GEOVANA DE MELLO ESPÍRITO SANTO

O MPLS–TP E SUA APLICAÇÃO NAS REDES DE COMUNICAÇÃO

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de São Carlos, da Universidade de São Paulo

Curso de Engenharia de Computação

ORIENTADORA: Mônica de Lacerda Rocha

São Carlos
2013

Espírito Santo, Geovana de Mello
E77o O MPLS-TP E SUA APLICAÇÃO NAS REDES DE COMUNICAÇÃO / Geovana de Mello Espírito Santo; orientadora Mônica de Lacerda Rocha. São Carlos, 2013.

Monografia (Graduação em Engenharia de Computação) -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2013.

1. MPLS-TP. 2. MPLS. 3. NGN. 4. Redes de Transporte (Telecomunicações). I. Título.

FOLHA DE APROVAÇÃO

Nome: Geovana de Mello Espírito Santo

Título: "O MPLS-TP e sua aplicação nas redes de comunicação"

Trabalho de Conclusão de Curso defendido em 25/11/2013.

Comissão Julgadora:	**Resultado:**
Profa. Dra. Mônica de Lacerda Rocha (Orientadora) - SEL/EESC/USP	Aprovada
Prof. Titular Amílcar Careli César SEL/EESC/USP	APROVADA
Mestre Daniel Fernando Pigatto Doutorando/ICMC/USP	Aprovada

Coordenador pela EESC/USP do Curso de Engenharia de Computação:

Prof. Associado Evandro Luís Linhari Rodrigues

Agradecimentos

A Deus, e à minha família por toda a força, apoio e carinho;
À minha orientadora Mônica pela ajuda de prontidão;
À USP, meus colegas de curso e amigos de São Carlos
pelo inesquecível período de vivência universitária;
A todos os meus professores e colegas de curso da Habilitação
em Telecomunicações da Universidade de Coimbra, pelo
despertar do interesse e estudo na área desse presente
trabalho. Em especial agradeço às professoras Teresa e Lúcia
que orientaram o início dessa pesquisa.

“O futuro pertence àqueles que acreditam
na beleza de seus sonhos.”
(Elleanor Roosevelt)

Resumo

Este trabalho tem por objetivo estudar a normalização, as características de funcionamento e os cenários de aplicação do *Multiprotocolo Label Switching – Transport Profile* (MPLS-TP), um novo perfil de transporte para o *Multiprotocolo Label Switching*(MPLS). Com a adoção de serviços baseados em nuvem, os padrões de tráfego nas redes de comunicação foram drasticamente transformados nos últimos anos. Hoje, o tráfego de pacotes já representa 80% da banda dos provedores de serviço o que torna urgente a migração de redes de transporte baseadas em multiplexação por divisão do tempo para tecnologias mais adaptadas ao tráfego de pacotes. O MPLS tradicional apesar de estar presente em muitas arquiteturas de núcleo servindo a importantes serviços de rede, não é capaz de oferecer capacidades *Operations, Administration and Maintenance* (OAM) e resiliência ao mesmo nível das atuais tecnologias empregadas em redes de transporte. O MPLS-TP foi então criado para remover a lacuna entre as tecnologias baseadas em circuitos e tecnologias baseadas em pacotes, integrando os benefícios de ambas. Para isso são recomendadas um conjunto de melhorias e a exclusão de certas funcionalidades do MPLS incompatíveis com as aplicações de transporte. As aplicações mais citadas hoje para a nova tecnologia são o *backhaul* de tráfego móvel e o transporte óptico de pacotes. Conclui-se que o MPLS-TP tem grande potencial de impacto na próxima geração de redes de transporte, devido principalmente à possibilidade de soluções MPLS fim-a-fim baseadas em sua interoperabilidade com redes MPLS tradicionais.

Palavras Chave: MPLS-TP, MPLS, NGN, Redes de Transporte (Telecomunicações).

Abstract

This work aims to study the normalization, operating characteristics and the application scenarios of *Multiprotocolo Label Switching – Transport Profile* (MPLS-TP), a new transport profile for *Multiprotocolo Label Switching* (MPLS). Due the adoption of cloud-based services, the traffic patterns on the communication networks have been dramatically transformed in the recent years. Today, the packet traffic already represents 80% of the bandwidth of the service providers, what makes urgent the migration from transport networks based on time division multiplexing to technologies more adapted to the packet traffic. Despite the traditional MPLS is present in many core architectures serving important network services, it is not able to provide *Operations, Administration and Maintenance* (OAM) capabilities and resilience to the same level of current technologies employed in transport networks. Then the MPLS - TP was created to remove the gap between both circuit-based and packet-based technologies. To achieve this, it was recommended a set of OAM improvements and the exclusion of certain features of MPLS that are incompatible with transportation applications. The applications of the new technology most cited today are the mobile traffic backhaul and the packet optical transport. It is concluded that the MPLS-TP has great potential to impact the NGN of transport due the possibility of solutions MPLS end-to-end based on its interoperability with the traditional MPLS networks.

Keywords: MPLS –TP, MPLS, NGN, Transport Networks (Telecommunications).

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

ACR	Adaptive Clock Recovery
ACH	Associated Channel Header
AIS	Alarm Indication Signal
APS	Automatic Protection Switching
ASON	Automatically Switched Optical Network
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BFD	Bidirectional Forwarding Detection
BSC	Base Station Control
BTS	Base Transceiver Station
CAPEX	Capital Expenditure
CC	Continuity Check
CE	Client Edge
CFI	Client Failure Indication
CoS	Class of Service
CR-LDP	Constraint-based Routing
DCC	Data Communication Channel
DCR	Differential Clock Recovery
ECMP	Equal Cost Multipath
FEC	Forwarding Equivalence Class
GACh	Generic Associated Channel
GAL	GACh Label
GFP	Generic Framing Procedure
GMPLS	Generalized Multiprotocol Label Switching

IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IPLS	Internet Protocol Local Area Network Service
IS-IS	Intermediate System to Intermediate System
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of the ITU
JWT	Joint Working Team
LDI	Link Down Indication
LDP	Label Distribution Protocol
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LKR	Lock Report
LMP	Link Management Protocol
LSE	Label Switched Edge
LSP	Label-Switched Path
LSR	Label Switched Router
LTE	Long Term Evolution
MAF	Management Application Function
MCC	Management Communication Channel
MCF	Message Communication Function
ME	Maintenance Entity
MEG	Maintenance Entity Group
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
MPLS	Multiprotocol Label Switching
MPLS-TP	Multiprotocol Label Switching Transport Profile
MS-PW	Multi-Segment Pseudowire
NE	Network Element
NGN	Next Generation Network
NMS	Network Management System
NNI	Network-Network Interface
NOC	Network Operations Center
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance

OPEX	Operational Expenditure
OS	Operations System
OSPF	Open Shortest Path First
P	Provider
P2MP	Point-to-Multipoint
P2P	Point-to-Point
PE	Provider Edge
PHP	Penultimate Hop Popping
PSC	Protection State Coordination
PSN	Packet Switched Network
PTP	Precision Time Protocol
PW	Pseudowire
QoS	Quality of Service
RAN	Radio Access Network
RDI	Remote Defect Indication
RFC	Request for Comment
RSVP-TE	Resource Reservation Protocol-TE
SCC	Signaling Communication Channel
SLA	Service Level of Agreement
S-PE	Pseudowire Switching Provider Edge
SS-PW	Single-Segment Pseudowire
TDM	Time Division Multiplexing
TE	Traffic Engineering
TFS	Time and Frequency Synchronization
TMN	Telecommunications Management Network
T-PE	Pseudowire Terminating Provider Edge
TTL	Time to Live
UNI	User-Network Interface
VC	Connectivity Verification
VPLS	Virtual Private Local Area Network Service
VPMS	Virtual Private Multicast Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire
WTR	Wait-To-Recovery

Introdução

Esta monografia apresenta uma revisão acerca do MPLS-TP e das suas diferenças com relação ao MPLS tradicional. Pretende-se assim analisar possíveis cenários de aplicação e seu potencial de impacto nas redes de comunicação. O estudo engloba as especificações do IETF e ITU-T e também outros documentos disponíveis relacionados a essa nova tecnologia, como *white papers* de grandes fabricantes.

Para melhor contextualizar as mudanças propostas pelo MPLS-TP, organizou-se o presente trabalho em três partes. No primeiro capítulo, são descritas motivações primárias para a padronização do MPLS, bem como suas características de funcionamento e conceitos técnicos com ele relacionados. No final desse capítulo, é apresentado o GMPLS, uma importante extensão que também é utilizada pelo MPLS-TP. No segundo capítulo, é iniciado o estudo acerca do MPLS-TP propriamente dito, englobando o histórico de sua padronização e também as novas características e funcionalidades por ele introduzidas, através dos RFCs do IETF. Por fim, no terceiro capítulo, trata-se dos possíveis cenários de aplicação da nova tecnologia, com o objetivo de obter-se uma projeção de seu emprego pelos provedores de serviços.

A motivação para este estudo partiu de uma visita acadêmica a PT Inovação, uma fornecedora portuguesa de equipamentos de rede de comunicação, sediada na cidade de Aveiro. Durante uma breve apresentação, a empresa

introduziu sua solução MPLS-TP lançada no mercado em 2011, e também seus estudos e desenvolvimentos acerca do desenvolvimento de novas plataformas IP/MPLS baseadas nas novas funcionalidades OAM para a esses padrões.

1 Multiprotocol Label Switching (MPLS)

Em meados da década de 1990, os equipamentos baseados em tecnologia *Asynchronous Transfer Mode* (ATM) detinham grande interesse por sua alta velocidade de encaminhamento de fluxos de comunicação, combinada ao suporte para gestão de tráfego. Surgiram, assim, esforços para aliar o uso desses equipamentos com as redes IP, até então incompatíveis. O intuito era melhorar o desempenho dessas redes e, ao mesmo tempo, manter sua flexibilidade.

Em meio a tais esforços, foi lançado o primeiro predecessor da tecnologia de troca de rótulos: o *IP Switching,* desenvolvido pela empresa Ipsilon em 1996. Após essa, inúmeras outras empresas anunciaram seus próprios produtos para competir no mercado, entre eles o *Tag Switching da* Cisco Systems, e o *Aggregate Route-based Ip Switching* da IBM. Todas essas tecnologias utilizavam comutadores ATM e um protocolo para definir caminhos entre os terminais, aos quais eram atribuídos os pacotes que entravam na rede. Um pacote deve ser entendido nesse contexto e no decorrer do trabalho como um fragmento ou parte de um fluxo de dados enviado de uma origem até um destino através de uma rede ou serviço de comunicação.

Em resposta a estas iniciativas, em 1997 o *Internet Engineering Task Force* (IETF) criou um grupo de trabalho com o intuito de desenvolver uma abordagem padronizada para a tecnologia, que foi intitulada *Multiprococol Label Switching* (MPLS).

Nos anos seguintes, a introdução de roteadores tão rápidos quanto os comutadores ATM eliminou a necessidade de utilização desses equipamentos nas redes IP. Entretanto, a tecnologia ainda podia trazer grandes benefícios. O MPLS reduzia a quantidade de processamento por pacote nos roteadores IP e, principalmente, trazia novas capacidades de suporte para qualidade de serviço (QoS), engenharia de tráfego (TE), redes privadas virtuais (VPNs) e suporte multiprotocolo [1].

A TE visa a reordenação do tráfego em uma rede de maneira uniforme, ela direciona parte do fluxo em caminhos sobrecarregados para caminhos que são menos utilizados e, dessa forma, evita o congestionamento e melhora a utilização dos recursos da rede. A TE também possibilita rápida recuperação em caso de falha de um nó, já que estabelece caminhos alternativos para o tráfego. O MPLS em seu funcionamento permite o estabelecimento de caminhos determinísticos e independentes baseados na decisão do administrador de rede, o que possibilita a utilização da TE.

Uma VPN pode estabelecer ligações privadas seguras sobre a infraestrutura de uma rede pública. Ela utiliza túneis que simulam conexões ponto a ponto e permitem integrar redes empresariais distribuídas, com custo inferior ao da utilização de linhas físicas dedicadas. Esses túneis, que dispensam a criptografia dos dados, podem ser facilmente estabelecidos através do uso do MPLS. A Figura 1 ilustra a utilização do MPLS para a implementação de VPNs.

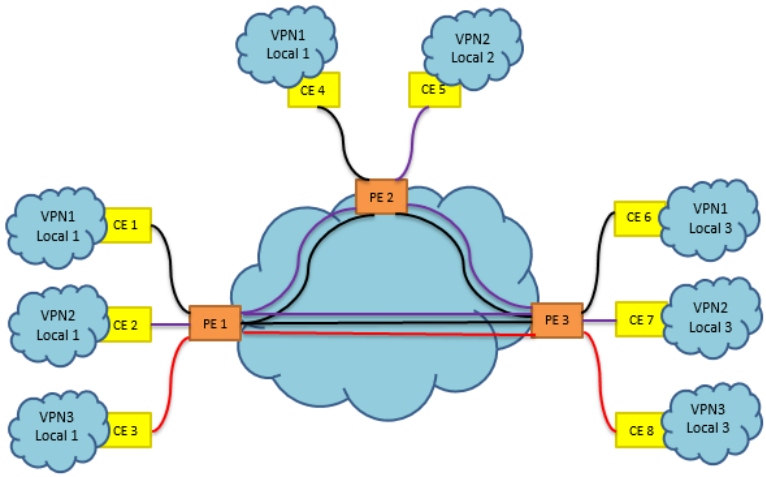

Figura 1 – Virtual Private Networks

Nesse cenário, um provedor de serviços fornece através de sua rede as conexões necessárias para unir redes de clientes geograficamente separadas. São estabelecidas três redes privadas virtuais distintas. Em cada posição geográfica as bordas de cada rede cliente são conectadas a um equipamento de borda da rede servidora.

O MPLS também possibilita a criação de várias classes de serviço, para que a rede atenda a cada uma com QoS específico. Os fluxos de dados podem ser diferenciados de acordo com o serviço que carregam. Por exemplo, serviços multimídia têm grande sensibilidade a atrasos de transmissão, diferentemente de uma serviço de e-mail, o que é levado em conta na decisão de a qual caminho atribuir cada fluxo de dados. Outro parâmetro importante que pode ser analisado é a taxa de erros de bits transmitidos.

Finalmente, numa transmissão MPLS o endereço IP do pacote não é considerado, o que faz com que o MPLS possa ser aplicado também sobre outros protocolos da camada de rede. Essa característica é bastante atrativa para a migração ou atualização de tecnologias, como a substituição do IPv4 pelo IPv6.

Graças a esses benefícios inerentes ao MPLS, os prestadores de serviço que o incorporaram em suas arquiteturas de rede diminuíram seus custos, e adquiriram vantagem competitiva contra aqueles que não contavam com a tecnologia [2] .A especificação formal do protocolo deu-se em 2001 no RFC 3031.

1.1 Fundamentos Operacionais do MPLS

Numa rede MPLS os pacotes recebem, a cada salto ou passo intermediário do caminho, um rótulo que indica o caminho ou interface que deverá ser utilizada pelo próximo roteador para comutá-lo. Ou seja, o rótulo representa um índice na tabela de roteamento do próximo roteador. O procedimento de troca de rótulo é denominado *label swap*.

O cabeçalho do MPLS tem tamanho fixo de 32 bits. É denominado de *shim header* ou cabeçalho de enchimento, por ser inserido entre os cabeçalhos de camada 2 e camada 3. A Figura 2 exibe a estrutura, desse cabeçalho, composto pelos seguintes campos:

- *Rótulo* – 20 bits – Indica o caminho de comutação a ser utilizado no salto atual. Os valores de 0 a 15 são reservados e utilizados para indicar operações especiais.
- *EXP* – 3 bits – Reservado para uso experimental. É utilizado em algumas implementações para indicar a classe de serviço (CoS) do pacote. A CoS determina sua prioridade e afeta os algoritmos de enfileiramento e descarte.
- *S ou* – 1 bit – "*Bottom of Stack*", *flag* que indica o topo da pilha de rótulos hierárquicos, utilizada em implementações de VPNs.
- *TTL ou Tempo de Sobrevivência* – 8 bits – Equivale ao número de roteadores pelos quais o pacote passou. Quando o valor chega a 255 o pacote é eliminado da rede, a fim de eliminar congestionamentos.

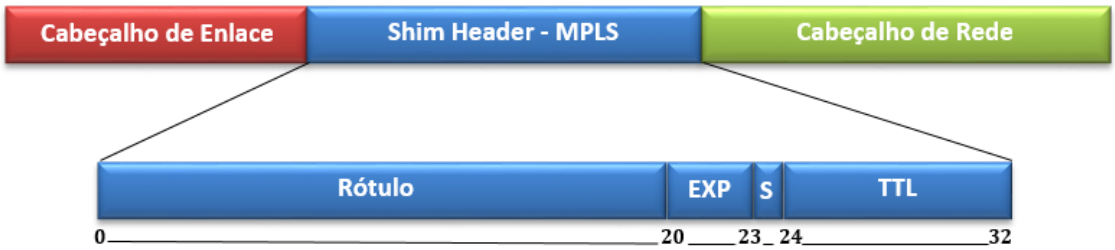

Figura 2 – Cabeçalho MPLS

Os fluxos de pacotes são diferenciados em *Forwarding Equivalence Classes*(FECs), de acordo com suas características. Pacotes com mesmo rótulo e mesma FEC não são diferenciados entre si, e recebem o mesmo tipo de tratamento. Em VPNs a FEC é atribuída de acordo com a porta em que o pacote foi recebido.

As FECs são transportadas em caminhos denominados *Label-Switched Paths* (LSPs), e definidos pelo rótulo atribuído a cada uma. Um LSP é unidirecional e tem significado abstrato, ou seja, trata-se de um caminho virtual.

Dentro do domínio de uma rede MPLS, os roteadores são especializados e chamados de *Label Switched Routers* (LSRs). Para realizar o encaminhamento dos pacotes, os LSRs mantêm em memória tabelas de repasse denominadas *Label Forwarding Information Base* (LFIB). Nessas tabelas são associados para cada rótulo e interface de entrada, a interface e rótulo de saída que devem ser utilizados.

Além da LFIB, cada nó armazena outra tabela denominada *Label Information Base* (LIB) que possibilita o mapeamento dos rótulos atribuídos pelo próprio nó para os rótulos recebidos de seus vizinhos. Ela é necessária porque o valor de cada rótulo tem apenas significado local, isto é, cada LSR utiliza um conjunto próprio de valores para os rótulos que só pode ser interpretado em seu domínio.

Tanto a LFIB quanto a LIB devem ser configuradas antes da comunicação ser estabelecida. Isto pode ser feito de forma manual ou automática. Na configuração manual a escolha dos rótulos que serão usados e a troca que deve ser feita são definidas pela equipe de gerência de rede, já na automática são utilizados protocolos para a negociação dos rótulos.

O algoritmo utilizado por um LSR é mais simples do que os algoritmos utilizados por um roteador comum, em alguns casos é implementado em *hardware*. A informação necessária para o encaminhamento do pacote, assim como a reserva de recursos, pode ser obtida com um único acesso à memória. Isso melhora a velocidade de repasse da rede.

Os roteadores na borda do domínio são denominados *Label Switched Edges* (LSEs). Na entrada da rede um LSE é responsável por atribuir um rótulo inicial para cada pacote.

Já na saída, o LSE deve remover o cabeçalho MPLS dos pacotes, antes desses deixarem o domínio. A partir disso o roteamento IP, ou outro mecanismo de comutação, pode ser instaurado.

Um procedimento denominado *Penultimate Hop Popping* (PHP) permite que o rótulo seja retirado do pacote antes de sua chegada no roteador E-LRS de saída. Nesse roteador o rótulo não tem mais utilidade, e geraria uma busca adicional. O LSE deve pedir a operação de PHP para o roteador de quem recebe os pacotes, seu LSR *upstream.* O PHP é indicado através da atribuição de rótulos com valor igual a 3, que denota um rótulo nulo implícito.

O funcionamento de uma rede MPLS é exemplificado na Figura 3. O LSE na entrada da rede recebe dois pacotes, um vindo de R1 em azul, e outro vindo de R2 em amarelo, ambos são endereçados ao destino B. Dadas as possíveis diferenças de característica de cada pacote, ou a preocupação em distribuir o tráfego uniformemente pela rede, opta-se por atribuir caminhos diferentes a cada um: o pacote em azul recebe um rótulo de valor 2, já o pacote em amarelo recebe um rótulo de valor 6. Em seguida, os pacotes são encaminhados por interfaces distintas, seguindo a tabela de repasse. No núcleo da rede ambos recebem um novo rótulo de valor 8, ao qual está atribuído o destino B. Por fim, ambos os pacotes são entregues a este destino.

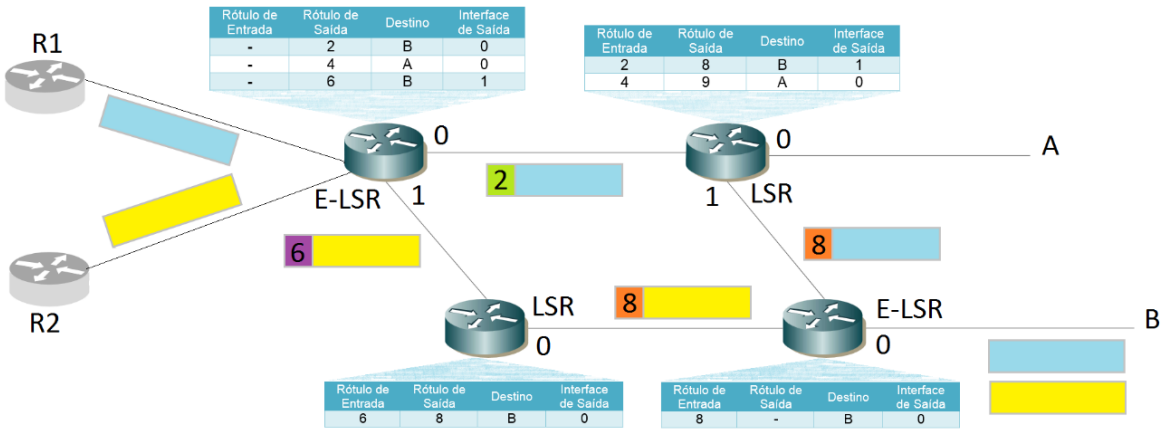

Figura 3 – Exemplo de Rede MPLS **[3]**

Assim como no exemplo, os pacotes endereçados a um mesmo destino podem receber diferentes rótulos, e assim, seguir rotas diferentes. Essa característica possibilita o estabelecimento de FECs para fornecer QoS específicas, e o emprego de engenharia de tráfego, de forma a otimizar o uso dos recursos da rede.

Quando dois ou mais pacotes possuem o mesmo LSE de destino, e passam pelo mesmo trecho da rede a partir de um determinado LSR, os rótulos podem ser mesclados em um valor único. Esse procedimento é denominado *label merging* e ilustrado na Figura 4. Sem ele os pacotes recebidos nas interfaces 1, 2 e 3 do LSR D seguem para um mesmo destino, mas utilizando rótulos diferentes. Com o *label merging* todos passam a receber o mesmo rótulo.

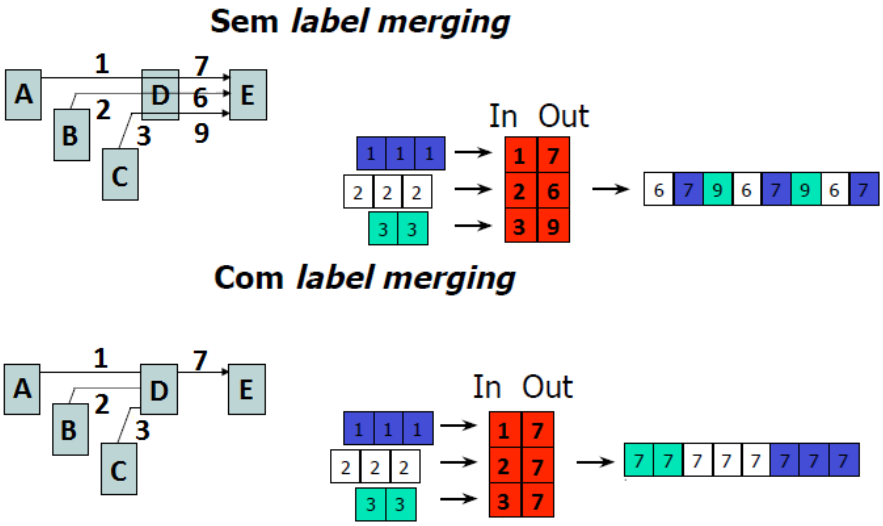

Figura 4 – Label Merging

Um LSR que suporta *label merging* necessita que apenas um rótulo por FEC seja utilizado. Em redes sem esse procedimento o número de rótulos necessários para determinada FEC depende de quantos LSRs são *upstream* em relação a ela. É possível ainda que por limitação de hardware possa haver alguns nós que suportem apenas a mescla de um número limitado de rótulos. [4]

Numa rede MPLS, é possível o estabelecimento de sub-redes hierárquicas e encapsuladas através da utilização de uma pilha de rótulos. Nesse caso, durante a operação de troca de *swap* apenas o rótulo no topo da pilha é considerado pelo LSR e indicado pela *flag* S presente no *shim header.*

Nas bordas de uma sub-rede ocorrem operações semelhantes àquelas realizadas pelos LSEs. Na entrada de um novo nível hierárquico, uma operação de *push* adiciona um rótulo desse nível ao topo da pilha de rótulos dos pacotes

que chegam ao domínio dessa sub-rede. Já na saída uma operação de *pop* retira o rótulo do topo da pilha e ativa a *flag* S do rótulo de nível logo abaixo ao seu.

Os LSPs são estabelecidos entre duplas de LSRs de mesmo nível hierárquico, ditos pares. Dessa forma as sub-redes e os LSPs de maior nível são transparentes em relação àqueles de menor nível.

Uma topologia hierárquica, e as operações descritas acima são exemplificadas na Figura 5. Entre os dois LSEs existem 3 diferentes níveis de LSPs. Um LSP de nível 1 é estabelecido entre os LSRs 1 e 13 e é indicado pelos rótulos em rosa. LSPs de nível dois são determinados pelos rótulos de cor verde. Por fim, os rótulos azuis utilizados no núcleo da rede denotam LSPs de nível 3.

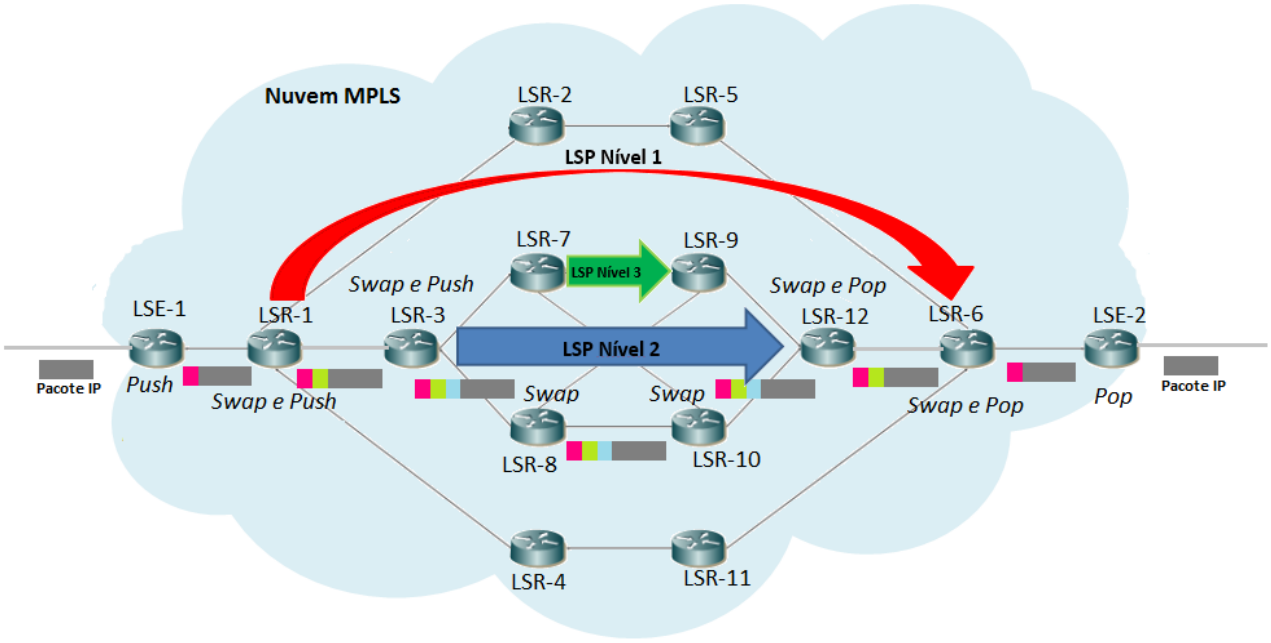

Figura 5 – Topologia MPLS Hierárquica

Esse tipo de topologia é abordado na implementação de VPNs. Já que a correspondência para o último rótulo da pilha só acontece quando os pacotes já estão em seu destino final. Nesse caso, a criptografia dos dados pode ser dispensada.

A arquitetura de uma rede MPLS é composta de dois planos: o plano de encaminhamento propriamente dito, e o plano de controle. Como ilustrado na

Figura 6, através de protocolos de roteamento e sinalização o plano de controle define as entradas da LFIB, utilizada no plano de encaminhamento.

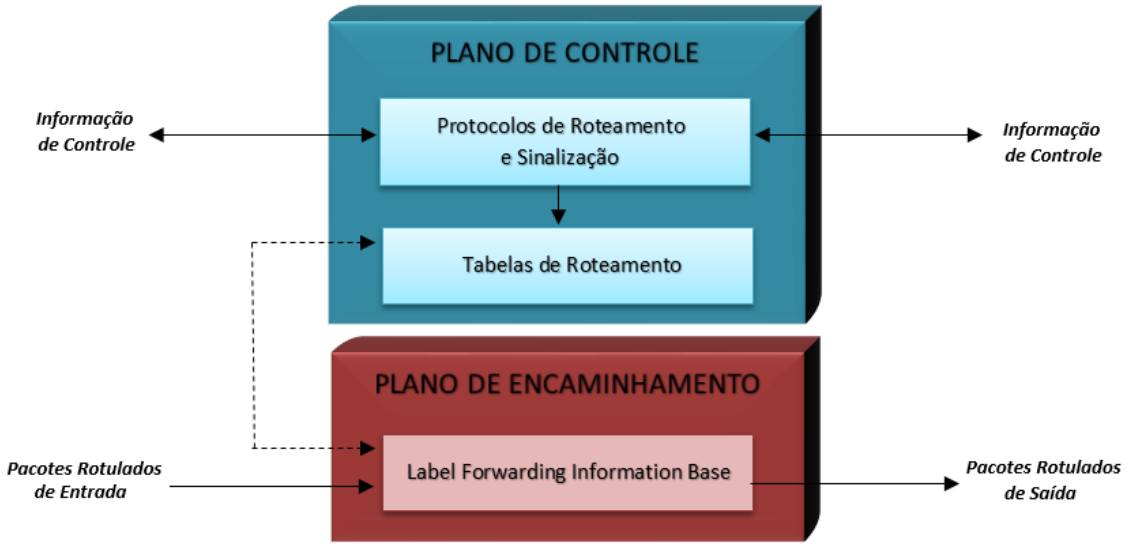

Figura 6 – Arquitetura Lógica de um nó MPLS

O plano de controle portanto é responsável por definir a política de trabalho do plano de encaminhamento, através do estabelecimento dos LSPs e da manutenção das tabelas de repasse. O modo como os LSPs e as tabelas de encaminhamento são estruturadas varia com a necessidade de atender requisitos de TE, QoS e proteção.

No roteamento estático, os LSPs são estabelecidos de forma explícita, e rotas inteiras podem ser traçadas. Nesse caso, o rótulo inicial, definido na borda da rede, determina todos os caminhos por onde o pacote passará até sair da rede através de mapeamentos pré-estabelecidos em todos os enlaces.

No roteamento dinâmico, para criar e estabelecer os LSPs o plano de controle faz o uso de outros protocolos, não definidos pelo MPLS. São necessários um protocolo de roteamento e um protocolo de sinalização. [5]

1.2 Protocolos de Roteamento e Sinalização

O protocolo de roteamento distribui informações sobre a topologia da rede, para que o caminho para um LSP possa ser calculado automaticamente. As tabelas de roteamento IP são utilizadas para fornecerem informação sobre a rede de destino e os prefixos de sub-rede utilizados para um rótulo. Desse modo, os protocolos de encaminhamento são capazes de definirem o alcance, as ligações, e o mapeamento entre uma FEC e o endereço para o próximo salto. [5]

Nas redes MPLS são normalmente utilizados protocolos de roteamento interno(IGPs), como o *Open Shortest Path First* (OSPF) e o *Intermediate System to Intermediate System Routing Exchange Protocol* (IS-IS). Tanto o OSPF quanto o IS-IS são baseados no algoritmo de estado de enlace. Nesse algoritmo, cada nó constrói um grafo de conectividade da rede, e calcula para cada destino possível o caminho para o próximo salto a partir dele baseado em uma métrica estabelecida administrativamente pelo gerente de rede. O caminho escolhido é aquele que minimiza a métrica escolhida [6]. Esses protocolos também podem utilizar a técnica de *Equal Cost Mutipath* (ECMP), com o intuito de balancear a carga entre caminhos de igual custo, já que essa possibilita que múltiplos caminhos sejam analisados a partir dos próximos saltos.

O protocolo de sinalização informa aos switches quais rótulos e interfaces utilizar para cada LSP, o que permite o estabelecimento da LFIB. As informações são distribuídas apenas entre equipamentos adjacentes, diferentemente dos protocolos de estado de enlace, que não são adequados para a distribuição dos rótulos. Para o MPLS, os protocolos de sinalização mais utilizados são o *Label Distribution Protocol* (LDP), o *Resource Reservation Protocol*-TE (RSVP-TE), e o *Border Gateway Protocol* (BGP) em uma versão de extensão.

O LDP é utilizado quando engenharia de tráfego não é necessária. Os LSPs são estabelecidos com base nas tabelas IP, e os rótulos são definidos utilizando as rotas que foram escolhidas pelo protocolo de roteamento. O LDP possibilita a solicitação, distribuição e liberação dos rótulos entre LSRs pares, através de mensagens encaminhadas salto-a-salto.

Os LSRs podem descobrir pares potenciais e estabelecer sessões com o propósito de trocar suas informações de mapeamento de rótulos. Para isso cada LSR envia a determinados intervalos de tempo mensagens de descoberta "*Hello*" que indicam sua presença ativa na rede, através de pacotes UDP para os demais roteadores de sua sub-rede, em um envio *multicast*. [7]

Quando um LSRs deseja se conectar a um LSR que não está diretamente conectado a ele, uma requisição é enviada para seu endereço específico utilizando a da tabela de roteamento. O pedido é encaminhado salto a salto até que retorne para o roteador que realizou o pedido.

As mensagens de descoberta ao serem recebidas podem ser utilizadas para manter as conexões existentes ativas, ou para criar uma nova sessão. Para isso, o par de roteadores troca parâmetros necessários, através de mensagens TCP, para estabelecer a conexão LDP e assim dar início à sessão. Com esse procedimento, caso não exista uma outra conexão entre os dois roteadores, é criado um novo LSP. Em seguida são enviadas mensagens de anúncio para criar o mapeamento de rótulos e FECs para utilizar em cada link para esse LSP. Enquanto as sessões estão ativas outras mensagens de anúncio poderão mudar e deletar os mapeamentos em cada LSR.

Cada sessão é associada a um espaço de rótulos, em que os valores utilizados por cada LSR devem concordar. Na troca de mensagens entre os LSRs, o identificador desse espaço é enviado juntamente com o identificador do LSR.

Por fim, o LDP também prevê a utilização de mensagens de notificação utilizadas entre os roteadores, para distribuir informações sobre a sessão e mensagens recebidas ou sinalizam a ocorrência de erros [8] [7].

O LDP é utilizado para fornecer certos serviços MPLS como *pseudowires* (PW - RFC 3985), capaz de simular o transporte de qualquer tipo de serviço fornecido por conexões de cabo fim-a-fim. Os PWs são muito utilizados na implementação de VPNs [9].

Para aplicações de engenharia de tráfego foi desenvolvida uma extensão do protocolo LDP, denominada *Constraint-based Routing (CR-LDP)*. Nesse protocolo o roteamento busca uma rota que otimize uma certa métrica e ao mesmo tempo não viole um conjunto de restrições, como por exemplo garantias de largura de banda mínima em cada enlace da rota, ou ainda impedir que certos tipos de tráfego atravessem enlaces específicos na rede por questões de segurança, ou mesmo gerenciamento. Entretanto, conforme o RFC 3468, o IETF optou por abandonar os trabalhos sobre seu desenvolvimento para concentrar esforços na utilização do protocolo RSVP-TE. [10]

O RSVP-TE, portanto, é utilizado quando existem requisitos de engenharia de tráfego. Esse protocolo é orientado a conexão, pois estabelece um caminho com reserva de recursos para o fluxo de dados, entre a origem e o destino.

Para iniciar a comunicação um equipamento de origem envia uma mensagem de *PATH* para um equipamento de destino, com o tipo de tráfego e a QoS das mensagens que devem ser trocadas entre eles. O caminho utilizado é definido pelo protocolo de roteamento, entretanto, em cada elemento da rota, é verificado se a banda necessária está disponível no enlace a ser utilizado, e se há disponibilidade para alocação de um rótulo para o LSP. Se as verificações forem válidas, a mensagem é encaminhada para o próximo salto, caso contrário uma mensagem de erro denominada *PathError*, é enviada para a origem.

Quando a mensagem de *PATH* chega ao destino, é enviada uma mensagem de *RESV* para a origem pelo mesmo caminho, com o intuito de realizar as reservas dos recursos necessários e estabelecer os rótulos para o LSP. Se algum pedido de reserva falhar é enviada uma mensagem de erro de reserva, *ResvError*.

Esse processo de sinalização é do tipo *soft state*, e as mensagens de PATH e RESV são trocadas periodicamente entre os elementos que compõem a rede. Caso algum dos elementos não receba essas mensagens dentro de limites pré-definidos, o LSP é desfeito. Essa característica permite o rápido redirecionamento de LSPs em caso de falha no circuito ou quando um caminho

melhor se tornar disponível, como ilustrado no balanceamento de carga na Figura 7. [11]

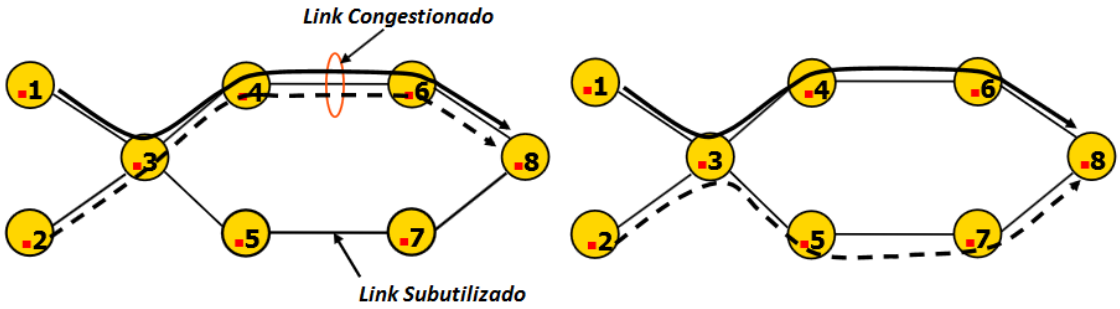

Figura 7 – Utilização do RSVP–TE para Engenharia de Tráfego

Nos casos de redirecionamento é utilizado o mecanismo *make-before-break,* e assim, os recursos alocados para o antigo LSP não são liberados antes que todo o tráfego seja transferido para o novo caminho. Isso evita interrupção de tráfego e queda de serviço.

O RSVP também possui uma extensão para redes ópticas, que permite sinalizar os comprimentos de onda, compartilhar grupos de ligação de risco, bem como, largura de banda, latência e outras características de ligações.

Os protocolos de roteamento utilizados pelo MPLS, e referenciados anteriormente, não são livres de *loops*, o que pode afetar no desempenho da rede MPLS. Quando um pacote é enviado para estabelecer um LSP entra em *loop*, o caminho não é criado, fora isso, se o pacote carregar dados por um LSP em *loop* ele não chegará ao destino até que o loop seja interrompido ou o valor TTL chegue ao limite. Portanto, o MPLS deve adotar medidas para preveni-los.

Um mecanismo de detecção de *loop* pode ser implementado com a inicialização do TTL de acordo com o número de saltos previstos pela rota. Em caso de transição da rede e formação de *loop,* a atribuição de rótulos falha e o LSP é derrubado. Já um mecanismo de prevenção pode utilizar uma lista carregada pelas mensagens de controle para solicitação de rótulos contendo os nós LSR, pelos quais elas foram comutadas. Quando o LSR encontra seu próprio endereço na lista o loop é detectado e previne-se sua criação. [2]

1.3 Generalized Multiprotocol Label Switching (GMPLS)

O *Generalized Multiprotocol Label Switching* (GMPLS), padronizado pelo IETF em 2004 no RFC 3945, permite que os objetivos do MPLS sejam estendidos a diferentes tipos de plataformas de comutação. Teve como predecessor o *Multiprotocol Lambda Switching (MPλS)* que estendia o MPLS apenas para plataformas ópticas.

No GMPLS, o rótulo não possui um valor explícito para distinguir um LSP. Ao invés disso, o LSP é definido através de alguma propriedade física do fluxo de dados recebido, como, o *timeslot* em um link TDM (Time Division Multiplexing), o comprimento de onda em um link WDM (Wavelength Division Multiplexing), ou ainda a porta em que o pacote foi recebido. Se a comutação GMPLS for baseada em uma propriedade contínua do fluxo de dados, circuitos podem ser estabelecidos.

Dessa forma o GMPLS permite a combinação de vários serviços sobre um transporte comum. Nessa arquitetura, um plano de controle único gerencia múltiplas tecnologias e unifica o gerenciamento de diferentes camadas.

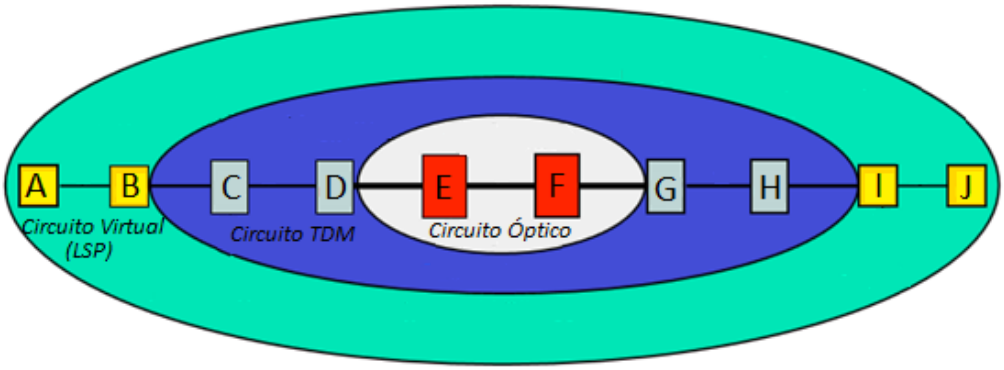

Figura 8 – Topologia GMPLS Hierárquica

Na rede híbrida ilustrada na Figura 8, temos a intercomunicação de dispositivos de diferentes tecnologias. Nela, a hierarquia de um LSP MPLS é estendida sobre um circuito TDM, e em seguida sobre um caminho óptico através do comprimento de onda do sinal que se propaga sobre uma fibra óptica. [5]

A principal característica do GMPLS é a separação entre o plano de controle e o plano de dados. A informação é transportada no plano de dados, e os protocolos de sinalização no plano de controle, onde são alocados os recursos e definidos os LSPs.

O GMPLS pode ser implementado através de dois modelos diferentes, sobreposição e pares. No modelo de sobreposição o roteador IP/MPLS é um cliente do domínio óptico e só interage com o nó óptico diretamente adjacente a ele. O caminho físico de propagação do sinal é decidido pela rede óptica. No modelo de pares a camada IP/MPLS opera em conjunto com a camada óptica, e os roteadores podem determinar toda a rota da comunicação. Os dois modelos são ilustrados na Figura 9. [12]

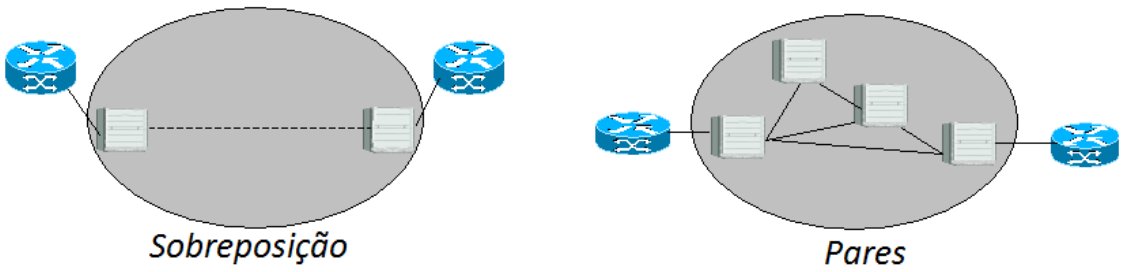

Figura 9 – Modelos de Arquitetura GMPLS

No GMPLS os caminhos LSPs devem ser bidirecionais, para isso são estabelecidos dois caminhos unidirecionais, e cada LSR envia uma mensagem ao seu *downstream* com um rótulo *upstream* e pede por um rótulo para o sentido inverso.

O GMPLS pode ser auxiliado pelo *Link Management Protocol* (LMP) para localizar falhas e validar a conectividade entre nós adjacentes. Esse protocolo prevê mecanismos de gerenciamento de canais de controle, verificação de conectividade dos links, gerenciamento de falhas e autenticação. [13]

Essa tecnologia dá maior simplicidade à infraestrutura e ao gerenciamento das redes de transporte. Isso pode auxiliar os provedores de serviço a diminuir os

custos com mão de obra e manutenção, a aproveitar melhor os recurso da rede e principalmente em oferecer melhores serviços com relação ao aumento da capacidade de restauro e ao fornecimento dinâmico das larguras de banda contratadas.

2 Multiprotocol Label Switching – Transport Profile (MPLS-TP)

As redes de transporte de comunicação foram projetadas e implementadas tradicionalmente com a utilização de dispositivos TDM como SDH/SONET. A função dessas redes é transportar informações entre dispositivos de borda de serviços. Estes dispositivos podem ser multiplexadores de acesso de linha digital de assinante (DSLAM), *gateways*, agregadores T1/E1, servidores de acesso remoto de banda larga (BRAS), etc. As redes de transporte TDM são capazes de fornecer serviços com granularidade de largura de banda de baixa velocidade, bem como serviços de transmissão de longa distância com altas velocidades.

Serviços de rede de transporte comutados por circuitos com granularidade de largura de banda fixa como 64 kbps, 1.5 Mbps, 2 Mbps, 50 Mbps, 150 Mbps e 600 Mbps são emulados através de tecnologias orientadas a conexão, e comutadas por pacotes e serviços comuns de gerenciamento de largura de banda. [14]

Essas redes possuem um centro de operações de rede (NOC), que utiliza um sistema de gerenciamento de rede (NMS). O NMS baseia-se na rede de gerenciamento de telecomunicações (TMN), definida pelo *Telecommunication Standardization Sector of the International Telecommunication Union* (ITU-T), no M.3010, para estabelecer a comunicação com cada elemento da rede.

O NMS fornece funções de gerenciamento para falhas, configuração, contabilidade, desempenho e gerenciamento de segurança (FCAPS), tal como definido pela ITU-T na M.3400. Juntamente com as funções de sobrevivência como proteção e restauração, o sistema tem alcançado taxas de disponibilidade superiores a 99,999%. Assim sendo, as funções *Operations, Administration and Maintance* (OAM) existentes em redes de transporte tradicionais são consideradas altamente sofisticadas. [15]

As redes baseadas em TDM, entretanto, tornaram-se ineficientes e custosas com o passar dos anos, dado o rápido crescimento da demanda por serviços e aplicações com alto consumo de largura de banda carregados por pacotes, sobretudo serviços multimídia, como IPTV e vídeo móvel. Os dispositivos TDM trabalham a taxas constantes mesmo quando não há tráfego, o que desperdiça largura de banda e impossibilita o alcance de maiores velocidades de transmissão.

Nesse cenário, os provedores começaram a mostrar interesse em substituir suas tecnologias baseadas em circuito para tecnologias baseadas em pacotes, com o objetivo de reduzir o custo por bit [16]. Começaram, assim, a surgir esforços para definir novas arquiteturas otimizadas para o transporte de pacotes.

Na última década, um número significativo de provedores de serviço migrou o núcleo de suas redes para a tecnologia MPLS e muitos outros gostariam de convergir suas próximas gerações de núcleo, agregação e acesso para a mesma [16]. Dessa forma, atualmente o MPLS está empregado em milhares de redes ao redor do mundo e é considerado tecnologia líder para redes de pacotes orientadas a conexão. [14]

Entretanto, como mencionado anteriormente grande parte das atuais redes de transporte foi construída utilizando comutação por circuitos e TDM. Assim, antes dessas redes migrarem para tecnologias baseadas em pacotes, como o MPLS, um conjunto de melhorias é necessário. É preciso garantir que a tecnologia ofereça recursos equivalentes ao legado das redes de transporte tradicionais, tanto em termos de funcionalidade quanto em termos de gerenciamento [16].

Para isso, é necessário a implementação de funções OAM, melhoria dos tempos de recuperação e detecção de falhas e a garantia de QoS fim-a-fim.

Muitos provedores de serviço e desenvolvedores de equipamentos reconhecem que algumas capacidades do MPLS não são necessárias, e que outras não estão de acordo com os requisitos das redes de transporte. Acredita-se que economias de custo poderiam ser atingidas com uma solução estritamente orientada a conexão e que não dependa do roteamento IP.

Esses fabricantes e operadores têm auxiliado no desenvolvimento de um perfil de transporte para o MPLS (MPLS-TP), padrão que uma *Joint Working Team*(JWT) entre IETF e o ITU-T está trabalhando desde 2008 [17]. O MPLS-TP pretende ser a base para a próxima geração de redes de transporte de pacotes e ser uma tecnologia de transporte de pacotes ao nível de operadora.

Como notado em [18], o objetivo principal do MPLS-TP é permitir que o MPLS seja empregado nas redes de transporte e opere de maneira similar às tecnologias de transporte existentes e, assim, permitir que o MPLS suporte o serviço de transporte de pacotes com grau de previsibilidade similar àquele encontrado nessas redes.

O MPLS-TP é uma extensão do MPLS que utiliza um subconjunto de suas funções, e adiciona algumas melhorias, principalmente na área de OAM. Essas melhorias aumentam a aplicabilidade do MPLS, e permitem sua adoção tanto para redes de transporte quanto para redes de serviços.

A nova tecnologia é planejada para interoperar com as redes MPLS já implementadas pelos servidores, utilizando a infraestrutura física já existente, e assim, aproveitar os investimentos em infraestrutura anteriores. [17]

A arquitetura das redes provedoras de serviço pode ser dividida em três partes: rede de acesso, rede de agregação e núcleo, conforme ilustra a Figura 10.

A rede de acesso faz a conexão dos equipamentos de cada cliente com equipamentos do provedor de serviço. A quantidade de nós é elevada e pode exigir diferentes tipos de conexão, como serviço móvel, conexões para residências, etc.

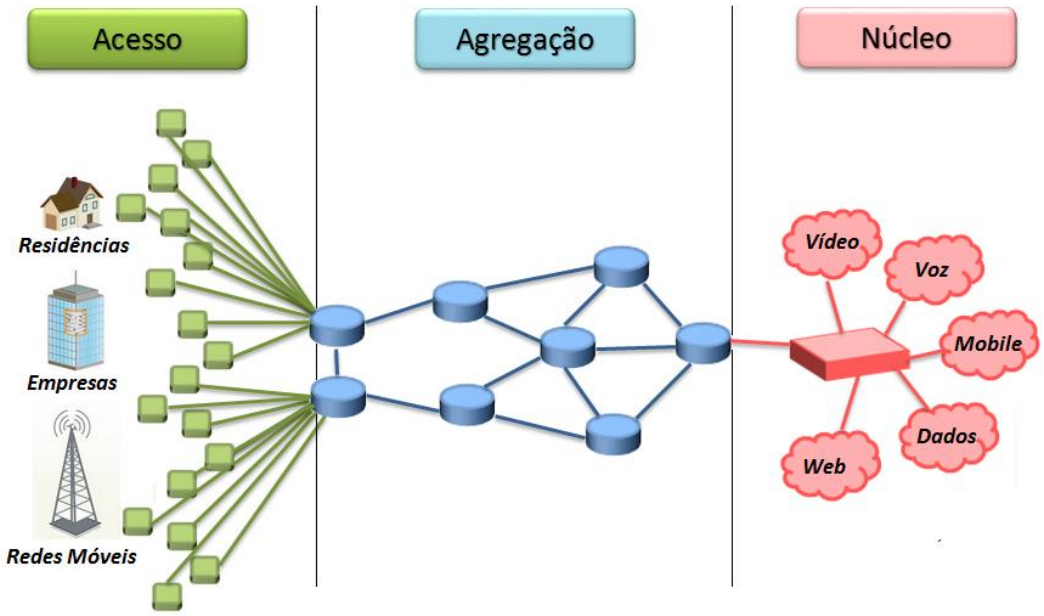

Figura 10 – Arquitetura de Rede Provedora de Serviços

A rede de agregação aglomera os fluxos de vários clientes por cidades, bairros ou até mesmo empresas e universidades. A quantidade de nós é menor do que na rede de agregação, mas ainda assim, grande.

O núcleo da rede diferencia-se por uma quantidade limitada de nós, entretanto a densidade de dados trafegados em cada enlace e nó é elevada.

As operadoras precisam convergir suas redes para uma infraestrutura comum, a fim de reduzir suas despesas de capital (CAPEX) e despesas operacionais (OPEX). Além disso, isso permite a utilização de novos serviços de rede baseados em IP, bem como serviços tradicionais de camada 2. A capacidade de suportar múltiplos serviços e aplicações sobre uma infraestrutura MPLS comum provê flexibilidade para escalar a demanda de tráfegos, instantaneamente, com melhor custo e eficiência.

No núcleo da rede, a maioria dos provedores já utiliza uma infraestrutura baseada em dispositivos MPLS. A utilização desses dispositivos ao longo de toda a rede, porém, pode elevar os custos operacionais nas redes de acesso e agregação. A complexidade do MPLS cresce exponencialmente com o aumento do número de nós, devido à massiva utilização de protocolos de roteamento e sinalização e de outros recursos da tecnologia [19]. Em um cenário de pouco dinamismo, em que as rotas utilizadas são quase sempre as mesmas, como o caso das redes de agregação, muitos dos recursos oferecidos não são de fato necessários.

Assim sendo, em alguns casos, um prestador de serviços pode não querer implementar, em algumas áreas de sua rede, um plano de controle dinâmico baseado em protocolos IP. Por exemplo, para uma aplicação de *backhaul* móvel em que o número de nós, e endereços IP são elevados e variam muito. Além disso, a proteção baseada em engenharia de tráfego, para esses milhares de nós e caminhos torna-se não gerenciável.

Uma solução MPLS-TP, portanto, deve permitir o provisionamento estático de caminhos virtuais. Essa abordagem facilita a transição do legado das tecnologias de transporte para uma infraestrutura MPLS comum, e possibilita que a rede seja gerenciada com maior facilidade e simplicidade de maneira a termos capacidade OAM fim-a-fim. [14]

As funcionalidades MPLS-TP deverão ser incorporadas em comutadores de borda de serviço, sistemas de transporte óptico de pacotes, plataformas de acesso e outros dispositivos que dão aos operadores a opção de desenvolver o MPLS-TP em qualquer lugar da rede.

Nesse contexto, de interligação entre redes baseadas em MPLS/MPLS-TP de clientes e operadores, deve-se ressaltar um importante requisito. A interligação deve manter operacionalmente o relacionamento cliente-servidor, através da gestão independente das entidades e de modo que elas possam ser funcionalmente dissociadas [14].

Em síntese, portanto, os provedores de serviço pretendem: substituir equipamentos TDM; consolidar uma infraestrutura MPLS comum com escalabilidade; utilizar taxas mais flexíveis e eficientes de multiplexação possibilitada pela tecnologia de pacotes; possibilitar o transporte de pacotes IP de vídeo, VPN, banda larga móvel, virtualização em nuvem e outros serviços com menor custo e maior controle desse custo [17].

2.1 Processo de Padronização

O esforço para otimizar o MPLS para as redes de transporte começou em 2006, sob o nome *Transport-MPLS* (T-MPLS), pelo Grupo de Estudo 15 (SG15) do ITU-T apoiado por grandes indústrias do ramo. Naquele ano, o IETF trabalhava encima de um novo mecanismo denominado *Pseudo Wire Emulation Edge-to-Edge* (PWE3), tecnologia que emula os atributos essenciais de um serviço tais como ATM, TDM, ou Ethernet sobre uma *Packet Switched Network* (PSN).

Porém, em 2008, apesar de alguns desenvolvedores começarem a dar soluções para a tecnologia, o ITU-T reconheceu a nocividade do desenvolvimento descoordenado de um novo protocolo MPLS, já que fora o IETF, o organismo de normalização que havia desenvolvido a versão original da tecnologia. Todos os trabalhos acerca do T- MPLS foram então interrompidos.

Entretanto, naquele mesmo ano, após algumas reuniões entre as duas instituições foi instaurado um *Joint Working Team* (JWT), entre o SG15 do ITU-T e os grupos MPLS, PWE3 e CCAMP do IETF. O grupo CCAMP desenvolvia estudos acerca do *Common Control and Measurement Plane* que define um plano comum de controle e medição entre o caminho físico e as tecnologias de tunelamento, o que inclui o encapsulamento de tecnologias como o MPLS.

Na ocasião, o IETF ficou responsável por definir as extensões necessárias ao protocolo MPLS, e o ITU-T por definir os requisitos de transporte a serem cumpridos. Além disso, os trabalhos do grupo deveriam seguir os procedimentos padrões para normalização adotados pelo IETF. [18]

Um ano depois da primeira reunião, o JWT publicou o RFC 5317, "*MPLS Architectural Considerations for Transport Profile*", que definiu a arquitetura inicial do MPLS-TP. Esse RFC recomendou que o IETF e o ITU-T trabalhassem juntos para "trazer requisitos de transporte para o IETF e estender o encaminhamento MPLS com capacidades OAM, sobrevivência, gerenciamento da rede e protocolos para o plano de controle compatíveis com aqueles requisitos durante o processo de padronização IETF". [17]

O IETF, portanto, concentrou seus esforços em desenvolver extensões para as ferramentas MPLS OAM existentes e criar alguns mecanismos novos para medidas de perda, atraso e gerenciamento de falhas. Esse esforço incluiu a extensão do *Bidirectional Forwarding Detection* (BFD) para possibilitar checagem contínua, verificações de conectividade e a dos mecanismos de *Ping e Traceroute* através dos LSPs, para permitir verificações sobre demanda dos operadores.

Para que o processo de criação do padrão ocorresse com consistência e de modo a convergir os interesses do IETF e ITU- T, foi decidido que quando os RFCs do MPLS- TP tivessem atingido nível de maturidade técnica comparável com o T- MPLS, a ITU- T iria alinhar seu padrão com as realizações do IETF, isso começou a ocorrer já em 2009. Esse processo é retratado na Figura 11.

Apesar do trabalho em cooperação, durante o processo, surgiram algumas divergências de opinião entre alguns membros das organizações com relação às ferramentas OAM, e a incerteza a respeito do que faria parte do MPLS-TP, e do que seria parte de estudos anteriores, ou de outras especificações que não deveriam constar no novo padrão.

Fora isso, em fevereiro de 2011, o SG15 do ITU-T enfrentou uma crise interna devido a discussões envolvendo duas diferentes abordagens da funções OAM do MPLS-TP. Em primeiro lugar uma solução específica para adicionar capacidade de rede de transporte de pacotes nas redes SDH/OTN, e em segundo lugar uma solução que adicionasse capacidade de rede de transporte no ambiente MPLS.

Depois de um debate, o grupo votou pela primeira solução e o mecanismo foi definido no ITU-T G.8113.1 "*Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks*". Entretanto como a solução divergia da linha de pesquisa do IETF, o mecanismo não foi aceito com padrão MPLS-TP, com base nos RFCs 5654 e 5680 que determinam que o protocolo deveria reutilizar padrões MPLS sempre que possível. Isso pressionou a definição de um mecanismo OAM pautado na segunda solução, e de acordo com o trabalho do IETF, o G.8113.2 "*Operations, administration and maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS*".

Para pôr fim ao impasse entre a coexistência das duas recomendações foi definido o processo de uma nova recomendação, definitiva para o padrão MPLS-TP, e sob nome provisório G.mpls-tpoam ou G.tpoam e intitulada "*Operation and maintenance mechanism for MPLS-TP layer networks*".

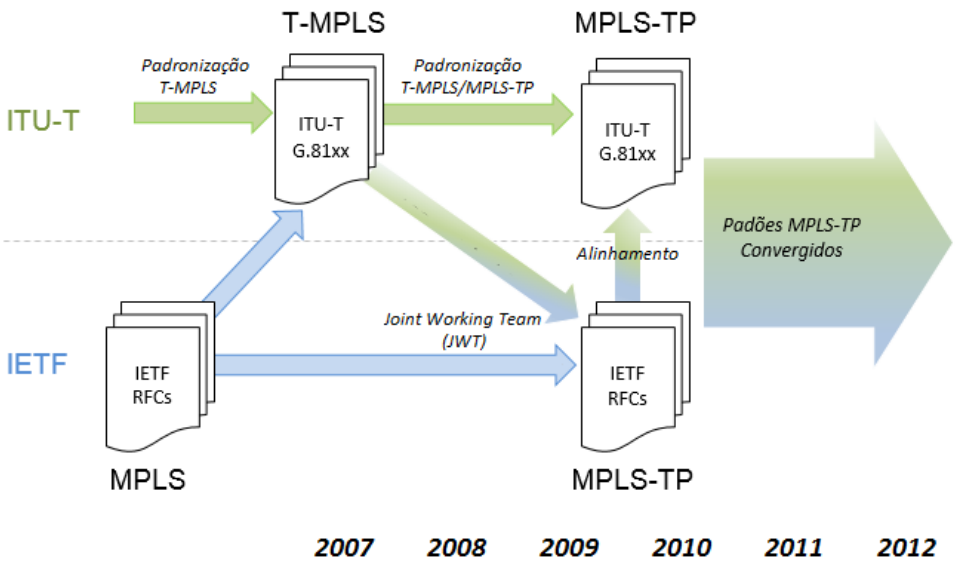

Figura 11 – Cronologia do Processo de Padronização MPLS-TP **[15]**

Até outubro de 2013, foram publicados pelo IETF trinta (30) RFCs referentes ao MPLS-TP desde o estabelecimento do JWT, e considera-se finalizada a parte central da padronização. Dezessete (17) *drafts* estão ativos atualmente, e ainda dois (2) documentos estão em fila para publicação. Com a consolidação de sua

padronização, o MPLS-TP começa a ganhar grande potencial de impacto nas arquiteturas de rede nos próximos anos. Dois resumos de todos os documentos publicados acerca do MPLS-TP pelo IETF e ITU-T são fornecidos respectivamente na Tabelas 1 e na Tabela 2.

Tabela 1 – RFCs MPLS-TP – IETF (Outubro/2013)

RFC	***Título***	***Data***
RFC 5317	MPLS Architectural Considerations for a Transport Profile	02/2009
RFC 5462	EXP field Renamed to Traffic Class field	06/2009
RFC 5586	MPLS Generic Associated Channel	06/2009
RFC 5654	MPLS-TP Requirements	09/2009
RFC 5718	An Inband Data Communication Network for the MPLS-TP	01/2010
RFC 5860	Requirements for OAM in MPLS Transport Networks	05/2010
RFC 5921	A framework for MPLS in Transport Networks	07/2010
RFC 5950	MPLS-TP Network Management framework	09/2010
RFC 5951	Network Management Requirements for MPLS-TP	09/2010
RFC 5960	MPLS-TP Data Plane Architecture	08/2010
RFC 6215	MPLS-TP User-to-Network and Network-to-Network Interfaces	04/2011
RFC 6370	MPLS-TP Identifiers	09/2011
RFC 6371	OAM framework for MPLS-TP	09/2011
RFC 6372	MPLS-TP Survivability	09/2011
RFC 6373	MPLS-TP Control Plane Framework	09/2011
RFC 6375	Packet Loss and Delay Measurement for the MPLS-TP	09/2011
RFC 6378	MPLS-TP Linear Protection	10/2011
RFC 6423	Using the GACh Label for Pseudowire in the MPLS-TP	11/2011
RFC 6426	MPLS on-demand Connectivity Verification and Route Tracing	11/2011
RFC 6427	MPLS fault Management OAM	11/2011
RFC 6428	Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication	11/2011
RFC 6435	MPLS-TP Lock Instruct and Loopback functions	11/2011
RFC 6639	MPLS-TP MIB-Based Management Overview	06/2012
RFC 6669	An OAM Toolset for MPLS-Based Transport Networks	07/2012
RFC 6670	The Reasons for Selecting a Single Solution for MPLS-TP OAM	07/2012
RFC 6923	MPLS-TP Identifiers Following ITU-T Conventions	05/2013
RFC 6941	MPLS-TP Security Framework	04/2013
RFC 6974	Applicability of MPLS-TP for Ring Topologies	07/2013
RFC 6965	MPLS-TP Applicability: Use Cases and Design	08/2013
RFC 7026	Retiring TLVs from the ACh Header of the MPLS GACh	09/2013

Tabela 2 – Recomendações MPLS-TP – ITU-T (Outubro/2013)

Recom.	***Título***	***Data de Publicação***	***Última Alteração***
G.7712	Architecture and Specification of data communication network	11/2001	10/2013
G.8101	Terms and definition for MPLS-TP	12/2006	09/2013
G.8110.1	Architecture of MPLS-TP Layer Network	11/2006	10/2012
G.8112	Interfaces for the MPLS-TP Hierarchy	10/2006	10/2012
G.8121	Characteristics of MPLS-TP Network Equipment Functional Blocks	03/2006	02/2012
G.8131	MPLS-TP linear Protection	02/2007	12/2012
G.8132	MPLS-TP Ring Protection	02/2008	12/2012
G.8151	Management aspects of the MPLS-TP network element	10/2007	12/2012
G.8152	Protocol-neutral management information model for the MPLS-TP	02/2008	12/2011
G.tpoam	Operation and maintenance mechanism for MPLS-TP layer networks	02/2011	11/2012
G.8080	Architecture for the automatically switched optical network	11/2001	02/2012

2.2 Fundamentos Operacionais do MPLS-TP

Como destacado anteriormente, o MPLS-TP é uma extensão do MPLS que o torna mais adequado para o emprego em redes de transporte. Portanto, antes de caracterizar em detalhes o funcionamento da tecnologia é preciso termos uma definição formal para o conceito.

Segundo [15], uma rede de transporte envolve o transporte e agregação confiável de qualquer tipo de tráfego, em qualquer escala e com o menor custo por bit. Dessa definição pode-se inferir que o conceito abrange quatro requisitos: escalabilidade, capacidade multisserviço, qualidade e boa relação custo/eficiência.

A escalabilidade deve garantir o suporte para qualquer volume de tráfego de clientes, do acesso ao núcleo, independentemente do tamanho da rede. Esse requisito pode ser atingido com o particionamento da rede, e a utilização de camadas.

Já a capacidade multisserviço possibilita a entrega de qualquer tipo de tráfego e a garantia de transparência de serviços. Dessa forma, a rede pode transportar serviços de qualquer camada.

Com relação à qualidade, a rede de transporte deve garantir que o tráfego seja entregue com confiança. Esse requisito exige que as redes sejam orientadas a conexão, e forneçam ferramentas OAM.

Finalmente, a rede de transporte deve fornecer boa relação custo/eficiência, utilizando operações simplificadas e protocolos de baixa complexidade, classicamente, protocolos de camada física e enlace.

Para ser capaz de fornecer o mesmo nível de previsibilidade e controle das tecnologias de transporte existentes o MPLS-TP, através de seu conjunto de normas e recomendações, prevê a implementação de um conjunto de melhorias e a exclusão de certas funcionalidades do MPLS incompatíveis com as aplicações de transporte. Enquadradas nesse último caso estão as funções de PHP, *label merging* e ECMP. Além disso, diferentemente da maioria das aplicações MPLS o MPLS-TP não assume conectividade IP entre os equipamentos da rede.

Figura 12 – Componentes da Padronização MPLS-TP **[16]**

As mudanças propostas podem ser divididas, conforme ilustra a Figura 12, em quatro componentes ou categorias: arquitetura de rede; plano de gerenciamento; plano de controle; e plano de dados que inclui as medias de proteção e restauração, ferramentas OAM, e finalmente o modo de enquadrar e encaminhar os dados.

2.2.1. Arquitetura de Rede

A arquitetura do MPLS-TP fornece o serviço de transporte de pacotes através de interfaces de serviço. Dependendo da aplicação é possível utilizar uma *User-Network Interface (*UNI) ou então uma *Network-Network Interface* (NNI).

A UNI pode ser uma interface de nível 2 que carrega apenas clientes da camada de rede, nesse caso a utilização dos LSPs é suficiente para o transporte dos pacotes. Há porém a alternativa de a UNI carregar também tráfegos de outras camadas, o que torna necessária a utilização de PWs para adaptar o tráfego recebido sobre a interface de serviço. Nesse caso, o PW torna-se um cliente da camada servidora MPLS-TP. Uma NNI fornece a ligação com outros LSPs ou PWs de outras redes que utilizam essas tecnologias. [20]

A Figura 13 mostra de forma genérica o processamento em uma interface de serviço. Quando o cliente envia dados para a rede provedora, os pacotes são desencapsulados de sua tecnologia específica, e associados a uma instância de serviço de transporte. Dessa forma, a rede de transporte pode encapsular o fluxo e mapeá-lo para um caminho de transporte pelo qual fará a transmissão. Já na situação oposta, quando o tráfego está destinado ao cliente, o procedimento é invertido, e ocorre o desencapsulamento e identificação da instância de serviço de transporte, para que o fluxo possa ser novamente encapsulado para a tecnologia utilizada pelo cliente.

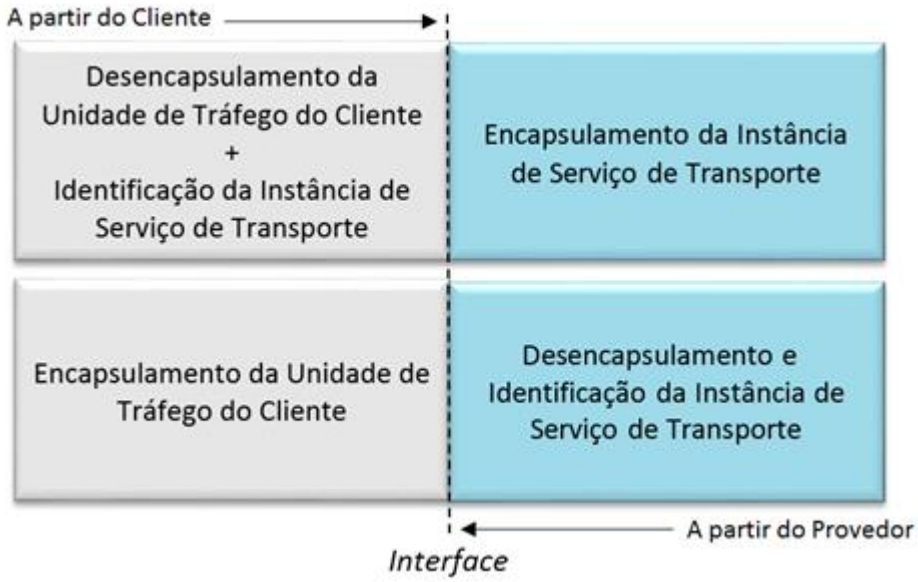

Figura 13 – Processamento na Interface de Serviço

O MPLS-TP não deve modificar a arquitetura de encaminhamento MPLS e deve portanto ter compatibilidade com os LSPs e PWs utilizados por essa tecnologia. As diferentes aplicações podem utilizar conexões *Point-to-Point*(P2P) e *Point-to-Multipoint* (P2MP), e os PWs podem ser, por sua vez, do tipo *Single-Segment Pseudowire* (SS-PW) ou *Multi-Segment Pseudowire* (MS-PW).

Entretanto, em adição à rede MPLS, os LSPs e PWs podem ser bidirecionais através da associação de dois caminhos unidirecionais fisicamente diferentes, ou então através de dois caminhos co-roteados e, portanto, fisicamente iguais em termos de nós e enlaces. Esse caso é o que tem maior similaridade com as redes de transporte.

A utilização de PWs pelo MPLS-TP o torna capaz de fornecer diversos tipos de serviços como: *Virtual Private Wire* (VPWS), *Virtual Private Local Area Network Service*(VPLS), *Virtual Private Multicast Service*(VPMS) e *Internet Protocol Local Area Network Service*(IPLS).

Uma característica fundamental da arquitetura MPLS-TP é permitir a configuração e provisionamento manual dos LSPs e PWs, de forma determinística e estática. Entretanto, a opção de provisionamento dinâmico através de um plano de controle também é possível.

A motivação chave para o provisionamento estático é eliminar o custo associado ao plano de controle dinâmico distribuído e integrado em cada nó, além de possibilitar que um NMS controle toda a rede em uma única aplicação centralizada. As duas configurações são ilustradas na Figura14.

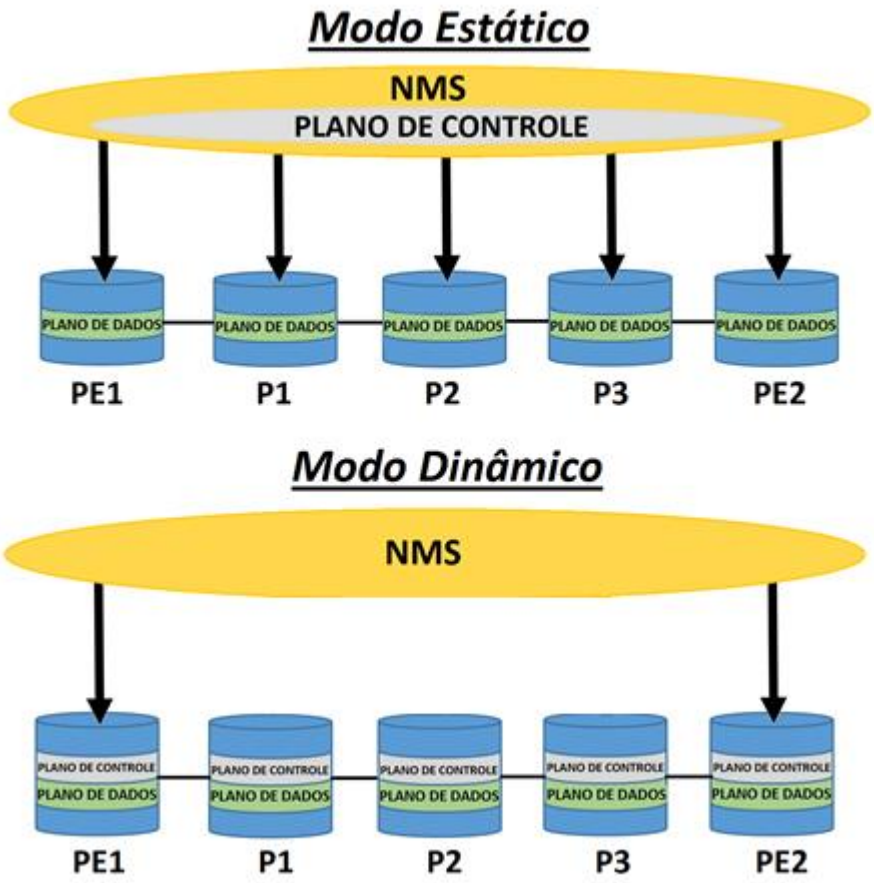

Figura 14 – Configuração Estática x Dinâmica **[17]**

A forma de implementação portanto depende do tipo de rede e dos interesses de cada operador. Pelas causas citadas anteriormente, a opção estática é indicada para porção de acesso e agregação das redes, já a opção dinâmica para a porção de núcleo. Os fornecedores de equipamentos em geral oferecem as duas opções.

Para uma rede MPLS-TP, conforme o RFC5921, adota-se além das denominações LSR e LER, os conceitos de *Provider*(P) para os LSRs localizados no interior das redes, e *Provider Edge*(PE) para os roteadores localizados nas bordas de um domínio MPLS-TP e que fornecem conexão com domínios clientes ou ainda com outros domínios MPLS-TP.

Um PE é responsável por adaptar e encapsular o tráfego dos clientes para que este seja transportado através de um LSP, de forma abstrata e independente da rede MPLS-TP. Dessa forma podem ser carregados serviços de diferentes níveis, como L1, L2 e L3.

O encapsulamento pode ser feito através da operação *push* que atribui o rótulo necessário aos pacotes, ou pode exigir o uso de um PW, nesse caso os roteadores são denominados *Pseudowire Switching Provider Edge* (S-PE) e *Pseudowire Terminating Provider Edge* (T-PE).

Um S-PE é capaz de comutar o plano de controle e o plano de dados de cada segmento de um SS-PW ou MS-PW para outros S-PEs, através da utilização de protocolos de configuração e gerenciamento. Os S-PEs são assim empregados nas porções da rede que requerem processamento de PWs, geralmente nas terminações de túneis das PSNs. Já os T-PEs estão presentes no primeiro e no último segmento de um MS-PW, e estabelecem os circuitos de ligação do cliente com uma PSN.

Na borda das redes clientes os roteadores são denominados *Client Edge* (CE). Sua função é garantir a conexão de sua rede com um domínio provedor, que possibilitará por sua vez a conexão com outros CEs pares a ele. Dessa forma a rede MPLS-TP pode ser vista pelo CE de forma transparente, como um único *link*, e assim possibilitar a emulação de serviços, como o transporte de pacotes. Deve-se observar que a rede cliente também pode ser uma rede MPLS-TP, de forma que o circuito de conexão seja feito através de LSPs.

Os elementos básicos de uma rede MPLS-TP citados acima são ilustrados na Figura 15. Na situação representada, é estabelecida a conexão entre duas redes clientes, através de CE1e CE2 para a emulação de um serviço sob a utilização de dois PWs. T-PE1 e T-PE2 promovem a conexão das redes dos clientes com nuvens MPLS-TP. Os dois domínios MPLS-TP são conectados através do S-PE e o fluxo de dados é transportado em túneis LSP com o encapsulamento dos segmentos dos PWs utilizados.

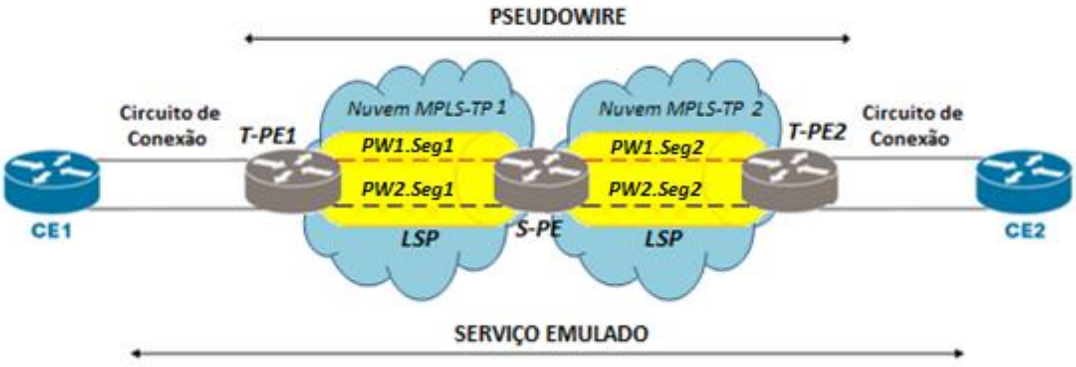

Figura 15 – Componentes da Arquitetura MPLS-TP **[14]**

Como definido anteriormente nesse capítulo, o MPLS-TP propõe a utilização de novas funções OAM para alcançar o grau de resiliência das redes de transporte TDM. Para tal, a componente de arquitetura do MPLS-TP prevê a utilização de pacotes OAM, que devem compartilhar a banda dos canais com os tráfegos normais de usuários (*in-band* OAM), e possibilitar assim o gerenciamento, diagnóstico e operação da rede na ausência de um plano de controle. A utilização dos pacotes OAM, podem ser feitas de maneira proativa ou sob demanda, dependendo da função implementa.

O monitoramento através das mensagens OAM é realizado entre múltiplos domínios pares baseado no conceito de Entidades de Monitoramento (MEs). Dessa forma, uma ME é constituída por uma associação de dois Pontos Finais de Monitoramento (MEPs). Os MEPs que formam um ME limitam as responsabilidades OAM dentro de seu

domínio, especificamente para camada de rede que está sendo monitorada.

Uma coleção de uma ou mais MEs que pertencem ao mesmo caminho e são mantidas e monitoradas de forma conjunta determinam um Grupo de Entidades de Monitoramento (MEG). Uma MEG pode também incluir um conjunto de Pontos Intermediários de Monitoramento (MIPs).

Para garantir a congruência entre os pacotes OAM e o caminho de dados, os pacotes OAM utilizam canais de controle em banda. Esse conceito consiste na marcação dos pacotes com um cabeçalho adicional, e foi introduzido pela primeira vez no contexto do MPLS com a utilização dos PWs através do *Associated Channel Header*(ACH), RFC 4485. O ACH indica a função OAM apropriada para processar o pacote identificado. No MPLS-TP esta ideia foi generalizada com o *Generic-Associated Channel* (G-ACh), para ser aplicada também a LSPs. Assim, o G-ACh é simplesmente um cabeçalho no pacote que fornece a função de discriminação para o manuseamento adequado de um pacote OAM. [18]

Antes, porém, da discriminação de função é preciso diferenciar os pacotes OAM dos pacotes normais do usuário. Para isso, é utilizado um rótulo reservado de valor 13, e denominado *G-ACh Label*(GAL). Assim, o uso do GAL permite a demultiplexação e a fácil extração dos pacotes OAM nos pontos finais de gerenciamento. [21] A Figura 16 mostra a estrutura de empilhamento de cabeçalhos em um quadro MPLS-TP, composto assim pelos seguintes campos:

- *Cebeçalho de Rótulo* – 32 bits – Cabeçalho utilizado pelo MPLS, composto pelo valor do rótulo, sua CoS que substituiu o campo EXP, a *flag* S que indica o topo da pilha hierárquica, e o campo de TTL. No caso de uma pilha hierárquica o quadro contém vários cabeçalhos de rótulos.

- *GAL* – 32 bits – Tem a mesma estrutura que o cabeçalho de rótulo, porém seu valor é reservado e igual a treze (13), sua posição é sempre logo em seguida ao rótulo no topo da pilha, em que S = 1.
- *G-ACh* – 32 bits – O G-ACh é composto por quarto campos: o *nibble* 0001 que indica a utilização do canal de controle, 4 bits que indicam a versão, a princípio igual a 0, 8 bits de reserva que não devem ser utilizados, e finalmente 16 bits com a codificação do tipo de canal e mensagem que está sendo enviada. Entre os possíveis tipos de canal estão: Canal de Comunicação de Dados (DCC), Canal de Comunicação de Sinalização (SCC) e Canal de Comunicação de Gerenciamento (MCC).
- *Mensagem OAM/ Dados do Usuário* – Informações da função OAM carregada, ou dos dados do usuário transportados pela rede.

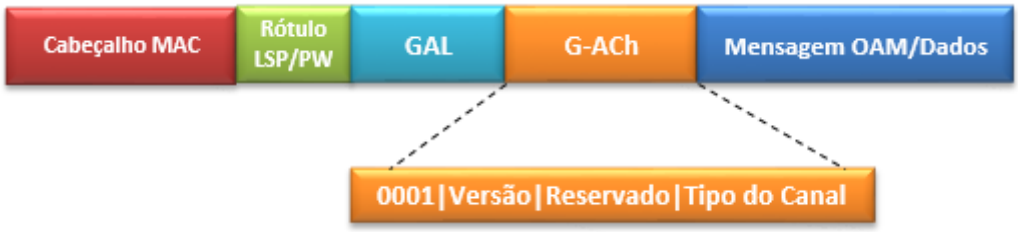

Figura 16 – Quadro MPLS-TP

Qualquer nó de um LSP ou PW pode enviar pacotes OAM, entretanto os pacotes só são recebidos para processamento nas extremidades dos caminhos pelos MEPs. O pacote só é processado por um MIP individual quando o TTL na entrada da pilha de rótulos expira. Por isso, para que um pacote seja destinado a este elemento deve-se conhecer sua localização e capacidade para executar mecanismos de *ping* ou *traceroute* para configurar precisamente o TTL.

2.2.2. Plano de Gerenciamento

O plano de gerenciamento (PG) engloba os protocolos e mecanismos que são utilizados para configurar e administrar a rede. No que diz respeito à

administração da rede o PG é responsável pelo monitoramento de falhas, performance e segurança da rede.

Já as configurações realizadas pelo PG englobam a configuração de funções básicas do sistema como o *clock*; a configuração das funções OAM e de proteção; a configuração do plano de controle; e por fim a configuração estática de LSPs e PWs através do NMS de modo semelhante à operação de redes SDH/SONET. Isso garante que os circuitos em operação continuem funcionando mesmo com uma interrupção ou falha no plano de controle.

A configuração de funções de proteção inclui a associação entre os caminhos ativos e os caminhos de proteção, e a definição do modo de proteção como manual ou automática, nesse último caso o PG também define o tempo de espera para restauração. Com relação às funções OAM, o PG escolhe as funções que estarão ativas, e então atribui cada uma delas à uma ME e define o modo de operação a ser feito de forma proativa ou sob demanda.

O monitoramento de falhas dentro de um elemento da rede permite supervisionar, detectar e corrigir operações anormais da rede MPLS-TP, com a utilização de alarmes. O monitoramento de desempenho realiza medidas de perda e atraso nos *links* e assim permite verificar se um serviço de transporte está indisponível.

O PG é distribuído entre vários componentes com capacidades e funções pré-definidas. Os componentes de menor nível englobam cada nó da rede (NE) e os Sistemas de Operações (SOs), que fornecem o intermédio entre as estações de gerenciamento e os NEs.

Dentro de cada NE o suporte para gestão é fornecido pela Função de Aplicação de Gestão (MAF), e a comunicação de gestão com os demais elementos da rede pela Função de Comunicação de Mensagens (MCF), através de MCCs implementados pelo G-ACh. A gestão da rede é

acessada através de um *Local Craft Terminal* (LCTs) conectado a um NE ou através de uma *Work Station* (WS) conectadas a um SO. [22]

2.2.3. Plano de Controle

O Plano de Controle (PC) é uma componente opcional no MPLS-TP e é responsável por estabelecer os LSPs e PWs de forma automática e rápida, através do uso de sinalização. Os protocolos e mecanismos são padronizados, o que garante grande interoperabilidade e menores despesas CAPEX. Eles englobam o Roteamento Baseado em Restrições(CBR), OSPF-TE, ISIS-TE, RSVP-TE, e o *Target*-LDP(T-LDP), versão do LDP adaptada para a utilização de PWs e com melhor orientação a conexão.

O PC também é responsável pelo fornecimento das funções OAM e pelas funções de proteção e de rápida restauração da rede em casos de falha. Quando falhas ocorrem é possível rapidamente acionar a restauração dinâmica. Sem um PC a recuperação requer intervenção do gerenciador de rede o que acaba sendo um processo lento. O PC permite ainda que os provedores utilizem recursos caros da rede com maior eficiência, atualizando automaticamente as mudanças na rede. [17]

O MPLS-TP reutiliza o PC do GMPLS ou seu equivalente ITU- T, *Automatically Switched Optical Network* (ASON) [G.8080] com algumas extensões, para permitir a utilização dos LSPs bidirecionais, o gerenciamento de falhas e controle *out-of-band*. Além da simplificação do gerenciamento da rede e a consequente redução das despesas OPEX e aumento da escalabilidade, o plano de controle GMPLS oferece recursos de restauração da rede, em adição aos recursos de proteção de rede que o plano de dados do MPLS-TP oferece. Isso resulta em uma rede com melhor resiliência [15].

O PC oferece recursos para garantir a sua própria sobrevivência e recuperação a partir de falhas e degradações. Isto inclui reinicialização e configurações redundantes. É, sempre que possível, dissociado do plano de dados de modo que as falhas no plano de controle não impactem o plano de dados e vice- versa.

Nas redes em que os PC e o PG são empregados, o provisionamento dos LSPs pode ser feito por ambos. Nessa situação, a rede deve então fornecer mecanismos para tornar possível a transferência de propriedade dos caminhos criados por cada entidade, para que uma possa utilizar e manipular os caminhos criados pela outra e vice e versa. Com relação também ao PG, o PC deve permitir o monitoramento de seu status e log para lhe fornecer acesso holístico sobre a disponibilidade de recursos, independentemente de ter seu funcionamento *out-of-band* com relação ao mesmo. [23]

É importante notar que pode haver independência no PC para os PWs e os LSPs. Dessa forma, é possível que uma rede utilize um PC somente para o provisionamento dos PWs, mas que os LSPs sejam provisionados estaticamente, bem como é possível o caso oposto.

2.2.4. Plano de Dados

O Plano de Dados (PD) engloba os protocolos e mecanismos que são utilizados para encaminhar os pacotes de dados e as informações *in-band* de gerenciamento e controle. Eles podem ser divididos em três categorias: funções de resiliência, funções OAM e de encaminhamento.

2.2.4.1. Resiliência

A resiliência ou sobrevivência da rede é a capacidade de uma rede de recuperar a entrega de tráfego após falha ou degradação dos recursos

de rede. Para a norma MPLS-TP, o tempo de restauração não deve ultrapassar 50ms. A sobrevivência é crítica para redes com garantia de serviços, sujeitas a rigorosos Acordos de Nível de Serviço (SLAs), que colocam limites máximos para o período de tempo que os serviços podem ficar indisponíveis.

A sobrevivência é conseguida através da implementação de mecanismos específicos de proteção ou restauração, que visam reparar os recursos da rede ou redirecionar o tráfego por outros caminhos. Ambos os mecanismos podem ser unidirecionais ou bidirecionais.

Na comutação de proteção, *Automatic Protection Switching* (APS), em condições normais o tráfego de dados é transmitido através da entidade de trabalho, enquanto uma entidade de proteção permanece em estado ocioso. Se ocorrer uma falha ou algum pedido administrativo, o tráfego é comutado para a entidade de proteção. Na proteção dedicada 1:1 ou 1+1, os recursos para a entidade de recuperação são pré-estabelecidos para uso exclusivo do caminho de transporte protegido. Já na proteção compartilhada 1:n ou m:n, os recursos para as entidades de recuperação são compartilhados entre vários serviços. A comutação de proteção pode ainda utilizar topologia linear, ou em anel.

A proteção linear é rápida e simples, e é empregada em redes de malha, que possuem interconectividade arbitrária entre os nós, podendo atuar entre qualquer par de pontos dentro da rede. A proteção abrange falhas em nós intermediários, intervalos, segmentos de caminho de transporte, e em caminhos fim-a-fim.

As topologias em anel são importantes já que as redes de circuito são tipicamente construídas através de anéis interligados, e espera-se que muitas implementações iniciais da MPLS- TP sejam feitas com

substituições pontuais dos antigos equipamentos. [16] A Figura 17 ilustra uma topologia de proteção MPLS-TP em anel.

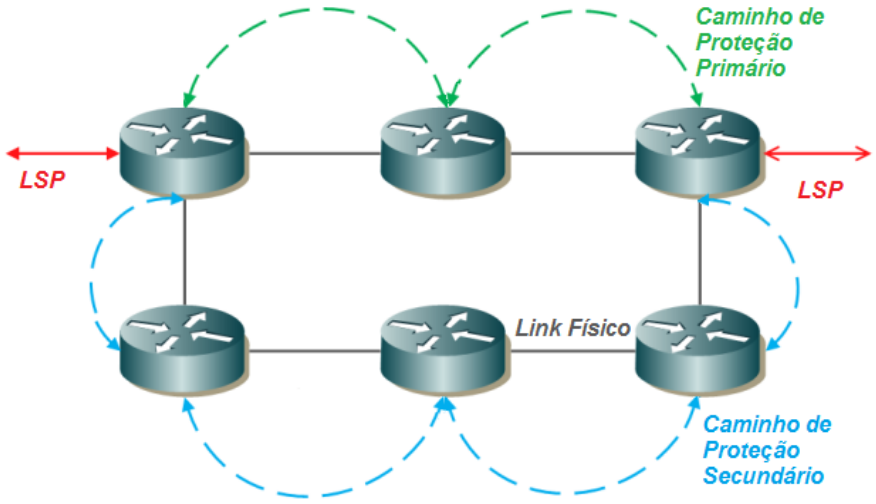

Figura 17 – Topologia de Proteção em Anel

O mecanismo de restauração utiliza qualquer capacidade disponível entre os nós e, geralmente, envolve reencaminhamento. Os recursos utilizados para a restauração podem também serem pré-determinados mas não são especificamente atribuídos à recuperação.

A técnica de restauração representa o uso mais eficiente dos recursos da rede, uma vez que os recursos não são reservados para a recuperação. No entanto, a restauração requer o cálculo de um novo caminho e a ativação de um novo LSP, o que pode consumir mais tempo de execução do que a recuperação usando técnicas de proteção. Fora isso, não há qualquer garantia de que a recuperação será possível, pois todos os recursos de rede adequados podem já estar em uso por outros LSPs, de modo que nenhum novo caminho possa ser encontrado.

Além disso, quando ocorre uma falha de rede, vários LSPs podem ser interrompidos por um mesmo evento, e se tiverem sido estabelecidos por diferentes estações de gerenciamento, teremos múltiplos pontos da rede tentando calcular e estabelecer a recuperação de seus LSPs

ao mesmo tempo. Isto pode levar a uma falta de recursos, e tempos de recuperação ainda mais lentos para alguns serviços.

Depois de um serviço ter sido recuperado e o tráfego estiver fluindo ao longo do LSP de recuperação, o recurso de rede defeituoso pode ser substituído. O tráfego pode, assim, ser redirecionado de volta para o LSP de trabalho original com o mecanismo de reversão, ou pode ser deixado no caminho de recuperação de modo que o caminho de trabalho anterior seja usado para recuperação.

No modo de reversão, é importante evitar a excessiva troca de caminhos de recuperação no caso de uma falha intermitente. Isso é resolvido por meio de um temporizador de atraso de reversão, denominado *Wait-To-Recovery* (WTR), que controla a duração do tempo de espera antes da reversão, após a reparação de uma falha. Deve ser possível a um operador configurar este temporizador para cada LSP, além de definir um valor padrão.

A comutação de proteção bidirecional requer a coordenação entre os dois pontos finais para determinar qual dos dois caminhos, de trabalho ou de proteção, está transmitindo o tráfego de dados. Quando a comutação de proteção é acionada, os pontos finais devem informar-se mutuamente sobre a mudança através do protocolo *Protection State Coordination* (PSC).

As ações de recuperação podem ser iniciadas pela detecção de uma falha, ou pela solicitação de uma fonte externa, como o pedido de um operador para o controle manual. O operador pode estabelecer políticas de proteção gerais para toda a rede ou políticas locais que determinam as ações que serão tomadas quando falhas forem detectadas. Em algumas circunstâncias, a falha pode ser comunicada ao operador, e o operador pode então selecionar e iniciar a ação de recuperação adequada. O operador também pode emitir comandos para ativar ou desativar a função de sobrevivência, invocar a

simulação de uma falha de rede, forçar uma transição a partir de um caminho de trabalho para um caminho de recuperação, e vice-versa, para fins de otimização de rede. [24]

Caso existente, o PC pode ser utilizado para a capacidade de sobrevivência, através da utilização do *Link Management Protocol* (LMP) que testa a continuidade e conectividade em cada *link*.

2.2.4.2. OAM

As funcionalidades OAM são o grande diferencial do MPLS-TP em relação ao MPLS. O legado das redes de transportes tradicionais utiliza ferramentas extensas e bem estabelecidas para monitorar e gerenciar a rede, através de SLAs. Assim, para poder ser aplicado nessas redes os equipamentos MPLS-TP devem oferecer mecanismos de gerenciamento equivalentes.

O novo protocolo define novos mecanismos de manutenção, novas funções de gerenciamento de falhas e o monitoramento de performance nos enlaces. Para tanto, as ferramentas de BFD, LSP *ping* e LSP *traceroute* são estendidas pelo MPLS-TP. Os alarmes de falhas podem ser gerados pelos pontos finais através da Indicação Remota de Defeito (RDI) ou pelo próprio cliente através de Indicação de Falha do Cliente (CFI).

A utilização de *pseudowires* bidirecionais sobre LSPs, permite o monitoramento OAM otimizado através do BFD com o fim de detectar e localizar possíveis falhas nos enlaces e equipamentos da rede. São implementados assim os mecanismos de Checagem de Continuidade (CC) e Verificação de Conectividade (CV). Na ausência de resposta de três mensagens CC consecutivas, uma condição de falha é declarada, e o tráfego poderá ser então transferido para um caminho de proteção.

A escolha do tempo de intervalo entre mensagens CC é uma decisão de projeto. Um intervalo mais curto, torna mais rápido o tempo de detecção de falhas, mas utiliza mais recursos. O valor adequado depende da aplicação e as necessidades de serviço, bem como o mecanismo de proteção previsto na camada inferior. Geralmente o tempo é inferior a 10ms. [25]

O BFD funciona da seguinte maneira: os dispositivos em ambas as extremidades de cada LSP enviam pacotes BFD pelo caminho, com intervalos muito curtos. Assim, caso o intervalo entre os pacotes BFD recebidos por um nó estiver acima de um certo limite pré-estabelecido, um alarme é gerado para o serviço que utiliza aquele LSP específico. O problema identificado é relatado no conteúdo do pacote BFD que o nó transmite. Quando um dispositivo recebe um pacote BFD com algum problema relatado, ele também repassa um alarme para aquele caminho. [26]

São definidos três tipos de notificações, utilizadas pela camada física servidora para alertar possíveis falhas à camada MPLS-TP. São eles: Sinal de Indicação de Alarme(AIS), Indicação de link Inativo (LDI) e Notificação de Bloqueio (LKR).

As mensagens são enviadas a partir de um MEP da camada servidora onde os LSPs são cruzados para uma MEP MPLS-TP, em direção contrária à falha, como mostra a Figura 18. Quando um MEP MPLS-TP recebe uma notificação de falha, ele repassa mensagens para cada um dos LSPs configurados ou sinalizados por ele.

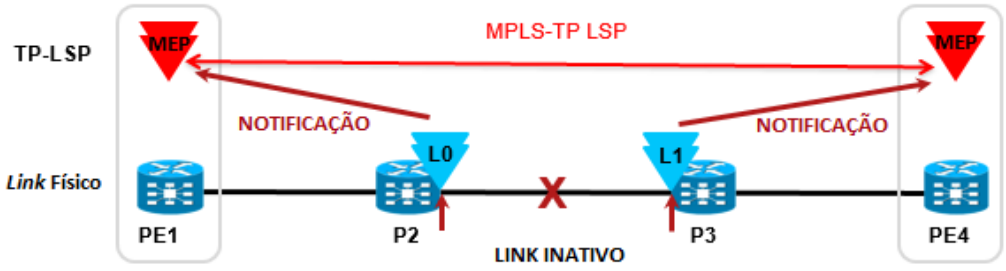

Figura 18 – Notificação de Falha em um Link

O AIS é utilizado quando ocorre uma falha transitória na camada do servidor, por exemplo, durante uma mudança de proteção. Esse tipo de notificação não deve ser enviada se a camada servidora está inativa, para isso uma LDI deve ser enviada. Uma LDI é enviada portanto sempre que a camada servidora entra em estado inativo. A LKR indica que o túnel ou ligação foi administrativamente bloqueada e não está disponível para transportar o tráfego do cliente.

Quando uma AIS ou LDI é recebida por um MEP, e ocorreu uma falha na CC os alarmes são suprimidos. Caso não tenha ocorrido falha na CC, isto é o BFD está em estado ativo ele é posto em estado negativo.

As novas funções OAM MPLS-TP também abrangem importantes mecanismos que são executados sob demanda do operador de rede, como a função de *Loopback* e *Lock*.

A função *Lock* é utilizada para solicitar que um MEP coloque determinado LSP fora de serviço, situação em que apenas testes e tráfego OAM podem ser enviados. O comando de bloqueio, *Lock Report* (LKR), deve ser enviado para o PE em ambas as extremidades do caminho, para garantir que nenhum tráfego seja enviado em qualquer direção.

A função de *Loopback* faz com que determinado nó em um LSP retorne todos os dados que recebe. O *Loopback* pode ser executado por um MEP, para testar a integridade do percurso de transporte a partir e para o nó em análise. O MEP portanto deve enviar dados de teste para um MIP, ou nó de um LSP em análise, e em seguida comparar com os dados que receber de volta. Durante a execução dessa função, o caminho deve permanecer bloqueado.

Os mecanismos OAM adotadas no MPLS -TP estão resumidas na Tabela3, e incluem a detecção e localização de falhas, e o monitoramentos de performance. [27]

Tabela 3 – Melhorias OAM do MPLS-TP **[16]**

Função OAM	***Sub-Função***	***Objetivo***	***Ferramenta Utilizada***
Gerenciamento de Falhas	Checagem de Continuidade (CC)	Utilização do BFD para fornecer rápida identificação de falhas.	Extensão BFD Extensão LSP Ping
	Verificação de Conectividade (CV)	Permitir localização sob demanda da falta após a detecção pela CC.	Extensão BFD Extensão LSP Ping
	Loopback	Permitir que um operador coloque um LSP em modo de *loopback* em situações de teste e medições.	Mensagem in-band pelo GACh ou Extensão LSP Ping
	Lock	Permitir um operador a colocar um LSP fora de serviço. Utiliza notificação *Lock Report* (LKR).	Mensagem in-band no GACh ou Extensão LSP Ping
	Indicação Remota de Defeito (RDI)	Utilizado pelos pontos finais para notificar defeitos através de um Sinal de Indicação de Alarme (AIS).	Extensão BFD
	Indicação de Falha do Cliente (CFI)	Permite o envio de informações a respeito de falhas de um cliente.	Extensão BFD
Monitoramento de Performance	Medição de Atraso	Permitir a medição de atraso no envio dos pacotes em um caminho.	Nova Ferramenta DM
	Medição de Perda	Permitir a medição de perda em um caminho.	Nova Ferramenta LM
	Medição de Débito	Permitir a medição de débito em um caminho.	Nova Ferramenta TM
	Medição de Variação de Atraso	Permitir a medição de variação de atraso em um caminho.	Nova Ferramenta DM

2.2.4.3. Encaminhamento

O Plano de Encaminhamento do MPLS-TP utiliza o mesmo plano de encaminhamento do MPLS, porém com algumas restrições já citadas como o PHP e O ECMP. Ele é responsável em encapsular os pacotes com os devidos cabeçalhos MPLS-TP e então encaminha-los pelos LSPs e PWs definidos para cada um.

Um pacote MPLS-TP pode ser considerado um pacote MPLS. Dessa forma, ele também possui uma pilha de rótulos associados, e pode ser processado pelas funções de *swap*, *push* e *pop*. Quando o TTL de algum dos rótulos da pilha expira, o rótulo no topo da pilha é inspecionado. Caso carregue um valor reservado, o pacote é processado de acordo com as regras pré-estabelecidas para sua operação. Esse é o mecanismo utilizado pelo GAL que tem reservado o valor 13 [28].

Como síntese desse capítulo, a Figura 19 ilustra uma contraposição entre os principais mecanismos adotados pelo MPLS-TP versus os mecanismos utilizados pelo MPLS baseado no protocolo IP.

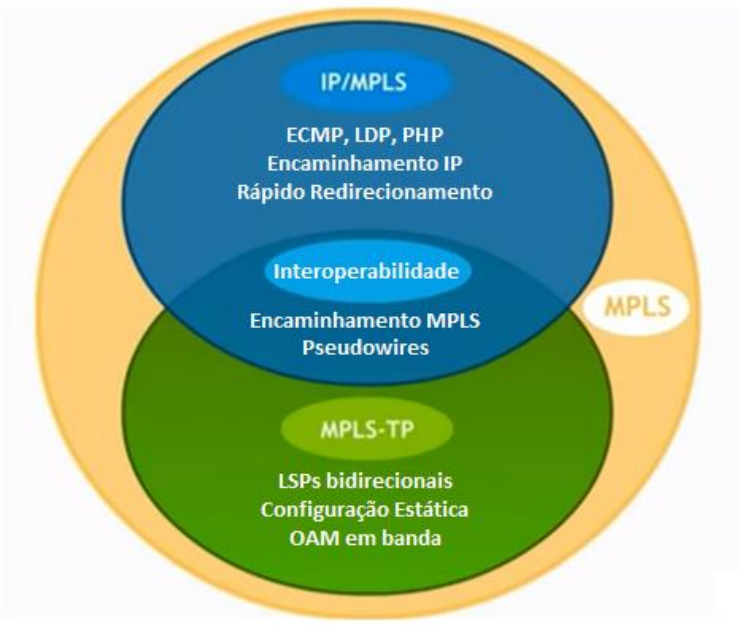

Figura 19 – Características MPLS-TP x IP/MPLS **[19]**

3 Estudo de Aplicações MPLS-TP

Seis anos após os primeiros desenvolvimentos, as bases do padrão MPLS-TP estão completas e vários desenvolvedores de equipamento de rede já lançaram soluções no mercado. Durante esses anos, diversos debates também foram feitos entre provedores de serviço de todo o mundo e, muitos escolheram adotar a tecnologia para sua próxima geração de redes de transporte.

Uma pesquisa realizada pelo Heavy Reading com um grande número de profissionais do segmento indica que uma grande parcela acredita que o MPLS-TP pode impactar na *Next Generation Network* (NGN). Dois terços dos 183 entrevistados afirmaram que esperavam ver um grande número de implementações MPLS-TP até o final de 2013 [17].

As fornecedoras Cisco e Ericsson apostam em implementações de arquiteturas que combinem os mais recentes desenvolvimentos acerca do IP/MPLS e do MPLS-TP para possibilitar soluções MPLS fim-a-fim altamente escaláveis e simplificadas, com sua implementação em todos os domínios de uma NGN. Tais arquiteturas podem ser divididas em dois domínios: a rede de acesso e agregação e as redes de núcleo [17].

Essa estratégia de criação de uma solução MPLS unificada, do núcleo até as redes de agregação e acesso é tida como atraente para muitos provedores, que poderão ter maior capacidade de suporte a serviços geradores de receita. Fora

isso, ela simplifica o funcionamento, reduz a complexidade global e melhora a convergência fim-a-fim tornando-se economicamente eficiente e confiável.

Essa infraestrutura MPLS comum, portanto, visa aplicar os dois perfis MPLS com base nas necessidades de cada cenário de implantação, e requer a utilização de sinalização adequada para interligar domínios estáticos MPLS-TP com domínios dinâmicos IP/MPLS, que deverão trabalhar de forma conjunta e transparente.

Assim, para implantação de uma solução MPLS fim-a-fim, é necessário garantir a consistência fim-a-fim das funções OAM. Entretanto, os equipamentos IP/MPLS já empregados no núcleo ainda não estão atualizados com as novas funcionalidades OAM provindas do MPLS-TP. Uma boa alternativa então é estabelecer tunelamento por LSPs MPLS-TP na rede IP/MPLS. Dessa forma, as funções OAM são executadas em túneis no núcleo, e as extremidades relatam os problemas em detalhes para os MIPs ao longo dos LSPs MPLS-TP.

Nota-se que ao longo do tempo, espera-se que roteadores de núcleo MPLS/IP sejam atualizados para suportar totalmente as características OAM provindas do MPLS-TP. Uma vez que isso tenha ocorrido, será possível executar LSPs MPLS-TP fim-a-fim através do núcleo [25].

Vários testes públicos foram realizados nos últimos anos para demonstrar a viabilidade da tecnologia e validar as soluções de cada fabricante. Foram testados os desempenhos dos equipamentos MPLS-TP, bem como sua interoperabilidade com equipamentos MPLS.

A interoperabilidade entre equipamentos de diferentes fabricantes, também tem sido alvo de muitos testes, pois pelo fato de algumas das especificações do padrão terem sido atualizadas ao longo do processo de normalização, podem haver algumas diferenças entre fornecedores que começaram a desenvolver seus produtos mais cedo e aqueles que começaram mais tarde.

A IXIA, uma importante fornecedora de sistemas de teste e verificação, desenvolveu um conjunto de *benchmarks*, para que os provedores de serviço

avaliem o desempenho do MPLS-TP, e obtenham informações essenciais para acelerar o investimento e implantação na tecnologia. As análises avaliam as possíveis limitações de desempenho e escalabilidade, a fim de melhorar o planejamento e configuração das redes. Esse *benchmarks* estão resumidos na Tabela 4.

Tabela 4 – Benchmarks IXIA

Requisito	**Medida de Desempenho**
Escalabilidade de Serviço	Quantidade de LSPs e PWs suportados por porta, cartão e sistema.
Qualidade de Serviço	Quantidade de níveis de serviços suportados para cumprir os SLAs.
Desempenho de Tráfego	Desempenho de encaminhamento em alta escala, incluindo latência e variações de atraso com vários tamanhos de pacotes.
Gerenciamento	Provisionamento estático e dinâmico em altas escalas; E suporte às funções OAM.
OAM	Teste com o conjunto completo de funções sobre dezenas a milhares de LSPs e PWs; Capacidade OAM fim-a-fim sobre múltiplos segmentos, alguns configurados de forma estática e outros de forma dinâmica.
Resiliência	Trocas de proteção para dezenas a milhares de LSPs com recuperação <50ms.

Em março de 2011, um teste da operadora Verizon validou o tempo de recuperação <50 ms e as funções OAM de gerenciamento de falhas, através de LSPs estaticamente configurados. O experimento utilizou equipamentos CPT

600s da Cisco em topologia de anel, com o equipamento de testes da IXIA, conforme Figura 20. O tempo de recuperação conseguido foi de 16 ms.

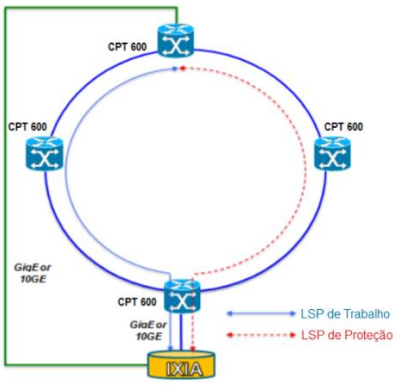

Figura 20 – Teste Verizon - Resiliência [29]

Importantes testes de interoperabilidade estão sendo desenvolvidos anualmente liderados pela empresa americana ISOCORE, atrelada a Conferência Anual MPLS/SDN, e também pela empresa alemã EANTC, com resultados apresentados no Congresso Mundial MPLS e Ethernet.

O teste realizado pela ISOCORE em 2010, empregou equipamentos *Cisco ASR 9000/7600, Ericsson SE1200, Ixia XM2, Hitachi AMN 1700 e NEC CX2800*, conforme ilustra a Figura 21. Foram estabelecidos LSPs bidirecionais estáticos com proteção Linear 1:1. O teste verificou o funcionamento das funções de CC, BFD e LSP Ping, a interoperabilidade MPLS e MPLS-TP utilizando PWs estáticos e dinâmicos e, por fim, o status de um serviço Ethernet fim-a-fim entregue pela rede MPLS-TP/MPLS.

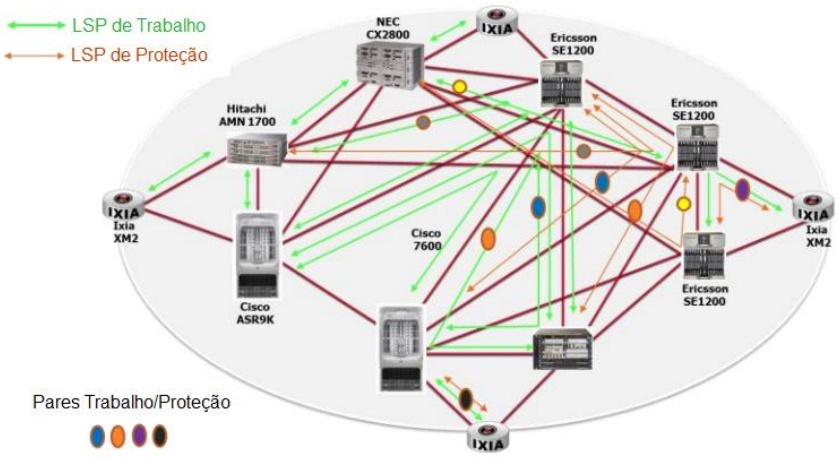

Figura 21 – Isocore: MPLS 2010 Public Interoperability Test Results [30]

Um outro teste realizado pela EANTC em 2012, testou os tempos de recuperação de falhas e também o tempo de retorno do caminho de proteção para o caminho de trabalho. Foram utilizados equipamentos *Cisco ASR 9006, Ericsson MINI-LINK SP 310, SE100 e SPO1410* e *Hitachi AMN 1710*. Também foram empregados geradores de falhas intermediários em cada LSP de trabalho com equipamentos *Calnex Paragon-X, IXIA ImpairNet* e *Spirent XGEN,* conforme mostra a Figura 22. Durante os testes, ocorreu falha de interoperabilidade com o *Ericson SPO1410* e um equipamento MPLS-TP não reverteu do caminho de proteção. Os tempos de envio de mensagens de verificação foram variados de 3,33ms até 100ms.

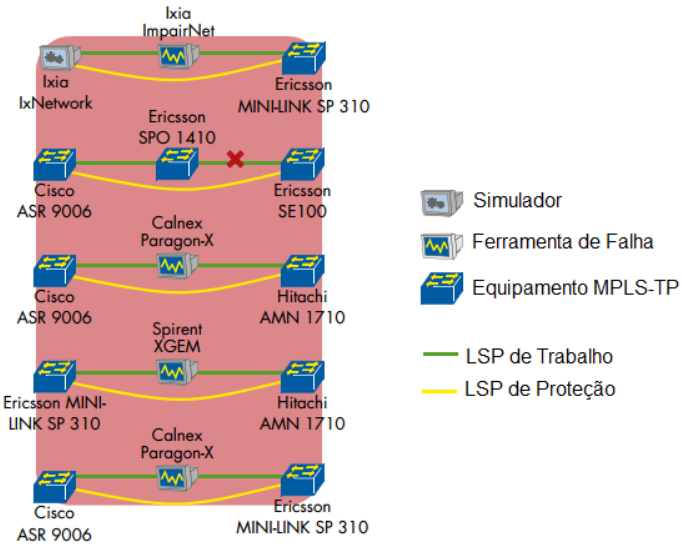

Figura 22 – EANTC: Puclib Multi-Vendor Interoperability Event 2012 [31]

As aplicações de maior destaque do MPLS-TP englobam: a substituição de equipamentos TDM em redes de acesso e agregação; o *backhaul* de serviços de telefonia móvel; e o emprego dinâmico sobre redes OTN / WDM.

Em geral a aplicação do MPLS-TP é muito importante em redes de serviços públicos, que estão cada vez mais voltadas para as tecnologias de pacotes. Através de seu plano de gestão e controle centralizado o MPLS-TP possibilita a aplicação de importantes normas de segurança contra potenciais ataques. Uma vez que muitas vulnerabilidades das redes são exploradas por ataques TCP/IP, uma rede MPLS-TP pode reduzir o perfil de risco de redes críticas.

3.1 Migração de Redes de Acesso e Agregação

A utilização do MPLS-TP para as redes de acesso e agregação é o cenário de aplicação mais comum observado pelo mercado. Nessas redes estão acontecendo a maioria dos esforços para migração de redes comutadas por circuitos TDM e ATM para redes baseadas em pacotes, devido a necessidade de maior escalabilidade e menor custo e complexidade [16]. Um esquema para o emprego do MPLS-TP nas redes de agregação é dado pela Figura 23.

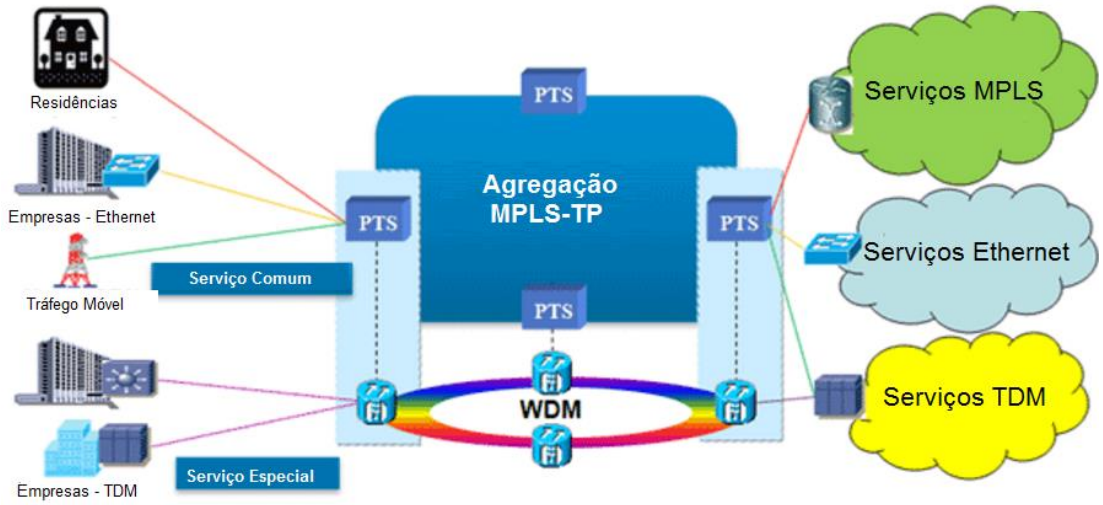

Figura 23 – Rede de Agregação MPLS-TP [17]

Algumas operadoras estão construindo infraestruturas *green-field*, ou seja sem considerar tecnologias e equipamentos anteriores, enquanto outros estão atualizando ou substituindo sua atual infraestrutura de transporte com as novas tecnologias baseadas em pacotes de maneira gradual [25].

A principal motivação dessa migração é o fato das tecnologias de legado ATM e TDM estarem se tornando insuficientes para atender as novas e aceleradas demandas por aplicações baseadas em pacotes. Nesse novo cenário multiplexação estatística é mais apropriada. Além disso, em muitos casos, os dispositivos desse legado estão aos poucos parando de ser fabricados.

Os requisitos dos provedores de serviço para a substituição dos equipamentos ATM e TDM na agregação englobam: apoio à rede de acesso existente, como

Ethernet, ADSL, ATM e TDM; e a continuidade de serviços geradores de receita, que incluem: L3VPN, L2VPN, E-LINE/E-LAN/E-VLAN, e Linha Dedicada.
Estender a tecnologia MPLS para as redes de agregação e acesso é uma estratégia atraente, pelo fato de as redes de núcleo dos prestadores de serviços em sua maioria serem baseadas em MPLS tradicional. Fora isso, o conjunto de ferramentas OAM e mecanismos de proteção do MPLS-TP ajudam a manter a alta confiabilidade das redes de transporte e alcançar baixos tempos de recuperação.

A adoção da tecnologia é adequada para as redes de acesso e agregação principalmente por sua previsibilidade e escalabilidade. A previsibilidade dos caminhos reduz significativamente as despesas operacionais associadas à solução de problemas e falhas em redes de grande tamanho. Já a preocupação com a escalabilidade deve-se ao fato de as redes de acesso e agregação geralmente possuírem milhares de nós, o que demanda um protocolo e arquitetura de rede que possam ser utilizados em larga escala sem aumentar significativamente a complexidade da rede.

As redes de transporte existentes são geralmente controladas por um plano de gerenciamento. Dessa forma, a adoção de equipamentos MPLS-TP pode oferecer uma outra vantagem competitiva, já que a tecnologia reutiliza o modelo de operação das rede de transportes para a configuração de LSPs e gerenciamento de falhas. Isso permite que os provedores utilizem suas técnicas já consolidadas durante a migração para redes de transporte de pacotes [25].

Os padrões IETF apoiam implementações MPLS-TP que suportem os dos dois modos de configuração de LSPs e PWs através dos planos de gerenciamento e controle. Mesmo que uma implementação MPLS-TP inicialmente não exija um plano de controle, ele pode ser adicionado para fornecer mais opções para aplicações futuras e que exijam maior escalabilidade em termos de trabalho operacional, e assim com economias OPEX e também com padrões de tráfego menos previsíveis.

A fornecedora *Metaswitch* argumenta que o plano de controle permite que as operadoras utilizem recursos caros de rede de forma mais eficiente, através da atualização automática sobre as alterações na rede. O plano de controle pode reduzir o tempo de provisionamento sob demanda, para apoiar novas oportunidades e serviços de receita para as operadoras, como banda larga sob demanda [17].

3.2 *Backhaul* de Redes Móveis

A comunicação sem fio é uma das áreas que mais crescem no campo das telecomunicações em todo o mundo. Em algumas regiões, o enorme crescimento móvel é alimentado pela falta de linhas telefônicas fixas e infraestrutura de cabos. Em outras regiões, a introdução de *smartphones* está fazendo o tráfego de dados móveis crescer rapidamente e dominar o consumo de largura de banda [25].

O *backhaul* de redes móveis é tido como uma das principais aplicações iniciais do MPLS-TP. A razão disso é a similaridade entre os modelos operacionais utilizado pela tecnologia e pelas operadoras de telefonia móvel. Atualmente, as plataformas TDM ainda dominam a maioria das atuais infraestruturas de *backhaul* 2G/3G, em que as conexões são P2P e formam topologias de estrela ou de anel. [17]

O MPLS-TP permite que as operadoras implementem dispositivos simples e de baixo custo em suas células para lidar com vários tipos de tráfego e com múltiplas classes de serviço. Além disso, a tecnologia é capaz de simplificar o provisionamento de serviços e aumentar a resiliência da rede através de múltiplas opções de proteção.

As redes de *backhaul* geralmente são operadas por equipes de transporte e têm pouca diversidade de caminhos, o que elimina a necessidade de grandes buscas em tabelas de encaminhamento. O MPLS-TP fornece uma solução simples, de alto custo-benefício a ser empregada pela base da NGN. Essa base poderá

incluir uma *Multiservice Provisioning Platform* (MSPP), que está implementada atualmente para apoiar o *backhaul* 3G, e que poderá conformar os padrões MPLS-TP para interoperar com as mais recentes plataformas *Carrier Ethernet* que estão sendo implantadas para suportar ligações de banda larga em redes 3G e 4G. O MPLS-TP permite assim uma transição suave das atuais redes de *backhaul* 3G, com capacidade de transporte de tráfegos multisserviço e apoio aos requisitos 4G, como VPLS hierárquicas [17].

Através da *Radio Access Network* (RAN) 3G, cada dispositivo móvel comunica-se com uma *Base Transceiver Station* (BTS) que por sua vez redireciona o tráfego para uma *Base Station Control* (BSC) através da rede de *backhaul* com conexões definidas quase sempre estaticamente, conforme ilustra a Figura 24. Arquiteturas hierárquicas ou centralizadas são frequentemente utilizadas nas camadas de agregação, que interligam-se com várias redes de acesso. [25]

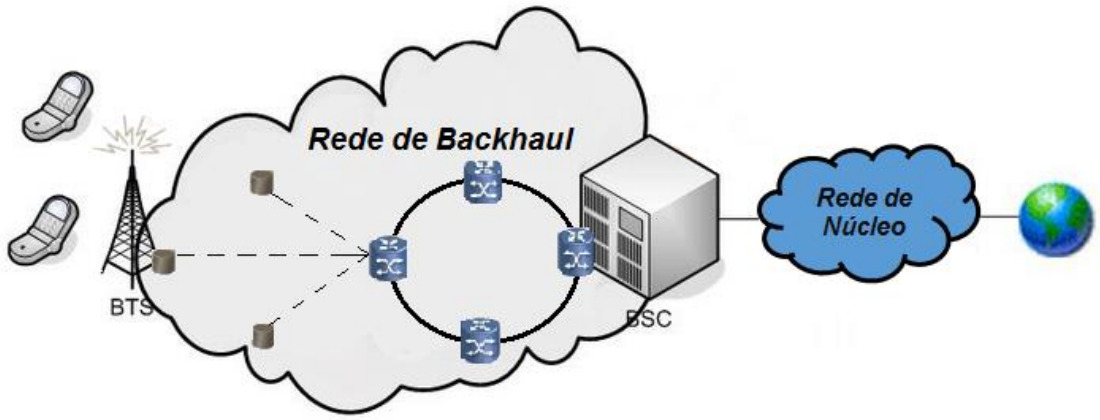

Figura 24 – Rede Backhaul 3G

A tecnologia ATM ainda domina a arquitetura de *backhaul*, mas muitos operadores já estão em fase de transição para tecnologias mais adaptadas ao tráfego de pacotes. Redes IP/MPLS já estão sendo utilizadas com grande sucesso por muitos provedores de serviço. Recentemente, porém, com o início da consolidação da tecnologia MPLS-TP pelo mercado sua implementação nessas redes também tem sido muito encorajada.

A nova tecnologia permite uma transição mais eficiente e linear das redes, já que

sua gestão em modo estático assemelha-se com a gestão das atuais redes ATM. Fora isso, sua natureza determinística fornece suporte à sincronização de pacotes através de protocolos *Time and Frequency Synchronization* (TFS) para manter a previsibilidade de desempenho em relação ao atraso de pacotes [25].

A tecnologia pode ainda oferecer uma série de vantagens em relação ao MPLS tradicional. A utilização de *in-band* OAM fornece caminhos de proteção determinísticos e permite rápida detecção de falhas para satisfazer SLAs, enquanto que os LSPs bidirecionais ajudam a simplificar o processo de provisionamento.

Redes mais modernas baseadas em *Long Term Evolution*(LTE) e 4G utilizam topologias de malha, diferentemente das redes 3G. Cada BTS comunica-se com múltiplos controladores de rede, e também pode comunicar-se diretamente com outras BTS [25].

IP/MPLS tem uma grande vantagem em relação a conectividade em ambientes de malha. Dessa forma, a aplicação de tecnologias IP e L3VPNs é comum no planejamento de implementações de redes LTE. Em um cenário de malha, o plano de controle dinâmico do GMPLS é adequado para a implementação do MPLS-TP, para suportar as mudanças na topologia de forma dinâmica.

Alguns operadores entretanto estão usando o mesmo modelo de *backhaul* das redes 2G e 3G, com o IP/MPLS no núcleo e o MPLS-TP com provisionamento estático na agregação e acesso. Isso acontece porque atualmente, a carga de tráfego nas interfaces X2, entre BTS em redes LTE, representa uma porcentagem muito pequena do tráfego total. Por isso, uma decisão de projeto pode ser transportar o tráfego X2 através dos mesmos túneis estáticos das redes de agregação e acesso, juntamente com tráfego das interfaces S1, entre as BTS e o núcleo das redes, que realizará o encaminhado [25].

Além disso, a proteção em malha apesar de utilizar a largura de banda de modo mais eficiente, é considerada mais complexa sob o ponto de vista de operação e manutenção, quando comparada à proteção linear e em anel.

Em geral, aplicar o MPLS-TP com provisionamento estático para o *backhaul* LTE é uma opção viável. O objetivo dessa abordagem é manter a operação simples e utilizar um modelo comum para *backhaul* móvel, especialmente durante o período de transição das redes, já que é inevitável a coexistência de tráfego TDM e ATM em redes 3G e 4G, tendo em vista o rápido crescimento de serviços de banda larga móvel [25].

A operadora Bharti Airtel foi umas das primeiras a implementar uma solução MPLS-TP fim-a-fim para *backhaul* móvel. Ela está implantando funcionalidade MPLS-TP com equipamentos ECI nas camadas de acesso e agregação com suporte para Ethernet PW [17].

Como citado anteriormente, o *backhaul* de tráfego móvel pode exigir sincronização de transmissão. Entretanto o MPLS-TP bem como os demais protocolos de rede baseados em pacotes são de natureza assíncrona. Por isso, para implementação de infraestruturas baseada nessa tecnologia, é necessária a utilização de alguns mecanismos para fornecer as devidas referências de relógio à rede. Três possíveis abordagens para tal são: a utilização de uma rede de cobertura de sincronização em paralelo à rede de pacotes; a distribuição da referência de *clock* através das bordas da rede; e por fim, o encaminhamento da referência de *clock* pela própria rede de pacotes através de um protocolo de sincronização.

Existem duas abordagens para a recuperação de clock: *Adaptive Clock Recovery* (ACR) e *Differential Clock Recovery* (DCR). Na ACR, a referência de clock é encapsulada e desencapsulada nos nós de borda entre as redes TDM e de pacotes, e um protocolo como o *Network Time Protocol* (NTP) ou o *Precision Time Protocol* (PTP) regenera a devida frequência de transmissão através do intervalo de tempo entre o recebimento de pacotes. Já na DCR, os dois equipamentos de borda têm acesso a uma referência comum de *clock*, e os tempos são marcados por *timestamps* [15].

3.3 Transporte Óptico de Pacotes

Por suportar provisionamento tanto estático quanto dinâmico, o MPLS-TP é visto como uma ferramenta natural para redes de transporte, geralmente constituídas por porções orientadas a pacotes e outras porções orientadas pelo transporte óptico OTN. Através de sua implementação, os operadores poderão utilizar os LSPs para gerenciar o tráfego de usuários como circuitos em ambos os domínios óptico e de pacotes.

O MPLS-TP oferece características essenciais na construção de uma rede de transporte de pacotes de baixo custo, como a possibilidade de se realizar a multiplexação estatística e realizar a alocação de largura de banda através dos LSPs conforme características de QoS. Enquanto isso, o enquadramento OTN fornece funcionalidade importante durante a transmissão óptica. Embora possa haver alguns casos em que as duas tecnologias possam ser aplicadas, existem cenários onde uma é preferível sobre a outra. Por exemplo, a comutação OTN é mais apropriada para serviços inelásticos de linha dedicada, enquanto os serviços de dados para Ethernet são favorecidos pelo MPLS-TP [17].

Em alguns casos, os provedores de serviço planejam implementar o MPLS-TP desde toda sua rede de transporte de pacotes óptico de longa distância até sua rede de agregação e acesso. A operadora *Verizon* pretende implantar MPLS-TP dinâmico sobre OTN/WDM no núcleo da rede. Como ilustrado na Figura 25, UNIs nas bordas de rede serão utilizadas para fornecer sinalização dinâmica de LSPs que se conectam com os serviços de borda. O objetivo da empresa é utilizar domínios MPLS-TP/MPLS para todos os seus serviços de transporte e tráfego de pacotes.

Várias técnicas de adaptação e encapsulamento são utilizadas para permitir que os pacotes MPLS-TP sejam carregados através de uma variedade de diferentes tecnologias físicas, incluindo redes OTN e Ethernet.

Através de um mecanismo denominado *Generic Framing Procedure* (GFP) é possível encapsular cargas de tamanho variável e de vários tipos de clientes

para o transporte sobre redes SONET/SDH, PDH, e OTN. O cabeçalho GFP contém um identificador denominado *User Payload Identifier* (UPI) que pode ser utilizado para indicar o pacote MPLS/MPLS-TP. De modo similar ao GFP, o MPLS-TP, pode ser carregado por links Ethernet. Para Ethernet um campo de 2 bytes denominado *EtherType* indica o tipo de protocolo que é encapsulado pelos quadros [15].

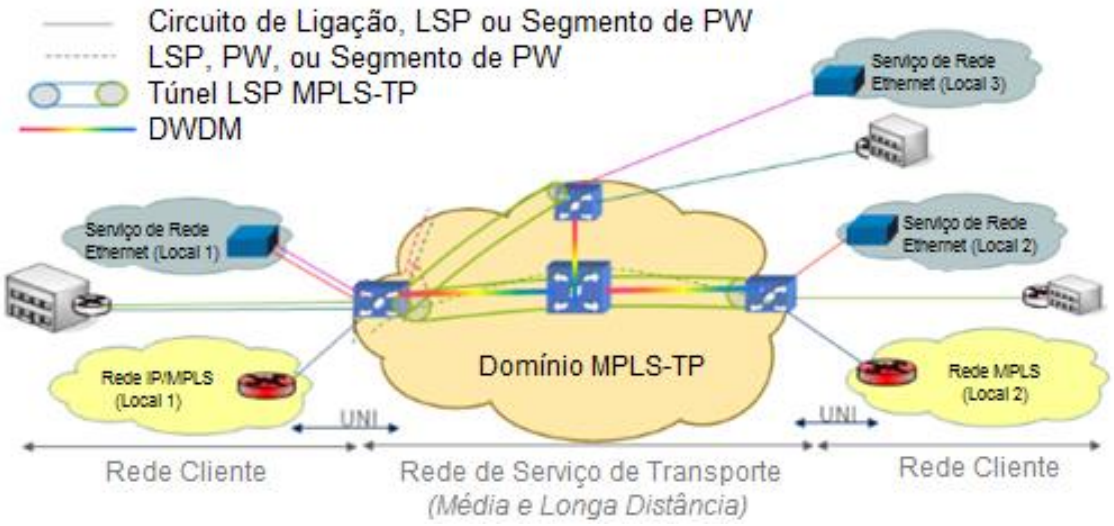

Figura 25 – MPLS-TP Dinâmico sobre OTN/WDM [17]

Conclusão

O MPLS-TP não deverá substituir as redes IP/MPLS, mas sim, possibilitar um significativo ganho de mercado pela tecnologia, que poderá ser aplicada em novos domínios da rede e assim permitir a criação de soluções MPLS fim-a-fim. Com isso, as importantes capacidades para o suporte de serviços, como VPNs e IPTV são mantidas enquanto outras importante s capacidades que dizem respeito ao transporte dos dados são adquiridas. As melhorias OAM propostas pelo MPLS-TP permitirão que os provedores de serviço tenham visibilidade holística e maior controle de suas redes, o que auxiliará importantes otimizações de custo, gerenciamento e uso de suas bandas.

A melhoria na qualidade de serviço fornecida aos clientes é urgente, tendo em vista a crescente exigência com relação à fidelidade entre o serviço pago e o que é recebido. Além disso, questões relacionadas à segurança exigem previsibilidade com relação aos caminhos percorridos por cada fluxo de dados. Muitos clientes precisam saber exatamente por onde seus dados estão trafegando. Essas questões impulsionam a adoção do MPLS-TP.

Após o consenso entre muitos fornecedores e provedores, é esperado nos próximos anos grandes investimentos de implementação na tecnologia, que deverá ter assim um papel fundamental na migração para a nova geração de redes de transporte baseada no transporte de pacotes, conforme citado muitas vezes.

O trabalho apresentado foi desenvolvido para ser apresentado como trabalho de conclusão do curso de Engenharia de Computação. Deve-se então destacar sua grande importância em termos acadêmicos para a autora. O tema possibilitou ganho de conhecimento e a consolidação de importantes conceitos na área de redes e telecomunicações, cujos conhecimentos podem ser bastante requisitados pela profissão nos próximos anos.

As maiores dificuldades encontradas durante a produção dessa monografia foram: convergir diversos conceitos na mesma linha de raciocínio, tento em vista a vasta área a que pertence o tema apresentado; sumarizar os estudos do IETF e ITU-T sobre a tecnologia, já que alguns tópicos foram interrompidos e outros ainda não foram oficialmente publicados; e por fim, conciliar as divergência de dados entre documentos de diferentes fabricantes e períodos, já que o MPLS-TP ainda estava em fase de desenvolvimento durante suas publicações;

Em conclusão, espera-se que esse trabalho sirva como material de consulta e estudo para pesquisadores e outros interessados em aprender os principais conceitos relacionados ao MPLS-TP e assim realizar projeções acerca de seu potencial de uso e aplicação.

Referências Bibliográficas

[1] STALLINGS, W. MPLS. The Internet Protocol Journal, vol. 4, nº 3, Setembro 2001.

[2] NAKAMURA, J.A. Evolução das Redes de Telecomunicação e o Multiprotocol Label Switching (MPLS). Monografia (Trabalho de Conclusão de Curso)- Escola de Engenharia de São Carlos, Universidade de São Paulo. São Carlos, 2009.

[3] KUROSE J. F; ROSSA, K. W. Redes de computadores e a internet (5ª edição). Pearson / Prentice Hal, 2010.

[4] IETF. Multiprotocol Label Switching Architecture. RFC 3031. Janeiro 2001.

[5] METASWITCH . What Is MPLS and GMPLS?. Disponíel em <http://network-technologies.metaswitch.com/mpls/what-is-mpls-and-gmpls>. Acesso em: 17 de Outubro de 2012.

[6] FALSARELLA, D. Tipos de Roteamento. Em: Seminário Internacional - Redes Inteligentes, Aplicações mais Rápidas. São Paulo, 2008.

[7] CISCO. MPLS Label Distribution Protocol (LDP). Cisco IOS Software Releases 12.4 Mainline.

[8] PERROS, H. G. Connection-Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks. Wiley, 2005. Capítulo 7.

[9] METASWITCH. What is LDP?. Disponíel em <http://network-technologies .metaswitch.com/mpls/what-is-ldp>. Acesso em 17 de Outubro de 2012.

[10] PORTONOI, M. CR-LDP: Aspectos e Funcionamento. Salvador: Universidade Salvador, 2005.

[11] JUNIPER. RSVP Signaling Extensions for MPLS Traffic Engineering. White Paper. Sunnyvale, 2002.

[12] STEWART, J. GMPLS unifies network layers - Network World. Disponível em <http://www.networkworld.com/news/tech/2003/0428techupdate.html>. Acesso em 24 de Outubro de 2013.

[13] YIN, L. MPLS and GMPLS. Berkeley School. Disponível em <http://bnrg.eecs.berkeley.edu/randy/Courses/CS294.S02/MPLS.ppt.>. Acesso em 11 de Agosto de 2013.

[14] CISCO. Understanding MPLS-TP and Its Benefits. White Paper. San Jose, 2009.

[15] DIETER BELLER, R. S. MPLS-TP – The New Technology for Packet Transport Networks. Em: II Fórum de Tecnologias em Comunicações DFN. Munique, 2009.

[16] JUNIPER. MPLS Transport Profile (MPLS-TP). White Paper. Sunnyvale, 2011.

[17] HUBBARD S. MPLS-TP in the Next-Generation Transport Networks. Heavy Reading. 2011.

[18] IETF. A Framework for MPLS in Transport Networks. RFC 5921. 2010.

[19] OTN SYSTEMS. MPLS-TP in Power. White Paper. 2012.

[20] IETF. A framework for MPLS in Transport Networks. RFC 5921. 2010.

[21] IETF. MPLS Generic Associated Channel. RFC 5586. 2010.

[22] IETF. Network Management Framework for MPLS-based Transport Networks. RFC 5950. 2010.

[23] IETF. MPLS Transport Profile Control Plane Framework. RFC 6373. 2011.

[24] IETF. MPLS Transport Profile (MPLS-TP) Survivability Framework. RFC 6372. 2011.

[25] IETF. MPLS-TP Applicability: Use Cases and Design. RFC 6965. 2013.

[26] METASWITCH, MPLS-TP Overview. Disponíel em <http://network-technologies .metaswitch.com/mpls/mpls-tp-overview>. Acesso em 18 de Novembro de 2012.

[27] IETF. MPLS Transport Profile Lock Instruct and Loopback Functions. RFC 6435. 2011.

[28] IETF. MPLS Transport Profile Data Plane Architecture. RFC 5960. 2010.

[29] VERIZON. MPLS-TP: Where Are We?. White Paper. 2012.

[30] ISOCORE, MPLS 2010 Public Interoperability Test Results, 2010.

[31] EANTC, Puclib Multi-Vendor Interoperability Results. Em: MPLS & Ethernet World Congress 2012 Event. 2012.