 2 serão revistas as várias formas possíveis de fazer recuperação por re-encaminhamento, segundo o RFC 3469 [SHMC+03]. Na secção 3 são revistas brevemente algumas propostas de re-encaminhamento e será chamada a atenção para as dificuldades de sinalização associadas (utilizando o RSVP-TE). Na secção 4 são analisadas as possibilidades de implementação de re-encaminhamento local sem extensão do RSVP-TE e são apontados os seus inconvenientes. Na secção 5 é feita uma proposta de extensão do RSVP-TE necessária à implementação eficiente de re-encaminhamento local. Na secção 6 é feita uma breve revisão de duas forma de fazer protecção: global (sub-secção 6.1) e local baseado no FRR (sub-secção 6.2). Na secção 7 é apresentada uma proposta de extensão do RSVP-TE, que permitirá a partilha de LB de protecção, baseada: a) no método proposto por Kodialam e Lakshman [KL02, KL03, KL01] que permite obter a informação necessária à partilha de LB entre LSPs de protecção de LSPs protegidos diferentes, o qual é revisto na sub-secção 7.2; b) numa proposta (*standalone* e proprietária) de utilização da sinalização do RSVP-TE que permite a partilha de LB entre LSPs de protecção de LSPs protegidos diferente (sub-secção 7.3). Na sub-secção 7.3.3 mostra-se como seria simples, com base nas aproximações anteriores, fazer a extensão do FRR para permitir partilha de LB de protecção entre *Detours* de LSPs protegidos diferentes. Finalmente são apresentadas algumas conclusões na secção 8.

Chama-se a atenção para que as propostas que aqui vão ser feitas, são apenas uma primeira aproximação a estes problemas e que carecem de aprofundamento, nomeadamente no que concerne às implicações da existência do DiffServ e dos modelos de partilha de largura de banda (MAM e RDM) [Min04].

2 Recuperação por re-encaminhamento local

2.1 Vantagens

A recuperação por re-encaminhamento local pode ser uma solução vantajosa quando comparada com a recuperação do tipo global (coordenada pelo LER de ingresso do caminho), de um LSP longo que (por razões económicas e/ou gestão) não foi estabelecido com protecção por comutação – em particular quando a falha ocorre perto do fim do caminho do LSP.

O re-encaminhamento local, face à protecção por comutação tem a vantagem de não consumir LB de protecção, entendendo-se por LB de protecção a LB que é reservada por caminhos de protecção antes da ocorrência de qualquer falha na rede. Possui ainda a capacidade de lidar com falhas múltiplas – a protecção por comutação não consegue ultrapassar uma falha múltipla que afecte o LSP activo e o de recuperação pré-estabelecido.

Esta aproximação poderá ser particularmente interessante, se o caminho activo se estende por vários domínios, fazendo com que a avaria (ou avarias) que possam ocorrer sejam contornadas num AS (*Autonomous System*), sobre o qual existe informação topológica detalhada no PSL deixando para mais tarde o re-encaminhamento do LSP pelo LER de ingresso.

A troca de sinalização na situação anterior será bastante rápida, se uma vez calculado o LSP de recuperação (a partir do PSL local) for possível a criação de um PML que não seja o LER de egresso do LSP activo. Esse PML existirá se o LSP activo e LSP de recuperação correspondente tiverem um segmento final comum: isto implica que a troca de sinalização necessária, para o restabelecimento do fluxo de tráfego do LSP activo afectado, apenas teria de ser trocada entre o PSL e o PML (LSRs próximos).

Numa rede DiffServ-TE (*Differentiated Services – Traffic Engineering*) com o modelo RDM (*Russian Dolls Model*) [Min04] de atribuição de LB existe a possibilidade de utilização eficiente da LB; nestas circunstâncias, tráfego originado por serviços de baixa prioridade (por exemplo *best effort*) poderá reservar LB classificada como sendo prioritariamente para utilização de serviços mais prioritários, até ao momento que este precisem de reservar essa largura de banda por exemplo num re-encaminhamento de recuperação (ou porque surgiu um novo pedido de estabelecimento de um LSP para esse serviço).

LSPs que não façam reserva de LB poderão utilizar qualquer arco na rede (mesmo um cuja capacidade esteja totalmente reservada) e a qualidade de serviço que experimentarão dependerá da utilização que desses arcos.

Na secção 4 verificar-se-á que (entre outras dificuldades) a existência de um PML que não seja o LER de egresso não é garantida no re-encaminhamento sem extensão do RSVP-TE.

2.2 Opções de gestão

O re-encaminhamento poderá ser feito com ou sem reserva de LB (Largura de Banda). Aqui pode haver duas estratégias:

(a) Re-Encaminhar, num caminho que satisfaça, **tanto quanto possível**, os requisitos de CoS do LSP, reservando a LB possível (que pode ser 0), mesmo que o LSP original

tivesse LB reservada.

Aqui podem ser introduzidos limiares de decisão para aceitação ou não desse caminho.

(b) Re-Encaminhar apenas se for encontrado um caminho que satisfaça todos os requisitos de CoS do LSP (reservando a LB adequada, se o LSP original tivesse sido estabelecido com reserva de LB).

A escolha de uma das estratégias anteriores deve ser uma decisão de gestão. O PSL procura a melhor solução de re-encaminhamento e se não encontra nenhuma que satisfaça inteiramente os requisitos do LSP, pode optar não a utilizar (opção (b)) ou apesar disso optar por re-encaminhar o LSP desviando-o da avaria (ou avarias existentes na rede).

2.3 Pré-calculado

Se for considerada que a avaria mais frequente é a falha isolada de nó ou arco, então o PSL poderá fazer o pré-cálculo do caminho de recuperação. Assim, quando uma falha é detectada, só será preciso sinalizar (sem calcular) o caminho de recuperação já pré-planeado.

Esse caminho pré-calculado poderá ser actualizado (recalculado) sempre que haja uma alteração do estado dos arcos (avaria, reserva, ou carga) da rede, mesmo que essa alteração não afecte directamente o LSP cuja recuperação se pretende garantir.

No caso de falhas múltiplas no domínio MPLS, tal como as que são induzidas por cortes em condutas, que afectem o caminho activo e o caminho de recuperação por re-encaminhamento local (pré-calculado pelo PSL), o PSL deverá estar preparado para calcular um novo caminho de recuperação que contorne todas as falhas simultâneas – ou seja um método que utiliza normalmente um caminho pré-calculado para recuperação deve estar preparado para calcular um novo caminho de recuperação, quando falhas múltiplas afectam simultaneamente o caminho activo e o pré-calculado.

Se ocorrer mais do que uma falha num LSP activo, os PSLs devem ser os nós mais a montante e mais próximo de cada uma das falhas e os candidatos a PML deverão os nós mais próximo, a jusante, de cada falha no LSP. Ou seja cada PSL desencadeará a acção de recuperação correspondente ao arco/nó que está a proteger (se o PML1 do PSL1 estiver a jusante do PSL2, isto apenas causará excesso de tráfego de sinalização, se for possível partilhar recursos entre os dois LSPs de recuperação). Na figura 1 é apresentado um LSP com duas falhas que são recuperadas com o estabelecimento de dois desvios.

2.4 Pré-qualificado (*pre-qualified*)

A escolha de um LSP (entre os já estabelecidos) para o qual seria redireccionado o tráfego do LSP afectado, tem a vantagem de poder ser uma técnica extremamente rápida.

No RFC 3469 [SHMC+03] não é claro o que acontece ao fluxo de tráfego que estaria a ser oferecido ao LSP pré-qualificado: é redireccionado ou continua a utilizar esse LSP?

O LSP escolhido poderá ser de três tipos:

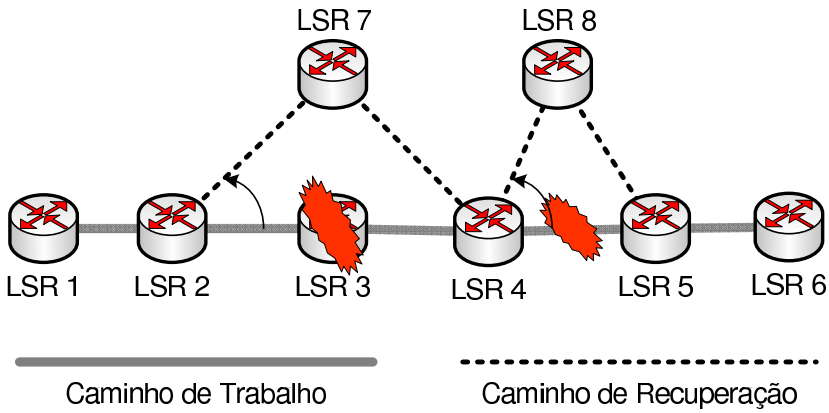

Figura 1: Um LSP com 2 falhas e dois LSPs de recuperação em acção

(a) O LSP que melhor satisfaça os requisitos de CoS do LSP a recuperar.

(b) Um LSP que satisfaça os requisitos da CoS do LSP a recuperar (no que concerne à LB requerida, a mesma será avaliada levando em consideração a capacidade disponível nos arcos do LSP pré-qualificado).

(c) Um LSP que satisfaça os requisitos da CoS do LSP activo a recuperar (no que concerne à LB, será necessário garantir que a soma da LB dos fluxos de tráfego que estão a utilizar esse LSP e do LSP a recuperar é igual ou inferior a LB reservada para esse LSP).

Mais uma vez, considerar a existência da opção (a) ou (b) deverá ser uma decisão de gestão. A existência da opção (c) depende de ser ou não usual o estabelecimento de LSPs com excesso de LB[2].

Se o tráfego do LSP que se está a recuperar for adicionado ao tráfego do LSP pré-qualificado (na opção (a) ou (b)) todos os fluxos de tráfego passarão a ter desempenho degradado, a não ser que os arcos no caminho do LSP pré-qualificado estivessem a ser muito pouco utilizados.

Na opção (b), se nos arcos desse LSP houver LB disponível suficiente para acomodar o segmento do LSP que foi re-encaminhado, pode ser pedido um aumento da LB do LSP seleccionado. Se o LSP recuperado for re-optimizado (re-encaminhado) num breve espaço de tempo, esta alteração de LB poderá ser desnecessária (pois seria seguida de uma redução de LB).

No caso de uma rede DiffServ, um LSP poderá transportar pacotes com diferentes *drop priorities* (expressa nos EXP bits) o que permitiria, no caso de haver degradação do serviço no LSP pré-qualificado que os fluxos por ele transportados sofressem degradação de acordo com essa prioridade. No caso dos E-LSPs a diferenciação de tratamento será estendida aos algoritmos de escalonamento (*scheduling behaviour*.

[2]Este tipo de aproximação implica uma maior granularidade de informação: quais os fluxos de tráfego que estão a ser oferecidos a cada LSP.

2.5 Mecanismos de Preempção

Poderá ser permitido a um mecanismo local fazer a preempção de um LSP (por exemplo o *pre-qualified*) desde que este tenha uma *holding priority* inferior à *setup priority* do LSP re-encaminhado. No entanto esta não parece ser uma boa opção, uma vez que o LSP re-encaminhado localmente muito provavelmente sofrerá posteriormente re-encaminhamento para optimização, desencadeado pelo LER de ingresso (quando receber o novo RRO do caminho, enviado pelo PSL),

Considerando que não foi possível calcular um caminho adequado para re-encaminhamento de um LSP inoperacional, e possuindo este LSP uma *setup priority* superior à *holding priority* doutro LSP já estabelecido (cujos recursos quando libertados permitirão a recuperação desse LSP) o LSR utilizará o mecanismo de preempção para re-encaminhar com sucesso o LSP. Havendo mais do que um LSP (de igual *holding priority*) candidato a preempção, surge o problema da selecção do LSP que sofrerá preempção.

A operação de preempção poderá ser mais eficiente se for escolhido prioritariamente um LSP que tenha o mesmo LER de egresso que o LSP que deseja ser re-encaminhado (e será particularmente interessante se esse caminho envolver vários AS). Neste caso o PSL pode obter o RRO (completo) do LSP que sofre preempção, e copiar a parte relevante para a mensagem *Path* de estabelecimento do novo LSP, pelo que este conseguirá ser sinalizado mais rapidamente.

O mecanismo de preempção funciona por interface: um nó, perante um LSP (cujo caminho já foi calculado, com base em possíveis preempções) escolhe (no arco de que é emissor), com base nas regras que regulam as prioridades *setup* e *holding*, o LSP que sofrerá preempção para encaminhar o LSP de prioridade superior. No nó seguinte, que recebeu uma mensagem *Path* de pedido de estabelecimento do novo LSP (que já expulsou um LSP no primeiro arco) esse processo poderá ser repetido. Ou seja não existe uma forma de escolher um LSP em particular a expulsar, cujos recursos sejam totalmente (extremo-a-extremo) disponibilizados para o LSP que desencadeou a preempção.

A cópia anteriormente sugerida, do RRO (ou de parte do RRO) de um LSP para o ERO doutro (após a preempção do primeiro), não é implementável (no sentido de não ser garantido que os recursos do primeiro ficariam disponíveis para o segundo). No entanto se o caminho escolhido pelo algoritmo de encaminhamento para o LSP de recuperação coincidir com o RRO do LSP que sofreu preempção, poderá ser utilizada essa técnica, mesmo que não garanta o sucesso da ligação!

Um mecanismo que conseguisse "usurpar" por inteiro os recursos doutro LSP, corresponderia na realidade a uma implementação do método *pre-qualified* e não à implementação de um mecanismo de preempção. Esta poderia ser uma característica *standalone* interessante a incluir nos nós da rede, e será abordada na sub-secção 4.3.1.

Em redes *DiffServ* a gestão da LB nos arcos usando o RDM, pode contribuir para uma boa gestão da LB através dos mecanismos de preempção.

3 Sinalização em métodos de re-encaminhamento

Os métodos que propõem re-encaminhamento local (dinâmico) para recuperação em caso de falha, nem sempre explicitam quais os requisitos de sinalização correspondentes. Nesta subsecção são revistos (muito brevemente) alguns desses métodos e a sinalização requerida para os implementar.

Em [PYK+04] é proposto um método de protecção dinâmica do caminho, em que o tráfego do LSP que falhou é "desviado" para outro LSP que tenha o mesmo LER de egresso (se esse LSP existir); caso contrário o PSL cria um novo LSP que termine no LER de egresso. Em ambos os casos os autores dizem que conseguem o redireccionamento (local) do LSP no PSL sem alterar a FTN (FEC to NHLFE) desde que o PSL não seja o LER de ingresso. Conseguem isso porque apenas alteram as tabelas de *in/out segment* de forma a que a partir do PSL os pacotes provenientes do primeiro segmento do LSP recuperado passem a ser etiquetados de forma idêntica (a partir do PSL) aos do LSP que foi usado como LSP de recuperação. Seguidamente o LER de ingresso será informado da necessidade de re-optimizar o LSP activo que foi re-encaminhado localmente.

No artigo em [HHY04] é proposto um método que os autores designam por recuperação hierárquica, em que, levando em conta os requisitos do LSP activo, tentam encontrar um caminho desde o PSL até ao nó destino (o PSL começa por ser o nó mais próximo da falha, a montante desta, mas caso esse nó não consiga obter um caminho solução, essa tarefa passa para o nó seguinte a montante). Em termos da sinalização necessária ao seu estabelecimento, requer o mesmo esforço que a criação de um novo LSP de recuperação em [PYK+04]. No entanto não é claro quais as mensagens que deveriam ser trocadas entre o nó que não conseguiu obter um caminho solução e o nó a montante que deverá seguidamente procurar resolver o problema de cálculo de caminho de protecção. Não parece que esta passagem de testemunho seja possível usando o RSVP-TE (sem extensão).

No esquema proposto por [AJC02] o caminho de recuperação é determinado e estabelecido depois de ocorrer a falha. O cálculo é realizado localmente pelo LSR a montante da falha (e que a detectou), o PSL. Esse caminho é calculado como o caminho de menor custo (a função utilizada para esse fim, poderia ser o resultado dos algoritmos *widest-shortest*, *shortest-widest*, etc) entre todos os caminhos cuja origem é o PSL e o destino é um dos candidatos a PML (geralmente qualquer LSR no LSP activo a jusante da falha).

Em [AJC02] os autores propõem-se usar o CR-LDP, em que indicam que assim que o PML envie de volta para o PSL uma *Mapping Message* este último enviará uma *Request Message* indicando que a *Explicit Route* após o PML é o LSP com `LSP_ID` do caminho activo recuperado. Este é um mecanismo que pretende conseguir uma fusão semelhante à conseguida nos *Detours*. Em [AJC02, pág. 485] é ainda afirmado que o método proposto também poderia ser implementado usando o RSVP:

> "A recovery path is established along the calculated explicit route from the upstream LSR to the PML. In the recovery path setup, the explicit route is inserted into the ER (Explicit Route) of MPLS signaling message (e.g., CR-LDP, RSVP). And LSPID (LSP Identifier) of the working LSP is used as an ER hop for the purpose of splicing the existing working LSP and its new recovery LSP to be

established."

No entanto parece incompatível a utilização de um `LSP_ID` num ERO no RSVP (à semelhança do que é exemplificado no caso do CR-LDP em [AJC02]). Na sub-secção 4.1 será analisada uma possível forma de implementação deste método, usando o RSVP-TE.

3.1 Comentários

O método [PYK+04] tem as seguintes vantagens:

1. Rapidez.
2. Muito simples de implementar (basta que o PSL tenha a inteligência necessária para modificar as *in/out segment tables*).
3. Se for usado um LSP já existente, o LSP recuperado poderá facilmente ser re-encaminhado (re-optimização) pelo LER de ingresso usando a técnica *make-before-break* [ABG+01, pág.12].

e as seguintes desvantagens:

1. Se por qualquer motivo o LSP re-encaminhado (devido a falha) não for re-optimizado, e ocorrer nova falha que afecte o LSP de recuperação nada impedirá o novo PSL de usar, no caminho que então calculasse, um arco do primeiro segmento do LSP activo recuperado, dando origem a um ciclo (*loop*)!
2. Se o LSP, cujas etiquetas foram pedidas emprestadas, for re-encaminhado num LSR a montante do PSL e deixar de passar pelo PSL do LSP recuperado esse LSR terá de repetir o processo de redireccionamento do LSP que tinha sido recuperado.
3. Se o LSP, cujas etiquetas foram pedidas emprestadas, for desligado o PSL terá de repetir o processo de redireccionamento do LSP que tinha sido recuperado.
4. Este mecanismo interfere com o controlo de fluxo que existe no início de cada LSP!

No método proposto por [AJC02] para obter uma fusão semelhante à conseguida com os *Detours*, o novo LSP de recuperação deveria ser estabelecido com o método *Sender Template-Specific*; em alternativa, poderia esse LSP ser criado a partir do PSL, com informação em tudo idêntica à do LSP activo, alterando apenas o `LSP_ID`. A partilha de LB será possível entre o LSP de recuperação e o segmento final do LSP activo se ambos tiverem sido estabelecidos com o estilo SE. Mas na realidade nenhum destes métodos garante que exista o PML proposto pelos autores (e nesse caso não terá qualquer utilidade a utilização do estilo SE), pois o mais natural será que o nó mais próximo a jusante da falha envie rapidamente[3] uma mensagem

[3]Quão rapidamente será esta mensagem enviada? No [BZB+97, pág. 41] diz-se que este tipo de mensagem é enviada apenas pelo *sender*, para desligar um LSP, ou por um LSR se o estado RSVP correspondente fizer *timeout*. No entanto em [PSA05, pág. 31-32] diz-se que quando um LSR detecta uma falha num arco ou nó de um LSP o estado *Path* e *Resv* não deve ser limpo e que mensagens *Path Tear* e *Resv Error* não devem ser enviadas imediatamente...

Path Tear, desligando o segmento final do LSP activo, antes da chegada a esse LSR da primeira mensagem *Path* de estabelecimento do LSP de recuperação.

O método de [AJC02] poderia ainda ser implementado usando o método de alteração das *in/out segment tables*, proposto por [PYK+04] (se ignorarmos os seus inconvenientes) fazendo com que o LSP de recuperação se estendesse até ao LER de egresso (seguindo desde o PML a mesma sequência de arcos que o LSP activo) em vez de terminar no PML. Se for desejado reservar LB este método levará a dupla reserva nos arcos que pertenciam ao LSP (antes de ser recuperado) após o hipotético PML (excepto se os nós a jusante da falha já tiverem desligado o LSP desde esse ponto até ao LER de egresso antes da chegada primeira mensagem *Path* de estabelecimento do LSP de recuperação).

4 Re-Encaminhamento local sem extensão do RSVP-TE

O re-encaminhamento local sem fazer nenhuma extensão do RSVP-TE considerando que:

- Todos os LSPs que não foram protegidos por FRR (e não são um *Detour* ou um túnel de *bypass*) poderão ser re-encaminhados localmente.
- Nem todos os nós poderão funcionar como PSL num re-encaminhamento local.
- Os LSRs num LSP não se comportam como PML potenciais desse LSP activo e de um LSP de recuperação (sinalizado após a detecção da falha no LSP activo), uma vez que esses LSRs não sabem à priori se um dado LSP poderá ou não ser re-encaminhado localmente.

  Em alternativa poderá considerar-se que numa AS onde se pretenda usar re-encaminhamento local como forma de recuperação, o LSR num LSP não protegido a jusante de um arco onde ocorreu uma falha, poderia limpar os temporizadores associados ao estado RSVP desse LSP e enviar a mensagem *Path Tear* apenas após decorrido um tempo pré-definido, T_r (definido para permitir re-encaminhamento local). Se entretanto, antes de esgotado T_r, o LSR receber uma mensagem de sinalização que o informa de que afinal é o PML do LSP de recuperação e do LSP activo em falha, o estado do LSP recuperado seria considerado refrescado.
- Os LSPs activos a recuperar não foram necessariamente estabelecidos usando o estilo SE;

é apenas possível em situações particulares (e com alguma perda de eficiência), como se verá nesta secção.

Obviamente que se o LSP a re-encaminhar não tiver LB reservada, tal simplifica o mecanismo de recuperação por re-encaminhamento (não é necessário permitir que o caminho antigo e o novo caminho partilhem reservas de LB).

Embora as conclusões possam ser repetitivas, passa-se a analisar cada um dos casos considerados à priori viáveis.

4.1 LSP a LSP, sem reserva de LB

O PSL terá pré-calculado um caminho alternativo para cada LSP de é que é LSR de trânsito (ou LER de ingresso), ou calculá-lo-á após a detecção da avaria. O PSL terá seguidamente de sinalizar o novo caminho desde si próprio até ao LER de egresso.

4.1.1 O PML é o LER de egresso

Neste caso o caminho recuperado ficará constituído por dois segmentos: o primeiro desde o LER de ingresso até ao PSL e o segundo desde o PSL até ao LER de egresso. O PSL criará um novo LSP (com origem no PSL e destino no LER de egresso), o LSP de recuperação, e seguidamente desviará[4] o tráfego do LSP activo para o LSP de recuperação. Poderá então enviar uma mensagem *Path Error* para o LER de ingresso. Entretanto o segmento do LSP original a jusante do local da avaria, será desligado por acção de temporizadores ou por acção do LSR mais próximo da avaria e a jusante desta, que enviará um *Path Tear*.

Como será sinalizado este novo LSP?

- Se for criado usando o método *Sender Template-Specific* o primeiro e o segundo segmento distinguir-se-ão apenas pelo campo `IPv4 tunnel sender address`.

  Se o LSP de recuperação e o segmento (após a falha) do LSP activo, tiverem algum LSR em comum, esses LSRs receberão ao fim de algum tempo uma mensagem *Path Tear* (enviada pelo nó mais próximo da falha e a jusante desta), que apenas eliminará o estado RSVP do segmento (após a falha) do LSP activo.

  Mesmo que o LSP activo e o LSP de recuperação tivessem sido estabelecidos com o estilo SE (e tivessem um segmento final idêntico), e as regras de fusão de estados RSVP (e de LSPs) tivessem sido aplicadas, o segmento LSP de recuperação não seria desligado, porque o PML não teria recebido um *Path Tear* para ambos os LSPs.

- Pode ser criado copiando toda a informação (do LSP activo) do objecto `SESSION` e do objecto `SENDER_TEMPLATE` e modificando apenas o campo `LSP_ID`. Poderia colocar-se em causa a possibilidade de criar um LSP, no qual se diz que o `IPv4 tunnel sender address` tem uma identidade que não é a do PSL, mas como isso também é feito na criação de *Detours* no método *Path-Specific*, tal não deve causar qualquer tipo de problema.

  Caso seja considerado necessário (ou conveniente) também se pode modificar o campo `IPv4 tunnel sender address` para a identidade do PSL (além de modificar o `LSP_ID`).

  O que foi dito no ponto anterior, para o método *Sender Template-Specific*, é válido também aqui.

Em qualquer dos casos é espectável que a mensagem *Path Tear*, enviada pelo LSR a jusante da falha no LSP activo, chegue ao LER de egresso antes da primeira mensagem *Path* de

[4] Esta acção de desviar tráfego de um LSP para outro é em tudo idêntica à realizada por um PLR quando há uma avaria e é preciso desviar o tráfego do LSP protegido para um dado *Detour*.

pedido de estabelecimento do LSP de recuperação. Após a recuperação do LSP o PSL deverá informar o LER de ingresso de que o LSP foi alterado através de uma mensagem *Path Error*.

A utilização do método *Sender Template-Specific* poderá possuir um **obstáculo** à sua utilização: se o LER de egresso associar a utilização deste mecanismo apenas ao FRR, poderá considerar que existe um erro, ao não conseguir identificar nenhuma mensagem *Path* como sendo relativa ao LSP protegido [PSA05, pág. 29] com o mesmo `IPv4 (or IPv6) tunnel end point address`, `Tunnel ID` e `LSP ID`.

A sinalização de um LSP de recuperação, enviando uma mensagem *Path* que apenas difere da mensagem *Path Error* do LSP recuperado no `LSP_ID`, poderá causar problemas caso seguidamente haja um re-encaminhamento global (de re-optimização) do LSP recuperado, que utilize o `LSP_ID` do LSP de recuperação. Uma vez que nas acções de re-optimização o usual é incrementar o `LSP_ID` de uma unidade, no caso da recuperação local o `LSP_ID` deverá ser decrementado de uma unidade (excepto se o nó responsável pela recuperação for o LER de ingresso do LSP). O nó de ingresso de um LSP, ao ser notificado de que terá havido uma alteração (local) do caminho desse LSP, deverá proceder à sua re-optimização, mesmo que tal consista apenas em confirmar o caminho agora seguido pelo LSP recuperado. Se um LSP sofrer mais do que uma falha (não contínua) no seu caminho, a alteração apenas do `LSP_ID` poderá não ser suficiente, pelo que também deverá ser modificado o campo `IPv4 tunnel sender address` para a identidade do PSL.

Uma vez re-optimizado o LSP activo, o LSP recuperado poderá ser desligado sem qualquer dificuldade, em qualquer dos métodos de sinalização anteriores porque o PSL fará seguir a mensagem *Path Tear* para o LSP de recuperação.

4.1.2 O PML é um LSR de trânsito

Neste caso o caminho do LSP recuperado ficará constituído por três segmentos: o primeiro desde o LER de ingresso até ao PSL e o segundo desde o PSL até ao PML (o LSP de recuperação) e o terceiro desde o PML até LER de egresso. O PSL criará um novo LSP (com origem no PSL e destino no LSR de egresso do LSP activo). Seguidamente o PSL desviará o tráfego do LSP activo para o LSP de recuperação. Um LSR passa a ser um PML de dois (ou mais) LSPs quando recebe mensagens *Path* (de *senders* diferentes) que identifica como sendo da mesma sessão.

Os LSRs a jusante de uma falha num LSP não protegido, não devem assumir que são PMLs potenciais (atrasaria o envio de mensagens de erro). Assim não há nenhuma garantia de que exista de facto um PML, que seja um LSR de trânsito do LSP activo. Porquê? Porque o LSR a jusante da falha (e mais próximo desta) no LSP activo enviará uma mensagem *Path Tear* para desligar esse LSP desse LSR até ao LER de egresso. Se esta mensagem passar no LSR (que seria o PML potencial) antes da mensagem *Path* de estabelecimento do LSP recuperação, obviamente que não pode haver fusão com algo que já não existe!

Se o LSR a jusante de uma falha pertencer a um domínio em que se assume a possibilidade de re-encaminhamento local como forma de protecção, então se esse LSR esperar T_r (e este tempo tiver sido bem escolhido), o PML poderá ser um LSR de trânsito.

4.2 LSP a LSP, com reserva de LB

Tal com na secção anterior 4.1, o PSL terá pré-calculado um caminho alternativo para cada LSP de que é LSR de trânsito (ou LER de ingresso), ou calculá-lo-á após a detecção da avaria; o PSL terá seguidamente que sinalizar o novo caminho desde si próprio até ao LER de egresso ou até um dos LSR de trânsito do caminho original.

4.2.1 O PML é o LER de egresso

Tudo o que foi dito na sub-secção 4.1.1 é válido aqui também. Surge no entanto uma dificuldade adicional: a possível tentativa de dupla captura de LB pelo LSP de recuperação, quando este e o LSP activo têm algum arco ou o segmento final comum até ao LER de egresso.

Em que situação poderá ocorrer esta tentativa de dupla captura de LB? Se o segmento após a falha, do LSP activo, não for desligado rapidamente (e se este não tiver sido estabelecido com o estilo SE) haverá uma tentativa de dupla captura de LB, a qual só é grave se inviabilizar o estabelecimento do LSP de recuperação, uma vez que essa dupla captura terá um tempo de vida curto.

Se o LSP activo a recuperar tiver sido estabelecido com o estilo SE (prevendo a possibilidade de ser re-encaminhado) esse problema não se coloca. Neste caso, se a mensagem *Path* de estabelecimento do LSP de recuperação chegar a um LSR de trânsito do LSP activo antes da mensagem *Path Tear* de remoção do segmento final (após a falha) desse LSP activo, tal resultará na criação de um PML nesse LSR de trânsito!

Ou seja embora o re-encaminhamento local seja viável, não é possível a partilha de LB entre o LSP de recuperação e o LSP activo a recuperar (se este não possuir o estilo SE) no segmento que possam ter em comum.

Após a recuperação do LSP o PSL pode informar o LER de ingresso de que o LSP foi alterado através de uma mensagem *Path Error*, para que este possa proceder à re-optimização do caminho. Caso este tivesse sido estabelecido sem o estilo SE, o LER de ingresso deveria enviar uma mensagem *Path* com a *flag* `SE Style desired` activa no objecto `SESSION_ATTRIBUTE`, uma vez que [BZB+97, pág. 23] o estado mantido pelo RSVP é dinâmico. Se o LER de egresso responder com uma mensagem *Resv* com o `SE Style`, o LER de ingresso pode em seguida proceder ao re-encaminhamento usando a técnica *make-before-break*, tal como é descrita no RFC 3209 [ABG+01, pág.12-13].

Uma vez re-optimizado o LSP activo, o LSP recuperado poderá ser desligado sem problemas, em qualquer dos métodos de sinalização anteriores porque o PSL fará seguir a mensagem *Path Tear* para o LSP de recuperação.

4.2.2 O PML é um LSR de trânsito

Tudo o que foi dito na sub-secção 4.1.2 é válido aqui também: continua a não haver garantia da existência de um PML (que seja um LSR de trânsito), excepto se os (alguns) LSRs no caminho do LSP afectado estiverem programados para serem um PML potencial.

Tal como na sub-secção anterior (4.2.1) surge da mesma forma o problema da dupla captura de LB se o LSP activo não tiver sido estabelecido com o estilo SE.

4.3 Re-Encaminhamento local utilizando um LSP pré-qualificado

A implementação deste método parece adequada em três cenários, considerando que as características de CoS do LSP pré-qualificado satisfaz os requisitos do LSP a recuperar, e que no que concerne à LB:

(a) o LSP pré-qualificado está sub-utilizado, e possui LB disponível suficiente para o LSP a recuperar;

(b) o LSP pré-qualificado não está sub-utilizado, mas existe LB nos arcos do seu caminho que torna viável (após um pedido de aumento de LB) satisfazer os requisitos do LSP a recuperar;

(c) admite-se que é aceitável "expulsar" o tráfego inicialmente no LSP pré-qualificado de forma a acomodar (com a LB adequada) o tráfego do LSP a recuperar.

Na descrição deste método em [SHMC$^+$03] não é claro como esse LSP seria escolhido. Terá de ser um LSP cujo LER de egresso coincida com o LER de egresso do LSP activo. O PSL do LSR activo a recuperar poderia não ser o LER de ingresso do LSP pré-qualificado, no entanto isso poderá ter consequências no controlo de fluxo na rede.

4.3.1 O PSL é o LER de ingresso do LSP activo e do LSP pré-qualificado

Se o re-encaminhamento é feito pelo LER de ingresso, isso significará que existe um LSP *paralelo* ao LSP que se deseja recuperar, cujas características são adequadas. O redireccionamento do tráfego do LER activo para o LER pré-qualificado equivale a uma operação de alteração da FTN (FEC to NHLFE).

No cenário (a) o método pode ser aplicado sem problemas. No cenário (b) após o redireccionamento do tráfego, deverá em seguida ser pedido um aumento de LB do LSP pré-qualificado; primeiro redirecciona-se e depois pede-se o aumento da LB, para que o redireccionamento seja rápido.

No cenário (b) poderia colocar-se a seguinte questão: se existe LB suficiente para re-encaminhar o LSP, porque razão se usa o LSP pré-qualificado, em vez de criar um novo LSP? A resposta é simples: rapidez! Desta forma todo o processo de transferência de tráfego é mais rápido: salta-se a fase de troca de sinalização de estabelecimento de um LSP.

No cenário (c), uma vez redireccionado o tráfego do LSP a recuperar para o LSP pré-qualificado, poderá em seguida desligar-se alguns (ou todos) o(s) fluxo(s) de tráfego inicialmente transportados neste LSP: equivale a alterar a FTN para esses fluxos! Este comportamento não requer alteração do RSVP-TE, apenas que um dado LSR tenha capacidades acrescidas!

4.3.2 O PSL é o LER de ingresso do LSP pré-qualificado

Tudo o que foi dito na sub-secção anterior é ainda válido neste caso.

A única diferença reside no facto do LSP recuperado ter dois segmentos: o primeiro do LER de ingresso até ao PSL, e o segundo formado pelo LSP pré-qualificado.

O único LSR que sabe que o LSP de recuperação é um dado LSP pré-qualificado é o PSL, pelo que este método poderá ter o mesmos problemas que o método proposto por [PYK+04] (ver sub-secção 3.1).

Se os LSPs envolvidos não tiveram reserva de LB, todo este processo teve apenas como objectivo tornar mais expedito o re-encaminhamento. Neste caso poderá não ser é possível evitar os problemas (como a possibilidade de criação de ciclos não detectáveis) desta aproximação. No entanto este tipo de ciclo, embora contribua para a ineficiência da rede (dupla captura de largura de banda e/ou caminhos desnecessariamente longos) não corresponde a um ciclo infinito para os pacotes que o percorrerão.

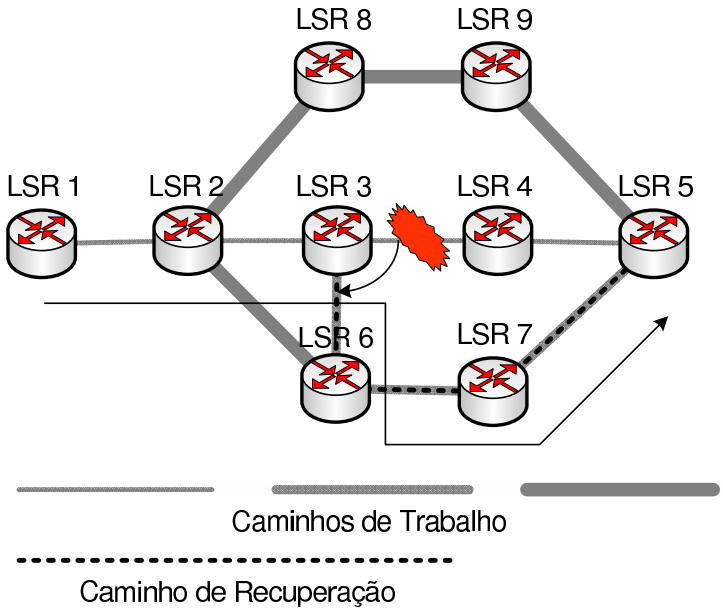

Figura 2: Utilização de um LSP pré-qualificado

Considere-se a figura 2 em que o LSP B ($3 \rightarrow 6 \rightarrow 7 \rightarrow 5$) é seleccionado para recuperar o LSP A ($1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$). Seguidamente, antes da re-optimização do LSP A, o arco (6,7) falha e, utilizando a mesma técnica de recuperação, os LSPs A e B são recuperados utilizando o LSP C ($6 \rightarrow 2 \rightarrow 8 \rightarrow 9 \rightarrow 5$), criando, para o tráfego do LSP A, o ciclo assinalado na figura 3 como sendo o percurso final dos pacotes desse LSP.

4.3.3 O PSL é um LSR de trânsito do LSP pré-qualificado

Tudo o que foi dito na sub-secção 4.3.1 é ainda válido neste caso, o qual equivale, mais uma vez, a uma implementação da aproximação proposta por [PYK+04].

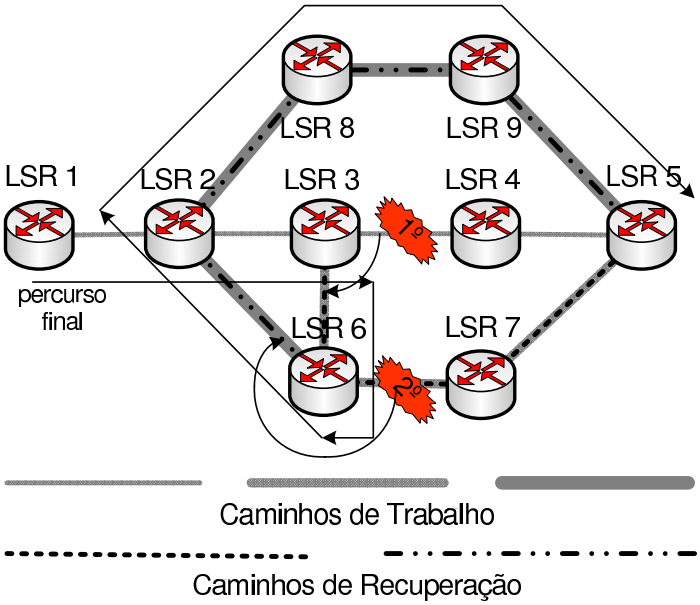

Figura 3: Duas falhas sucessivas: utilização de dois LSPs pré-qualificados

No caso do FRR os *Detours* são previamente sinalizados, e são associados de forma única ao LSP que protegem através dos métodos de sinalização *Sender Template Specific* e *Path-Specific* [PSA05]. No caso do re-encaminhamento local, utilizando um LSP pré-qualificado, apenas o PSL saberá associar o LSP activo ao LSP de recuperação utilizado (um segmento do LSP pré-qualificado).

Este tipo de solução poderá provocar problemas de controlo de fluxo na rede, a não ser que o PSL escolha criteriosamente o LSP de recuperação e que seja possível ao LER de ingresso fazer em seguida o re-encaminhamento de optimização do LSP de recuperação.

Independentemente da forma como for implementada poderá também dar origem a ciclos se entretanto ocorrer uma avaria que afecte o LSP activo.

4.4 Re-Encaminhamento utilizando túneis de *bypass*

Um PSL, em vez de calcular (ou pré-calcular) um caminho de protecção para cada LSP que transporta, poderá pré-calcular túneis de *bypass* para recuperar conjuntos de LSPs que o cruzam (assumindo que não é possível recuperá-los todos usando apenas um túnel) e que não são protegidos de outra forma.

Assim, quando um LSP activo fosse estabelecido (sem protecção por comutação), cada nó no seu caminho teria de actualizar o cálculo dos túneis de *bypass* que iria utilizar (em caso de falha isolada de nó e ou arco).

Em caso de avaria, estes túneis teriam de ser sinalizados com a LB requerida pelos LSPs activos que deverão recuperar. Seguidamente os LSPs seriam desviados do arco (ou nó) avariado pelo PSL e usando empilhamento de etiquetas, cada um dos LSPs afectados poderia ser re-encaminhado para o túnel adequado (ou seja levando em conta restrições de CoS).

O PSL poderia em seguida enviar uma mensagem *Path Error* para o LER de ingresso, avisando que algo se tinha passado com o caminho e que talvez devesse ser re-optimizado.

Inconvenientes deste método:

- Lentidão: será necessário que pacotes de sinalização vão desde o PSL até ao PML e voltem (sinalização do túnel) e que seguidamente chegue ao PML uma mensagem de sinalização relacionada com cada um dos LSPs re-encaminhados, ou uma mensagem de refrescamento do estado desses LSPs.

  Se o PML utilizar um espaço de etiquetas global, apenas quando o PML receber (dum interface inesperado) uma mensagem de refrescamento do estado de um LSP recuperado é que saberá que esse LSP foi desviado e saberá que não deverá fazer seguir para a frente mensagens *Path Tear* que venha a receber do segmento contornado do LSP activo. No caso do PML utilizar um espaço de etiquetas por interface, só quando chegar ao PML um pedido acerca da etiqueta a utilizar pelo PSL (antes de enviar os pacotes de cada LSP recuperado através do túnel de *bypass*) é que este fica a saber que o referido LSP está a ser recuperado.

  Se estas operações não forem suficientemente expeditas o PML poderá desligar o segmento final dos LSPs que estão a ser re-encaminhados.

- De cada vez que um LSP (que usasse o túnel) fosse objecto de re-encaminhamento (por re-optimização) deveria ser feita uma diminuição da LB do túnel.

- Complexidade de cálculo dos túneis.

Se em alternativa se definisse inicialmente o túnel com LB 0, os LSPs protegidos seriam re-encaminhados para o túnel e o PSL:

- Não alteraria a LB do túnel, mas contabilizaria a LB utilizada no túnel por cada um deles (aqui seria necessário criar uma aplicação entre o estado visto pelo RSVP-TE e pelo PSL e que depois é distribuído pelo LSA).

  Irrealizável: os nós entre o PSL e o PML do túnel ficariam sem saber qual a LB que efectivamente estava a ser usada nos arcos de que eles são a origem! Assim daria origem a que a LB apenas fosse contabilizada (correctamente) no primeiro arco do túnel de *bypass*.

- Ou desencadearia um *bandwidth increase procedure* para a soma das LB de cada LSP que ele transportasse.

A utilização destes túneis poderá não ser viável, numa rede em que os LSRs não estejam pré-configurados para funcionar como PMLs, porque o risco de que os LSRs a jusante de uma falha enviem, para jusante, mensagens *Path Tear* relativas a todos os LSPs (não protegidos) que foram afectados, antes da chegada, através do túnel de *bypass*, de mensagens de sinalização relatrivas aos LSPs desviados, não é desprezável!

4.5 Comentários finais

No re-encaminhamento local sem extensão do RSVP-TE, não é garantida a existência de um PML que não seja o LER de egresso do LSP a recuperar, a não ser que os LSR estejam pré-configurados para se comportarem como PMLs de LSPs não protegidos. A inexistência de um PML que não seja o LER de egresso do LSP a recuperar não impede a recuperação por re-encaminhamento local, embora a possa tornar bastante mais lenta!

No re-encaminhamento local, para garantir que não ocorre dupla captura de LB, é preciso que todos os LSPs não protegidos, com reserva de LB, sejam estabelecidos com o estilo SE. Isto poderá acontecer nos LSPs cujos LERs de ingresso pertencem a uma AS que prevê o re-encaminhamento local como opção de recuperação para LSPs não protegidos, mas julga-se que esta não será uma opção comum a todas as redes MPLS.

A utilização de um LSP *pre-qualified* para recuperar um LSP, só parece ser muito vantajosa quando o PSL é o LER de ingresso do LSP activo a recuperar (e do *pre-qualified*) e bastante interessante quando o PSL é o LER de ingresso do LSP *pre-qualified*.

Os LSRs a jusante de uma falha, enviarão (para jusante) mensagens *Path Tear* relativas a todos os LSPs (não protegidos) que estes julgam afectados pela falha detectada. Assim a utilização de túneis de *bypass* não é viável, porque a probabilidade de eliminação do segmento do LSP activo após o PML não é desprezável.

5 Proposta de extensão do RSVP-TE para suportar re-encaminhamento local

Na secção 4 verificou-se que a utilização de re-encaminhamento local sem extensão do RSVP-TE, em redes em que LSRs não foram configurados para se comportarem como PMLs de LSPs não protegidos, tem dois grandes inconvenientes:

1. A impossibilidade de garantir que existe um PML, que seja um LSR de trânsito do LSP activo, cuja existência pode reduzir significativamente a velocidade deste mecanismo de recuperação.
2. A impossibilidade de utilizar túneis de *bypass* sinalizados dinamicamente.

e um outro inconveniente, um pouco menos grave, porque se estima que será menos frequente: a possibilidade (ainda que reduzida) de inviabilizar uma acção de recuperação devido a dupla captura de LB entre o LSP de recuperação e o LSP activo.

Seguidamente vai ser esboçada uma extensão simples do RSVP-TE que permitiria resolver os problemas atrás apontados.

5.1 Proposta de sinalização para re-encaminhamento local do tipo *Detour*

Um LSR, que desejasse criar LSPs que pudessem ser re-encaminhados localmente, deveria estabelece-los usando uma mensagem *Path* com as seguintes características: possuir uma nova

bandeira *Local rerouting desired*, no objecto `SESSION_ATTRIBUTE`; se esta bandeira estivesse activa, também deveria estar activa a bandeira *SE Style desired*, a qual implicaria que a mensagem *Resv* correspondente utilizasse o estilo de reserva SE. Isto permitirá que um LSP de recuperação e um LSP activo possam partilhar recursos, resolvendo assim o problema da possível dupla captura de LB.

Os LSRs no caminho activo de um LSP que foi estabelecido com a bandeira *Local rerouting desired* ficam a saber que este LSP poderá ser re-encaminhado localmente em caso de falha (por qualquer um deles, geralmente o mais próximo da falha com capacidade para tal), e deverão assumir que são PMLs potenciais, da mesma forma que no FRR, os LSRs no caminho activo de um LSP protegido devem assumir que são MP potenciais [PSA05, pág. 31-32]. Fica assim viabilizada a existência de PMLs entre o LSP activo e o LSP de recuperação, e torna possível a utilização de túneis de *bypass* sinalizados dinamicamente, para efectuar recuperação por re-encaminhamento.

Quando o LSP fosse re-encaminhado, por falha de algum dos seus elementos, deveria ser efectuado um procedimento semelhante ao descrito em [PSA05, pág 26-27] (secção 6.5). Tal implica a criação de uma nova bandeira, *Local rerouting in use* no objecto `RRO`. Considera-se que o código de erro indicando que o LSP tinha sido reparado localmente poderá ser o mesmo que o utilizado no FRR (ver secção 1.3 ou [PSA05, pág. 26-27]).

A sinalização do LSP de recuperação, com o estilo SE, poderá ser feita usando a alteração do `LSP_ID` ou o método *Sender Template-Specific* desde que o possível "obstáculo" referido na sub-secção 4.1.1 não exista.

Se for considerado que existe a possibilidade de utilização de túneis de *bypass*, para que um PSL saiba se deve criar um LSP de recuperação para cada LSP afectado ou optar por criar um túnel de *bypass* seria necessária uma bandeira adicional (ou então isso fica ao critério de cada LSR!).

5.2 Proposta de sinalização para re-encaminhamento local usando um túnel de *bypass* dinâmico

Como foi referido na secção anterior, a utilização da nova bandeira *Local rerouting desired* permite que todos os LSRs de trânsito no caminho activo do LSP se considerem PML potenciais.

Será preciso averiguar, se o compasso de espera introduzido no(s) LSR(s) de trânsito imediatamente a jusante de uma falha, quando este(s) apresenta(m) um comportamento semelhante ao dos MP no FRR [PSA05, pág. 31-32], é suficiente para estabelecer um túnel dinamicamente e redireccionar todos os LSPs que solicitaram re-encaminhamento local.

6 Protecção por comutação

Os mecanismos de protecção por comutação têm recebido muita atenção, nomeadamente o cálculo de soluções *offline* que minimizam a LB adicional que é preciso providenciar de forma a garantir a protecção de todos os LSPs (que se deseja proteger) em cenários de falha isolada,

através da partilha de LB de protecção.

O estabelecimento de LSPs com protecção local, em que os mesmos são redireccionados pelo LSR mais próximo da falha, utilizando caminhos pré-sinalizados (e com LB reservada) foi objecto de normalização e a sinalização necessária está no RFC 4090 [PSA05] – FRR (*Fast Reroute*).

Apesar desta normalização encontram-se outras abordagens na literatura acerca de mecanismos com protecção local e partilha de largura entre LSPs de protecção – para uma resenha dessas abordagens, ver [JG05].

6.1 Protecção extremo-a-extremo

Alguns autores debruçaram-se sobre cálculo de um caminho activo e um caminho de protecção (disjunto com o activo que protege). Este tipo de protecção tem como desvantagem o tempo que demora a mensagem de aviso de falha a viajar desde o ponto onde ocorreu a falha até ao LER de ingresso – o qual pode ser significativo se a falha ocorrer num dos últimos arcos do caminho.

É possível uma boa gestão da LB (excedente necessária para protecção) se a escolha dos dois caminhos for feita em conjunto e/ou levar em consideração a possibilidade de partilha de LB entre caminhos de protecção de LSPs activos disjuntos nos arcos (e/ou nós).

A recomendação Y.1720 da ITU-T [ITU03] apresenta os requisitos e mecanismos para protecção por comutação global (extremo-a-extremo) em redes MPLS, dos tipos: 1:1, 1+1, *shared mesh*, e protecção ao pacote 1+1.

Em [ITU03, pág. 9] considera-se que é reservada uma porção da LB existente na rede, especificamente para protecção. No apêndice I dessa recomendação é apresentada uma tabela com a informação que é preciso armazenar para permitir a partilha de LB de protecção, a qual corresponde à construção de uma tabela com os valores δ_{ij}^{uv} e G^{uv} que serão introduzidos na secção 7.2. Na recomendação Y.1720 não é explicado se o método deveria ser implementado de forma centralizado ou se seria possível uma implementação distribuída; também não é feita nenhuma referência à forma como seriam sinalizados os LSPs de protecção com partilha de LB.

6.2 *Fast Reroute* – FRR

O FRR (*Fast Reroute*) prevê dois mecanismos básicos de protecção por comutação: *one-to-one backup* e *facility backup*. No caso do *one-to-one backup* são estabelecidos LSPs de recuperação (os *Detours*) em que cada um deles protege o LSP da falha de um nó ou de um arco do LSP protegido. Os *Detours*, sinalizados usando o método *Path Specific*, e o LSP protegido podem partilhar LB, porque os seus LSPs são considerados como fazendo parte da mesma sessão RSVP-TE. Se os *Detours*, tiverem sido sinalizados usando o método *Sender Template-Specific* e o LSP protegido tiver sido sido estabelecido com o estilo SE os *Detours* e o LSP protegido podem também partilhar LB [ABG+01, PSA05].

O mecanismo *facility backup* não é mais que uma proposta de implementação dos túneis de

bypass, em que cada túnel de *bypass* protege um conjunto de LSPs que utilizam um dado arco ou um dado nó.

O FRR não contempla partilha de LB entre LSPs (*Detours*) de protecção de LSPs protegidos diferentes [VPD04, pág. 343].

O FRR poderá permitir partilha de LB entre túneis de *bypass* (que protegem recursos diferentes), se estes tiverem algum arco em comum [VPD04, pág. 416]. Os autores sugerem que os túneis sejam sinalizados (por mecanismos de gestão da rede) com LB 0, apesar de terem sido calculados de forma a garantirem a protecção dos LSPs que usam o recurso que protegem – a justificação para esta opção será referida mais à frente, na sub-secção 7.1.

Se existir uma separação de recursos de LB para LSP activos e de protecção, essa LB não correrá o risco de ser capturada para LSPs activos. Se, adicionalmente, a LB a ser usada pelos túneis de *bypass* **for** uma classe à parte, que apenas possa ser usada pelo método *facility backup*, então essa LB fica livre do eventual "assalto" de *Detours* que venham a ser estabelecidos para proteger novos LSPs.

Se a LB a ser usada pelos túneis de *bypass* **não for** uma classe à parte, **julga-se** que a informação divulgada pelo LSA dirá que a LB reservada nos arcos que suportam o túnel de *bypass* é 0, e isto provocará que os algoritmos de cálculo dos *Detours* possam seleccionar esses arcos. No entanto, em cenários de falha isolada, a utilização desses arcos em *Detours* não causará problemas (se o *bypass* tiver sido calculado para proteger toda a LB do recurso que protege).

7 Partilha de LB de protecção com e sem extensão do RSVP-TE – uma proposta

O problema da partilha de LB entre LSPs de protecção reveste-se de duas dificuldades:

- qual a informação que será necessário distribuir na rede e/ou armazenar nos nós de forma a que seja possível calcular caminhos de protecção que possam partilhar LB entre si;
- como sinalizar LSPs de protecção de LSPs activos, que podem ter nós extremos diferentes, de forma a que possam partilhar largura de banda utilizando o RSVP-TE.

7.1 Limitações do RSVP-TE

Em [VPD04, pág. 343] diz-se que não está prevista a partilha de LB em *one-to-one backup*:

> "Bandwidth can be shared via merging but not between backup tunnels protecting independent resources. This would require very expensive signalling and routing overhead, as well as synchronization between various PLRs, wich would increase the scalability impact even more."

Os túneis de *bypass* no FRR não deverão ser sinalizados com a LB que cada um deles requer (isoladamente) porque tal levaria a um excessivo consumo de LB, uma vez que dessa forma não seria possível partilha de largura de banda entre os túneis, sem alteração da sinalização, como é explicado em [VPD04, pág. 415].

Em [OS03, pág. 171] diz-se que o quinteto (`IPv4 (or IPv6) tunnel end point address`, `Tunnel ID`, `Extended Tunnel ID`, `IPv4 (or IPv6) tunnel sender address`, `LSP ID`) permite a partilha de LB entre dois LSPs, estabelecidos com o estilo SE, desde que os 3 primeiros elementos, pertencentes ao objecto `SESSION` sejam iguais, variando o valor do campo `LSP ID`[5]:

> "The rule of SE reservation process for MPLS TE is that if two reservations are seen with the same five-tuple, except that they have different LSP IDs, the two reservations are for the different LSPs, but they share bandwidth."

Assim, pode concluir-se que a partilha de LB (de protecção) de LSPs de protecção, de LSPs activos de sessões diferentes (não correlacionados) não é possível usando os mecanismos actualmente previstos no RSVP-TE.

Na secção 7.3 será proposta uma solução (viável?) para este problema.

7.2 Um modelo de utilização de informação agregada dos arcos que permite partilha de LB de protecção

Nesta subsecção vai ser revisto brevemente um modelo proposto por Kodialam & Lakshman [KL02, KL03, KL01], por se considerar que com pouco *overhead* na informação que é preciso tocar na rede, os LSR ficam na posse da informação necessária para lhes permitir gerir a partilha de largura de banda entre LSPs de protecção de LSPs activos diferentes[6] (em cenários de falha isolada). Este modelo tem no entanto o inconveniente de precisar de alterações no RSVP-TE e LSA.

Embora Kodialam & Lakshman tratem sempre o problema da protecção extremo-a-extremo (e local) através do cálculo do caminho activo e do(s) caminho(s) de protecção, com partilha de LB entre caminhos de protecção, apenas em [KL02] se referem às alterações de sinalização necessárias ao seu método.

Tendo como objectivo seguir de perto a notação em [KL02], no caso da protecção extremo-a-extremo, falar-se-á (nesta sub-secção) sempre no caminho activo e no caminho de protecção de uma sessão (ponto a ponto) RSVP-TE, e não no LSP protegido e de protecção. Isso é útil especialmente quando mais à frente é definida a intersecção, $A_{ij} \cap B_{uv}$ em que A_{ij} representa o conjunto das sessões RSVP-TE que usam o arco (i, j) no caminho activo e B_{uv} representa o conjunto de sessões que usam o arco (u, v) no caminho de protecção.

Kodialam e Lakshman [KL02] propuseram um modelo com informação parcial (*Partial Information Model*) o qual se baseia na existência das seguintes trocas de informação:

[5] No método *Path-Specific*, muda o `IPv4 (or IPv6) tunnel sender address`.

[6] Os autores também propõem, sem detalhar, um modelo de protecção local (do tipo *Detour*), com partilha de LB intra LSPs e entre LSPs.

1. Alteração do LSA, de forma a incluir agora a LB utilizada em cada arco por caminhos de protecção.

2. Alteração do RSVP-TE: sempre que é estabelecido um caminho de protecção, a mensagem associada a esse caminho transporta também um RRO[7] referente ao caminho activo que este protege.

Devido à alteração do LSA em 1, **todos os nós** ficam a saber a seguinte informação acerca do arco (i, j): LB usada pelos caminhos activos (F_{ij}), LB usada pelos caminhos de protecção (G_{ij}) e a LB residual (R_{ij}).

Por seu lado a alteração do RSVP-TE em 2, permite saber qual a LB que pode ser partilhada ou não. Seja AP um caminho activo (*Active Path*), que requer uma largura de banda igual a b, e BP o correspondente caminho de protecção (*Backup Path*). Suponhamos que o caminho AP foi seleccionado independentemente de BP. Seja M a capacidade máxima usada nalgum arco (i, j) de AP (antes de ser reservada a LB b para AP):

$$M = \max_{(i,j)\in AP} F_{ij} \tag{1}$$

Para um arco potencial (u, v) do BP, as seguintes situações podem ocorrer:

- se $M + b \leq G_{uv}$ então não é necessário reservar LB adicional no arco (u, v), porque uma falha em qualquer arco de AP, implicará no máximo um pedido de $M + b$ nos caminhos de protecção.

- se $M + b > G_{uv}$ então vai ser preciso reservar uma LB adicional de protecção igual a $M + b - G_{uv}$, no arco (u, v).

Será com base nestes custos *imprecisos* (quando comparados com os custos que se obteriam no modelo de informação completa (*Complete Information Model*)) que será calculado o BP.

No entanto, cada nó sabe exactamente $\Phi_{ij}^{uv} = A_{ij} \cap B_{uv}$, em que A_{ij} representa o conjunto das sessões RSVP-TE que usam o arco (i, j) no caminho activo e B_{uv} representa o conjunto sessões RSVP-TE que usam o arco (u, v) no caminho de protecção. A LB necessária no arco (u, v) para proteger todos as sessões RSVP-TE k que usam o arco (i, j) no seu caminho activo é: $\delta_{ij}^{uv} = \sum_{k\in\Phi_{ij}^{uv}} b_k$, em que b_k é a LB requerida pela sessão k.

No modelo de informação completa considera-se que todos os nós da rede conhecem todos os caminhos activos e de protecção de todas as sessões RSVT-TE [KL02, pág.74], donde todos os nós podem calcular Φ_{ij}^{uv}.

No modelo de informação parcial considera-se que cada arco[8] (u, v) sabe calcular os Φ_{ij}^{uv}, sempre que o RRO do AP passa pelos nós do BP, donde também sabe calcular o δ_{ij}^{uv}.

[7] O LSP de protecção só é sinalizado quando o LSR de ingresso recebe a confirmação do estabelecimento do caminho activo através de uma mensagem *Resv*.

Se a sinalização do caminho activo e de protecção fosse feita em paralelo, então a única informação disponível seria o ERO. O rigor com que se conhece o caminho activo poderia limitar a utilização da partilha de LB. No entanto essa aproximação funcionaria bem no interior de uma AS, desde que o ERO não contivesse *loose nodes*!

[8] Os autores dizem cada arco, mas deverá ser antes cada nó extremo, ou um dos nós extremos!

Assim o símbolo $\theta_{ij}^{u,v}$ definido em [KL02, pág. 75], como a LB que poderá ser necessário reservar no arco (u, v) para proteger o arco (i, j) no AP que se pretende usar, é dado por:

$$\theta_{ij}^{uv} = \begin{cases} 0 & \text{se } \delta_{ij}^{uv} + b \leq G_{uv} \text{ e } (i,j) \neq (u,v) \\ \delta_{ij}^{uv} + b - G_{uv} & \text{se } R_{uv} \geq \delta_{ij}^{uv} + b - G_{uv} \text{ e } (i,j) \neq (u,v) \\ \infty & \text{restantes casos} \end{cases} \quad (2)$$

Com base neste valor é possível fazer reserva exacta (no arco (u, v)) tal como se conseguiria no modelo de informação completa:

$$\max_{(i,j) \in AP} \theta_{ij}^{uv} \quad (3)$$

A quantidade adicional de informação que um nó u precisa de armazenar resume-se aos vectores δ_{ij}^{uv} em que v é (ou foi) um LSR adjacente a u, num domínio MPLS, e ao vector G^{uv} (distribuído pelo LSA), com a LB de protecção reservada em cada arco da rede.

7.2.1 Comentários

Para além das alterações sugeridas ao LSA e ao RSVP-TE em [KL02] não há mais nenhuma indicação de que seria necessária qualquer extensão ao RSVP-TE para suportar a partilha de LB entre LSPs com LERs de ingresso/egresso diferentes (e aparentemente não relacionados). Os autores dizem apenas que os LSPs seriam estabelecidos usando o RSVP-TE ou CR-LDP[9].

Tanto quanto foi possível perceber no RSVP-TE não está previsto nenhum mecanismo que suporte a partilha de LB entre LSPs de protecção de LSPs activos com LERs de ingresso/egresso diferentes (e não relacionados).

7.3 Proposta de um mecanismo que permite partilha de LB usando o RSVP-TE

7.3.1 Ideia base[10]

Defina-se em cada arco, que fará parte de um caminho de protecção de um LSP, um LSP auxiliar com origem e destino nos nós extremos desse arco, no qual é reservada apenas a LB efectivamente necessária, menor ou igual à pedida pela mensagem *Path* (a qual terá de ser confirmada pela mensagem *Resv* de resposta) do RSVP-TE. Esse LSP nunca terá qualquer tráfego oferecido: é criado unicamente para reservar LB! Não será reservada (explicitamente) nenhuma LB para o LSP de protecção, sendo este estabelecido com reserva nula de LB (embora a reserva anterior lhe garanta a LB de que ele precisa).

Este procedimento não provocará problemas de CAC, quando o arco é o primeiro de um LSP? A resposta parece ser não uma vez que o LSR responsável pelo CAC é o nó de ingresso do LSP de protecção.

[9] Em [Min04, pág. 13] é dito que o IETF decidiu não fazer mais desenvolvimento do CR-LDP (ver RFC 3468 [AS03]).

[10] Esta ideia base foi sugerida pelo Pedro Nunes e desenvolvida em diálogo com Teresa Gomes.

Numa ambiente DiffServ, a reserva de LB deverá ser por classe de serviço. Assim não se alterará a classe de serviço do LSP quando este tiver de ser re-encaminhado após falha na rede.

7.3.2 Exemplificando

Considere-se que existe um método de cálculo e de estabelecimento de LSPs de protecção extremo-a-extremo, em que se pretende a partilha de LB entre LSPs de protecção (que protegem diferentes LSPs activos, com LERs de ingresso e egresso diferentes).

Considere-se ainda que cada nó possui (não interessa como) a informação necessária para saber qual a LB que **efectivamente** é preciso reservar no arco do caminho de que ele é o emissor, de forma a garantir que todos os LSPs activos protegidos neste arco, continuam protegidos desde que o cenário de avaria seja o de falha isolada (no domínio MPLS).

A primeira vez que um arco é usado por um caminho de protecção, terá de ceder para reserva toda a LB pedida pelo caminho de protecção para satisfazer esse pedido. Mas se o fizesse da forma convencional, não poderia seguidamente partilhá-la com outro LSP de protecção, que posteriormente viesse a solicitar também reserva de LB nesse mesmo arco.

Assim o nó emissor desse arco, criará um LSP auxiliar cujo LER de egresso é o LER extremo desse mesmo arco, solicitando uma reserva de LB igual à pedida pelo LSP de protecção. Esse LSP auxiliar uma vez estabelecido nunca oferecerá tráfego real à rede (o nó que o criou sabe para que finalidade o fez!). Seguidamente esse nó envia a mensagem *Path* para o nó seguinte do caminho. E o processo repete-se em cada nó do caminho de recuperação. O LER de egresso enviará, como habitualmente, uma mensagem *Resv* a confirmar o estabelecimento do LSP de protecção (não haverá dupla captura porque os nós mantêm um registo das reservas pedidas e efectuadas para cada LSP de protecção). Os nós terão de manter um registo dos LSPs de protecção que estabeleceram e da LB solicitada e reservada, e possivelmente um estado RSVP mais elaborado que o do RSVP-TE normalizado.

Se um arco é utilizado uma segunda vez como arco de um LSP de protecção, que solicita (através do RSVP-TE) b_1 de LB, mas o LSR emissor desse arco sabe que naquele arco em particular basta reservar $b_2 < b_1$, uma vez que pode usar parte da LB já reservada para protecção (doutros LSPs), então ele solicitará um aumento de LB de valor b_2 (no LSP auxiliar) e fará seguir a mensagem de estabelecimento de protecção para o nó seguinte.

Do ponto de vista do RSVP-TE tudo se passa com normalidade. Os LSRs terão que manter um duplo registo do estado dos LSPs de protecção, para saber qual a LB que estes solicitaram e a que efectivamente foi reservada. O RSVP-TE deverá informar o IGP (OSPF-TE ou IS-IS-TE) das reservas efectuadas.

Num cenário de avaria isolada, quando esta ocorrer, os LSPs de protecção passarão a transportar o tráfego dos LSPs activos afectados e terão à disposição a LB que foi reservada através dos LSPs auxiliares.

7.3.3 Partilha de LB no FRR

Uma vez que o FRR já está estabilizado no RFC 4090 [PSA05], se for possível a implementação do mecanismo proposto na secção 7.3, a partilha de LB entre *Detours* não precisa de nenhuma extensão do RSVP-TE, mas apenas de nós com capacidades acrescidas de gestão da LB.

Se o objecto `DETOUR` for enviado na mensagem *Path* inicial de estabelecimento de um *Detour* fica resolvido o problema do envio do segmento do LSP activo a proteger. Relembra-se que o objecto `DETOUR` é obrigatoriamente enviado se o *Detour* for sinalizado usando o método *Path Specific* e poderá ser enviado no caso de ser sinalizado usando o método *Sender Template-Specific*.

O PLR sabe sempre qual é o arco do caminho activo que está a ser protegido pelo *Detour* de que ele é o nó origem. Assim o PLR poderá sempre calcular a LB a reservar no primeiro arco do *Detour* levando em conta a possibilidade de partilha de LB entre *Detours* de sessões RSVP-TE diferentes.

Se existir um DMP que faça a fusão de vários *Detours*, não há qualquer problema porque esse nó criará um novo objecto `DETOUR` com todos pares (`PLR, Avoid Node ID`) transportados pelos *Detours* fundidos. Ou seja o DMP sabe quais são todos os arcos que o arco seguinte do caminho de protecção deverá proteger (os quais pertencem ao LSP protegido) e todos os arcos de LPSs que utilizam (explicitamente) esse arco como parte de um caminho de protecção, e pode assim calcular a LB adicional que precisa efectivamente de ser reservada nesse arco para esse *Detour*.

Note bem: se ocorrer a fusão de *Detours* o cálculo da partilha de LB só é possível porque a identificação da sessão RSVP-TE, a que cada *Detour* pertence, está contida na mensagem *Path* correspondente.

Numa rede em que se deseje considerar falhas dos nós, o método proposto em [KL02] também pode ser utilizado. Conforme sugerido em [KL02] basta substituir cada nó por um sub-nó de ingresso, onde todos os arcos incidentes no nó terminam, e por um sub-nó de egresso de onde saem todos os arcos emergentes desse nó; esses sub-nós são ligados por um arco fictício (de capacidade ilimitada) cuja falha representa a falha do nó.

Numa rede em que se considerem falhas de nós além de falhas de arcos o par (`PLR, Avoid Node ID`) transporta a informação necessária para o cálculo da LB de protecção partilhável nos *Detours*. Num *Detour* apenas o PLR sabe se o LSP protegido solicitou ou não protecção de nó. Um nó intermédio de um *Detour* assumirá que deve considerar protecção de nó se nenhum `Avoid Node ID` no objecto `DETOUR` pertencer ao seu ERO – isto não garante que foi pedida protecção de nó, mas aponta nesse sentido.

Assim será possível partilhar largura de banda de protecção (para proteger um LSP activo da falha de um arco ou de um nó) no primeiro arco do *Detour*, porque o PLR sabe se o LSP activo solicitou protecção de nó ou apenas de arco. Os nós intermédios terão que inferir que tipo de protecção foi solicitada com base no ERO e no objecto `DETOUR`, contidos da mensagem *Path* de sinalização:

- Se o ERO do *Detour* não contiver nenhum `Avoid Node ID` (no objecto `DETOUR`) então os nós intermédios do LSP de protecção deverão assumir que o LSP activo solicitou

protecção de nó.

- Se o ERO do *Detour*, num dado nó intermédio, contiver alguns nós (mas não todos) `Avoid Node ID` (no objecto `DETOUR`) então esse nó intermédio do LSP de protecção deverá comportar-se como se o LSP activo tivesse solicitado protecção de nó para o(s) nó(s) `Avoid Node ID` não contido(s) no ERO do *Detour*.
- Se o ERO do *Detour*, num dado nó intermédio, contiver todos os nós `Avoid Node ID` (no objecto `DETOUR`) então esse nó intermédio deve assumir que o LSP activo não solicitou protecção de nó, mas apenas de arco[11]

Esta solução é compatível com a existência de *Detours* (fundidos num DMP) que conseguiram satisfazer o pedido de protecção de nó do LSP activo com outros que apenas conseguiram satisfazer a protecção de arco (para os arcos contidos no objecto `DETOUR`).

A existência de túneis de *bypass*, sinalizados dinamicamente, em que existe partilha de LB de protecção, mesmo quando a LB que estes utilizam não pertence a um conjunto de recursos separados, torna-se possível usando também o mecanismo proposto em 7.3. No caso dos *Detours* é enviada uma mensagem *Path* de estabelecimento de um novo LSP de protecção por cada LSP protegido, enquanto no caso presente o "LSP de protecção" (o túnel de *bypass*) é sempre o mesmo para um dado conjunto de LSPs activos (à medida que estes vão sendo sinalizados). Esta operação é semelhante à sinalização requerida sempre que um *Detour* é re-encaminhado ou o respectivo LSP activo sofre um aumento de LB (que se reflecte num igual aumento de LB dos repectivos *Detours* de protecção).

Considere-se em primeiro lugar o caso túneis de *bypass* NHOP (*Next Hop*):

1. A mensagem de estabelecimento do túnel deve solicitar uma LB igual à requerida pelo LSP que deve ser protegido. Deve ainda ser incluído um objecto `DETOUR` na mensagem *Path* com a identidade do arco que está a ser protegido pelo túnel.

   Os nós no caminho do túnel, ao detectarem o objecto `DETOUR` ficam avisados de que estão a criar um LSP de protecção. Então devem ser criados (se ainda não existirem) em cada arco os LSPs auxiliares, com a LB requerida pelo LSP que deve ser protegido por esse túnel (de forma semelhante ao que foi proposto no caso dos *Detours*).

   Se algum nó no caminho deste túnel não reconhecer o objecto `DETOUR`, então o estabelecimento do túnel é recusado, e o PLR será informado da impossibilidade de sinalizar o túnel desta forma, podendo em seguida optar pela sinalização tradicional (com LB de banda 0, ou com LB diferente de 0 e sem possibilidade de partilha de LB entre arcos de túneis de *bypass*).

2. Sempre que um PLR, utilizando o método *facility backup* selecciona um túnel de *bypass* (anteriormente sinalizado dinamicamente) para proteger um dado LSP activo, os nós no túnel devem proceder a um pedido de aumento de LB para um valor final igual à

[11] Assumindo que quando um LSP não solicita protecção de nó, e este é sinalizado usando o método *Path-Specific*, um objecto `DETOUR` terá de ser colocado na mensagem *Path*. Se neste caso se optar por utilizar sempre o método *Sender Template-Specific* então, para ser possível a partilha de LB de protecção, teria de ser enviado um objecto `DETOUR`, contendo um `Avoid Node ID` que coincidirá com MP do *Detour* (e que pertence ao seu ERO).

soma da LB de todos os LSPs que estão a ser protegidos contra a falha do arco (`PLR, IPv4 (or IPv6) tunnel end point address`), incluindo a LB do novo LSP.

Será usada a técnica *make-before-break* para sinalizar o pedido de aumento de LB do túnel, que se reflectirá sobre a LB dos LSPs auxiliares (usando a mesma técnica). A mensagem *Path* correspondente ao aumento da LB do túnel de *bypass* deverá transportar um objecto `DETOUR` que indicará ao túnel a identidade do arco que está a ser protegido.

Neste caso não é necessário (nem possível sem a criação de novos objectos) enviar a identidade de cada LSP que está a ser protegido, uma vez que em cada acção de aumento de LB está em causa a protecção de uma certa quantidade de LB que pertence a um único arco. Além disso os nós intermédios de um túnel NHOP podem verificar que o seu LER de egresso (o PML) coincide com o `Avoid Node ID` (no objecto `DETOUR`) logo ficam a saber que se trata de um túnel de protecção ao arco (`PLR`,`Avoid Node ID`).

No caso de túneis de *bypass* NNHOP (*Next-Next Hop*), tudo se passa como no caso anterior, mas com uma diferença importante: os nós intermédios ao verificarem que o LER de egresso do túnel (o PML) não coincide com o `Avoid Node ID` (no objecto `DETOUR`), assumirão que estão a proteger a rede da falha do nó `Avoid Node ID`, e utilizarão essa informação no cálculo da LB de protecção partilhável.

No ponto 1 poderá surgir uma dificuldade à sua utilização: se o LER de egresso do túnel (o PML) associar a utilização de objectos `DETOUR` apenas ao FRR, poderá considerar que existe um erro, ao não conseguir identificar nenhuma mensagem *Path* como sendo relativa ao LSP protegido [PSA05, pág. 29].

Esta proposta de partilha de LB não requer a extensão do LSA. Isso implica que a informação disponível num LER de ingresso não é tão completa como seria desejável e que os caminhos escolhidos não farão uma utilização tão eficiente da LB como a que seria conseguida, se essa informação estivesse disponível. Mas, como já foi referido, se os nós armazenarem a informação requerida para fazerem partilha de LB, poderão continuar a fazer reserva exacta da LB de protecção (partilhada) em cada arco [KL02].

No caso dos túneis de *bypass* o objecto `DETOUR` será utilizado com uma semântica diferente daquela com que foi proposto no âmbito do FRR. Assim deveria ser definido um novo "C-type", da mesma forma que isso foi considerado necessário para os objectos `SENDER_TEMPLATE` e `FILTER_SPEC` [ABG+01, pág. 13]. Esta aproximação poderia resolver o problema, no caso do método *facility backup*, da dependência do comportamento do LER de egresso no estabelecimento o LSP de protecção correspondente (o *bypass tunnel*), com possibilidade de partilha de LB.

Este problema também deixaria de existir se o penúltimo LSR removesse o objecto `DETOUR` da mensagem Path antes de a enviar para o LER de egresso do túnel. No entanto não havendo forma de um LSR distinguir uma mensagem *Path* relativa ao estabelecimento de um *Detour* e de um *bypass tunnel* (com um `DETOUR` object), esta remoção, feita de forma determinística, iria contra as regras do FRR.

7.4 Proposta de utilização do RSVP-TE de forma a suportar um esquema de protecção extremo-a-extremo com partilha de LB

O método proposto por [KL02], para partilha de LB de protecção, necessita que a mensagem *Path*, de estabelecimento do caminho de protecção, leve consigo o RRO do LSP protegido. Assim a sinalização do LSP de protecção só deverá ser iniciada quando o LER de ingresso do LSP protegido tiver recebido o RRO com o caminho completo, o qual indica todos os nós (ou arcos) que devem ser evitados pelo caminho de protecção.

Uma vez que não é possível colocar mais do que um RRO na mensagem *Path*, que seja posteriormente analisado [ABG+01, pág. 31], propõe-se a utilização do objecto `DETOUR` para transportar a informação do caminho do LSP activo a proteger. Na realidade a protecção extremo-a-extremo pode ser encarada como um mecanismo de protecção em que apenas é usado um único *Detour* com um objecto `DETOUR` contendo todos os arcos do LPS activo, desde o LSR de ingresso até ao LER de egresso.

Se um *Detour* for sinalizado usando o método *Path-Specific*, a correspondente mensagem *Path* deverá conter obrigatoriamente um objecto `DETOUR`. Baseando-se em na informação em [PSA05, pág. 21-22], a mensagem *Path*, de estabelecimento do LSP de protecção (e que contém o objecto `DETOUR`), deverá no presente caso ser construída da seguinte forma:

- The path-specific method must be used and the PLR MUST add a DETOUR object to the PATH message.
- This DETOUR object will contain a sequence of pairs PLR_ID, Avoid_Node_ID, (including the ingress and egress nodes) until all nodes (and arcs) in the protected path are included.
- The Include-any, Exclude-any, and Include-all fields of the SESSION_ATTRIBUTE object (of the protected path) SHOULD be copied to the corresponding fields of the SESSION_ATTRIBUTE object.
- The "Label recording desired" flag MAY be modified.
- The PLR (which is the ingress LER) MUST generate an EXPLICIT_ROUTE object toward the egress which must be node or link disjoint with the protected path.
- The SENDER_TSPEC object SHOULD contain the bandwidth information from the SENDER_TSPEC object, included in the protected LSP's PATH message.
- The RSVP_HOP object containing the LER ingress IP address.
- The detour LSP MUST use the same reservation style as the protected LSP. This must be correctly reflected in the SESSION_ATTRIBUTE object.

O caminho de protecção procurará ser disjunto nos nós com o LSP activo, e se não for possível procurará um LSP activo disjunto nos arcos (esta é apenas uma possibilidade; o LSR de ingresso poderá estar configurado de forma diferente).

Uma vez que os nós do caminho de protecção não modificam o objecto `DETOUR`, introduzido na mensagem *Path* de estabelecimento do caminho de protecção pelo PLR (neste caso o PLR

coincide sempre com o LSR de ingresso e o MP é com o LER de egresso) a não ser em acções de fusão, que aqui não ocorrerão! Desta forma (que parece simples) ficaria resolvido o problema do envio da informação do caminho do LSP activo. Conjugando esta solução com o método proposto na sub-secção 7.3 será possível fazer partilha de LB (num esquema de protecção global).

A partilha de LB entre túneis de *bypass* e entre LSPs de protecção (extremo-a-extremo) só é possível, sem extensão do RSVP-TE se o LER de egresso permitir o estabelecimento de um LSP com um objecto `DETOUR` sem que seja obrigatório o estabelecimento do LSP activo correspondente.

No entanto para que este mecanismo possa co-existir com mecanismos de recuperação com re-encaminhamento local sem extensão do RSVP-TE uma nova bandeira será necessária. Considere-se que é utilizada a nova bandeira *end-to-end protection desired* na mensagem *Path* the estabelecimento de um LSP activo, então isso desencadeará a criação da mensagem *Path* de estabelecimento do LSP de protecção (o qual poderá ser disjunto nos arcos e/ou nós com o caminho do LSP activo correspondente), assumindo que as correspondentes bandeiras estariam activas no objecto `SESSION_ATTRIBUTE`:

- The SESSION_ATTRIBUTE flags "End-to-end protection desired", "Bandwidth protection desired" and "Node protection desired" MUST be cleared.
- The PLR MUST generate an EXPLICIT_ROUTE object toward the egress which must be node (if the flag "Node protection desired" was set) or link disjoint with the potected path.

Se um LER de egresso não permitir estabelecimento de um LSP com um objecto `DETOUR` sem que seja estabelecido o LSP activo correspondente, esta bandeira resolveria igualmente este problema.

Tal como no caso dos túneis de *bypass* o objecto `DETOUR` será utilizado com uma semântica diferente daquela com que foi proposto no âmbito do FRR. Assim deveria ser definido um novo "C-type", da mesma forma que isso foi considerado necessário para os objectos `SENDER_TEMPLATE` e `FILTER_SPEC` [ABG+01, pág. 13]. Esta aproximação poderia resolver o problema da dependência do estabelecimento do LSP de protecção do comportamento do LER de egresso.

Uma vez que o mecanismo de protecção extremo-a-extremo (sem extensão do RSVP-TE) não tem a possibilidade de indicar se o LSP de protecção é disjunto nos nós ou nos arcos com o LSP protegido, deverá ser considerado, pelos nós intermédios do LSP de protecção, que se deseja protecção dos nós. Sempre que um nó verificar que está a calcular a LB de protecção de um arco incidente num nó `Avoid Node ID` dar-se-á conta de que nesse caso basta fazer protecção do arco (`PLR, Avoid Node ID`). Isto conduzirá a uma menor partilha de LB de protecção, mas garante que caso tenha sido desejada protecção de nó a mesma é garantida num cenário de falha isolada.

8 Conclusões

As principais contribuições deste relatório são as seguintes:

1. Foi feita a avaliação da possibilidade de fazer re-encaminhamento local sem extensão do RSVP-TE, tendo-se concluído que a mesma apresenta algumas limitações/dificuldades. Em particular a utilização de túneis de *bypass* parece ser inviável devido a problemas de temporização, os quais poderão ser contornados num AS.

   O re-encaminhamento local sem extensão do RSVP-TE só será interessante se o PLR estiver próximo do LER de egresso do LSP em falha.

2. Foi proposta uma extensão (simples) do RSVP-TE de forma a permitir fazer re-encaminhamento local de forma eficiente.

3. Foi proposto um mecanismo que em conjunção como modelo de informação incompleto proposto por Kodialam & Lakshman [KL02], permitirá a partilha de largura de banda de protecção, com extensão do LSA e do RSVP-TE.

4. Mostrou-se que o mecanismo proposto de partilha de LB permite que *Detours* (FRR) de LSPs activos diferentes possam partilhar LB, com ou sem extensão do LSA e do RSVP-TE.

   Utilizando ainda esse mesmo mecanismo mostrou-se que a partilha de LB entre arcos comuns a túneis de *bypass* de protecção de nós diferentes poderá ser possível, sem extensão do RSVP-TE, dependo do comportamento do LER de egresso do túnel.

5. A protecção extremo-a-extremo sem extensão do RSVP-TE também será possível, dependo do comportamento do LER de egresso do túnel, desde que se utilize o mecanismo proposto na sub-secção 7.3.

A partilha de LB entre túneis de *bypass* e entre LSPs de protecção (extremo-a-extremo) só é possível, sem extensão do RSVP-TE se o LER de egresso permitir o estabelecimento de um LSP com um objecto `DETOUR` sem que seja obrigatório o estabelecimento do LSP activo correspondente.

Questões que em aberto:

1. Valerá a pena extender o RSVP-TE para suportar eficientemente o re-encaminhamento local?

2. Será realmente viável a implementação do mecanismo proposto na sub-secção 7.3?

3. O uso abusivo do objecto `DETOUR`, tal como foi proposto para permitir a partilha de LB entre túneis de *bypass* e entre LSPs de protecção extremo-a-extremo, é viável?

As principais linhas de trabalho possíveis são:

1. Avaliar a redução de LB de protecção conseguida com a utilização do FRR, quando é permitida partilha de LB, sem extensão do RSVP-TE e do LSA, tal como foi proposto na sub-secção 7.3.3.

2. LSPs bidireccionais:

3. LSPs ponto-multiponto.

4. Encaminhamento:
   (a) Algoritmo de cálculo (e pré-cálculo) do LSP de recuperação por re-encaminhamento.
   (b) Algoritmo de cálculo do caminho activo, em conjunto (ou não) com LSPs de protecção.
   (c) Algoritmo de selecção de um LSP pré-qualificado.
   (d) Algoritmo de selecção de LSPs que devem sofrer preempção.
5. Definição clara de quais os parâmetros/critérios que devem ser consideradas no estudo do desempenho de uma rede MPLS com protecção.
6. Desenvolvimento de um simulador que permita comparar o desempenho de várias estratégias de protecção/encaminhamento.

Referências

[ABG+01] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow. RSVP-TE: Extensions to RSVP for LSP tunnels. IETF RFC 3209, December 2001.

[AHX01] D. Awduche, A. Hannan, and X. Xiao. Applicability statement for extensions to RSVP for LSP-tunnels. IETF RFC 3210, December 2001.

[AJC02] G. Ahn, J. Jang, and W. Chun. An efficient rerouting scheme for MPLS-based recovery and its performance evaluation. *Telecommunication Systems*, 19(3,4):481–495, 2002.

[AS03] L. Andersson and G. Swallow. The multiprotocol label switching (MPLS) working group decision on MPLS signalling protocols. IETF RFC 3468, February 2003.

[BZB+97] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource reservation protocol (RSVP – version 1 functional specification. IETF RFC 2205, September 1997.

[HHS94] R. Händel, M. N. Huber, and S. Schröder. *ATM Networks, Concepts, Protocols, Applications*. Addisson-Wesley Publishing Company, 1994.

[HHY04] D. W.-K. Hong, C. S. Hong, and D. Yun. A hierarchical restoration scheme with dynamic adjustment of restoration scope in a MPLS network. In *Network Operations and Management Symposium*, pages 191–204. IEEE, 2004.

[ITU03] ITU-T. Recommendation Y.1720: Protection switching for mpls networks, September 2003.

[JG05] L. Jorge and T. Gomes. Recuperação em redes MPLS – uma resenha de esquemas de recuperação. Technical Report 10/2005, INESC Coimbra, 2005. ISSN 1645-2631.

[KL01] M. Kodialam and T. V. Lakshman. Dynamic routing of locally restorable bandwidth-guaranteed tunnels using aggregated link usage information. In *IEEE INFOCOM 2001*, pages 376–385, 2001.

[KL02] M. Kodialam and T. V. Lakshman. Restorable dynamic quality of service routing. *IEEE Communications Magazine*, 40(6):72–81, June 2002.

[KL03] M. Kodialam and T. V. Lakshman. Dynamic routing of restorable bandwidth-guaranteed tunnels using aggregated network resource usage information. *IEEE/ACM Transactions on Networking*, 11(3):399–410, June 2003.

[Min04] I. Minei. MPLS DiffServ-aware traffic engineering. White Paper 200048-001, Juniper Networks, 2004.

[OS03] E. Osborne and A. Simha. *Traffic Engineering with MPLS*. Cisco Press, 2003.

[PSA05] P. Pan, G. Swallow, , and A. Atlas. Fast reroute extensions to RSVP-TE for LSP tunnels. IETF RFC 4090, May 2005.

[PYK+04] P.-K. Park, H.-S. Yoon, S. C. Kim, J. Park, and S. Yang. Design of a dynamic protection mechanism in MPLS networks. In *The 6th International Conference on Advanced Communication Technology*, volume 2, pages 857–861, 2004.

[RTF+01] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, and A. Conta. MPLS label stack encoding. IETF RFC 3032, January 2001.

[SHMC+03] V. Sharma, F. Hellstrand, B. Mack-Crane, S. Makam, K. Owens, C. Huang, J. Weil, B Cain, L. Anderson, B. Jamoussi, A. Chiu, and S Civanlar. Framework for multi-protocol label switching (MPLS)-based recovery. IETF RFC 3469, February 2003.

[VPD04] J.-P. Vasseur, M. Pickavet, and P. Demeester. *Network Recovery – Protection and Restoration of optical, SONET-SDH, IP, and MPLS*. Elsevier, 2004.