**TUTORIAL N° 2**

**Plano de Controle do MPLS-TE:**

**Base para o GMPLS.**

1. **OBJETIVO**

O objetivo do presente tutorial é apresentar o plano de controle do MPLS-TE, não só por sua própria importância, mas também porque ele representa a fundamentação do GMPLS.

De fato, os protocolos de roteamento opcionalmente utilizados no GMPLS, que são o GMPLS OSPF-TE e o GMPLS ISIS-TE, são extensões dos protocolos de roteamento OSPF-TE e ISIS-TE, respectivamente, que constituem a essência do plano de controle do MPLS-TE.

O mesmo ocorre na sinalização, onde o protocolo GMPLS RSVP-TE representa uma extensão do RSVP-TE utilizado no MPLS-T

Primeiramente estamos apresentando as fases de roteamento, de especificação e configuração de parâmetros de TE LSP e de cálculo de rotas, que representam, nessa ordem, as primeiras etapas na constituição de um TE LSP. Na realidade, se considerarmos o conjunto de TE LSPs constituídos na rede, essas etapas, mais a sinalização, ocorrem concomitantemente.

De início, apresentamos, em linhas gerais, o OSPF e o IS-IS, que constituem os protocolos IGP na métrica *link-state* convencional da arquitetura TCP/IP. Destacamos a aplicação desses protocolos em redes IPv4 e em redes IPv6.

Em prosseguimento, desenvolvemos o caminho lógico para a introdução de TE nesses protocolos, com a definição dos protocolos OSPF-TE Versão 2 (IPv4) e OSPF-TE Versão 3 (IPv6) na linha do OSPF, além da definição dos protocolos ISIS-TE para IPv4 e ISIS-TE para IPv6 na linha do IS-IS.

Apresentamos então o processo de especificação e de configuração de atributos de TE LSP relativos a cada um dos TE LSPs a serem constituídos.

Por fim, abordamos a realização da fase de cálculo de rotas, quando os atributos de TE LSP de um TE LSP a ser constituído são comparados com os atributos de link conduzidos pelo roteamento para o ponto onde a comparação ocorre.

Como resultado do cálculo de rotas resulta a definição do melhor caminho, pelo qual a sinalização constituirá o TE LSP.

Finalmente, apresentamos o protocolo RSVP-TE, que especifica a sinalização no MPLS-TE.

**2 – INTRODUÇÃO**

A RFC 2702 (*Requirements for Traffic Engineering over MPLS*) descreve a funcionalidade básica de *Traffic Engineering* (TE) em um sistema autônomo de roteamento com enfoque em sua utilização em redes MPLS-TE e em GMPLS. As limitações dos protocolos IGP utilizando a métrica do tipo *link state* convencional são apontadas, mostrando a necessidade de novas formas de roteamento para o uso de TE.

Engenharia de Tráfego tem como propósito criar condições para a operação de uma rede com eficiência e confiabilidade, utilizando ou mesmo alocando, de forma eficiente, os recursos da rede e garantindo padrões de desempenho de tráfego.

Tais propósitos são alcançados mediante a correta distribuição de tráfego pela rede, considerando as características e o nível de utilização de seus links, preferencialmente com a reserva prévia de largura de faixa ao longo da rede.

A RFC 2702 endereça particularmente a utilização de TE para a rede *Internet* global, com a sua enorme extensão. O MPLS tem se mostrado uma opção de rede *backbone* de grande importância para a *Internet*. Por outro lado, as capacitações de TE sobre MPLS apresentadas na RFC 2702 podem ser também adotadas em redes privativas de qualquer porte e em diferentes aplicações do MPLS.

A aplicação de TE em MPLS concretizou-se pela definição, de início, do plano de controle do MPLS-TE e, posteriormente, pela definição do GMPLS e de sua aplicação para o MPLS-TP.

Um plano de controle utilizando TE consiste basicamente em um protocolo de roteamento IGP suportando *constraining routing* e *source routing* e de um protocolo de sinalização compatível com esse roteamento.

No plano de controle do MPLS–TE, o roteamento ocorre com base no protocolo OSPF-TE ou no protocolo ISIS-TE (IS-IS TE). Abordaremos adiante o OSPF-TE com bom nível de profundidade, enquanto o ISIS-TE, pela similaridade com o OSPF-TE, será apresentado de forma mais genérica.

A sinalização no MPLS-TE utiliza o protocolo RSVP-TE.

No GMPLS, e consequentemente no MPLS-TP, o protocolo de roteamento usado é o GMPLS OSPF-TE (extensão do OSPF-TE) ou o GMPLS ISIS-TE (extensão do ISIS-TE) A sinalização utiliza o protocolo GMPLS RSVP-TE que por sua vez é uma extensão do RSVP-TE.

O autor pretende elaborar próximos tutoriais abordando os diversos aspectos do GMPLS e de sua aplicação no MPLS-TP e nas diferentes redes ópticas de transporte.

Em uma etapa posterior, pretendemos apresentar uma nova tecnologia, denominada *Segment Routing* (SR), que supostamente destina-se a suplantar o GMPLS.

O presente tutorial é totalmente dedicado ao plano de controle do MPLS-TE, constituindo dessa forma o embasamento necessário para o pleno entendimento do GMPLS.

**3 – ROTEAMENTO NO MPLS-TE**

O roteamento no MPLS-TE tem como base as extensões para TE do protocolo OSPF (*Open Shortest Path First*) e do protocolo IS-IS (*Intermediate System-to-Intermediate Systems*).

**3.1 – Roteamento com Base no OSPF**

Com base no OSPF, tudo teve início com a emissão da RFC 3630 (*Traffic Engineering (*TE*) Extensions to* OSPF *Version* 2), dando origem ao que se denominou protocolo OSPFv2 TE ou OSPF-TE Versão 2.

O protocolo OSPFv2, no qual se baseia o protocolo OSPF-TE Versão 2, foi definido na RFC 2328 (OSPF *Version 2*) e destina-se à aplicação do OSPF em redes IPv4.

Com o desenvolvimento do IPv6, foi emitida a RFC 5340 (OSPF *for* IPv6), especificando o protocolo OSPFv3, destinado à aplicação do OSPF em redes IPv6.

Foi posteriormente emitida a RFC 5329 (*Traffic Engineering (*TE*) Extensions to* OSPF *Version* 3), definindo o protocolo OSPFv3 TE ou OSPF-TE Versão 3. O protocolo OSPF-TE Versão 3 é parte integrante do plano de controle do MPLS-TE com suporte no IPv6.

Por fim, o IETF emitiu a RFC 7471 (OSPF *Traffic Engineering (*TE*) Metric Extensions*), definindo extensões de métricas de TE aplicáveis tanto ao OSPF-TE versão 2 quanto ao OSPF-TE Versão 3.

**3.2 – Roteamento com Base no IS-IS**

No caso do IS-IS como suporte ao roteamento no MPLS-TE, o IETF adotou uma linha similar à do OSPF.

A partir do protocolo IS-IS para redes OSI, especificado no padrão ISO 10588, foi emitida inicialmente a RFC 1195 (*Use of* OSI IS-IS *for Routing in* TCP/IP *and Dual Environments*), aplicável ao roteamento em redes OSI e redes IPv4, definindo o que denominaremos protocolo IS-IS para IPv4.

O IS-IS foi então estendido para redes IPv6, mediante a publicação da RFC 5308 (*Routing* IPv6 *with* IS-IS). Define-se assim o protocolo IS-IS para IPv6.

O início do uso do IS-IS para TE ocorreu pela emissão da RFC 5305 (IS-IS *Extensions for Traffic Engineering*), dedicada exclusivamente ao MPLS-TE com o plano de controle suportado por redes IPv4. Define-se, dessa forma, o protocolo ISIS-TE para IPv4.

Como ocorre no caso do OSPF, o IS-IS TE foi estendido para o MPLS-TE com o plano de controle suportado por redes IPv6, dando origem ao protocolo ISIS-TE para IPv6. Esse fato ocorreu pela emissão da RFC 6119 (IPv6 *Traffic Engineering in* IS-IS).

No final dessa sequência, o IETF emitiu a RFC 7810 (IS-IS *Traffic Engineering (*TE*) Metric Extensions*), definindo extensões de métricas de TE aplicáveis apenas ao protocolo ISIS-TE para IPv4. As extensões de métricas definidas na RFC 7810 não se aplicam ao protocolo ISIS-TE para IPv6.

Registramos que todos os protocolos de roteamento acima relacionados, sejam da família OSPF sejam da família IS-IS, são do tipo IGP (*Interior Gateway Protocol*), por se restringirem ao âmbito de um único domínio de roteamento.

Os protocolos de roteamento entre domínios são referidos como protocolos do tipo EGP (*Exterior Gateway Protocol*), cujo principal exemplo no momento é o protocolo BGP-4 (*Border Gateway Protocol Version* 4).

Abordaremos em linhas gerais, a seguir, as RFCs acima citadas com os respectivos protocolos, com exceção do protocolo OSPF-TE Versão 2 (RFC 3630), que será abordado com maior profundidade.

**4 – EXTENSÕES DO OSPF PARA TE**

Este item apresenta os protocolos da família OSPF, levando à sua aplicação com TE no MPLS-TE.

Conforme menção anterior, esses protocolos são do tipo IGP.

**4.1 – Protocolo OSPF Version 2 (OSPFv2)**

O protocolo OSPFv2, definido na RFC 2328, fundamenta-se na tecnologia *link state,* também referida como tecnologia SPF *(Shortest Path First)* e destina-se ao roteamento em redes IPv4. Embora seja basicamente um protocolo de roteamento unicast, o OSPF pode suportar também roteamento multicast, porém de forma limitada.

O OSPF responde rapidamente a mudanças topológicas, envolvendo pouco tráfego de roteamento, e provê a autenticação dessas mudanças.

O roteamento no OSPF baseia-se exclusivamente nos endereços IP contidos nos cabeçalhos dos datagramas IP transmitidos, sem a ocorrência de encapsulamento desses datagramas.

O roteamento no OSPF tem como fundamento a constituição de FIBs *(Forwarding Information Bases),* também referidas como *link–state databases,* nos roteadores da rede IP. Essas bases de dados consistem em um conjunto de entradas que representa a constituição de todo um domínio de roteamento*.*

Como primeira etapa, os roteadores do domínio encontram os seus vizinhos, utilizando para isso *hello packets*.

A seguir, esses roteadores repassam essas informações ao longo do domínio, por inundação, com a adição dos custos relativos a cada um dos *links* do AS e das identificações desses *links*. São também disponibilizadas, para os roteadores do domínio, listas de prefixos de endereços IP alcançáveis por cada um desses roteadores.

A inundação do domínio ocorre pela distribuição de pacotes denominados LSAs (*Link State Advertisements*) entre todos os roteadores do domínio. Ao final, as FIBs de todos os roteadores do domínio passam a conter a constituição de todo o domínio.

A RFC 2328 especifica cinco tipos de LSA, tendo cada um desses tipos o seu próprio payload.

Passa-se então à fase de cálculo de um conjunto de árvores de rotas de menores custos acumulados (*shortest paths*) centradas em cada um dos roteadores e alcançando todos os demais roteadores do domínio. Cada um desses roteadores dispõe também das listas de prefixos de endereços IP alcançáveis por cada um dos roteadores.

Para melhor administração do processo de roteamento na rede IP e para reduzir o tráfego de roteamento na rede e a ocupação de espaços de memória, o OSPF divide a rede em domínios hierarquizados, dentro dos quais individualiza-se o roteamento.

No primeiro nível dessa hierarquia encontram-se os ASs (*Autonomous Systems*).

O cálculo de rotas em um domínio de roteamento ocorre normalmente pela aplicação do algoritmo de *Dijskstra*, também referido como algoritmo SPF (*Shortest Path First*).

Se existirem rotas com custos iguais, o roteador distribui o tráfego entre elas, de acordo com um algoritmo para isso definido, como o ECMP (*Equal-Cost Multi-Path*), por exemplo.

A partir do prefixo de endereço IP de destino de um datagrama IP, um roteador é capaz de identificar a árvore SPF e, em consequência, de obter também a identificação do próximo roteador (*next hop*) a receber o datagrama e do link a utilizar com esse propósito. Essa relação é disponibilizada em tabelas de roteamento contidas nos roteadores.

Para a plena operacionalização do OSPF, são utilizados pacotes (mensagens) OSPF de cinco diferentes tipos. Todos esses pacotes possuem um cabeçalho comum, onde podem ser identificados os diferentes tipos de pacotes.

Dentre os tipos de pacotes, destaca-se a importância do *Link State Update Packet*, responsável pela difusão das LSAs nos ASs. Um desses pacotes pode transportar diferentes LSAs.

Os ASs são interconectados por meio de roteadores especiais, denominados AS *Boundary Routers* (ASBRs), que além de delimitar os ASs, são os responsáveis pelo intercâmbio de informações de roteamento entre ASs (obtidas por meio de um protocolo de roteamento do tipo EGP).

A própria divisão de uma rede IP global em ASs já conduz o melhor uso dos recursos da rede IP para roteamento, mas o OSPF caminha adiante nesse propósito, pela eventual subdivisão dos ASs em Áreas OSPF.

As Áreas OSPF são interconectadas por meio de roteadores especiais, referidos como ABRs (*Area Border Routers*).

Um AS pode ser constituído como um todo ou pode ser dividido em Áreas OSPF.

No primeiro caso, o domínio de roteamento é o próprio AS. Quando o AS é dividido em Áreas OSPF, cada uma das áreas constitui um domínio de roteamento.

**4.2 – Protocolo OSPF Versão 3 (OSPFv3)**

A RFC 5340 descreve as modificações do protocolo OSPFv2 para suportar o IPv6, do que resultou o protocolo OSPFv3.

Os mecanismos fundamentais do OSPF são mantidos, tais como inundação, eleição de roteadores designados, suporte a áreas, algoritmo SPF, dentre outros.

No entanto, algumas mudanças foram necessárias, seja devido a diferenças semânticas entre o IPv4 e o IPv6, seja para apenas ajustar o aumento do tamanho dos endereços no IPv6. Essas mudanças demandam alguns aprimoramentos do OSPFv2 para o OSPFv3, e constituem o objetivo da RFC 5340.

Dentre tais aprimoramentos, pode ser citada a criação de novas LSAs para o transporte de endereços e prefixos do IPv6. O OSPF passa a ocorrer na base per-*link* e não mais na base per-IP-*subnet*, o que afeta a recepção de pacotes do protocolo OSPF e o conteúdo de pacotes *Hello* e de *network-LSAs*.

Outro aprimoramento introduzido na RFC 5340 são alterações no formato do cabeçalho das LSAS, embora o seu tamanho permaneça o mesmo (20 octetos). Tais alterações projetam-se no OSPF-TE Versão 3.

Uma dessas alterações diz respeito à generalização e à explicitação do alcance da inundação por LSAs. Os limites desse alcance passam agora a ser explicitamente separados para âmbito do *link* local, âmbito de uma única área OSPF e âmbito de único AS.

Essa separação de âmbitos para a inundação de LSAs no OSPFv3 veio a ser utilizada nas extensões do OSPF para TE, tanto no OSPF-TE Versão 2 quanto no OSPF-TE Versão 3, como veremos adiante neste item.

**4.3 – Protocolo OSPF-TE Versão 2**

A RFC 3630 define extensões do protocolo OSPF versão 2 (OSPFv2) para TE. Essas extensões são referidas como protocolo OSPFv2 TE ou protocolo OSPF-TE Versão 2.

O OSPF-TE Versão 2 destina-se ao roteamento IGP no plano de controle do MPLS-TE com suporte em redes IPv4.

Essas extensões, partindo da descrição da topologia e dos parâmetros de QoS da rede que suporta TE (incluindo largura de banda e restrições administrativas), proveem os mecanismos de distribuição dessas informações dentro de uma área de roteamento OSPF (área OSPF).

A RFC 3630 não aborda a aplicação dos mecanismos nela descritos para TE entre áreas OSPF, ou seja, a aplicação de protocolos EGP, deixando essa tarefa para futuros documentos de padronização.

Outra restrição da RFC 3630 diz respeito à sua aplicabilidade apenas a links ponto a ponto, não contemplando o seu alcance a links multi-acesso, exceto para o caso de existência de apenas dois terminais no link multi-acesso.

O OSPF-TE Versão 2, objeto da RFC 3630, descreve e define uma forma de distribuição de atributos de linkestendidos (*extended link attributes*) no plano de controle do MPLS-TE com suporte em redes IPv4, distribuição essa que se baseia em *constraint-based routing* e em *source routing*. Ao contrário do OSPF convencional, onde cada roteador realiza o roteamento de pacotes com base em tabelas de roteamento local, o OSPF-TE centraliza as informações em bases de dados estendidas localizadas nos comutadores de borda da rede (PEs, no caso de rede MPLS-TE), bases de dados essas que são denominadas TE *database*s (TEDs)

Quando um desses PEs se torna o *head end* LSR de um LSP, as informações, que se encontram na TED desse LSR, serão comparadas aos atributos de TE LSP do TE LSP a ser constituído, configurados ou contidos nesse *head end* LSR.

A partir dessa comparação, realizada por meio de um algoritmo de cálculo de rotas como o CSPF (*Constrained Shortest Path First*), resulta a definição da rota a ser utilizada pelo LSP em constituição, desencadeando-se então o processo de sinalização pelo *head end* LSR. A rota definida irá constar explicitamente das mensagens do processo de sinalização.

**4.3.1 – LSAs Opacas**

No OSPF *Version* 2, que é um protocolo de roteamento que opera de forma distribuída, a transmissão das informações de roteamento ocorre por meio de LSAs, que são processadas por todos os roteadores da rede.

No OSPF-TE, por se tratar de um protocolo que opera por *source routing*, somente os LSRs de borda, ou seja, os PEs, necessitam processar as informações contidas nas LSAs, cabendo aos LSRs no interior da rede, ou seja, aos Ps, apenas receber, gerar e transmitir informações de roteamento.

Por essa razão, foi definida, na RFC 5250 (*OSPF Opaque LSA Option*), uma nova modalidade de LSA, referida como LSA opaca, assim denominada por não requerer processamento nos LSRs no interior da rede.

Foram definidos três tipos de LSA opaca:

─ LSA opaca tipo 8.

─ LSA opaca tipo 10.

─ LSA opaca tipo 11.

Esses tipos de LSA opaca diferem quanto à abrangência de suas inundações. A LSA opaca tipo 8 abrange apenas um link, enquanto a LSA opaca tipo 10 abrange uma área OSPF. A LSA opaca tipo 11, por sua vez, abrange todo um sistema autônomo OSPF.

A RFC 3630 especifica apenas a utilização da LSA opaca tipo 10, ou seja, restringe a sua aplicabilidade ao interior de uma área OSPF.

Dentro do tipo 10 de LSAs opacas foi definida uma LSA específica para TE, denominada *Traffic Engineering* (TE LSA), identificada pelo código 1.

**4.3.1.1 – Formatos de TE LSAs**

A Figura 1 apresenta o formato do cabeçalho de TE LSAs

*0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| LS age | Options | 10 |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| 1 | Instance |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| Advertising Router |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| LS sequence number |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| LS checksum | Length |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

**Figura 1 - Formato do cabeçalho de TE LSAs.**

O *payload* das TE LSAs*,* que se encontra imediatamente abaixo do cabeçalho nessa figura, é constituído por um dentre dois tipos de *top-level* TLV, que pode ou não ser seguido por uma sucessão de sub-TLVs. Uma TE LSA contém apenas um dos tipos de *top-level* TLV de cada vez.

Os *top-level* TLVs, assim como os sub-TLVs eventualmente utilizados, adotam o formato padrão dos TLVs. Esse formato consiste em um campo tipo (2 octetos), um campo comprimento (2 octetos) e um campo valor (número variável de octetos). O campo comprimento indica o número de octetos contidos no campo valor.

A Figura 2 mostra o formato padrão dos TLVs.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

*| Type | Length |*

*+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+*

*| Value... |*

*.* .

. .

. .

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

**Figura 2 – Formato padrão dos TLVs**.

Os dois tipos de *top-level TLV* definidos são os seguintes:

─ *Router address TLV*

─ *Link TLV.*

**4.3.1.2 – Campos do Cabeçalho de TE LSAs**

Abordaremos, a seguir, os campos do cabeçalho de TE LSAs.

* **Campo LS Age**

O campo *LS Age*, definido na RFC 2328, representa a idade da LSA medida em segundos, sendo setado para 0 quando a LSA é originada. O seu propósito é assegurar a sincronização das bases de dados dos roteadores ou LSRs.

* **Campo Options**

O campo *Options* habilita os roteadores ou LSRs a comunicar, por intermédio de TE LSAs, o seu nível de capacidade para suportar (ou não) determinadas funções de roteamento.

Foi criada uma nova opção de função para as LSAs opacas, de nominada *O-bit* (2º bit à esquerda no campo *Options*), com o objetivo de indicar a capacidade de um roteador (ou LSR) de enviar LSAs opacas.

* **Campo LSA Type**

Esse campo recebe o valor 10, para indicar LSA opaca tipo 10.

* **Campo LSA ID**

Esse campo, com 32 bits, sem qualquer significado topológico, é subdividido em um campo *type* (8 bits) e em um campo *instance* (24 bits). O campo *type* recebe o valor 1 para indicar se tratar de uma TE LSA.

O campo *instance* compõe-se de valores arbitrários, utilizados para identificar as múltiplas instâncias de TE LSAs.

**4.3.1.3 – Router Address (Top Level) TLV**

O *router address TLV*, que é um *top-level* TLV, especifica um endereço IP estável do roteador (ou LSR) que envia a LSA.

Esse endereço é tipicamente configurado como um *loopback address*, o que significa que ele é sempre alcançável enquanto houver conectividade para o correspondente roteador, em qualquer uma de suas interfaces.

O *router address TLV* é do tipo 1 e ocupa os 32 bits correspondentes a endereços IPV4, não utilizando sub-TLVs.

**4.3.1.4 *–* Link (Top Level*)* TLV**

O *link TLV,* que é um *top-level TLV*, descreve os atributos de link de cada um dos links da rede. Ele é constituído por um conjunto de sub-TLVs após o cabeçalho do próprio TLV, sendo que cada sub-TLV corresponde a um atributo de link de cada um dos links da rede. Os sub-TLVs podem ser posicionados em qualquer ordem, após o cabeçalho do *link TLV*.

O *link TLV* é do tipo 2 e o seu comprimento é variável. A relação inicial dos atributos de *link*(sub-TLVs) para o *link TLV* definidos na RFC 3630, acrescida do sub-TLV SRLG (*Shared Risk Link Group*) definido na RFC 4203, encontra-se na Figura 3.

|  |  |  |
| --- | --- | --- |
| **TIPO** | **SUB-TLVs** | **OCTETOS** |
| 1 | *Link Type* | 1 |
| 2 | *Link* ID | 4 |
| 3 | *Local Interface* IP *Address* | 4 |
| 4 | *Remote Interface* IP *Address* | 4 |
| 5 | *Traffic Engineering Metric* | 4 |
| 6 | *Maximum Bandwidth* | 4 |
| 7 | *Maximum Reservable Bandwidth* | 4 |
| 8 | *Unreserved Bandwidth* | 4 |
| 9 | *Administrative Group* | 4 |
| 16 | *Shared Risk Link Groups* (SRLGs) | Variável |

**Figura 3 - Relação de sub-TLVs do *link* TLV.**

A RFC 3630 definiu os nove primeiros sub-TLVs acima relacionados, mas deixou aberta a possibilidade de definição de novos atributos de link (sub-TLVs)*.*

Os sub-TLVs *Link Type* e *Link ID* são obrigatórios, isto é, devem aparecer em todas as LSAs originárias de um roteador (LSR), enquanto as demais são opcionais. Os futuros sub-TLVs poderão ser ou não obrigatórios.

Alguns atributos de link são configuráveis, a exemplo do atributo *Maximum Reservable Bandwidth*, enquanto outros não o são, a exemplo do atributo *Unreserved Bandwidth*.

**4.3.1.5 - Descrição dos Atributos de Link do Link TLV**

Serão apresentados, a seguir, os sub-TLVs do *Link TLV* relacionados na Figura 3.

* **Link Type Sub-TLV**

Esse sub-TLV, que é do tipo 1 e possui um octeto, define o tipo de link utilizado, dentre as seguintes opções:

─Link ponto a ponto.

─Link multi-acesso.

* **Link ID Sub-TLV**

Esse sub-TLV, que é do tipo 2 e possui 4 octetos, identifica o outro extremo do link. Para links ponto a ponto, esse sub-TLV indica o *router ID* do roteador vizinho no extremo do link.

Para links multi-acesso, esse sub-TLV representa o endereço da interface do roteador designado.

* **Local Interface IP Address Sub-TLV**

Esse sub-TLV especifica o(s) endereço(s) IP da interface correspondente a esse link. Se existem múltiplos endereços locais no link, eles são todos relacionados nesse sub-TLV.

O sub-TLV *Local Interface IP Address* é do tipo 3 e o seu tamanho é igual a 4N octetos, onde N é o número de endereços locais.

* **Remote Interface IP Address Sub-TLV**

Esse sub-TLV especifica o(s) endereço(s) IP da interface do roteador (ou LSR) vizinho correspondente ao link. Esse sub-TLV, associado ao sub-TLV Local *Interface IP Address*, é utilizado para discernir múltiplos links paralelos entre dois roteadores (ou LSRs).

O sub-TLV *Remote Interface IP Address* é do tipo 4 e o seu tamanho é igual a 4N, onde N é o número de endereços no roteador (ou LSR) no extremo do link.

* **Traffic Engineering Metric Sub-TLV**

Esse sub-TLV especifica a métrica *link-state* utilizada no *link* para fins de TE. Essa métrica é tipicamente configurada pela supervisão da rede.

Admite-se a utilização da métrica OSPF convencional e de uma métrica TE no MPLS TE para diferentes classes de tráfego.

Um TE LSP para uma aplicação de voz, por exemplo, pode utilizar a métrica OSPF convencional relativa a retardos e a *jitters* de quadros na rede, enquanto um TE LSP para transferência de grandes arquivos pode utilizar uma métrica TE relativa a larguras de banda disponíveis.

O sub-TLV *Traffic Engineering Metric* é do tipo 5 e o seu tamanho é igual a 4 octetos.

* **Maximum Bandwidth Sub-TLV**

Esse sub-TLV, que é do tipo 6 e possui 4 octetos, especifica a largura de banda máxima que pode ser utilizada no sentido do link. Na realidade, esse sub-TLV representa a velocidade no sentido do link, medida em bytes por segundo.

É possível que parte dessa largura de banda não seja usada para TE.

* **Maximum Reservable Bandwidth Sub-TLV**

Esse sub-TLV especifica a largura de banda máxima que pode ser reservada no link, no sentido do link.

O seu valor, que é configurado pela supervisão da rede, pode ser superior ao da *maximum bandwidth* (o que se denomina *oversubscription*), devido à natureza estatística do tráfego na rede. O valor default corresponde ao da *maximum bandwidth*.

O sub-TLV *Maximum Reservable Bandwidth* é do tipo7 e o seu tamanho é igual a 4 octetos.

A RFC 2702 define esse sub-TLV em termos de proporção relativamente ao sub-TLV *Maximum Bandwidth*, sendo essa proporção denominada *Maximum Allocation Multiplier* (MAM).

* **Unreserved Bandwidth Sub-TLV**

Esse sub-TLV especifica a quantidade de largura de banda ainda não reservada, separadamente para cada um dos oito níveis de prioridade de *setup* utilizados. A ordem dos valores de largura de banda não-reservada no sub-TLV começa com o nível zero e termina com o valor 7.

O uso deste sub-TLV possibilita a segmentação e o controle da preempção da largura de banda disponível, por nível de prioridade de *setup*.

O sub-TLV *Unreserved Bandwidth* é do tipo 8 e o seu tamanho é igual a 4 octetos.

* **Administrative Group Sub-TLV**

Esse sub-TLV transporta um conjunto de 32 *bits* configurados pela supervisão da rede. O valor de cada um desses bits corresponde a um grupo administrativo desejado no link considerado.

A supervisão da rede define uma relação de no máximo 32 parâmetros expressos de forma binária como, dentre outros, os seguintes exemplos:

─ O link tem velocidade superior (ou não) a um determinado valor.

─ O link apresenta retardo inferior (ou não) a um determinado valor.

─ O link tem confiabilidade superior (ou não) a um determinado padrão.

─ O link localiza–se (ou não) em uma determinada área geográfica.

─ O link é privativo ou alugado de terceiros.

─ O link trafega (ou não) via satélite.

Nessa relação, o bit menos significativo é referido como grupo zero, e o mais significativo como grupo 31.

Essa relação é configurada nos LSRs que participam do MPLS TE. Para cada link, esses LSRs utilizam um conjunto de valores para cada um dos 32 bits, configurados pela supervisão de rede. Esses valores são denominados grupos administrativos, e definem os correspondentes atributos para cada um desses links.

Conforme descrição adiante neste tutorial, esses conjuntos de atributos são confrontados com outros conjuntos, também de 32 bitse com a mesma semântica, configurados nos PEs para os TE LSPs a serem constituídos. Dessa comparação resulta a definição dos caminhos que apropriadamente atendam a esses TE LSPs.

Um grupo administrativo é também denominado uma classe de recursos ou uma “cor”, de acordo com a RFC 2702.

O sub-TLV *Administrative Group* é do tipo 9 e o seu tamanho é igual a 4 octetos.

* **SRLG Sub-TLV**

O sub-TLV SRLG, definido na RFC 4203 *(OSPF Extensions in Support of Generalized Multiprotocol Label Switching),* objetiva identificar o meio de transmissão utilizado por cada um dos links que participam da rede MPLS-TE. Tal meio de transmissão pode ser, por exemplo, uma fibra óptica, um cabo coaxial ou um link de satélite.

Quando se constitui um TE LSP para servir como backup de outro TE LSP, deve ser evitado o uso de um mesmo SRLG para esses dois TE LSPs.

De posse desse atributo, o *head end* LSR pode evitar esse fato indesejável quando da definição dos EROs para os TE LSPs.

**4.3.1.5 - Procedimentos no OSPF-TE Versão 2**

Uma vez configurados os atributos de link, iniciam-se os procedimentos para a operacionalização do OSPF-TE Versão 2. As TE LSAs são enviadas pelas interfaces dos LSRs para todos os seus vizinhos, ou seja, por inundação.

Cada LSR, além de enviar as suas LSAs, repassa adiante as LSAs recebidas de seus vizinhos. Vai resultar, então, no recebimento, pelos PEs, de todas as LSAs emitidas na rede MPLS TE.

As informações conduzidas nos sub-TLVs de TE LSAs são armazenadas em bases de dados, referidas como TEDs (TE *databases)*, contidas em cada um dos PEs da área OSPF onde se processa o MPLS-TE. Essas informações alimentam o processo de cálculo de rotas.

Deve haver, periodicamente, novas etapas de inundação de LSAs na rede. O valor default desse período no OSPF é de 20 minutos, mas o período pode ser alterado pela supervisão da rede. No caso do OSPF-TE, esse período deve ser reduzido para um valor default igual a 3 minutos.

Além desse modo periódico de envio, pode também ocorrer a transmissão de TE LSAs quando houver mudanças de estado na rede. Isso não significa, necessariamente, que qualquer mudança deva ser comunicada imediatamente.

A rede pode selecionar mudanças que devem ocasionar o envio de TE LSAs de imediato, e outras que provocam esse envio após um curto intervalo de tempo.

**4.4 – Protocolo OSPF-TE Versão 3**

O protocolo OSPE-TE Versão 3 foi especificado na RFC 5329. Esse protocolo contém extensões ao protocolo OSPFv3 para o suporte a Engenharia de Tráfego intra-área. Ao mesmo tempo, o OSPF-TE Versão 3 contém também extensões ao protocolo OSPF-TE Versão 2 para redes IPv6.

A RFC 5329 define uma nova LSA, referida como Intra-Area- TE-LSA, em substituição à TE LSA do OSPF-TE Versão 2. A Intra-Area-TE-LSA corresponde a um novo tipo de LS identificado pelo código de função LSA igual a 10.

A TE LSA representa um tipo de LSA opaca, o que não é o caso da Intra-Area-TE-LSA.

Como no caso da TE LSA, existem dois tipos de *top-level TLV* nas Intra-Area-TE-LSAs, sendo utilizado apenas um deles em um dado momento em uma LSA.

Um desses tipos de *top-level TLV* é o *Link TLV,* e o outro é o *Router* IPv6 *Address TLV.* As funções básicas desses TLVs correspondem àquelas dos TLVs do OSPF-TE Versão 2.

O *Link TLV* do OSPF-TE Versão 3 utiliza todos os sub-TLVs do *Link* TLV do OSPF-TE Versão 2, à exceção do Sub-TLV *Link ID,* cujas funções passam a ser desempenhadas por um dos novos sub-TLVs definidos para o OSPF-TE Versão 3.

Os novos sub-TLVs para o *Link TLV* criados na RFC 5329 são os seguintes:

─*Neighbor ID Sub-TLV* (tipo de sub-TLV 18).

─*Local Interface* IPv6 *Address Sub-TLV* (tipo de sub-TLV 19).

─*Remote Interface* IPv6 *Address Sub-TLV* (tipo de sub-TLV 20).

O *Neighbor ID Sub-TLV* passa a desempenhar as funções do *Link ID Sub-TLV* do OSPF-TE Versão 2.

**4.5 – Extensões de Métricas de TE para os Protocolos OSPF-TE**

A RFC 7471 descreve extensões de métricas de TE aplicáveis tanto ao protocolo OSPF-TE Versão 2 (RFC 3630) quanto ao protocolo OSPF-TE Versão 3 (RFC 5329), com o propósito de habilitar a rede para transmitir informações de roteamento concernentes ao desempenho de rede de modo escalável.

Algumas aplicações vêm se tornando cada vez mais críticas com relação ao desempenho das redes (redes MPLS, em particular), demanda essa que foi não atendida pela RFC 3639 e RFC 5329, o que gerou a necessidade da emissão da RFC 7471.

As informações transmitidas com base na RFC 7471 são consideradas no cálculo de rotas no MPLS-TE, juntamente com as informações de roteamento TE já normalmente transmitidas.

A RFC 7471 não define mecanismos para a medição das métricas transmitidas, nem tampouco para a sua utilização após a transmissão.

Dependendo do algoritmo de cálculo de rotas utilizado, as extensões de métricas de desempenho de rede para OSPF-TE podem substituir as métricas de custo (delay de propagação no *link* em substituição ao custo do link, por exemplo), ou podem ser sutilizadas de forma associada com as métricas de custo.

Efetivamente, a RFC 7471 define um conjunto de sub-TLVs a serem utilizados no *Link TLV* dos protocolos OSPF-TE para a distribuição de informações de desempenho de rede.

Essa distribuição ocorre pela inclusão desses novos sub-TLVs no *payload* do *Link TLV* das TE LSAs no caso do OSPF-TE Versão 2 e no *payload* do *Link TLV* das Intra-Area-TE-LSAs no caso do OSPF-TE Versão 3.

A Figura 4 apresenta os sub-TLVs adicionais definidos na RFC 7471 e RFC 7810 para o *link TLV.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tipo** | | **Sub - TLV** | **Tamanho**  **(octetos)** |
| RFC  7471 | RFC  7810 |
| 27 | 33 | *Unidirectional Link Delay* | 4 |
| 28 | 34 | *Min / Max Unidirectional Link Delay* | 8 |
| 29 | 35 | *Unidirectional Delay Variation* | 4 |
| 30 | 36 | *Unidirectional Link Loss* | 4 |
| 31 | 37 | *Unidirectional Residual Bandwidth* | 4 |
| 32 | 38 | *Unidirectional Available Bandwidth* | 4 |
| 33 | 39 | *Unidirectional Utilized Bandwidth* | 4 |

**Figura 4 - Sub-TLVs das RFC 7471 e RFC 7810 para o Link TLV.**

A RFC 7810, referente a extensões do IS-IS para TE será vista no subitem 5.4 do item subsequente.

**5 – EXTENSÕES DO IS-IS PARA TE**

Este item apresenta os protocolos da família IS-IS, levando à sua aplicação com TE no MPLS-TE.

Conforme menção anterior, esses protocolos são do tipo IGP.

**5.1 – IS-IS para IPv4 e IS-IS para IPv6**

O protocolo IS-IS foi especificado no padrão ISO 10588, para definir o roteamento em redes CLNP (*Connectionless Network Protocol*), dentro da arquitetura OSI.

Posteriormente, o IETF emitiu a RFC 1195, definindo extensões do IS-IS para uso como um protocolo IGP para roteamento em ambiente TCP/IP, em ambiente OSI e em ambiente dual (ou seja, o IS-IS atendendo integradamente TCP/IP e OSI).

Quando da emissão da RFC 1195 em 1990, só existia o IPv4, do que se conclui que essa RFC se destina à especificação do IS-IS para IPv4 (além do OSI, é claro). No contexto deste tutorial, estamos abordando neste momento apenas o IS-IS para IPv4.

Cada roteador distribui uma ou mais LSPs (*link state protocol data units ou link state packets*) com informações de roteamento, sendo que as LSPs correspondem às LSAs do OSPF.

Da mesma forma que nas LSAs, as LSPs são compostas por um cabeçalho fixo e por um conjunto de TLVs.

É preciso não confundir LSP (*label switching path*), que significa caminho no MPLS, com essa outra utilização da sigla LSP.

Como no OSPF, os pacotes do IS-IS utilizam técnicas de autenticação de seus conteúdos.

Ao final é aplicada uma versão do algoritmo SPF para o IPv4 e para uso dual, resultando as tabelas de roteamento nos roteadores da rede.

Para a aplicação do IS-IS no roteamento de redes IPv6, foi publicada a RFC 5308, estendendo a RFC 1195 com esse propósito. Dessa forma, é possível rotear IPv6 juntamente com IPv4 e OSI no interior de um mesmo domínio de roteamento.

A RFC 5308 descreve dois novos TLVs, que são o IPv6 *Reachability* TLV e o IPv6 *Interface Address* TLV.

**5.2 – Protocolo ISIS-TE para IPv4**

Com o objetivo de especificar o uso do protocolo IS-IS para IPV4 com o uso de TE para roteamento no MPLS-TE, foi emitida a RFC 5305. Essa RFC define o protocolo ISIS-TE para IPv4.

A RFC 5305 descreve três novos TLVs, que podem ou não conter sub-TLVs.

Os novos TLVs definidos na RFC 5305 são os seguintes:

─*Extended* IS *Reachability TLV* (tipo de TLV 22).

─*Traffic Engineering Router ID TLV* (tipo de TLV 134).

─*Extended* IP *Reachability TLV* (tipo de TLV 135).

O *Extended* IS *Reachability TLV* desempenha, no IS-IS TE para IPv4, o mesmo papel que o *Link TLV* desempenha no OSPF-TE Versão 2, que é o de transportar as informações e as restrições (*constraints*) de roteamento contidas em diferentes sub-TLVs.

**5.3 – Protocolo ISIS-TE para IPv6**

A RFC 6119 especifica um método para o intercâmbio de informações de roteamento com TE utilizando o protocolo IS-IS para IPv6. Essas informações habilitam os roteadores de uma rede IS-IS a calcular rotas com TE utilizando endereços IPv6 no plano de controle dessa rede.

O método definido na RFC 6119 constitui o protocolo ISIS-TE para IPv6.

O uso de engenharia de tráfego no MPLS vem obtendo um grande sucesso, e, na medida em que a utilização do IPv6 aumenta, torna-se necessário o suporte a TE em redes IPv6.

A RFC 6119 define os TLVs que possibilitam o transporte de informações com TE em redes (incluindo redes GMPLS) utilizando o protocolo ISIS-TE, criando uma abordagem que possibilita que *links* e nós sejam identificados por endereços IPv6.

Foram definidos na RFC 6119 os seguintes novos TLVs:

─ *IPv6 SRLG TLV* (tipo de TLV 139).

─ *IPv6 TE Router ID TLV* (tipo de TLV 140).

*─ IPv6 Global Interface Address TLV* (tipo de TLV 233).

O *Extended* IS *Reachability TLV,* definido na RFC 5305 para o protocolo ISIS-TE para IPv4, permanece válido também para o protocolo ISIS-TE para IPv6.

**5.4 – Extensões de Métricas de TE para o ISIS-TE para IPv4**

A RFC 7810 descreve extensões de métricas de TE aplicáveis apenas ao protocolo ISIS-TE para IPv4 (RFC 5305), com o propósito de habilitar a rede a transmitir informações de roteamento concernentes ao desempenho de rede de modo escalável.

As razões que justificam a RFC 7810 como extensão do protocolo ISIS-TE para IPv4, são as mesmas que justificam a RFC 7471 como extensão dos protocolos OSPF-TE Versão 2 e Versão 3.

Como no caso da RFC 7471, a RFC 7810 restringe-se ao transporte de informações referentes ao desempenho de rede, não se envolvendo com o processamento dessas informações.

As duas RFCs admitem a substituição de métricas de custos por parâmetros de desempenho de rede, ou o uso associado de ambos.

A RFC 7810 resume-se na definição de sub-TLVs relativos a desempenho de rede, a serem transportados no *payload* do IS-IS *Extended Reachability TLV.*

Observa-se que as denominações dos tipos de sub-TLV da RFC 7471 e da RFC 7810 são as mesmas, variando, contudo, os códigos identificadores dos respectivos tipos.

**6─CÁLCULO DE ROTAS COM BASE EM CONDICIONANTES**

O presente item apresenta o processo de cálculo de rotas com base em condicionantes (*constraint-based path computation*), utilizado no plano de controle do MPLS-TE e no GMPLS. Estamos nos limitando neste tutorial ao caso do MPLS-TE.

**6.1 - Cálculo de Rotas e Constituição de TE LSPs**

Como foi visto nos itens anteriores deste tutorial, como resultado dos protocolos OSPF-TE e dos protocolos ISIS-TE, são constituídas as TEDs em todos os PEs das redes MPLS-TE.

Como temos conhecimento, a TED contém todos os atributos condicionantes (*constraints*) referentes aos links da rede, atributos esses conduzidos nos diferentes sub-TLVs contidos em LSAs (protocolos OSPF-TE) ou em LSPs (protocolos ISIS-TE).

Quando um dos PEs vai iniciar a constituição de um TE LSP, esse PE torna-se o *head end LSR* (ou simplesmente o PE de ingresso) para o TE LSP.

A solicitação para a constituição de um TE LSP é feita por um cliente, que pode ser um usuário ou o próprio provedor de serviço. O solicitante define o conjunto de atributos condicionantes aplicáveis ao TE LSP e encaminha esses atributos para o provedor de serviço.

Nos termos da RFC 4655 (*A Computation Element* (PCE)*-Based Architecture*), o provedor de serviço configura o conjunto de atributos do TE LSP em uma unidade referida como PCC (*Path Computation Client).*

O provedor de serviço configura também o PCE (*Path Computation Element*), onde são processados os algoritmos de cálculo de rotas. Podem ser utilizados diferentes algoritmos, sendo o CSPF (*Constrained Shortest Path First*) o algoritmo mais utilizado no MPLS-TE.

O PCE pode ser utilizado em diferentes configurações. O PCE pode constituir-se em uma única unidade ou em múltiplas unidades fisicamente dispersas. Quando em uma única unidade, o PCE pode se localizar interna ou externamente ao respectivo *head end LSR*.

O PCE é alimentado pela TED e pelo PCC com os atributos de *link* e com os atributos do TE LSP, respectivamente.

No PCE, os atributos definidos para o TE LSP são confrontados com as combinações dos atributos de link dos links que compõem os caminhos com a mesma origem e o mesmo destino do TE LSP.

Como resultado dessa confrontação, ou dessa comparação, o PCE define, mediante a aplicação do algoritmo de cálculo de rotas, o caminho (ou seja, a sucessão de LSRs) que melhor atenda a solicitação do cliente. Esse melhor caminho é explicitado no objeto ERO (*Explicit Route Object*).

A Figura 5 exibe o processo de cálculo de rotas na hipótese de utilização do PCE em uma única unidade no interior do *head end LSR.*



**Figura 5 - Configuração com PCE no interior do head end LSR.**

Na parte superior da figura, observa-se a interação da TED com o protocolo de roteamento. Verifica-se também a alimentação do PCE pela TED.

Observa-se também a presença do dispositivo de sinalização (*Signaling Engine*), que se comunica bidirecionalmente com o PCE.

O dispositivo de sinalização é responsável pelo processo de sinalização e pela transmissão e recepção das mensagens de sinalização.

O PCC não está explicitado, mas ele se encontra na parte esquerda inferior da figura, alimentando o PCE com os atributos de TE LSPs pelo envio da solicitação de serviço (*Service Request*).

Como se verifica pelos sentidos das setas na figura, a solicitação de serviço é encaminhada ao PCE via o dispositivo de sinalização.

Uma vez definido o ERO para o LSP, o CPE envia esse objeto para o dispositivo de sinalização, que inicializa o processo de sinalização pelo protocolo RSVP-TE, do que resulta o estabelecimento do TE LSP. O protocolo RSVP-TE será apresentado no item 8 subsequente neste tutorial.

**6.2 – Algoritmo CSPF**

O algoritmo CSPF é uma versão avançada do algoritmo SPF utilizada para cálculo de rotas em OSPF-TE e em ISIS-TE. O CSPF é utilizado na definição de rotas mais curtas para TE LSPs respeitando um conjunto de atributos condicionantes (*constraints*).

No cálculo do melhor caminho para um TE LSP, o CSPF leva em consideração a topologia da rede, os atributos configurados aplicáveis ao TE LSP e os atributos de link dos links da rede.

Se resultarem caminhos com custos iguais (*equal-cost paths*) após a aplicação do CSPF, o caminho a ser utilizado será então selecionado de acordo com algumas regras.

A primeira dessas regras resume-se na escolha do caminho com o menor número de links.

Se ainda persistir a igualdade na escolha do caminho, deve ser aplicada a regra de balanceamento de carga no CSPF configurada para o TE LSP. Existem três alternativas:

─*Random*: Um dos caminhos remanescentes é selecionado ao acaso.

─*Least fill*: Essa regra atribui a preferência ao caminho que apresenta a maior taxa de banda mínima disponível.

─*Most fill*: Essa regra atribui a preferência ao caminho que apresenta a menor taxa de banda mínima disponível.

Taxa de banda disponível é a razão entre a banda disponível e a banda reservável em um link.

Os links que não sejam full-duplex devem ser eliminados.

O CSPF é simplesmente uma aplicação do SPF após a eliminação dos links e dos caminhos que violam determinadas condições impostas pelo cliente solicitante do TE LSP em constituição.

A violação pode ser constatada nos valores de atributos dos próprios links ou no somatório dos valores de atributos dos links que compõem cada um dos possíveis caminhos.

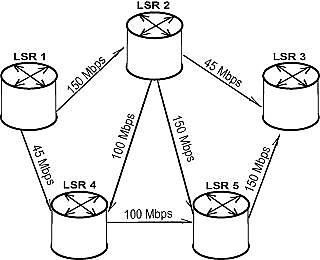
Um importante exemplo do primeiro caso é a largura de banda desejada pelo cliente comparativamente às larguras de banda disponíveis em cada um dos links considerados, no momento da solicitação de ativação do TE LSP. Os links que individualmente não disponham, nesse momento, no mínimo da largura de banda desejada devem ser eliminados. A eliminação de um *link* redunda na eliminação dos caminhos que o contém.

Para o segundo caso vamos citar dois exemplos.

Um primeiro exemplo é o delay fim a fim máximo estabelecido pelo cliente para o TE LSP. Se um dos possíveis caminhos apresenta um delay acumulado superior ao valor máximo estabelecido, esse caminho deve ser eliminado.

O outro exemplo diz respeito ao número máximo de links que constituem um caminho. Se um caminho viola o valor definido, esse caminho deve ser eliminado.

Para melhor entendimento do CSPF, vamos considerar o exemplo de configuração de rede MPLS TE da figura 6.



**Figura 6 - Exemplo de configuração de rede MPLS- TE.**

Vamos admitir as seguintes hipóteses com relação a essa figura:

─ Objetiva-se definir o melhor caminho entre o LSR 1 e o LSR 3.

─ Todos os links têm a mesma distância na métrica SPF adotada.

─ OS links<LSR 1, LSR 2>, <LSR 2, LSR 5> e <LSR 5, LSR 3> têm uma largura de banda disponível de 150 Mbps.

─ Os links<LSR 2, LSR 4> e <LSR 4, LSR 5> têm uma largura de banda disponível de 100 Mbps

─ Os links<LSR 1, LSR 4> e <LSR 2, LSR 3> têm uma largura de banda disponível de 45 Mbps.

Vamos supor inicialmente que o TE LSP demande uma largura de banda de 120 Mbps. O *head end LSR* (LSR 1) elimina, pela aplicação do CSPF, o *link*<LSR 1, LSR 4>, escolhendo o link <LSR 1, LSR 2>, em função da disponibilidade de largura de banda.

No próximo passo, o LSR 2 elimina, pelo CSPF, os links <LSR 2, LSR 4> e <LSR 2, LSR 3>, e escolhe o link<LSR 2, LSR 5>. No passo seguinte, a única opção é o *link*<LSR 5, LSR 3> que, por satisfazer o CSPF, é utilizado.

Assim, considerando-se o atributo largura de banda, o único caminho que satisfaz o CSPF é <LSR 1, LSR 2, LSR 5, LSR 3>.

Observa-se que, pelo SPF, o caminho escolhido seria <LSR 1, LSR 2, LSR 3>, cuja distância no IGP convencional é a menor de todas.

Vamos supor uma segunda alternativa, em que a classe de tráfego demande uma largura de banda de 80 Mbps. Aplicando-se os critérios acima, o CSPF, em sua primeira ação, define os caminhos <LSR 1, LSR 2, LSR 4, LSR 5, LSR 3> e < LSR 1, LSR 2, LSR 5, LSR 3> como viáveis.

Em uma segunda etapa, o CSPF define o caminho <LSR 1, LSR 2, LSR 5, LSR 3> como preferencial, por possuir uma distância IGP inferior à da segunda opção viável. Ou seja, no CSPF, após a eliminação dos links que não satisfazem as condições (*constraints*) consideradas (a largura de banda nos exemplos acima), aplica-se o SPF nos links remanescentes para a determinação do caminho a ser utilizado pelo TE LSP.

**6.3 – Atributos de TE LSP**

Como dissemos anteriormente neste tutorial, o cálculo de rotas consiste na determinação do ERO a ser utilizado pelo TE LSP em constituição, determinação essa que resulta da comparação, no CPE, dos valores dos atributos de TE LSP configurados para o TE LSP com os valores dos atributos de link dos links da rede.

Os valores dos atributos de TE LSP configurados são normalmente determinados pelo cliente, mas podem ser excepcionalmente determinados pelo provedor de serviço.

Apresentamos a seguir a relação alguns dos principais atributos de TE LSP:

─ Endereço do *tail end LSR.*

─ Largura de banda desejada.

─ Número máximo de links.

─ *Dela*y fim a fim máximo.

─ Variação de delay fim a fim máxima.

─ Taxa de perda de quadros máxima

─ Atributos de afinidade.

─ Atributo de adaptividade.

─ Atributo de preempção.

Por entendermos que os significados dos seis primeiros desses atributos são de fácil entendimento, abordaremos apenas os três últimos.

**6.3.1 - Atributos de Afinidade**

Como vimos no subitem 5.3.1.4 deste tutorial, os links utilizam um atributo de link denominado Grupo Administrativo (*Administrative Group*). Esse sub-TLV é composto por 32 parâmetros de significado binário (32 bits), configurados pela supervisão da rede para cada um dos links da rede.

O Atributo de Afinidade de um TE LSP consiste em uma máscara de 32 bits aplicada, no *head end LSR* do TE LSP, sobre cada um dos links da rede. Cada um desses bits é configurado com um valor com o mesmo significado que o do correspondente grupo administrativo dos links da rede para seja possível a sua comparação.

Como resultado dessa comparação, o link pode ser ou não eliminado, sendo a comparação realizada sobre todos os bits configurados. Qualquer um dos bits pode causar a eliminação do link.

A eliminação de um link em decorrência da comparação de valores em um grupo administrativo pode ocorrer pela atribuição de dois diferentes valores ao parâmetro de afinidade no *head end LSR*. Tais valores são a inclusão explícita e a exclusão explícita.

Na inclusão explícita, a comparação dos valores de um grupo administrativo em um *l*ink elimina o link se o valor do grupo no *link* não for igual ou não satisfizer o valor desse grupo na máscara.

Por exemplo, suponhamos que no grupo administrativo considerado o valor nos links possa ser **A** (bit igual a 1) ou não ser **A (**bit igual a 0). Suponhamos também que no link em análise o valor do bit seja 1 (ou seja, o valor é **A**).

Suponhamos, mais uma vez, que se utilize inclusão explícita e que tenha sido configurado o valor **B** (igual a **A** ou que seja satisfeito por **A)** para esse grupo administrativo na máscara. Isso indica que o link deve ser eliminado se o valor no link não for **A**. Como o valor no link é **A**, o link não será eliminado devido a esse grupo administrativo.

Consideremos novamente as mesmas condições anteriores, mas na hipótese de uso de exclusão explícita ainda com o valor B para o grupo administrativo na máscara. Isso significa que o link deve ser eliminado se o valor no link for A. Como o valor no link é A, o link será eliminado devido a esse grupo administrativo.

Aplicando-se os procedimentos acima para todos os grupos administrativos de um link, fica definido se o link deve ser ou não eliminado do TE LSP em constituição.

Caso não se observe plena afinidade para todos os grupos administrativos em um link, cabe à supervisão da rede rejeitar ou não esse link.

Se não ocorrer a especificação de atributos de afinidade para os grupos administrativos na máscara de um TE LSP, então é assumida uma relação de afinidade *“don’t care”* entre o TE LSP e os grupos administrativos. Em outras palavras, não existe qualquer requisito para incluir ou excluir explicitamente links devido a atributos de afinidade. Essa forma deve ser adotada como default na prática.

**6.3.2 – Atributo de Adaptatividade**

Como as características e estado das redes mudam ao longo do tempo em decorrência da inclusão, exclusão e alteração de recursos, torna-se necessária a definição de mecanismos para responder a esse dinamismo.

O processo de aplicação desses mecanismos adaptativos é referido como reotimização.

Utiliza-se um atributo de adaptatividade para indicar, quando da constituição de um TE LSP, se esse TE LSP é passível ou não de reotimização.

Um atributo de adaptatividade é uma variável binária que assume um dos seguintes valores:

─ Habilita-se a reotimização para o TE LSP.

─ Desabilita-se a reotimização para o TE LSP.

Se a reotimização encontra-se habilitada, então o TE LSP pode ser rerroteado para diferentes caminhos em resposta a uma alteração no estado da rede.

Por uma questão de compromisso entre a estabilidade e a rapidez de adaptação da rede ao rerroteamento, a frequência de reotimização deve ser administrativamente configurável.

Observamos que reotimização é distinta de resiliência. A reotimização implica resiliência a falhas, mas resiliência a falhas não implica adaptatividade geral por meio de reotimização.

**6.3.3 - Atributo de Preempção**

Esse atributo possibilita que um TE LSP tenha primazia ou não sobre outro na ocupação dos recursos da rede, particularmente no que diz respeito a larguras de faixa.

Essa condição é verificada, no *head end LSR*, durante a fase de constituição dos dois TE LSPs ou mesmo quando um deles já se encontra em funcionamento.

A preempção pode ser utilizada para garantir que TE LSPs com alta prioridade de permanência em filas, possam sempre utilizar caminhos mais favoráveis caso se utilize *DiffServ.*

O atributo de preempção pode ser utilizado para especificar quatro modos de preempção para um TE LSP:

─ *Preemptor enabled (1)*.

─ *Non-preemptor (2).*

─ *Preemptable (3)*.

─ *Non-preemptable (4)*.

Um TE LSP *preemptor enabled* pode *preemptar* um TE LSP *preemptable*, se o primeiro tiver a *setup priority* superior à *holding priority* do segundo.

Um TE LSP *non-preemptor* não pode *preemptar* outro TE LSP, independentemente de prioridades.

Um TE LSP *preemptable* pode ser *preemptado* por um TE LSP *preemptor enabled* com o valor de *setup priority* superior ao da *holding priority* do TE LSP *preemptable*.

Um TE *non-preemptable* não pode ser *preemptado* por outro TE LSP, independentemente de prioridades.

Um TE LSP pode ser configurado com múltiplos modos de preempção, mas alguns desses modos são mutuamente exclusivos. Utilizando a numeração acima, as combinações de modos de preempção viáveis são as seguintes: [1,3], [1,4], [2,3] e [2,4]. A combinação [2,4], quando o TE LSP é *non-preemptor* e *non-preemptable*, deveria ser a default.

A escala de prioridades vai de zero a 7, sendo zero a maior prioridade. Existe uma escala de prioridade para obter a cessão de recursos (*setup priority*) e outra para permitir a cessão (*holding priority*).

Para obter a cessão, a prioridade do TE LSP *preemptor enabled* deve ser superior à prioridade do TE LSP *preemptable* para conceder o recurso. É recomendável que um TE LSP *preemptor enabled*, com *setup priority* alta, tenha também uma alta *holding priority* caso esse TE LSP seja também um TE LSP *preemptable*.

**7 – SINALIZAÇÃO NO MPLS-TE**

A sinalização para a constituição e a desativação de TE-LSPs no MPLS-TE efetiva-se pelo protocolo RSVP-TE (*Resource Reservation Protocol* -TE).

O RSVP-TE foi definido inicialmente na RFC 3209 (RSVP-TE: *Extensions to RSVP for LSP Tunnels*), que estabelece o modo de operação básico desse protocolo. A RFC 3209 restringe-se à transmissão unicast, sendo a transmissão multicast postergada para definição futura.

O protocolo RSVP-TE representa uma extensão do protocolo RSVP versão 1 definido na RFC 2205 *(Resource Reservation Protocol (RSVP)),* com o propósito de permitir o seu uso no estabelecimento de LSPs em MPLS. O RSVP-TE foi posteriormente estendido para o GMPLS, mediante a definição do protocolo GMPLS RSVP-TE.

Além de sinalizar para a constituição de LSPs no MPLS Básico (da mesma forma que o LDP), o RSVP-TE encontrou maior aplicação no MPLS-TE. No MPLS básico prevalece a utilização do LDP para distribuição de labels.

O RSVP-TE opera por meio do intercâmbio de mensagens de sinalização entre o *head end LSR* e o *tail end LSR* de um TE-LSP em ativação ou em desativação, com a intermediação dos LSRs no interior da rede MPLS-TE.

As mensagens de sinalização são compostas por unidades de informação referidas como objetos. A RFC 3209 adotou os objetos já definidos para o RSVP e criou novos objetos. Além disso, foram acrescentados novos *C-Types* para os objetos trazidos do RSVP.

As funções dos objetos são desempenhadas por meio dos C*-Types* que os constituem. Quando um objeto admite diferentes modos de ocorrência, cada um desses modos representa um subobjeto.

Uma alternativa para a sinalização no MPLS - TE seria o uso do CR-LDP (*constraint-based routing-*LDP). Contudo, prevaleceu o uso do RSVP-TE, considerando-se a natureza do RSVP, originalmente desenhado para possibilitar a reserva de recursos e o tratamento de parâmetros de QoS no IP.

Essa preferência do RSVP-TE relativamente ao CR-LDP foi resultado da análise comparativa realizada no âmbito do IETF, e tornada pública através da RFC 3468 *(The Multiprotocol Label Switching (MPLS) Working Group Decision on MPLS Signaling Protocols).*

A RFC 3209 foi objeto de algumas extensões, que introduziram importantes aprimoramentos do protocolo RSVP-TE. Dentre as RFCs que definem tais extensões, vamos abordar as seguintes:

─RFC 4090 *(Fast Reroute Extensions to RSVP-TE for LSP Tunnels).*

─RFC 4874 *(Exclude Routes – Extension to Resource ReserVation Protocol – Traffic Engineering* (RSVP-TE)).

─RFC 5420 *(Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering* (RSVP-TE))*.*

As RFCs acima relacionadas serão abordadas adiante neste item.

**7.1 – Protocolo RSVP Versão 1**

A RFC 2205 descreve a versão 1 do RSVP, um protocolo para o estabelecimento de reservas de recursos para fluxos simplex de dados, unicast ou multicast, em redes IPv4 e em redes IPv6.

Embora não seja de interesse específico no presente tutorial e a despeito de seu insucesso, o protocolo RSVP foi objeto de extensões que possibilitam a sinalização no MPLS-TE e no GMPLS.

Da mesma forma do que ocorre em suas extensões, o RSVP utiliza mensagens que transportam unidades de informação referidas como objetos.

O RSVP provê diferentes modelos, ou estilos, para a reserva de recursos, de modo a atender a uma variedade de aplicações. Como se verá adiante neste tutorial, os estilos de reserva de recursos assumem grande importância no RSVP-TE.

A RFC 2205 define os seguintes tipos de mensagem:

─ Mensagens *RSVP Path*.

─ Mensagens *RSVP Resv.*

─ Mensagens *RSVP PathErr* (*Path Error)*.

─ Mensagens RSVP *ResvErr*.

─ Mensagens *RSVP PathTear* (*Path Teardown*).

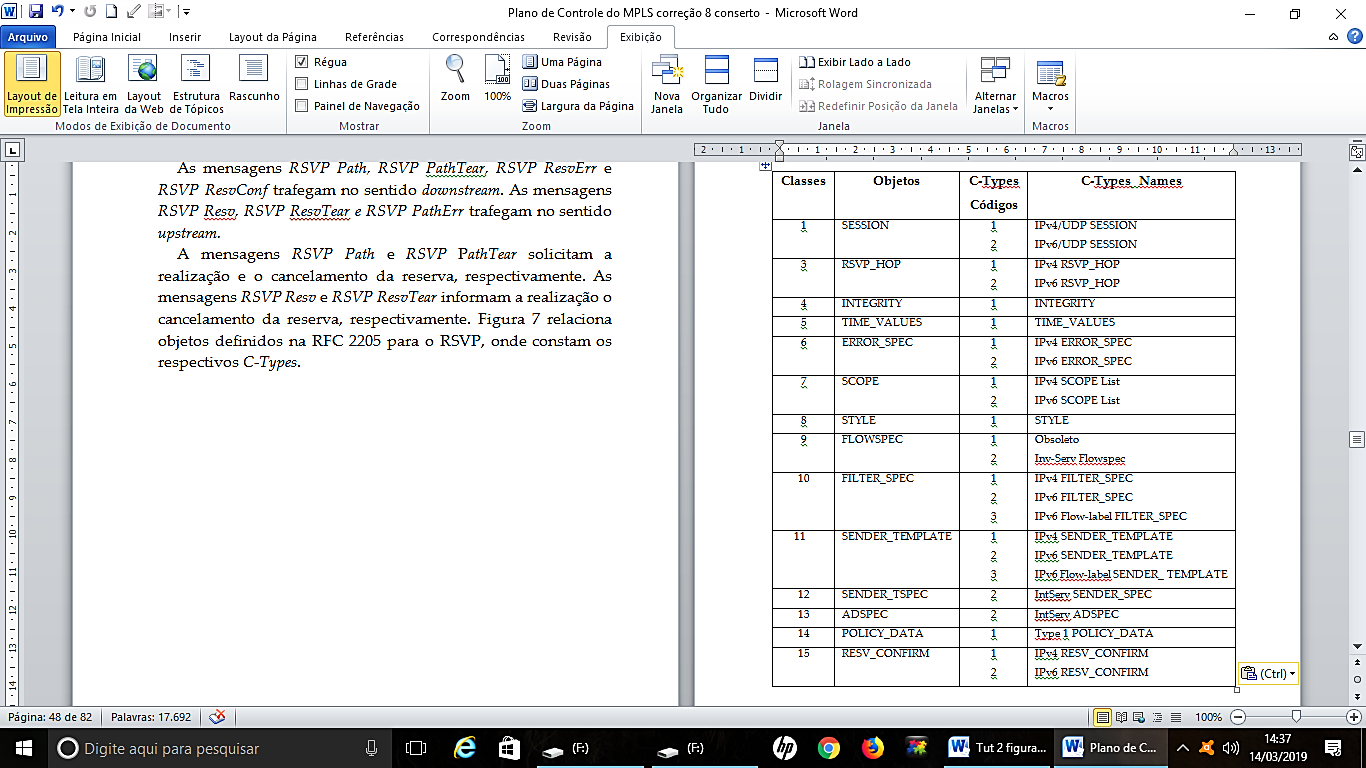
─ Mensagens *RSVP ResvTea*r.

─ Mensagens *RSVP ResvConf* (*Resv Confirmation*).

As mensagens *RSVP Path, RSVP PathTear, RSVP ResvErr* e *RSVP ResvConf* trafegam no sentido *downstream*. As mensagens *RSVP Resv,* *RSVP ResvTear e RSVP PathErr* trafegam no sentido *upstream.*

A mensagens *RSVP Path* e *RSVP* P*athTear* solicitam a realização e o cancelamento da reserva, respectivamente. As mensagens *RSVP Resv* e *RSVP ResvTear* informam a realização o cancelamento da reserva, respectivamente.

Figura 7 relaciona objetos definidos na RFC 2205 para o RSVP, onde constam os respectivos *C-Types*.



**Figura 7 - Objetos do RSVP (RFC 2205).**

**7.2 – RSVP-TE (RFC 3209)**

Conforme a RFC 3209, o protocolo RSVP-TE utiliza a distribuição de labels no modo DOD *(Downstream-on-Demand)*, com controle ordenado. Como no RSVP, o processo de sinalização no RSVP-TE tem como base as mensagens *RSVP Path* e *RSVP Resv*.

O processo de requisição de labels para a constituição de um LSP, inicia-se no *head end LSR* e prossegue pelo caminho explícito desejado, até atingir-se o *tail end LSR*.

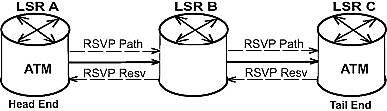
Com esse propósito, o *head end LSR* envia uma mensagem *RSVP Path* contendo os abjetos necessários conforme a RFC 3209.

No sentido contrário, pelo caminho inverso, o *tail end LSR* envia uma mensagem *RSVP Resv*, também formatada de acordo com a RFC 3209.

Os labels são solicitados aos LSRs no sentido *downstream* por meio da mensagem *RSVP Path*, sendo os seus valores atribuídos pelos LSRs ao longo do caminho explicitado no objeto ERO.

Esses valores são então distribuídos no sentido *upstream* por meio da mensagem *RSVP Resv.*

A Figura 8 ilustra o funcionamento básico do RSVP-TE.



**Figura 8 - Funcionamento básico do RSVP-TE.**

Existe a possibilidade do envio de uma mensagem *RSVP ResvConf* pelo *head end LSR,* com o objetivo de confirmar a constituição do túnel MPLS TE, caso o *tail end LSR* o tenha solicitado.

O funcionamento do RSVP-TE baseia-se em roteamento explícito, o que possibilita a otimização da utilização dos recursos da rede e a orientação do tráfego conforme as características de desempenho desejadas.

O conceito de caminho explícito pode ser generalizado através da noção de nós abstratos. Um nó abstrato é um grupo de nós cuja topologia interna é opaca para o *head end* *LSR.*

Um nó abstrato, em sua forma mais simples, é um único nó, mas ele pode ser constituído por uma sequência de nós, por uma sequência de sistemas autônomos ou mesmo por um meio de transmissão (uma fibra óptica, por exemplo).

Um caminho explícito pode conter *strict routes* e *loose routes*. Uma *loose route* constitui um hiato em um caminho explícito, posto que nela o roteamento realiza-se por tabelas de roteamento IGP, no modo convencional de funcionamento desse tipo de protocolo.

Embora de grande importância, a reserva de recursos não é obrigatória no funcionamento do RSVP-TE. Esse protocolo foi concebido inclusive para a constituição de LSPs no MPLS básico, sem a utilização da aplicação MPLS - TE.

Essa alternativa pode ser utilizada com o objetivo da transmissão de tráfego *best effort* ou em outros contextos, a exemplo do uso de políticas de recuperação da rede em caso de falha de recursos.

**7.2.1 - Mensagens do RSVP-TE**

Em conformidade com a RFC 3209, o RSVP-TE utiliza as mensagens da Figura 9.

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Mensagem** | **Sentido** |
| 1 | Mensagens RSVP *Path*. | *downstream* |
| 2 | Mensagens RSVP *Resv*. | *upstream* |
| 3 | Mensagens RSVP *PathErr.* | *upstream* |
| 4 | Mensagens RSVP *ResvErr.* | *downstream* |
| 5 | Mensagens RSVP *PathTear.* | *downstream* |
| 6 | Mensagens RSVP *ResvTear*. | *upstream* |
| 7 | Mensagens RSVP *ResvConfirm*. | *upstream* |
| 20 | Mensagens *Hello*. | ambos |

**Figura 9 – Mensagens do RSVP-TE.**

Como se observa na figura, essa relação é a mesma que a utilizada no RSVP, com o acréscimo das mensagens *Hello*. As mensagens *Hello* foram às únicas acrescentadas pela RFC 3209.

As mensagens *RSVP PathTear* e *RSVP ResvTear* constituem o grupo de mensagens *teardown,* utilizadas para remover, de imediato, os estados estabelecidos nos LSRs de um TE LSP por mensagens *RSVP Path* e *RSVP Resv*, respectivamente.

Quando, por exemplo, o *head end LSR* envia uma mensagem *RSVP PathTear*, o *tail end LSR* responde com uma mensagem *RSVP ResvTear*.

As mensagens *RSVP error*, que são as mensagens *RSVP PathErr* e *RSVP ResvErr*, são aquelas enviadas através dos TE LSPs para notificar a ocorrência de erros. As mensagens *RSVP PathErr* são enviadas, na realidade, no sentido contrário ao das mensagens *RSVP Path*, isto é, no sentido *upstream*. Com as mensagens *RSVP ResvErr* ocorre o contrário, ou seja, elas são enviadas no sentido *downstream.*

As mensagens *RSVP Path, RSVP Resv* e *Hello* serão objeto de maior detalhamento a seguir.

Registra-se que as mensagens do RSVP-TE são envelopadas como datagramas IP, e contêm um cabeçalho próprio, seguido dos objetos que compõem cada uma das mensagens.

A figura 10 apresenta o formato geral dos datagramas IP contendo as mensagens do RSVP-TE.

|  |
| --- |
| **Cabeçalho do IP** |
| **Cabeçalho do RSVP-TE** |
| **Objetos do RSVP-TE** |

**Figura 10 - Formato geral das mensagens do RSVP-TE.**

O cabeçalho comum das mensagens do RSVP-TE possui o formato exposto na Figura 11.

*0 1 2 3*

*+-------------+-------------+-------------+-------------+*

*| Vers | Flags| Msg Type | RSVP Checksum |*

*+-------------+-------------+-------------+-------------+*

*| Send\_TTL | (Reserved) | RSVP Length* |

+-------------+-------------+-------------+-------------+

**Figura 11 – Cabeçalho comum das mensagens do RSVP-TE.**

Os objetos das mensagens do RSVP-TE, por sua vez, apresentam o formato apresentado na figura 12.

*0 1 2 3*

*+-------------+-------------+-------------+-------------+*

*| Length* (bytes) *| Class-Num | C-Type |*

*+-------------+-------------+-------------+-------------+*

*| |*

*// (Object contents)* //

| |

+-------------+-------------+-------------+-------------+

**Figura 12 – Formato dos objetos das mensagens do RSVP-TE.**

No cabeçalho dos objetos, o campo *Class-Num* (*class number*), ou simplesmente classe, identifica a classe do objeto, enquanto o campo *C-Type (class type)* identifica o tipo de objeto dentro de cada classe de objeto.

**7.2.2 – Novos Objetos, C-Types e Subobjetos**

A Figura 13 apresenta a relação dos novos objetos e dos novos C-*Types* definidos na RFC 3209.

|  |  |  |  |
| --- | --- | --- | --- |
| **Classes** | **Objetos** | **C-Types Códigos** | **C-*Types* Nomes** |
| 1 | *SESSION* | 7  8 | LSP *Tunnel* IPv4  LSP *Tunnel* IPv6 |
| 10 | *FILTER\_SPEC* | 7  8 | LSP *Tunnel* IPv4  LSP *Tunnel* IPv6 |
| 11 | *SENDER\_TEMPLATE* | 7  8 | LSP *Tunnel* IPv4  LSP *Tunnel* IPv6 |
| 16 | *RSVP\_LABEL* | 1 | *Type 1 Label* |
| 19 | *LABEL\_REQUEST* | 1  2  3 | *Without Label Range*  *With* ATM *Label Range*  *With Frame Relay Label Range* |
| 20 | *EXPLICIT\_ROUTE* | 1 | *Type 1 Explicit Route* |
| 21 | *RECORD\_ROUTE* | 1 | *Type* 1 *Record Route* |
| 22 | *HELLO* | 1  2 | *Hello Request*  *Hello* ACK |
| 207 | *SESSION\_ATTRIBUTE* | 1  2 | LSP*\_TUNNEL\_*RA  LSP*\_TUNNEL* |

**Figura 13 - Novos objetos e C-Types acrescentados na RFC 3209.**

Ademais, a RFC 3209 define subobjetos para o *C-Type 1* dos objetos ERO e RRO, conforme a Figura 14.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Objetos** | **Subobjetos Códigos** | **Subobjetos Nomes** |
| 20 | *EXPLICIT\_ROUTE* | 1  2  32 | Prefixo IPv4  Prefixo IPv6  Número do AS |
| 21 | *RECORD\_ROUTE* | 1  2  3 | Endereço IPv4  Endereço IPv6  Label |

**Figura 14 - Subobjetos para o C-Type 1 dos objetos ERO e RRO.**

Para as novas mensagens *Hello*, a RFC 3209 definiu o objeto HELLO, cuja classe é 22, com dois C*-Types*: C*-Type 1,* denominado *HELLO REQUEST Object* e C*-Type 2,* denominado *HELLO ACK Object* (onde ACK significa *ackowledgment)*.

**7.2.3 - Mensagens RSVP-TE Path**

As mensagens *RSVP-TE Path* utilizam os objetos relacionados na figura 15.

|  |  |  |
| --- | --- | --- |
| **Classes** | **Objetos** | **RFCs** |
| - | Cabeçalho Comum | 2205 |
| 4 | *INTEGRITY* | 2205 |
| 1 | *SESSION* | 2205 |
| 3 | *RSVP\_HOP* | 2205 |
| 5 | *TIME\_VALUES* | 2205 |
| 20 | *EXPLICIT\_ROUTE (*ERO*)* | 3209 |
| 19 | *LABEL\_REQUEST* | 3209 |
| 207 | *SESSION\_ATTRIBUTE* | 3209 |
| 14 | *POLICY\_DATA* | 2205 |
| 11 | *SENDER\_TEMPLATE* | 2205 |
| 12 | *SENDER\_TSPEC* | 2205 |
| 13 | *ADSPEC* | 2205 |
| 21 | *RECORD\_ROUTE (*RRO*)* | 3209 |

**Figura 15 - Objetos das mensagens RSVP-TE Path.**

Alguns desses objetos são legados do RSVP convencional, enquanto outros foram definidos na RFC 3209 especificamente para o RSVP-TE. Os novos objetos são o *LABEL REQUEST*, o ERO, o RRO e o *SESSION\_ATTRIBUTE*.

Parte dos objetos legados do RSVP tiveram os seus *C-Types* inalterados na RFC 3209, enquanto os demais sofreram alterações em seus *C-Types*.

**7.2.3.1 – Objetos Legados do RSVP sem Alteração de C-Types**

São apresentados, a seguir, os objetos legados do RSVP sem alteração de *C-Types* na RFC 3209 e que são utilizados nas mensagens *RSVP Path*.

**+INTEGRITY**: Transporta informações criptografadas para autenticar o nó de origem e para verificar o conteúdo da mensagem RSVP que o transporta. Utilizado em qualquer tipo de mensagem RSVP.

+***RSVP\_HOP***: Transporta o endereço IP do nó que enviou essa mensagem, transportando também um LIH *(Logical Interface Handle)* da interface de saída do PHOP.

**+TIME\_VALUES**: Contém o valor do período de *refresh* **R** utilizado pelo criador da mensagem. Utilizado em todas mensagens *RSVP Path* ou mensagem *RSVP Resv*.

**+POLICY\_DATA**: Transporta informações que permitem a um módulo local de política decidir se uma reserva associada é administrativamente permitida. Utilizado em mensagens *RSVP Path,* *PathErr* ou *ResvErr*.

**+SENDER\_TSPEC**: Define as características de tráfego do TE LSP em constituição, particularmente o valor da banda passante desejada, expressa em bytes por segundo. Utilizado em mensagens *RSVP Path.*

**+ADSPEC**: Objetiva divulgar, para os receptores, todas as características fim a fim do TE LSP em constituição. Essa informação pode ser utilizada pelos receptores para determinar o nível de reserva de banda passante necessária para obter-se a QoS fim a fim desejada.

Esse objeto é utilizado em mensagens *RSVP Path.*

**7.2.3.2 – Objetos Legados do RSVP com Alteração de C-Types**

São apresentados, a seguir, os objetos legados do RSVP cujos *C-Types* foram alterados na RFC 3209 e que são utilizadas nas mensagens *RSVP Path.*

**+ SESSION Object**

Essa classe de objeto (classe 1) tem como propósito definir uma sessão RSVP específica.

Uma sessão no RSVP-TE representa uma convergência de circuitos virtuais para um LSR particular de um TE LSP, de modo a possibilitar uma forma organizada de compartilhamento de larguras de banda passante entre esses circuitos virtuais.

Uma sessão é identificada pelo endereço IP (IPv4 ou IPv6) do LSR de destino (onde se concentram os circuitos virtuais participantes da sessão), assim como de alguma forma de identificação da porta de destino nesse LSR.

O *tail end LSR* de TE LSPs nele convergentes é tipicamente utilizado como destino de uma sessão RSVP-TE. Nesse caso, a sessão é constituída pela convergência dos TE LSPs que a compõem.

Os circuitos virtuais de uma sessão, quando originários de diferentes fontes (LSRs), convergem normalmente para um LSR intermediário, anterior ao LSR de destino da sessão.

Forma-se então um túnel entre esses dois LSRs, onde se concentram a totalidade dos circuitos virtuais da sessão. Esse tipo de túnel é referido como um *TE Tunnel* ou *MPLS Tunnel* (não confundir com *TE LSP Tunnels*, que são outra denominação de TE LSPs).

Como o propósito é a organização de formas de compartilhamento de bandas passantes, que ocorre apenas no interior de *TE Tunnels*, a RFC 3209 especificou o formato do objeto *RSVP SESSION* adotando os termos do *TE Tunnel* que o transporta.

Assim, a RFC 3209 criou dois novos tipos de *C-Type* para a classe de objeto *SESSION*, que foram denominados objetos *LSP*\_*TUNNEL*, apresentados a seguir:

*─LSP\_TUNNEL\_IPV4object* (C*-Type7*).

*─LSP\_TUNNEL\_IPV6object* (*C-Type* 8).

Em ambos os casos, o formato do objeto é constituído por três campos principais:

*─IPv4/IPv6 Tunnel End Point Address*.

*─Tunnel ID.*

*─Extended Tunnel ID.*

O campo *Tunnel ID* identifica o *TE Tunnel* compartilhado pelos circuitos virtuais que constituem a sessão. Por associação, esse campo tem a missão de definir qual a interface do LSR final deve ser utilizada pela sessão.

O campo *Extended Tunnel ID* destina-se ao caso em que se deseja o estabelecimento de reserve separada para uma dada fonte de tráfego. Nesse caso, a fonte insere usualmente o seu próprio endereço IP nesse campo.

O objeto *SESSION* tem presença obrigatória em qualquer mensagem RSVP.

**+SENDER\_TEMPLATE Object**

As mensagens *RSVP Path* transportam o objeto *SENDER\_TEMPLATE* (classe 11), com o objetivo de prover a identificação do TE LSP em constituição (campo LSP ID) e o endereço IP (IPv4 ou IPv6) do *head end LSR.*

Foram definidos dois C*-Types*:

─*LSP*\_*TUNNEL*\_*IPV4* (C*-Type*7).

─*LSP*\_*TUNNEL\_IPV6* (C*-Type* 8)

**7.2.3.3 – Objetos Definidos na RFC 3209**

São apresentados, a seguir, os objetos definidos na RFC 3209 para as mensagens *RSVP Path****.***

***+*LABEL\_REQUEST Object**

O objeto *LABEL\_REQUEST*, cuja classe é 19, corresponde funcionalmente à mensagem *LABEL\_REQUEST* do LDP.

Esse objeto indica, no campo L3PID, o protocolo de camada de rede que vai ser utilizado no respectivo TE LSP.

Existem três *C*-*Types* definidos pela RFC 3209 para esse objeto:

─*Label Request* sem faixa de labels (*C*-*Type* 1).

─*Label Request* com faixa de labels ATM (*C*-*Type* 2).

─*Label Request* com faixa de labels Frame Relay (*C-Type* 3).

O objeto *LABEL\_REQUEST*, conduzido pelas mensagens *RSVP Path*, permite aos LSRs que compõem o caminho explícito, o armazenamento dos pedidos de labels e a tomada das providências prévias necessárias. Quando do retorno da mensagem *RSVP Resv*, os labels são distribuídos no sentido *upstream*, dentro das faixas registradas, se for o caso.

O *C-Type* 1 corresponde aos top labels com envelopamento genérico

Os *C-Types* 2 e 3 são utilizados quando o MPLS-TE é suportado, respectivamente, por uma rede ATM ou por uma rede Frame Relay.

Os ATM-LSRs e os FR-LSRs que não possam realizar *label merging,* indicam essa condição nos respectivos *C*-*Type*s do objeto *LABEL\_REQUEST*.

+**EXPLICIT\_ROUTE Object (ERO)**

As rotas explícitas, por onde serão constituídos os TE LSPs, são especificadas nas mensagens *RSVP Path* por meio do *EXPLICIT\_ROUTE Object* (ERO), cuja classe é 20. A RFC 3209 define apenas um *C-Type* (*C-Type* 1) para esse objeto, denominado *Type 1 Explicit Route*. Esse objeto é dividido em subobjetos, com diferentes propósitos.

O objeto *EXPLICIT\_ROUTE* restringe-se ao tráfego unicast. O uso desse objeto para tráfego multicast não foi considerado na RFC 3209.

Uma rota explícita consiste em uma lista de LSRs ou de grupos de LSRs ao longo dessa rota. Cada um desses componentes corresponde a um subobjeto, sendo que um grupo de LSRs pode corresponder a um sistema autônomo.

Como uma rota de um caminho pode ser uma *strict route* ou uma *loose route*, os subobjetos correspondentes devem indicar essa condição, por meio de um *bit* específico **L** (*loose route bit*).

Se esse bit for setado para 1, indica-se uma *loose route* inserida no caminho explícito, enquanto que se o valor desse bit for igual a zero, o subobjeto corresponde a uma *strict route*.

Em uma *loose route*, como foi mencionado anteriormente, o encaminhamento de tráfego obedece ao roteamento IGP (OSPF ou IS-IS), enquanto em uma *strict route* o encaminhamento segue o caminho explícito.

Os subobjetos do ERO contêm um campo denominado tipo, que indica o respectivo conteúdo. Alguns valores definidos para esse campo são os seguintes:

─Subobjeto tipo 1: prefixo IPV4.

─Subobjeto tipo 2: prefixo IPV6.

─Subobjeto tipo 32: número do sistema autônomo.

Quando um LSR recebe uma mensagem *RSVP Path*, esse LSR deve determinar, com base no objeto *EXPLICIT\_ROUTE* contido nessa mensagem, qual o *next-hop* nesse caminho.

OS LSRs podem alterar o ERO de mensagens RSVP *Path* por meio de alterações nos subobjetos. Por exemplo, uma *strict route* pode ser inserida em substituição a uma *loose route*, para forçar o tráfego para um determinado *next-hop*.

A presença de *loose routes* pode ensejar a ocorrência de loops na rede durante fases transientes. A presença desses loops pode ser detectada pelo *head end LSR* por meio do objeto RECORD\_ROUTE, que será visto adiante.

+**RECORD\_ROUTE Object *(*RRO*)***

O objeto ERO enviado por uma mensagem *RSVP Path* pode não corresponder ao caminho real pelo qual será estabelecido o TE LSP. Uma primeira razão para isso é a possível existência de *loose routes* no caminho, que poderão ser evitadas. Uma segunda razão é a possibilidade de alteração da ERO ao longo do caminho.

Em consequência, a rota real é registrada pelos LSRs e distribuída no sentido *downstream* pelo objeto *RECORD\_ROUTE* (classe 21) contido na mensagem *RSVP Path*.

O *tail end LSR* pode reenviar o objeto *RECORD\_ROUTE* no sentido *upstream* por meio da mensagem *RSVP Resv* de retorno. Foi definido apenas um C-*Type* (C-*Type* 1), denominado *Type* 1 *Record Route*, para o objeto RRO.

Foram definidos os seguintes subobjetos para esse objeto:

─Subobjeto tipo 1: endereço IPv4.

─Subobjeto tipo 2: endereço IPv6.

─Subobjeto tipo 3: label.

1. aplicabilidade do RRO, restrita a sessões unicast, concretiza-se por meio de três possibilidades:

─Mecanismo de detecção de loops.

─Coleção de informações reais sobre caminhos.

─*Feedback* para próximos EROs.

**+SESSION\_ATTRIBUTE Object**

O objeto *SESSION\_ATTRIBUTE* (classe 207) objetiva conduzir os valores de atributos necessários para o perfeito funcionamento dos requisitos do RSVP-TE nos túneis MPLS TE constituídos. A RFC 3209 define dois *C*-*Types*:

─*LSP*\_*TUNNEL* (*C*-*Type* 7).

─*LSP*\_*TUNNEL*\_*RA* (*C-Type* 1).

*O C-Type LSP*\_*TUNNEL*\_*RA* (onde *RA* significa *Resource Affinities)* contém os mesmos campos que o *C-Type LSP*\_*TUNNEL*, com a adição de informações relativas a afinidades de recursos.

Informações de afinidades referem-se à presença de conjuntos de atributos de filtragem associados com um TE LSP, que podem estabelecer que um dado link seja ou não aceitável.

A inclusão ou a exclusão do link pode ser definida pela presença de qualquer um dos atributos *(include/exclude any)* ou a inclusão requer a presença de todos os atributos *(include all).*

O *C-Type* 7 transporta duas classes de parâmetros:

─*Setup priority* e *holding priority*.

─*Flags*.

Os parâmetros *setup priority* e *holding priority* definem a ocorrência de preempção, como já foi discutido anteriormente neste tutorial.

Foram definidos três valores de *flag*:

─*Local protection desired* (*flag* 0x01).

─*Label recording desired* (*flag* 0x02).

─SE *style desired* (*flag* 0x04).

O *flag* 0x01 autoriza os LSRs de trânsito a violar a rota explícita indicada no ERO, em caso de falhas em links *downstream* adjacentes. Nesse caso um LSR de trânsito pode utilizar o mecanismo *fast rerouting* (FRR).

O *flag* 0x02 indica que os valores de label devem ser incluídos no objeto *RECORD-ROUTE*.

O *flag* 0x04 indica que o *head end LSR* pode optar pelo rerroteamento desse túnel MPLS TE sem a necessidade de desfazê-lo (mecanismo referido como *make-before-break*).

Para isso, o *tail end LSR* deve utilizar o estilo SE em sua resposta na mensagem *RSVP Resv*, com o propósito de possibilitar o compartilhamento provisório das reservas nos links comuns ao TE LSP existente e o novo TE LSP que vai substituí-lo.

**7.2.4 - Mensagens RSVP-TE Resv**

As mensagens *RSVP-TE Resv* utilizam os objetos relacionados na Figura 16.

|  |  |  |
| --- | --- | --- |
| **Classe** | **Objeto** | **RFC** |
| - | *Cabeçalho Comum* | 2205 |
| 4 | *INTEGRITY* | 2205 |
| 1 | *SESSION* | 2205 |
| 3 | *RSVP\_HOP* | 2205 |
| 5 | *TIME\_VALUES* | 2205 |
| 15 | *RSVP\_CONFIRM* | 2205 |
| 7 | *SCOPE* | 2205 |
| 14 | *POLICY\_DATA* | 2205 |
| 8 | *STYLE* | 2205 |
| 9 | *FLOWSPEC* | 2205 |
| 10 | *FILTER\_SPEC* | 2205 |
| 16 | *LABEL* | 3209 |
| 21 | *RECORD\_ROUTE* | 3209 |

**Figura 16 - Objetos das mensagens RSVP-TE Resv.**

**7.2.4.1 – Objetos Legados do RSVP**

Abordaremos, a seguir, os objetos legados do RSVP que são utilizados nas mensagens *RSVP-TE Resv* e que não são comuns às mensagens *RSVP Path*. Esses objetos comuns foram já abordados nos subitens anteriores.

Dentre os objetos legados do RSVP utilizados nas mensagens *RSVP-TE Resv* ainda não abordados, somente o objeto *FILTER\_SPEC* sofreu alterações em seus *C-Types*. Os demais mantiveram os mesmos *C-Types.*

**+RSVP\_CONFIRM**: O recebimento desse objeto confirma a realização de uma reserva de recurso que fora solicitada. Contém o endereço IP do nó que solicitou a confirmação. Pode ser utilizado em mensagens *RSVP Resv* ou em mensagens *RSVP ResvConf*.

**+SCOPE**: Transporta uma relação explícita dos hosts enviadores para os quais a informação na mensagem deve ser enviada. Pode ser utilizado em mensagens *RSVP* Resv, em mensagens *RSVP ResvErr* ou em mensagens *RSVP ResvTear*.

**+STYLE**: Define o estilo de reserva, assim como as informações específicas de estilo que não constam no objeto *FLOWSPEC* ou no objeto *FILTER\_SPEC*. Pode ser utilizado em qualquer mensagem *RSVP Resv.*

Os estilos de reserva de recursos serão abordados adiante neste item.

**+*FLOWSPEC***: Define as características de QoS do fluxo de dados, em uma mensagem *RSVP Resv.*

**+FILTER\_SPEC**: Especifica o endereço IP (IPv4 ou IPv6) do nó que enviou a mensagem, assim como o TE LSP ID, em uma mensagem *RSVP Resv.*

Assim como o objeto *SENDER\_TEMPLATE*, o objeto *FILTER\_SPEC* recebeu dois novos *C-Types (C*-*Type* 7 e *C-Type* 8) na RFC 3209. Esse objeto utiliza o mesmo formato e a mesma semântica que o objeto *SENDER\_TEMPLATE*, porém em sentido inverso.

**7.2.4.2 – LABEL Object**

O objeto *LABEL* (classe 16), definido na RFC 3209, desempenha a mesma função que a mensagem *Label Mapping* do LDP, ou seja, ele distribui, no sentido *upstream*, os labels atribuídos pelos LSRs que compõem o TE LSP sendo constituído.

Esse objeto é transportado por uma mensagem *RSVP Resv* imediatamente após o objeto *FILTER\_SPEC* contido nessa mensagem.

O conteúdo de um objeto *LABEL*, que possui apenas um *C-Type* (*C-Type* 1), definido na RFC 3209, é um único label codificado em quatro octetos.

Para os labels genéricos e os labels para Frame Relay (DLCIs), os respectivos valores são números inteiros ocupando os quatro octetos.

No caso de labels para o ATM, no entanto, o VPI e o VCI ocupam, individualmente, 16 octetos.

Um LSR *downstream* atribui um label (label *downstream*) para o link subsequente no TE LSP em constituição. Esse label deve se encontrar dentro das faixas de labels definidas, quando for o caso (rede de suporte ATM ou Frame Relay).

No caso de estilo de reserva SE com *label merging* em uma sessão, o LSR *downstream* envia um único label para o LSR *upstream*, para todos os TE LSPs que participam da sessão. Ressalva-se o caso de ATM-LSRs e FR-LSRs, que não podem realizar *label merging*.

**7.2.5 - Mensagens Hello**

A RFC3208 define uma extensão do mecanismo *Hello* do RSVP, que possibilita aos LSRs detectar quando os LSRs vizinhos não são alcançáveis, isto é, permite a detecção de falhas entre pares de LSRs vizinhos.

Esse mecanismo *Hello* estendido é utilizado quando o processo de notificação de falhas provido pela camada 2 não é utilizado ou não é suficiente para uma rápida detecção de falhas.

Essa extensão permite que cada LSR utilize o mecanismo independentemente do seu LSR vizinho, e a utilização pode ocorrer a qualquer momento desde o início do processo RSVP-TE. Ele é composto por uma mensagem *Hello*, com um objeto *HELLO REQUEST* e um objeto *HELLO ACK* (*aknowledgment*).

Cada vizinho, pode de modo autônomo, enviar uma mensagem *Hello* contendo um objeto *HELLO REQUEST*. Essa mensagem é respondida por outra mensagem *Hello* contendo o objeto *HELLO* ACK.

A extensão *Hello* é de classe 22, e possui dois *C-Types*, que correspondem a seus objetos. O objeto *HELLO REQUEST* corresponde ao *C-Type* 1 e o objeto *HELLO ACK* ao *C-Type 2.*

**7.2.6 – Estilos de Reserva**

Como vimos, quando fica concluída a troca de mensagens *RSVP Path* e *RSVP Resv* entre um par de LSRs nos extremos de um circuito virtual TE (um TE LSP ou parte de um TE LSP), fica estabelecida uma sessão RSVP entre esses LSRs. Outros circuitos virtuais TE podem participar dessa sessão.

Quando da ocorrência da convergência de circuitos virtuais TE de uma sessão para um LSR, fica constituído um túnel TE a partir desse LSR. Um túnel TE pode utilizar um único ERO, ou pode divergir e convergir novamente adiante em um LSR, utilizando, portanto, diferentes EROs.

Os túneis TE representam a base para os denominados estilos de reserva de recursos, cujas alternativas são as seguintes:

─ Estilo *fixed filter* (FF).

─ Estilo *shared explicit*.

─ Estilo *wildcard filter* (WF).

Uma sessão RSVP pode resultar em um ou mais TE LSPs, dependendo do estilo de reserva escolhido.

Os nós enviadores não têm qualquer influência na escolha do estilo de reserva para cada sessão, cabendo ao nó receptor essa escolha. Cada sessão deve ter um estilo particular, e o nó receptor pode escolher diferentes estilos de reserva para diferentes TE LSPs.

**7.2.6.1** - **Estilo Fixed Filter (FF)**

O estilo FF representa o modo default de estabelecimento de reservas. Nesse caso, uma reserva particular é dedicada a um nó enviador individual. Essa reserva não é compartilhada por outros nós enviadores.

Como cada enviador tem a sua própria reserva, é atribuído um label particular para cada um dos enviadores. Isso pode resultar em um TE LSP ponto a ponto entre cada par enviador/receptor.

Esse estilo é apropriado para aplicações independentes e concorrentes no tempo. A soma das reservas individuais de banda passante em um link para uma sessão utilizando FF, representa a reserva total de banda passante nesse link.

**7.2.6.2 - Estilo Shared Explicit (SE)**

O estilo SE possibilita a um nó receptor especificar explicitamente os nós enviadores a serem incluídos em uma reserva. Existe uma única reserva em um link para todos os nós enviadores listados.

Como cada enviador é explicitamente relacionado na mensagem *RSVP Resv*, torna-se possível atribuir-se diferentes *labels* para diferentes enviadores, e dessa forma criar TE LSPs separados.

O estilo SE é apropriado para aplicações cujos tráfegos originários de diferentes enviadores não sejam concorrentes no tempo. Nesse caso, uma única reserva em um link utilizado por TE LSPs participantes da reserva, é compartilhada por esses TE LSPs, o que representa uma significativa economia de recursos da rede.

Outra importante utilização do estilo SE se verifica quando, de imediato ou em um tempo mais longo, ocorrerá a substituição de um TE LSP por outro TE LSP também participante da reserva. Essas possibilidades serão vistas adiante neste item.

Existem duas formas de utilização do estilo SE:

─ Caminhos com os mesmos EROs.

─ Caminhos com diferentes EROs.

Na primeira dessas formas, todos os TE LSPs participantes da reserva SE utilizam uma sucessão única de labels no túnel.

No segundo caso, os caminhos seguidos pelos tráfegos originários dos enviadores participantes podem convergir ou divergir em qualquer ponto, utilizando os seus próprios EROs.

Aos circuitos virtuais TE (ou mesmo TE LSPs) que utilizam um dado ERO no túnel, é atribuída uma sucessão própria de labels.

Como se observa, o estilo SE com diferentes EROs funciona de modo assemelhado ao FF.

A diferença ocorre apenas no que se refere à reserva de recursos nos links onde os circuitos virtuais TE coexistem. Enquanto no estilo FF cada circuito virtual TE possui reserva própria, no estilo SE os recursos são compartilhados pelos circuitos virtuais TE que participam da reserva.

**7.2.6.3 -Estilo Wildcard Filter (WF)**

No estilo WF, uma única reserva compartilhada é utilizada por todos os nós enviadores na sessão, sem a necessidade de explicitação. A reserva permanece a mesma, mesmo em caso de variação no número de LSRs.

Quando existe apenas um enviador, constitui-se um circuito virtual ponto a ponto. Quando da existência de múltiplos enviadores, um circuito virtual TE multiponto a ponto é criado. Nos links em que ocorre compartilhamento pelos enviadores em uma sessão, um único label é atribuído para a sessão.

O estilo WF é útil para aplicações nas quais nem todos os enviadores transmitem ao mesmo tempo, como por exemplo, em conferências telefônicas. Caso ocorra simultaneidade de transmissão, torna-se inviável a realização apropriada da reserva.

Por outro lado, os EROs não podem ser utilizados devido as regras de aglutinação *(merging)* do estilo WF.

Devido às duas limitações acima citadas, ou seja, a inviabilidade de reserva apropriada em caso de excesso de tráfego simultâneo e a impossibilidade de uso de EROs, o estilo WF não é aplicável a *Traffic Engineering*, não sendo então considerado na RFC 3209.

**7.2.7 – Make-Before-Break**

*Make-before-break* é uma técnica utilizada para reduzir o tempo de interrupção de serviço quando da substituição de um TE LSP, ou de parte dele, por um outro LSP, preservando a continuidade do serviço.

A ideia básica é a constituição, do que denominaremos LSP substituto, antes da desativação do LSP em serviço, que denominaremos LSP primário.

Quando existem links comuns aos LSP primário e LSP substituto, utiliza-se reserva SE entre eles, com o propósito de reduzir o uso de banda passante nesses links.

A substituição de um LSP primário pode ocorrer em diferentes circunstâncias, dentre as quais destacamos as seguintes:

─ Substituição deliberada por razões administrativas ou operacionais.

─ Reparo fim a fim em caso de falhas em LSRs e/ou em links da rede.

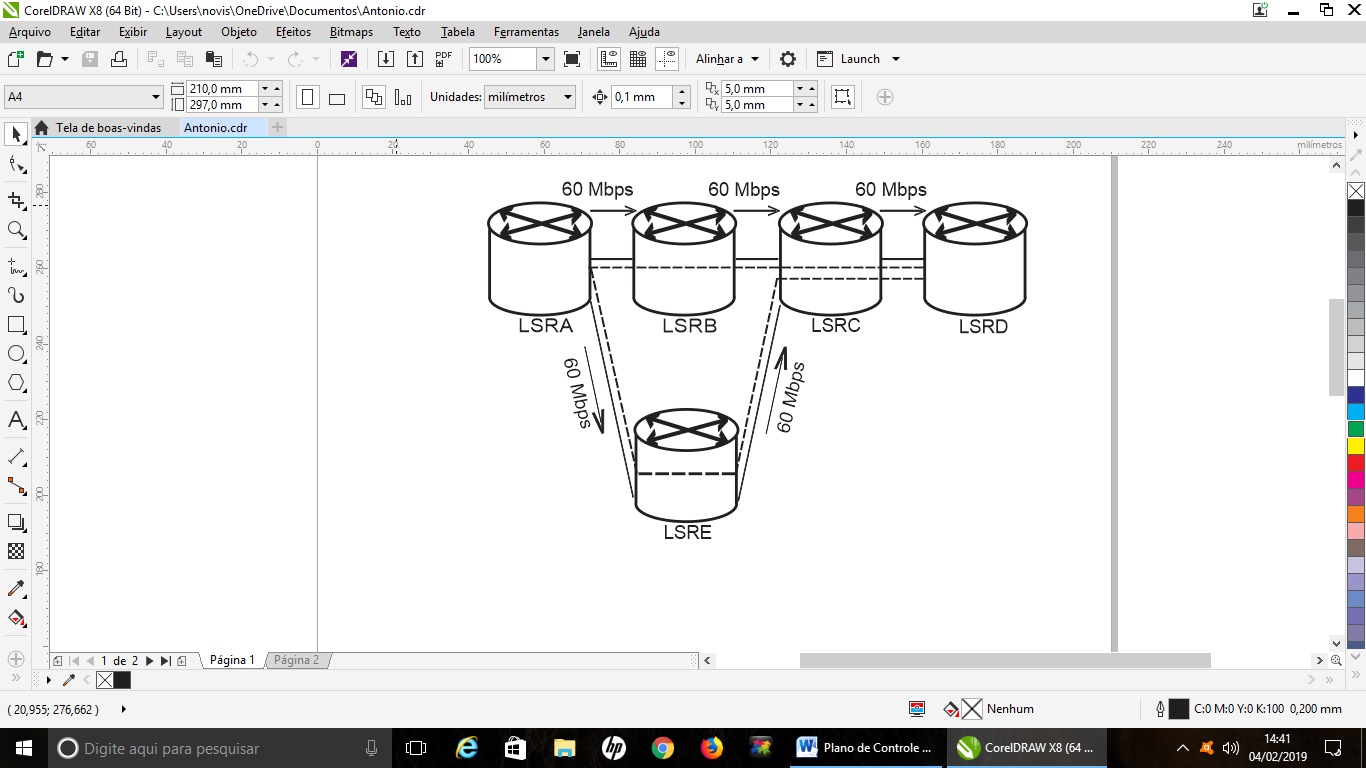
─ Reparo local em caso de falhas em LSRs e/ou em links da rede.

O reparo local é denominado *fast rerouting* (FRR), que será abordado adiante neste tutorial.

**7.2.7.1 – Substituição Deliberada**

A substituição deliberada de um LSP primário por um LSP substituto pode ocorrer por diversas razões, normalmente com um curto tempo de coexistência entre os LSPs.

Para melhor entendimento dessa forma de substituição, consideremos o exemplo da Figura 17, onde todos os links possuem uma banda passante máxima reservável de 60 Mbps.

.

**Figura 17 – Exemplo de substituição deliberada.**

Nessa figura, por hipótese, temos um LSP primário constituído pela sequência <LSRA, LSRB, LSRC, LSRD>.

Por alguma razão, a gerência da rede decidiu substituir o LSP primário pelo LSP<LSRA, LSRE, LSRC, LSRD>.

Suponhamos agora que o LSP primário ocupe 40 Mbps de banda, e que se pretende manter essa ocupação no LSP substituto.

Admitindo-se que os links<LSRA, LSRE> e <LSRE, LSRC> disponham de bandas não reservadas acima de 40 Mbps, a substituição pode ocorrer normalmente nesses links, tendo havido a necessária reserva prévia de banda.

No link<LSRC, LSRD> não importa a disponibilidade de banda não reservada, uma vez que pode ser usada, por compartilhamento no estilo SE, a banda de 40 Mbps ocupada pelo LSP primário nesse link.

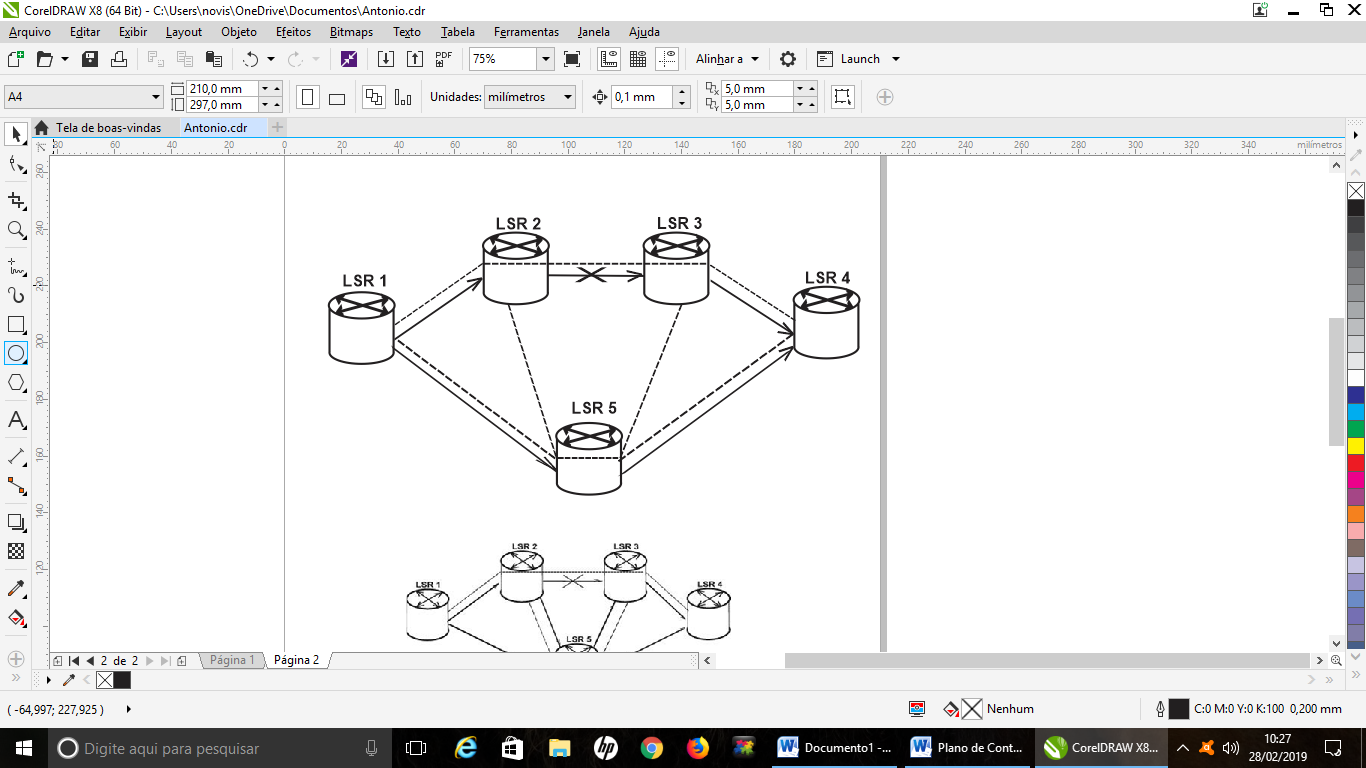
Vamos considerar uma segunda hipótese, na qual se deseja que o LSP substituto passe a ocupar uma banda de 50 Mbps, admitindo-se que os links <LSRA, LSRE> e <LSRE, LSRC> tenham capacidade para tanto.

Suponhamos que o link <LSRC, LSRD> disponha de 20 Mbps de banda não reservada. Nesse caso, o LSP substituto pode compartilhar os 40 Mbps da ocupação do link, acrescidos de 10 Mbps retirados da banda não reservada, perfazendo assim os 50 Mbps requeridos.

**7.2.7.2 – Reparo Fim a Fim**

No rerroteamento com reparo fim a fim, assim como na substituição deliberada de TE LSPs, é constituído um TE LSP *backup* em paralelo com o TE LSP primário. Em ambos os casos, a substituição ocorre a partir do *head end LSR*.

Para exemplificar o rerroteamento com reparo fim a fim, vamos considerar a Figura 18.



**Figura 18 – Rerroteamento com reparo fim a fim.**

Nessa figura, o TE LSP primário <LSR 1, LSR 2, LSR 3, LSR 4> encontra-se protegido pelo TE LSP backup <LSR 1, LSR 5, LSR 4>, não sendo utilizado qualquer tipo de reserva de banda passante.

Na hipótese de uma falha no link <LSR 2, LSR 3>, o *head end LSR* (LSR 1) é notificado, acionando então o mecanismo de comutação automática para a transferência do tráfego para o TE LSP backup.

Deve ocorrer também uma notificação ao centro de gerência da rede para que providencie o reparo do link com falha.

**7.3 – RFCs Posteriores à RFC 3209**

Posteriormente à RFC 3209, o IETF emitiu algumas RFCs complementares, voltadas para sinalização no MPLS-TE.

Mais adiante, o IETF publicou uma série de RFCs para sinalização no GMPLS, algumas delas aplicáveis também para o MPLS-TE. Contudo, essas RFCs não serão abordadas no presente texto.

Vamos aqui apresentar as seguintes RFCs:

─ RFC 4090 (*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*);

- RFC 4874 (*Exclude Routes Extension to Resource* *Reservation Protocol – Traffic Engineering (RSVP-TE*));

─ RFC 5420 (*Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE*)).

A Figura 19 antecipa a relação de objetos definidos nessas RFCs que serão apresentados nos subitens a seguir, juntamente com outras informações atinentes.

|  |  |  |
| --- | --- | --- |
| **Classes** | **Objetos** | **RFC** |
| 63 | *DETOUR* | 4090 |
| 205 | *FAST\_REROUTE* | 4090 |
| 67 | LSP*\_REQUIRED-ATTRIBUTES* | 5420 |
| 197 | LSP*\_ATTRIBUTES* | 5420 |
| 232 | *EXCLUDE \_ROUTE OBJECT* (XRO) | 4874 |

**Figura 19 – Objetos definidos após a RFC 3209.**

**7.3.1 - Fast ReRouting (FRR)**

Um dos requisitos para *Traffic Engineering* é a capacidade para um rápido rerroteamento de um trecho de um TE LSP, em caso de ocorrência de falha nesse trecho. As ações de rerroteamento devem ocorrer o mais próximo possível da falha, no que se denomina reparo local, para que o rerroteamento se realize com a maior rapidez.

Os mecanismos que viabilizam essa capacidade são denominados, em conjunto, *Fast ReRouting* (FRR).

A RFC 4090 estende o RSVP-TE para possibilitar o estabelecimento de circuitos virtuais TE para backup de trechos de TE LSPS, para reparo local em menos que dezenas de milisegundos.

As situações típicas em que deve ocorrer rerroteamento em TE LSPs são as seguintes:

─ Disponibilidade de uma nova rota mais otimizada.

─ Ocorrência de falhas de recursos do túnel MPLS TE.

─ Conveniência de retornar ao túnel MPLS TE original quando da reativação de recursos com falhas.

O trecho (circuito virtual TE) protegido de um TE LSP é referido como LSP protegido. Um LSP protegido deve utilizar obrigatoriamente roteamento explícito. Em outras palavras, a RFC 4090 não se aplica para protocolos de roteamento convencional como, por exemplo, o OSPF.

Existem dois métodos independentes para a realização de FRR:

─ Método *backup* um a um *(one-to-one backup*).

─ Método *facility backup*.

No método *one-to-one backup*, um circuito virtual TE backup, referido como *detour LSP*, é estabelecido especificamente para um LSP protegido (*protected LSP*).

No método *facility backup*, ao contrário, cria-se um único LSP, referido como *bypass tunnel*, para operar como backup para um conjunto de LSPs protegidos.

A RFC 4090 especifica dois novos objetos para sinalização em FRR, ambos transportados exclusivamente em mensagens RSVP *Path*, denominados objeto *FAST\_REROUTE* e objeto *DETOUR.*

Adicionalmente, foram também definidos dois novos *flags* para os C-Types 1 e 7 do objeto *SESSION\_ATTRIBUTE*, assim como dois novos *flags* para os subobjetos RRO IPv4 e RRO IPv6 do objeto RRO.

O objeto *FAST\_REROUTE* é utilizado para controlar o backup do LSP protegido, sendo inserido exclusivamente em mensagens RSVP *Path* pelo *head end LSR*, e não pode ser alterado por LSRs *downstream.*

Esse objeto é de classe 205 e utiliza o C*-Type* 1 e o C*-Type* 7.

O objeto *DETOUR* é utilizado no método *one-to-one backup* para identificar LSPs *detours*.

Esse objeto é de classe 63 e utiliza o *C-Type* 7 e o *C-Type* 8.

É altamente desejável que, quando possível, o rerroteamento ocorra sem interrupção de tráfego ou sem impactar o funcionamento da rede na fase de rerroteamento.

Essa forma de rerroteamento requer o estabelecimento de um novo circuito virtual (todo um TE LSP ou parte dele) em paralelo ao circuito virtual a ser substituído, requerendo também a manutenção desse circuito virtual enquanto não for concluído por completo o rerroteamento. Esse conceito é denominado *make-before-break*.

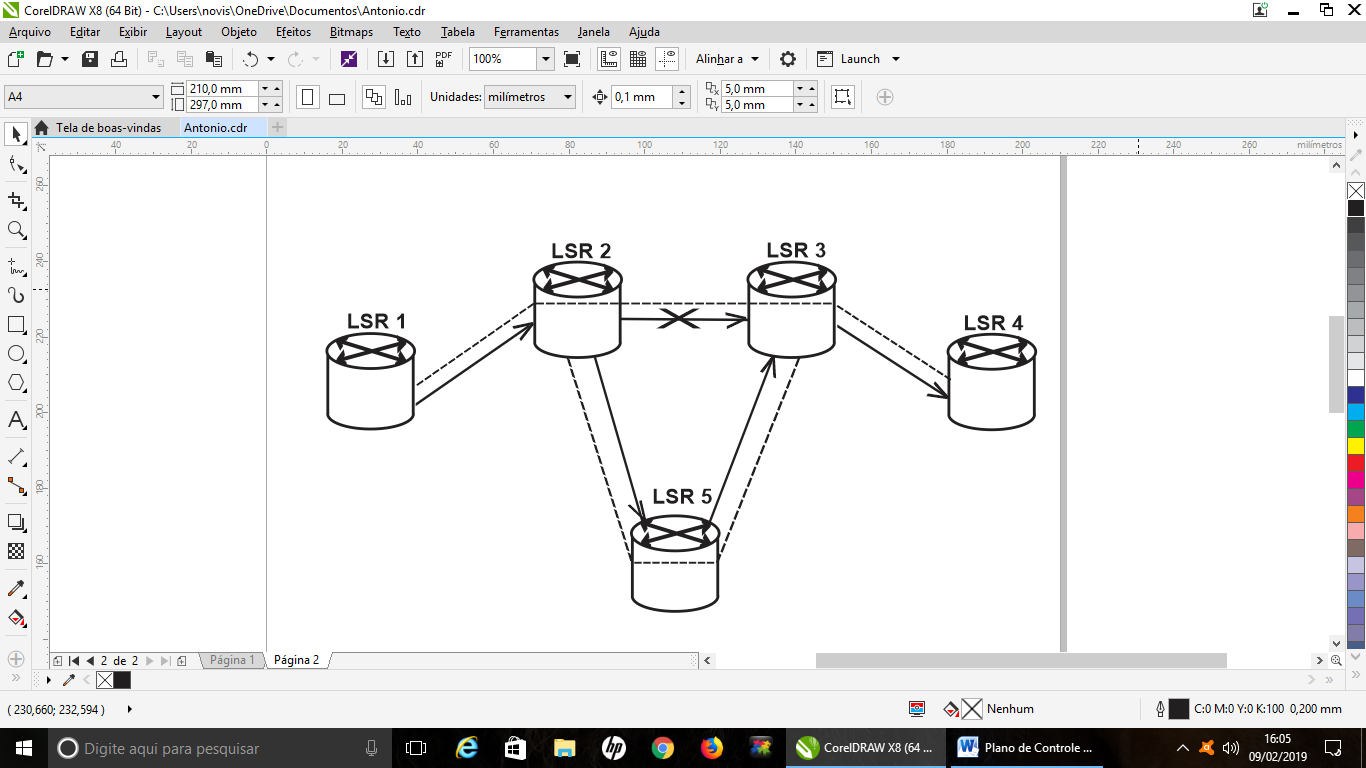
Para a implementação do conceito *make-before-break* são necessárias algumas medidas relativamente à reserva de recursos nos LSRs comuns aos circuitos virtuais. É necessário que se evite duplicidade de reserva de recursos, o que se obtém pela utilização do estilo de reserva SE para ambos os circuitos virtuais.

**7.3.1.1 - Reparo Local**

Para que o FRR se viabilize, é necessário que as ações ocorram no ponto onde a falha ocorreu, ponto esse denominado *point of local repair* (PLR). Além do reparo local, existe a possibilidade de reparo fim-a-fim vista anteriormente neste item, quando todo TE LSP é transferido para uma nova alternativa de túnel, mas não com a mesma velocidade do reparo local.

Em qualquer dessas hipóteses, os caminhos paralelos já devem estar estabelecidos, sem necessidade de sinalização quando ocorre uma falha, para minimizar o tempo necessário para início de operação do novo túnel MPLS-TE. No caso de reparo local, o rerroteamento pode ocorrer em dezenas de milissegundos, sendo 50 ms um valor de referência que caracteriza o FRR.

A Figura 20 exemplifica a ocorrência de rerroteamento com reparo local.



**Figura 20**- R**erroteamento com reparo local (fast rerouting).**

Como no exemplo anterior, o tráfego flui normalmente pelo TE LSP <R1, R2, R3, R4>. Pressupõe-se que existe um circuito virtual *detour*<R2, R5, R3> previamente estabelecido, sem a existência de reserva de banda passante.

falha Uma no link<R2, R3> provoca a entrada em funcionamento do circuito virtual TE < R2, R5, R3 >, ocorrendo o rerroteamento no LSR R2, que é o PLR. O tráfego passa a escoar pelo TE LSP <R1, R2, R5, R3, R4>.

O tempo de rerroteamento é menor que no caso de rerroteamento com reparo fim a fim, dada a maior proximidade entre a falha e o PLR.

**7.3.1.2 - Proteção de Links e de LSRs**

O FRR pode ocorrer em duas circunstâncias:

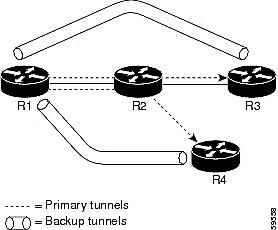
─Proteção de links.

─Proteção de LSRs.

A proteção de links foi já vista no exemplo da figura 19 anterior. Nesse exemplo, o circuito virtual backup, um *detour LSP*, foi constituído entre dois LSRs vizinhos, quando protege apenas um link. Para o LSR *upstream*, o LSR *downstream* vizinho é referido como NHOP *(next-hop).*

No caso de proteção de LSRs, quando ocorre inevitavelmente também a proteção de dois ou mais links, o *detour LSP* não pode ser constituído entre LSRs vizinhos. O *detour LSP*, que se inicia no PLR, tem que terminar, no mínimo, no *next-next-hop* (NNHOP).

A Figura 21 mostra um exemplo de proteção de LSRs (e de links, consequentemente).



**Figura 21 – Proteção de LSRs e de links.**

Observa-se nessa figura a presença dos TE LSPs primários <R1, R2, R3> e <R1, R2, R4>, protegidos, respectivamente, pelo TE LSP <R1, R3> e pelo TE LSP <R1, R4>.

Existe proteção para o link<R1, R2> e para o LSR R2 por ambos os TE LSPs backup, cada um para o respectivo destino.

**7.3.2 – RFC 4874 (Exclusão de Rotas)**

A RFC 3209, e mesmo a RFC 3473 (*Generalized Multiprotocol Label Switching (GMPLS*)), não definiram mecanismos para a exclusão explícita de rotas (ou seja, de nós abstratos e de recursos) após o início da sinalização.

O mesmo não ocorre com a inclusão explícita, que constitui um mecanismo naturalmente realizado pelas mensagens *RSVP Path*, utilizando o ERO.

Essa lacuna foi solucionada por meio da emissão da RFC 4874, que especifica formas de comunicar a exclusão de rotas durante a sinalização, por meio do protocolo RSVP-TE.

Em algumas redes, onde caminhos explícitos precisos não são calculados no *head end LSR*, torna-se útil especificar e sinalizar os nós abstratos e os recursos que podem ser explicitamente excluídos dos caminhos.

A RFC 4874 requer o uso de dois tipos de exclusão:

─Exclusão de determinados nós abstratos ou recursos em um caminho inteiro. Esse conjunto de nós abstratos ou de recursos é referido como uma *Exclude Route List*.

─Exclusão de determinados nós abstratos ou recursos situados entre um dado par de nós abstratos presente em uma ERO. Tais exclusões específicas são referidas como *Explicit Exclusion Route*.

Para o atendimento dessas duas concepções no processo de sinalização, foram definidos um novo objeto RSV e um novo subobjeto para o ERO.

**7.3.2.1 – EXCLUDE\_ROUTE Object (XRO)**

O novo objeto, denominado *EXCLUDE\_ROUTE Object* (XRO), possui a classe 232. Esse objeto tem como propósito especificar os nós abstratos a serem excluídos do caminho e que constam consequentemente da *Exclude Route List.*

Foi definido apenas o *C-Type 1* para esse objeto, referido como *Type 1 EXCLUDE\_ROUTE*, que suporta os seguintes subobjetos:

─Subobjeto *IPv4 Prefix* (tipo 1).

─Subobjeto *IPv6 Prefix* (tipo 2).

─Subobjeto *Unnumbered Interface* ID (tipo 4).

─Subobjeto *Autonomous System Number* (tipo 32).

─Subobjeto SRLG (tipo 34).

Esses subobjetos utilizam o formato para os subobjetos definido na RFC 3209 para os subobjetos do *ERO*. Como os conceitos de *loose* ou *strict routes* não têm significado em exclusão de rotas, o bit L definido na RFC 3209 é reutilizado para indicar que um nó abstrato deve ser excluído (valor 0) ou deveria ser evitado (valor 1).

Dentre os subobjetos definidos na RFC 4874 para o novo objeto XRO, merece destaque o subobjeto SRLG, que, diferentemente do sub-TLV SRLG do OSPF-TE utilizado pelo *head end LSR* no cálculo do ERO, é utilizado pelo RSVP-TE para a exclusão explícita de rotas.

Embora definido como um subobjeto do objeto XRO, o subobjeto SRLG poderia ser também apropriado para uso no ERO ou no RRO.

**7.3.2.2– Explicit Exclusion Route Subobject (EXRS)**

O subobjeto EXRS do objeto ERO, cujo tipo é 33, tem como propósito indicar a exclusão de nós abstratos ou de recursos que constam da respectiva *Explicit Exclusion Route*, ou seja, que se encontram entre inclusive dois nós abstratos ou dois recursos na rota explícita.

Embora seja um subobjeto, o EXRS contém um ou mais subobjetos próprios, denominados *EXRS subobjects.*

**7.3.3 – RFC 5420 (Codificação de Atributos)**

A RFC 5420, que substituiu a RFC 4420, define dois novos objetos, além de um novo subobjeto para o objeto RRO, com o objetivo de ampliar a capacidade do RSVP-TE (e também do GMPLS RSVP-TE) para a definição de opções e de atributos adicionais.

Os objetos definidos na RFC 5420 são o LSP\_*ATTRIBUTES* e o LSP\_*REQUIRED*\_*ATTRIBUTES*, enquanto o subobjeto definido para o objeto RRO é denominado *RRO Attributes*.

Registra-se que os dois novos objetos definidos na RFC 5420, utilizam excepcionalmente o formato TLV em seus payload, para possibilitar a fácil inclusão de novas opções e de novos atributos.

Anteriormente à RFC 4420, as opções e atributos no RSVP-TE eram definidos apenas pela utilização do campo *Flags* do objeto *SESSION\_ATRRIBUTE*, com 8 bits.

Como 5 desses bits já foram utilizados e dada a possível demanda prevista para novos usos desses bits, o IETF decidiu emitir a RFC 5420 para viabilizar futuras definições de atributos.

**7.3.3.1– Objeto LSP\_ATTRIBUTES**

O objeto LSP\_*ATTRIBUTES*, de caráter opcional, é utilizado para sinalizar atributos requeridos por um TE LSP, de forma tal que ele seja reconhecido, e processado, apenas pelos LSRs de trânsito que o suportam.

A classe desse objeto é 197, tendo sido definido apenas o *C-Type* 1, denominado *LSP Attributes.*

OS LSRs que não suportam esse objeto, reencaminham-no sem examiná-lo e sem alterá-lo. Isso facilita o intercâmbio de atributos através de redes legadas que não o suportam.

Esse objeto efetivamente estende a função do objeto *SESSION\_ATTRIBUTE* em mensagens *RSVP Path*.

O objeto LSP\_*ATTRIBUTES* pode ser também utilizado para reportar o estado operacional de um TE LSP em uma mensagem *RSVP Resv,* mesmo na hipótese de não existir qualquer objeto LSP\_*ATTRIBUTES* ou objeto LSP\_*REQUIRED\_ATTRIBUTES* transportado na correspondente mensagem *RSVP Path.*

**7.3.3.2 – Objeto LSP\_REQUIRED\_ATTRIBUTES**

O objeto LSP\_*REQUIRED\_ATTRIBUTES*, de caráter opcional, é utilizado para sinalizar atributos requeridos por um TE LSP, de forma tal que cada LSR de trânsito deve examinar os atributos nele transportados e não deve encaminhá-lo sem atuar em seu conteúdo.

A classe desse objeto é 67, tendo sido definido apenas o *C-Type* 1, denominado *LSP Required Attributes*.

Esse objeto efetivamente estende a função do objeto *SESSION\_ATTRIBUTE* em mensagens *RSVP Path*, não sendo utilizado em mensagens *RSVP Resv*.

**7.3.3.3 –Subobjeto RRO Attributes**

Correntemente, as ações ocorridas nos LSRs são reportadas ao LSR de ingresso por meio do campo *Flags* contido nos subobjetos atuais do RRO. Foi prevista, de maneira análoga ao que ocorre no objeto *SESSION\_ATTRIBUTE*, a escassez de bits nos campos *Flags* dos subobjetos do RRO para reportar ações dos LSRs sobre futuros atributos.

Em consequência, foi especificado na RFC 5420 o novo subobjeto *RRO Attributes* para o ERO, com comprimento variável, de modo a poder reportar ações dos LSRs sobre múltiplos atributos que venham a ser eventualmente definidos. A esse subobjeto foi atribuído o tipo 5.

Foi estabelecida uma correspondência um a um entre os atributos do TLV *Attribute Flags* dos novos objetos definidos e os atributos do subobjeto *RRO Attributes*.

**8 - CONSIDERAÇÔES FINAIS**

O GMPLS é um conjunto de protocolos de plano de controle de uso generalizado, no sentido que se destina ao controle indiscriminado de redes orientadas a conexão, tanto no modo circuito (conexões reais) quanto no modo pacote (conexões virtuais).

O plano de controle do MPLS-TE representa a fundamentação do GMPLS. De fato, a sinalização no GMPLS utiliza, para roteamento, extensões do protocolo OSPF-TE ou do protocolo ISIS-TE (IS-IS TE), ambos do MPLS-TE.

Na sinalização, igualmente, o GMPLS adota o protocolo GMPLS RSVP-TE, uma extensão do RSVP-TE do MPLS-TE.

Por outro lado, a lógica utilizada para o cálculo de rotas no GMPLS é a mesma que a do MPLS-TE.

O presente tutorial, que objetiva apresentar o plano de controle do MPLS-TE em um enfoque abrangente, foi dividido em duas partes, dada a sua extensão.

A primeira parte incorpora uma visão geral do plano de controle, acrescida da abordagem do roteamento no MPLS-TE em um considerável nível de profundidade.

A parte 2 é dedicada à sinalização no MPLS-TE, que utiliza o protocolo RSVP-TE. O alicerce desse protocolo é a RFC 3209, complementada por algumas outras RFCs.

Parte das RFCs posteriormente emitidas para o roteamento e a sinalização no GMPLS, aplicam-se retroativamente também para o MPLS-TE.

**9 – REFERÊNCIAS**

**9.1 – Livros**

– ENNE, A. J. F. – TCP/IP sobre MPLS. Rio de Janeiro: Ciência Moderna 2009.

– ENNE, A. J. F. – Frame Relay: Redes, Protocolos e Serviços. Rio de Janeiro: Axel Books e Embratel, 1998.

– FARREL, A., BRYNSKIN, I. – GMPLS: Architecture and Applications. San Francisco, USA: Morgan and Kaufmann, 2006.

-FARREL, A., DAVIE, B. S. – MPLS: Next Steps. San Francisco, USA: Morgan and Kaufmann, 2008.

- DAVIE, B. S., RECKHTER, Y. – MPLS: Technology and Applications. San Francisco, USA: Morgan and Kaufmann, 2000.

- CAVANAGH, J. P. – Frame Relay Applications. San Francisco, USA: Morgan and Kaufmann, 1998.

- SACKET, G. C., METZ, C. Y. – ATM and Multiprotocol Networking, New York, USA: McGraw Hill, 1997.

**9.2 – Padrões do IETF (RFCs)**

─RFC 1195 (*Use of* OSI IS-IS *for Routing in TCP/IP and Dual Environments*).

─RFC 2205 (*Resource Reservation Protocol (RSVP*)).

─ RFC 2328 (*OSPF Version* 2).

─ RFC 2702 (*Requirements for Traffic Engineering over MPLS*).

--RFC 3209 (*RSVP-TE: Extensions to RSVP for LSP Tunnels*).

--RFC 3473 (*Generalized Multiprotocol Label Switching (GMPLS*) *Signaling Resource Reservation Protocol–Traffic* *Engineering (RSVP-TE) Extensions*).

--RFC 3486 (*The Multiprotocol Label Switching (MPLS) Working Group Decision on MPLS Signaling Protocols*).

─ RFC 3630 (*Traffic Engineering* (*TE*) *Extensions to OSPF*

*Version* 2).

--RFC 4090 (*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*).

─ RFC 4655 (A *Computation Element* (*PCE)* – *Based Architectur*e).

--RFC 4874 (*Exclude Routes Extension to Resource Reservation Protocol Traffic Engineering (RSVP-TE*)).

─ RFC 5250 (*OSPF Opaque LSA Option*).

─ RFC 5305 (*IS-IS Extensions for Traffic Engineering*).

─ RFC 5308 (*RoutingIPv6withIS-IS*).

─ RFC 5329 (*Traffic Engineering* (TE) *Extensions to OSPF*

v*ersion* 3).

─ RFC 5340 (*OSPF forIPv6*).

--RFC 5420 (*Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE*)).

─ RFC 6119 (*IPv6 Traffic Engineering in* IS-IS).

─ RFC 7471 (*OSPF Traffic Engineering* (*TE*) *Metric Extensions*).

─ RFC 7810 (*IS-IS Traffic Engineering* (*TE*) *Metric Extensio*ns).

**10 – TESTE SEU CONHECIMENTO**

**1 - Qual a frase correta?**

1. As informações de roteamento no OSPF-TE são processadas em todos os LSRs da rede**.**
2. As informações de roteamento no OSPF-TE são processadas apenas nos *head end LSRs*.
3. No OSPF-TE utiliza-se o mesmo tipo de LSA que no OSPF.
4. Todas elas.

**2 – Qual a frase correta?**

1. Os atributos de roteamento no OSPF-TE são transportados no *top-level Link TLV.*
2. Os atributos de roteamento no OSPF-TE são transportados em LSAs opacas tipo 10.
3. Os atributos de roteamento no OSPF-TE são transportados em TE LSAs.
4. Todas elas.

**3 – Qual a frase correta?**

1. O PCE calcula rotas com base apenas nas informações contidas na TED.
2. O PCE calcula rotas com base nas informações contidas na TED e na solicitação de serviço.
3. O PCE localiza-se apenas no interior dos *head end LSRs.*
4. O CSPF é um protocolo de roteamento.

**4– Qual a frase correta?**

1. As mensagens *RSVP-TE Resv* trafegam no sentido *downstream.*
2. Quando o *head end LSR* envia uma mensagem *RSVP-TE PathTear*, o *tail end* *LSR* responde com uma mensagem *RSVP-TE ResvErr*.
3. As mensagens do RSVP-TE trafegam como datagramas IP.

d)Os objetos das mensagens do RSVP-TE utilizam o formato padrão dos TLVs.

**5** – **Qual a frase correta?**

1. O objeto SENDER\_TSPEC transporta a banda passante desejada para o TE LSP em constituição, em mensagens *RSVP-TE Path.*
2. O objeto SESSION\_ATTRIBUTE é enviado em mensagens *RSVP-TE Path* com o propósito de definir uma sessão RSVP específica;
3. O objeto SENDER\_TEMPLATE transporta a identificação do TE LSP em constituição, em mensagens *RSVP-TE Resv*.

d)Os labels são solicitados em mensagens *RSVP-TE Resv* e enviados *downstream* em mensagens *RSVP-TE Path*.

**6 – Qual a frase correta?**

1. O objeto RRO é utilizado apenas em mensagens *RSVP-TE Path*.
2. O objeto ERO é definido pelos LSRs ao longo do caminho a ser utilizado para o TE LSP em constituição.
3. O objeto ERO é enviado pelo *head end* *LSR*, e pode sofrer eventuais alterações ao longo da rota.
4. Conforme a RFC 3209, o objeto ERO pode conter rotas multicast e *loose routes.*

**ATENÇÂO: RESPOSTAS NA PÁGINA SEGUINTE**

**RESPOSTAS:**

1. **b)**
2. **d)**
3. **b)**
4. **c)**
5. **a)**
6. **c)**