CLAUDIO ROBERTO FERREIRA COSTA

**Mecanismos para determinação de rotas de proteção em redes MPLS-TP com
topologia em malha**

São Paulo

(2016)

CLAUDIO ROBERTO FERREIRA COSTA

**Mecanismos para determinação de rotas de proteção em redes MPLS-TP com
topologia em malha**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo para obtenção
do título de Doutor em Ciências -
Programa de Engenharia Elétrica

Orientador: Prof. Dr. Wagner Luiz Zucchi

São Paulo
(2016)

CLAUDIO ROBERTO FERREIRA COSTA

**Mecanismos para determinação de rotas de proteção em redes MPLS-TP com
topologia em malha**

Tese apresentada à Escola Politécnica da
Universidade de São Paulo para obtenção
do título de Doutor em Ciências -
Programa de Engenharia Elétrica

Área de Concentração: Sistemas
Eletrônicos

Orientador: Prof. Dr. Wagner Luiz Zucchi

São Paulo

(2016)

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, _____ de _____ de _____

Assinatura do autor: _____

Assinatura do orientador: _____

Catálogo-na-publicação

Costa, Claudio Roberto Ferreira

Mecanismos para determinação de rotas de proteção em redes MPLS-TP com topologia em malha / C. R. F. Costa -- versão corr. -- São Paulo, 2016. 124 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1.Redes de Computadores 2.Redes MPLS-TP em malha 3.Seleção de caminhos de LSPs 4.Proteção em malha compartilhada I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II.t.

Dedico este trabalho à minha querida esposa Niraildes, com amor, admiração e gratidão por sua compreensão, carinho, presença, paciência e incansável apoio durante todo o longo período de elaboração desta Tese de Doutorado.

AGRADECIMENTOS

Primeiramente a Deus, que me deu forças, saúde, sabedoria, entendimento, inspiração, motivação e ânimo para a conclusão deste trabalho.

Ao Prof. Dr. Wagner Luiz Zucchi, pela orientação e constante estímulo durante toda esta longa trajetória.

À minha esposa, pela compreensão de, nesse longo período, muitas vezes eu ter me dedicado mais aos estudos do que à família.

Aos familiares e amigos, que muitas vezes se sentiram preteridos pelos livros.

A todos que colaboraram, direta ou indiretamente, na execução deste trabalho.

Os que se encantam com a prática sem a ciência são como os timoneiros que entram no navio sem timão nem bússola, nunca tendo certeza do seu destino.

Leonardo da Vinci

Consagre ao Senhor tudo o que faz, e tuas obras serão bem-sucedidas.

Provérbios 16:3

RESUMO

As redes atuais de telecomunicações utilizam tecnologias de comutação de pacotes para integração de voz, dados, imagens e outros serviços. O tráfego nessas redes costuma ser feito por meio de tecnologias como o MPLS-TP e com regras heurísticas para a determinação dos melhores caminhos. O uso de boas regras afeta diretamente o desempenho e a segurança da operação. Este trabalho propõe o uso de simulação de baixo custo para prever o comportamento e avaliar regras de escolha de caminhos. Para isso, este trabalho avalia três métodos de seleção de caminhos de LSPs, combinados com duas heurísticas de recuperação, usados em redes MPLS-TP em malha com mecanismos de proteção em malha compartilhada. Os resultados das simulações medem o impacto dos métodos e heurísticas utilizados, demonstrando o quanto uma melhor seleção de caminhos pode contribuir para a redução do uso dos recursos da rede e do número máximo de LSPs afetados em caso de falhas na rede. Os resultados deste trabalho, bem como a técnica de análise proposta, almejam ser uma contribuição para a padronização de regras de seleção de LSPs em redes heterogêneas.

Palavras-Chave: Redes de computadores. Redes MPLS-TP em malha. Seleção de caminhos de LSPs. Proteção em malha compartilhada.

ABSTRACT

The telecommunications networks nowadays use packet-switching technologies for integration of voice, data, images and other services. The traffic on these networks is usually done through technologies such as MPLS-TP and with heuristic rules to determine the best paths. The use of good rules directly affect the performance and security of operation. This paper proposes the inexpensive use of simulation to predict the behavior and evaluate rules for choosing paths. For this, this study evaluates three methods of selection of LSPs paths, combined with two recovery heuristics, used in MPLS-TP mesh networks with shared mesh protection mechanisms. The results of the simulations measure the impact of the methods and heuristics used, demonstrating how much better path selection can contribute to reducing the use of network resources and the maximum number of LSPs affected in the event of network failures. These results and the proposed analysis technique yearn to be a contribution to the standardization of LSPs selection rules in heterogeneous networks.

Keywords: Computer networks. MPLS-TP mesh networks. LSP path selection. Shared mesh protection.

LISTA DE ILUSTRAÇÕES

Figura 1	– Crescimento do uso da Internet.....	21
Figura 2	– Relacionamento entre uma rede MPLS-TP e sua rede cliente..	39
Figura 3	– Arquitetura MPLS-TP (PW de simples segmento).....	39
Figura 4	– Arquitetura MPLS-TP (PW de múltiplos segmentos).....	40
Figura 5	– Arquitetura MPLS-TP (LSP de simples seção).....	40
Figura 6	– Arquitetura MPLS-TP (LSP de múltiplas seções).....	41
Figura 7	– Contexto da Arquitetura do Plano de Controle MPLS-TP.....	42
Figura 8	– SPME (Sub-Path Maintenance Element) ou Elemento de Manutenção de Segmentos MPLS-TP.....	43
Figura 9	– Modelo de Referência de Segurança 1 - Exemplo 1 (a).....	45
Figura 10	– Modelo de Referência de Segurança 1 - Exemplo 1 (b).....	46
Figura 11	– Modelo de Referência de Segurança 2 - Exemplo 2 (a).....	46
Figura 12	– Modelo de Referência de Segurança 2 - Exemplo 2 (b).....	47
Figura 13	– Exemplo de Proteção Linear “1 : 2” em uma rede em Malha.....	65
Figura 14	– Exemplo de Proteção Linear “1 + 1” em uma rede em Malha....	65
Figura 15	– Topologia de Proteção em Malha Compartilhada.....	66
Figura 16	– Lógica do Controle de Coordenação do Chaveamento de Proteção.....	68
Figura 17	– Exemplo de Proteção “Wrapping” ponto-a-ponto em Anel Simples.....	69
Figura 18	– Exemplo de Proteção “Steering” ponto-a-ponto em Anel Simples.....	70

Figura 19	– Exemplo de Proteção “Wrapping” ponto-a-multiponto em Anel Simples.....	70
Figura 20	– Exemplo de Proteção “ROM-Wrapping” em Anel Simples.....	71
Figura 21	– Exemplo de Proteção “Steering” ponto-a-multiponto em Anel Simples.....	72
Figura 22	– Modelo de Makam.....	72
Figura 23	– Modelo de Haskin e Krishnan.....	73
Figura 24	– Modelo MPLS Fast Reroute um-para-um.....	73
Figura 25	– Modelo MPLS Fast Reroute um-para-um com merging.....	74
Figura 26	– Restauração de segmentos e fim-a-fim.....	75
Figura 27	– Backbone MPLS Norte-Americano.....	78
Figura 28	– Backbone MPLS Europeu.....	78
Figura 29	– Exemplo de Caminho em “Trap”.....	80
Figura 30	– Exemplo 1 de cargas em uma rede em malha.....	84
Figura 31	– Exemplo 2 de cargas em uma rede em malha.....	84
Figura 32	– Exemplo 1 de Abordagem para Evitar Caminhos em “Trap”.....	97
Figura 33	– Exemplo 2 de Abordagem para Evitar Caminhos em “Trap”.....	98
Figura 34	– Topologias de redes em malha utilizadas nas simulações.....	99
Figura 35	– Densidade média de tráfego (Gbps/salto) da rede de 26-nós/39-links.....	102
Figura 36	– Tamanho médio dos LSPs (em número de saltos) da rede de 26-nós/39-links.....	104
Figura 37	– Número máximo de LSPs afetados em caso de falhas na rede 26-nós/39-links.....	105

LISTA DE TABELAS

Tabela 4.1	– Exemplo de cargas e capacidade residuais de links de rede em malha.....	85
Tabela 5.1	– Número de simulações de falhas de rede.....	100
Tabela 5.2	– Densidade média de tráfego dos LSPs (em Gbps/salto).....	101
Tabela 5.3	– Tamanho médio dos LSPs (em número de saltos).....	103
Tabela 5.4	– Número máximo de LSPs afetados em caso de falhas na rede.....	104
Tabela 5.5	– Resumo dos resultados das simulações da rede 26-nós/39-links.....	106

LISTA DE ABREVIATURAS E SIGLAS

ATM	Asynchronous Transfer Mode
BCRA	Bandwidth Constrained Routing Algorithm
BGLC	Bandwidth Guarantee with Low Complexity
CapEx	Capital Expenditure (Despesas de Capital)
CE	Customer Edge
CSPF	Constrained Shortest Path First
CTN	Circuit Transport Networks
DORA	Dynamic Online Routing Algorithm
DoS	Denial of Service
EMF	Equipment Management Function
FR	Frame-Relay
GB	Giba Byte
Gbps	Giga bits por segundo
GMPLS	Generalized Multi-Protocol Label Switching
HDTV	High Definition TV
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunication standardization sector
LAN	Local Area Network
LER	Label Edge Router
LIOA	Least Interference Optimization Algorithm
LSP	Label Switched Path
LSR	Label Switching Router

MAN	Metropolitan Area Network
Mbps	Mega bits por segundo
MCC	Management Communication Channel
MHA	Minimum Hop Algorithm
MIRA	Minimum Interference Routing Algorithm
MPLS	Multi-Protocol Label Switching
MPLS-TP	Multi-Protocol Label Switching – Transport Profile
NG-SDH	Next Generation - Synchronous Digital Hierarchy
NMS	Network Management System
OAM	Operação, Administração e Manutenção
OpEx	Operational Expenditure (Despesas Operacionais)
OTN	Optical Transport Network
P	Provider
P2MP	Ponto a Multi-Ponto
PCE	Path Computation Element
PDH	Plesiochronous Digital Hierarchy
PDU	Protocol Data Unit
PE	Provider Edge
PSC	Protection State Coordination
PTN	Packet Transport Networks
PW	PseudoWire
QoS	Quality of Service
RFC	Request for Comments
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
SDH	Synchronous Digital Hierarchy
SDTV	Standard Definition TV
SONET	Synchronous Optical Network

S-PE	Switching - Provider Edge
SPF	Shortest Path First
SPME	Sub-Path Maintenance Element
TDM	Time Division Multiplexing
T-PE	Terminating - Provider Edge
VPN	Virtual Private Network
WAN	Wide Area Network
WSEAS	World Scientific and Engineering Academy and Society
WSP	Widest Shortest Path

LISTA DE RFCs

- RFC-3031 Multiprotocol Label Switching Architecture (ROSEN; VISWANATHAN, 2001)
- RFC-3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture (BRYANT; PATE, 2005)
- RFC-4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels (PAN; SWALLOW; ATLAS, 2005)
- RFC-4428 Analysis of Generalized Multi-Protocol Label Switching (GMPLS) – based Recovery Mechanisms (including Protection and Restoration) (MANNIE; PAPADIMITRIOU, 2006)
- RFC-5654 Requirements of an MPLS Transport Profile (NIVEN-JENKINS et al., 2009)
- RFC-5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge (BRYANT, 2009)
- RFC-5860 Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks (VIGOUREUX; WARD; BETTS, 2010)
- RFC-5920 Security Framework for MPLS and GMPLS Networks (FANG, 2010)
- RFC-5921 A Framework for MPLS in Transport Networks (BOCCI et al., 2010)
- RFC-5950 Network Management Framework for MPLS-based Transport Networks (LAM; MANSFIELD; GRAY, 2010)
- RFC-5951 Network Management Requirements for MPLS-based Transport Networks (LAM; MANSFIELD; GRAY, 2010)
- RFC-5960 MPLS Transport Profile Data Plane Architecture (FROST; BRYANT; BOCCI, 2010)
- RFC-6372 MPLS-TP Survivability Framework (SPRECHER; FARREL, 2011)
- RFC-6373 MPLS Transport Profile (MPLS-TP) Control Plane Framework (ANDERSSON et al., 2011)
- RFC-6378 MPLS Transport Profile (MPLS-TP) Linear Protection (WEIGARTEN et al., 2011)

- RFC-6941 MPLS Transport Profile (MPLS-TP) Security Framework (FANG et al., 2013)
- RFC-6965 MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design (FANG et al., 2013)
- RFC-6974 Applicability of MPLS Transport Profile for Ring Topologies (WEIGARTEN et al., 2013)
- RFC-7412 Requirements for MPLS-TP Shared Mesh Protection (WEINGARTEN et al., 2014)

SUMÁRIO

1	INTRODUÇÃO.....	21
1.1	OBJETIVO DA TESE.....	26
1.2	CONTRIBUIÇÕES.....	26
1.3	ESTRUTURA DA TESE.....	28
2	VISÃO GERAL DA TECNOLOGIA MPLS-TP.....	30
2.1	BREVE INTRODUÇÃO AO MPLS-TP.....	30
2.2	DEFINIÇÕES.....	31
2.3	ASPECTOS GERAIS DA TECNOLOGIA MPLS-TP.....	37
2.3.1	Arquitetura Básica da Tecnologia MPLS-TP.....	38
2.3.2	Funções de OAM (Operação, Administração e Manutenção).....	41
2.3.3	Manutenção de Segmentos MPLS-TP.....	43
2.3.4	Gerenciamento de Redes MPLS-TP.....	44
2.3.5	Segurança (Security) de Redes MPLS-TP.....	45
2.4	REQUISITOS DA TECNOLOGIA MPLS-TP.....	48
2.5	APLICABILIDADE DA TECNOLOGIA MPLS-TP.....	52
2.6	SÍNTESE DO CAPÍTULO.....	54
3	SOBREVIVÊNCIA DE REDES MPLS-TP.....	55
3.1	ARCABOUÇO DE SOBREVIVÊNCIA DA TECNOLOGIA MPLS-TP....	55
3.1.1	Recuperação no Ambiente MPLS-TP.....	56

3.1.2	Escopos da Recuperação MPLS-TP	59
3.1.3	Graus de Recuperação MPLS-TP	61
3.1.4	Domínios de Recuperação MPLS-TP	63
3.1.5	Recuperação de Redes MPLS-TP em Anel	64
3.1.6	Proteção de Redes MPLS-TP em Malha	64
3.2	PROTOCOLO PARA COORDENAÇÃO DO ESTADO DE PROTEÇÃO LINEAR EM REDES MPLS-TP EM MALHA.....	66
3.3	APLICABILIDADE DE PROTEÇÕES MPLS-TP EM TOPOLOGIAS EM ANEL.....	68
3.4	TRABALHOS RELACIONADOS.....	72
3.5	SÍNTESE DO CAPÍTULO.....	76
4	ESTABELECIMENTO DE LSPs EM REDES MPLS-TP EM MALHA	78
4.1	DIFICULDADE PARA SE ESTABELECEM LSPs EM REDES EM MALHA.....	79
4.1.1	Problema NP-Completo	80
4.1.2	Caminhos em “Trap”	80
4.1.3	Cálculo Centralizado ou Distribuído	81
4.1.4	Métrica a Ser Utilizada	83
4.2	TRABALHOS RELACIONADOS.....	86
4.3	COMPARAÇÃO DE MÉTODOS DE ESTABELECIMENTO DE CAMINHOS.....	90
4.3.1	Métodos (de Escolha de Caminhos) que Foram Comparados	91
4.3.2	Heurísticas de Recuperação Empregadas	93

4.4	SÍNTESE DO CAPÍTULO.....	95
5	SIMULAÇÕES E RESULTADOS.....	96
5.1	SIMULAÇÕES.....	96
5.1.1	Simulador.....	96
5.1.2	Abordagem para Evitar Caminhos em “Trap”	96
5.1.3	Cenários de Simulação.....	98
5.2	RESULTADOS.....	100
5.2.1	Densidade Média de Tráfego dos LSPs (em Gbps/salto).....	101
5.2.2	Tamanho Médio dos LSPs (em Número de Saltos).....	102
5.2.3	Número Máximo de LSPs Afetados em Caso de Falhas na Rede.....	104
5.2.4	Sumário dos Resultados.....	105
5.3	SÍNTESE DO CAPÍTULO.....	107
6	CONCLUSÕES.....	109
6.1	CONTRIBUIÇÕES.....	110
6.2	TRABALHOS FUTUROS.....	111
	REFERÊNCIAS.....	112
	APÊNDICE A – Cópia de Artigo Científico Publicado.....	118

1 INTRODUÇÃO

A popularização do uso da Internet e o avanço tecnológico das interfaces de rede (com taxas de transferências de dados cada vez maiores) têm causado um explosivo crescimento da demanda de serviços de alta velocidade de transferência de dados, conforme ilustrado na figura 1 abaixo. Pressionados a atender tal crescimento da demanda, os provedores de serviços de Internet (*Internet Service Providers – ISP's*) têm buscado aumentar a capacidade de suas redes sem aumentar demasiadamente seus custos.

Figura 1 - Crescimento do uso da Internet
Fonte: Virtual Network Index (2015)

O avanço tecnológico das interfaces de rede, por sua vez, pode ser exemplificado pela velocidade cronológica da padronização de algumas de suas taxas de transferência: na Hierarquia Digital Síncrona (*Synchronous Digital Hierarchy – SDH*) para redes comutadas por circuitos (*circuit-switched networks*), a taxa de 622 Mbps foi especificada em 1988, a taxa de 2,4 Gbps foi especificada em 1991, a taxa de 10 Gbps foi especificada em 1996 e a taxa de 40 Gbps foi especificada em 2000 (OISHI et al., 2010), (ITU-T G.707, 2007). Em paralelo a isso, nas interfaces Ethernet das redes comutadas por pacotes (*packet-switched networks*), a taxa de 100 Mbps foi especificada em 1995, a taxa de 1 Gbps foi especificada em 1998, a taxa de 10 Gbps foi especificada em 2002, a taxa de 100 Gbps foi especificada em 2010 (OISHI et al., 2010), (IEEE 802.3) e já há um grupo trabalhando na padronização da taxa de 400 Gbps (IEEE 802.3bs).

Na hierarquia digital todos os nós devem ser sincronizados, mas esse requisito de sincronização torna os nós complexos e caros, acarretando um alto

custo financeiro para redes desse tipo. Por outro lado, nas redes comutadas por pacotes a sincronização dos nós tem requisitos menos rígidos, pois todos os referidos pacotes trazem informações suficientes para que sejam processados um por um em cada nó. Desta forma, as redes comutadas por pacotes se tornam mais baratas que as comutadas por circuitos (OISHI et al., 2010).

Conforme pode ser visto na ordem cronológica da padronização das taxas de transferência exemplificadas acima, as redes comutadas por pacotes eram, inicialmente, muito mais lentas que as comutadas por circuitos. No entanto, devido ao esforço em se conseguir maiores taxas de transferências nas redes de menor custo, as redes comutadas por pacotes tiveram suas taxas de transferência gradativamente aumentadas, até superar as taxas das redes comutadas por circuitos.

Para aumentar a eficiência de suas redes e, ao mesmo tempo, reduzir custos, os provedores de serviços de Internet têm buscado utilizar, ao máximo, a comutação de pacotes. No entanto, a infraestrutura já instalada (das redes comutadas por circuitos) não pode ser simplesmente descartada. Para amortizar o investimento realizado nas redes comutadas por circuitos, uma das soluções possíveis é o emprego de uma rede de transporte que, utilizando ao máximo a infraestrutura física existente, seja capaz de prover, para qualquer tipo de tráfego, uma infraestrutura de transporte confiável (BELLER; SPERBER, 2009).

Importante ressaltar que as redes comutadas por pacotes possuem eficiência superior (melhor aproveitamento dos recursos da rede) que as redes comutadas por circuitos. Por outro lado, as redes comutadas por circuitos possuem funcionalidades que possibilitam melhor controle e gerenciamento da rede (UTSTARCOM, 2009).

As tecnologias baseadas em comutação de pacotes (ex.: Ethernet) têm sido amplamente utilizadas nas redes locais (LANs – *Local Area Networks*). Já nas redes metropolitanas (MANs – *Metropolitan Area Networks*) e nas redes de grandes áreas (WANs – *Wide Area Networks*), o tráfego de dados (ou o transporte de dados) tem sido tradicionalmente feito sobre a infraestrutura física instalada para a telefonia, baseada na comutação de circuitos, ou mais especificamente na tecnologia SONET/SDH (*Synchronous Optical Network / Synchronous Digital Hierarchy*) (HAN et al., 2009). No entanto, devido ao aumento explosivo da demanda de transferência de dados, o transporte de dados entre MANs e WANs precisa ser melhorado (ou seja, se tornar mais eficiente, a um menor custo).

A tecnologia Ethernet, apesar dos seus avanços, ainda não pode ser perfeitamente empregada em WANs, onde existe um número muito grande de usuários e de serviços. Nas WANs, é preciso se diferenciar e se processar inúmeros serviços, de diferentes requisitos (como diferentes tolerâncias a erros, a retardos ou à variação de retardos, por exemplo). Além disso, nas WANs, a rápida restauração dos serviços é de importância crítica. Outro fator complicador das WANs é a sua grande abrangência tanto em área de cobertura quanto em número de redes, o que faz com que seja de crucial importância a capacidade de se gerenciar falhas e se monitorar o desempenho dessas diversas redes (VAEZ-GHAEMI, 2010).

Faz-se necessário, portanto, que seja desenvolvida uma tecnologia capaz de transportar qualquer tipo de tráfego, de uma extremidade à outra de uma WAN, de forma confiável (sem degradar o tráfego). Em outras palavras, se faz necessário, portanto, que seja encontrada uma tecnologia capaz de prover, a uma WAN, uma rede de transporte confiável para qualquer tipo de tráfego.

Historicamente, as redes de transporte têm sido providas pela tecnologia SONET/SDH (baseada em circuitos). Esta tecnologia garante, a um determinado canal, uma capacidade (de transporte de dados) fixa, independentemente do tráfego nesse canal ou nos demais canais da rede.

Para suportar a demanda por serviços baseados em pacotes, a tecnologia SONET/SDH evoluiu para a tecnologia *Next-Generation-SDH* (NG-SDH), que consiste (resumidamente) em encapsular “pacotes” em frames SDH e transmiti-los pela rede (UTSTARCOM, 2009).

No entanto, os serviços baseados em pacotes são em rajadas e, por isso, não requerem uma banda fixa dedicada. Ou seja, apesar da sua “evolução” em relação à tecnologia da qual derivou (SONET/SDH), a tecnologia NG-SDH apresenta ainda algumas ineficiências, tais como a alocação de banda inflexível (pouco eficiente para serviços baseados em pacotes) e a baixa utilização média da rede (devido à necessidade de se alocar banda fixa para se garantir QoS mínimo, em um tráfego predominantemente em rajadas e com taxas de pico acima da média alocada).

Várias tecnologias, tais como **PDH** (*Plesiochronous Digital Hierarchy*), **SONET/SDH** (*Synchronous Optical Network / Synchronous Digital Hierarchy*), **ATM** (*Asynchronous Transfer Mode*), **OTN** (*Optical Transport Network*), **Ethernet** ou **MPLS/MPLS-TP** (*Multi-Protocol Label Switching / MPLS Transport Profile*) em teoria poderiam prover, a uma WAN, uma rede de transporte confiável para qualquer tipo

de tráfego. No entanto, para fazer isso atendendo à atual demanda explosiva, cada uma dessas tecnologias precisaria sofrer ajustes e ser padronizada em termos de vários aspectos, como arquitetura, estrutura, serviços, características funcionais dos equipamentos, OAM (*Operation, Administration and Maintenance*), características físicas, desempenho, etc (ITU-T 16, 2012).

Nesse contexto, segundo Beller e Sperber (2009), a tecnologia emergente que aparenta ser a mais promissora é o MPLS-TP, tecnologia que está atualmente em desenvolvimento conjunto pelo IETF (*Internet Engineering Task Force*) e pelo ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*). O objetivo desse esforço conjunto de padronização é desenvolver as extensões necessárias para que o MPLS possa alcançar os requisitos (de escalabilidade, suporte a múltiplos serviços, qualidade, baixo-custo, etc.) de uma moderna rede de transporte (ITU-T 16, 2012).

Atualmente, o tráfego predominante nas redes de todo o mundo é o tráfego IP, baseado em pacotes. O explosivo crescimento da demanda de transferência de dados aumentou drasticamente a necessidade de eficiência das redes de transporte. O MPLS-TP é a tecnologia que promete oferecer serviços baseados em pacotes mais eficientemente (e a menor custo) que as tradicionais redes baseadas na tecnologia de comutação de circuitos SONET/SDH (WINTER, 2011).

O MPLS “original” já é utilizado no núcleo de diversas redes, facilitando, portanto, a migração dessas redes para a tecnologia MPLS-TP (que pode ser considerada uma extensão da tecnologia MPLS). Portanto, o MPLS-TP é forte candidato a ser amplamente utilizado nas redes de todo o mundo, devido às suas características de alta eficiência e relativamente baixo custo. No entanto, a tecnologia MPLS-TP ainda está em fase de desenvolvimento (em conjunto pelo IETF e pelo ITU-T) e, portanto, ainda não está totalmente padronizada.

Em uma rede MPLS-TP, uma rota (ou caminho) de transporte de dados corresponde a um Label Switched Path (LSP), no qual os pacotes de mesmo rótulo (label) são roteados fazendo um caminho fixo (ROSEN, VISWANATHAN, 2001).

As modernas redes de transporte têm tipicamente topologia em malha (com ligações arbitrárias entre seus nós). O estabelecimento de LSPs entre dois nós quaisquer em uma rede MPLS-TP em malha pode não ser simples, dependendo da complexidade da rede e do número de LSPs já estabelecidos anteriormente nessa rede inteira. Por exemplo, o uso dos caminhos mais curtos entre dois nós por

diferentes LSPs pode sobrecarregar alguns links, enquanto outros ficam sub-utilizados.

Em uma rede MPLS-TP, quanto mais sobrecarregados forem os links, maior a chance deles eventualmente se tornarem congestionados devido à ocorrência de picos ou ao aumento gradativo da demanda. Por outro lado, quanto mais balanceado for o uso da rede (ou seja, quanto menos sobrecarregados forem os links), maior será a capacidade de essa rede suportar um posterior acréscimo do tráfego.

No caso de eventuais falhas afetarem um LSP, o tráfego fim-a-fim deve ser restabelecido o mais rapidamente possível. Para evitar demoras nesse processo de restabelecimento, quando é criado um LSP entre dois pontos quaisquer, são escolhidos dois caminhos distintos (que não se cruzam, ou seja, que não compartilham nós ou links intermediários) entre esses dois pontos: um deles, denominado “caminho de trabalho”, é por onde o tráfego de pacotes do LSP seguirá normalmente; e o outro, denominado “caminho de proteção”, recebe o tráfego de dados do LSP caso alguma falha afete o caminho de trabalho. O caminho de proteção pode ser dedicado (não permitindo tráfego que não seja do LSP que protege) ou compartilhado (permitindo tráfego de outros LSPs). Nas redes em malha, dois ou mais LSPs distintos podem compartilhar trechos do mesmo caminho de proteção, o que caracteriza o esquema de proteção em malha compartilhada.

Nas redes MPLS-TP em malha com proteção em malha compartilhada, durante o estabelecimento de um LSP, os caminhos de trabalho devem ser criados concomitantemente com seus respectivos caminhos de proteção (WEINGARTEN et al., 2014).

Para aumentar a capacidade de uma rede MPLS-TP de absorver o aumento da demanda dos serviços por ela providos e para suportar eventuais falhas, o estabelecimento de LSPs deve priorizar o uso eficiente dos recursos dessa rede. Entretanto, os estudos de Ou et al. (2003) e (2006) demonstram que a questão de se encontrar, em uma rede em malha, um par elegível de caminho de trabalho e respectivo caminho de proteção para a instauração (de forma otimizada na rede) de qualquer novo LSP, considerando-se a existência dos LSPs já estabelecidos na rede, é um problema NP-Completo¹.

¹ Problema NP-Completo: problema que, utilizando-se as técnicas atuais conhecidas de resolução de problemas, não possui solução em tempo determinístico polinomial (nota do autor).

Devido à dificuldade de se determinar caminhos de forma otimizada para a rede como um todo, as normas que padronizam a tecnologia MPLS-TP ainda não definiram um modelo para o estabelecimento desses caminhos.

Portanto, o problema de escolha conjunta de caminhos de trabalho e de proteção de um LSP, considerando todos os LSPs de uma determinada rede MPLS-TP em malha, precisa ser melhor estudado.

1.1 OBJETIVO DA TESE

Tendo em vista a dificuldade de se determinar caminhos de forma otimizada para a rede MPLS-TP como um todo, este trabalho tem o objetivo de contribuir para o estudo da solução, otimizada em rede, do problema de escolha de caminhos em redes MPLS-TP com esquema de proteção em malha compartilhada, sem a pretensão, no entanto, de esgotar o assunto.

Para atender esse objetivo, este trabalho aplica, em redes MPLS-TP com esquema de proteção em malha compartilhada, três métodos de escolha de caminhos: um que não considera os demais LSPs já estabelecidos na rede e dois que fazem tal consideração, de modo a avaliar, de acordo com a aplicação desses métodos, o impacto no uso dos recursos da rede, com a rede sem falhas e com falhas.

1.2 CONTRIBUIÇÕES

A principal contribuição deste trabalho é a comparação entre os impactos ao uso dos recursos da rede (com a rede sem falhas) e à sobrevivência da rede (em caso de falhas na rede) decorrentes da forma como são estabelecidos os LSPs na rede MPLS-TP em malha.

Esta contribuição pode ser útil na busca de um modelo de determinação ótima de caminhos em redes MPLS-TP com esquema de proteção em malha compartilhada, considerando os demais LSPs existentes na rede (o que é um problema NP-Completo).

O processo de escolha de caminhos propriamente dito, nessas redes, também envolve desafios, que serão explicados ao longo do trabalho, e cujas

soluções aplicadas também podem ser úteis na busca do modelo ótimo de determinação de caminhos nessas referidas redes. Neste caso, como contribuição secundária, é apresentada uma abordagem de solução ao problema dos caminhos em “trap”, solução esta até então inédita segundo a bibliografia pesquisada.

Durante o desenvolvimento do trabalho, foram submetidos artigos científicos à aceitação em Congressos Internacionais para apresentação e publicação em seus respectivos anais. Dos 5 Congressos Internacionais a que os artigos científicos foram submetidos, 4 os aceitaram (conforme abaixo). Desses 4, devido à impossibilidade (por motivos diversos) do autor comparecer aos locais dos referidos congressos, somente 1 deles aceitou publicar o artigo proposto mesmo na ausência do autor.

Congressos Internacionais que aceitaram os artigos científicos submetidos:

- a) Congresso Internacional: The 13th International Conference on Data Networks, Communications and Computers (DNCOCO '15) - WSEAS International Conference in Budapest, Hungary, 12-14/dez, 2015.

Título do artigo científico submetido: **“LSP placement in an MPLS-TP mesh network with shared mesh protection mechanism”**.

Obs: o artigo científico foi publicado nos anais desse Congresso Internacional, e uma cópia do mesmo se encontra no Apêndice A deste trabalho.

- b) Congresso Internacional: The Seventh International Conference on Intelligent Computing and Information Systems – ICICIS 2015. IEEE International Conference in Cairo, Egypt, 12-14/dez, 2015.

Título do artigo científico submetido: **“LSP placement in an MPLS-TP mesh network with shared mesh protection mechanism”**.

- c) Congresso Internacional: The 30th International Conference on Information Networking (ICOIN – 2016). IEEE International Conference in Kota Kinabalu, Malaysia; 13-15/jan, 2016.

Título do artigo científico submetido: **“Methods for LSP Selection in MPLS-TP Mesh Networks”**.

- d) Congresso Internacional: The 30th IEEE International Conference on Advanced Information Networking and Applications (AINA-2016), IEEE International Conference in Le Régent Congress, Centre, Crans-Montana, Switzerland, 23-25/mar, 2016;

Título do artigo científico submetido: “**LSP selection in an MPLS-TP mesh network**”.

1.3 ESTRUTURA DA TESE

A presente tese está estruturada em seis capítulos, uma lista de referências e um apêndice, conforme abaixo:

- Capítulo 1: Introdução – onde são apresentados o assunto, o objetivo, as contribuições e a estrutura desta Tese.
- Capítulo 2: Visão Geral da Tecnologia MPLS-TP – onde são apresentados uma breve introdução ao MPLS-TP, uma visão geral dessa tecnologia, seus requisitos, sua arquitetura de gerenciamento, seus respectivos requisitos de gerenciamento e a aplicabilidade dessa tecnologia; e também são comentados alguns trabalhos acadêmicos relacionados a essa abordagem introdutória ao assunto.
- Capítulo 3: Sobrevivência de Redes MPLS-TP – onde são apresentados uma visão geral dos aspectos de sobrevivência da tecnologia MPLS-TP, seu arcabouço de sobrevivência e seus mecanismos de proteção já aprovados: os de proteção linear e os de proteção linear em topologias em anel. Ao final do capítulo são comentados alguns trabalhos acadêmicos relacionados à sobrevivência de redes MPLS-TP.
- Capítulo 4: Estabelecimento de LSPs em Redes MPLS-TP em Malha – onde é apresentada a dificuldade de se estabelecer LSPs em uma rede MPLS-TP em malha, são comentados alguns trabalhos acadêmicos a respeito desse assunto e são explicados os métodos de estabelecimentos de LSPs que foram comparados, mediante simulações, no presente estudo.

- Capítulo 5: Simulações e Resultados – onde são apresentados o simulador, a abordagem utilizada para se evitar caminhos em “trap”, os cenários de simulação e os resultados alcançados. São também realizados comentários a respeito dos resultados obtidos.
- Capítulo 6: Conclusões – onde são apresentadas as conclusões e as considerações finais do trabalho, além de comentar novamente as contribuições e apresentar propostas de trabalhos futuros.
- Referências: onde são apresentadas as referências utilizadas no desenvolvimento deste trabalho.
- Apêndice A: Cópia de Artigo Científico Publicado
COSTA, C. R. F.; ZUCCHI, W. L., **LSP placement in an MPLS-TP mesh network with shared mesh protection mechanism**. In: Recent Advances on Systems, Signals, Control, Communications and Computers. Proceedings of the 13th International Conference on Data Networks, Communications and Computers (DNCOCO '15), p. 65-71. WSEAS International Conference; Budapest, Hungary, 12-14/dez, 2015.

2 VISÃO GERAL DA TECNOLOGIA MPLS-TP

Este capítulo apresenta: uma breve introdução ao MPLS-TP; uma visão geral dessa tecnologia, conforme apresentada na RFC-5921: “A Framework for MPLS in Transport Networks” (BOCCI et al., 2010); seus requisitos, de acordo com a RFC-5654: “Requirements of an MPLS Transport Profile” (NIVEN-JENKINS et al., 2009); sua arquitetura de gerenciamento, conforme definida na RFC-5950: “Network Management Framework for MPLS-based Transport Networks” (LAM; MANSFIELD; GRAY, 2010); seus respectivos requisitos de gerenciamento, estabelecidos na RFC-5951: “Network Management Requirements for MPLS-based Transport Networks” (LAM; MANSFIELD; GRAY, 2010); sua aplicabilidade, exemplificada na RFC-6965: “MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design” (FANG et al., 2013); e comenta alguns trabalhos acadêmicos relacionados a essa abordagem introdutória ao assunto.

2.1 BREVE INTRODUÇÃO AO MPLS-TP

O MPLS (*Multi-Protocol Label Switching*) é um sistema de roteamento rápido de pacotes por meio de rótulos: o rótulo de cada pacote permite aos roteadores direcioná-lo de acordo com o caminho a ser seguido, sem o “*overhead*” de ter de verificar o endereço completo de cada um dos pacotes. Desta maneira, o MPLS suporta múltiplos protocolos e oferece uma solução para aumentar a velocidade e a escalabilidade das redes. Já o MPLS-TP (MPLS - *Transport Profile*) é uma tecnologia em desenvolvimento (portanto ainda não consolidada), resultante do esforço para se fazer com que a tecnologia MPLS “original” adquira algumas extensões que permitam à mesma ser utilizada como uma rede de transporte confiável para qualquer tipo de tráfego.

A meta do MPLS-TP é prover, sobre redes legadas (baseadas em circuitos), transporte orientado a conexão para serviços baseados em pacotes, aproveitando a tecnologia MPLS já amplamente conhecida e empregada. Para isso, a rede MPLS-TP deve ser capaz de utilizar a infraestrutura física de rede instalada e transportar (encapsulados em pacotes) dados oriundos de uma grande variedade de tecnologias, desde SONET/SDH e OTN até Gigabit Ethernet (BELLER; SPERBER, 2009).

Em suma, o MPLS-TP é uma tentativa de evolução das redes de transporte de dados tradicionais (baseadas em comutação de circuitos, como SONET/SDH), de modo a torná-las aptas a transportar pacotes de dados sem perder suas características, como alta disponibilidade, suporte a QoS (*Quality of Service*), funções de OAM, “survivability” ou sobrevivência, etc (WINTER, 2011).

2.2 DEFINIÇÕES

Neste item são apresentadas as definições dos principais termos utilizados neste trabalho.

a) Rede-em-Camada

Uma rede-em-camada é uma construção lógica que independe do arranjo dos elementos físicos da rede. Um elemento físico da rede pode pertencer a uma ou mais redes-em-camadas, dependendo das suas ações em relação à pilha de rótulos dos pacotes transportados pelas redes. Uma rede-em-camada pode ter uma ou mais subcamadas (NIVEN-JENKINS et al., 2009).

Uma rede-em-camada provê a seus clientes um **serviço de transporte** e a operação de uma rede-em-camada independe do uso que o cliente faz da rede.

Uma rede-em-camada pode fornecer o serviço de transporte a uma rede de camada superior ou ser cliente do serviço de transporte fornecido por uma rede de camada inferior. A rede-em-camada que fornece o serviço de transporte é denominada **rede-em-camada servidora**, e a que recebe o serviço é denominada **rede-em-camada cliente**. Uma rede-em-camada pode ser servidora a uma camada superior e ser cliente de uma camada inferior ao mesmo tempo.

O serviço de transporte fornecido por uma rede-em-camada pode ser não orientado à conexão; comutado por pacotes e orientado à conexão; ou comutado por circuitos. Um mesmo cliente pode requerer, a uma determinada rede-em-camada, diferentes tipos de serviço de transporte.

A carga útil (payload) transportada pelo serviço de transporte pode ser livremente utilizada pelos clientes do serviço, sem que isso afete qualquer operação da rede-em-camada. Portanto, a carga útil do serviço de transporte pode ser formada por pacotes individuais (no caso de redes sem conexões); sequências de

pacotes (no caso de redes comutadas por pacotes e orientadas à conexão); ou um agendamento determinístico de dados (no caso de redes comutadas por circuitos).

b) Rede de Transporte

Rede de transporte é a rede que provê, de forma transparente, o transporte de dados entre os equipamentos clientes conectados à rede. Esse transporte de dados é realizado por meio de conexões ponto-a-ponto ou ponto-a-multiponto. Uma rede de transporte é independente de qualquer eventual rede de nível mais alto. Além de dados dos usuários, a rede de transporte deve suportar também o seu próprio tráfego operacional (tráfego gerado pelas atividades de controle de conexões, gerenciamento da rede, OAM, etc.) (BOCCI et al., 2010).

c) MPLS e MPLS-TP

O MPLS (Multi Protocol Label Switching) é um sistema de roteamento rápido de pacotes, no qual os roteadores direcionam os pacotes acordo com seus respectivos rótulos, sem verificar o endereço completo de cada um deles.

O MPLS-TP (Multi Protocol Label Switching – Transport Profile) é o **subconjunto** das funções MPLS que atendem aos requisitos estabelecidos na RFC-5654: “Requirements of an MPLS Transport Profile” (NIVEN-JENKINS et al., 2009); para a aplicação do MPLS na construção e operação de uma rede de transporte comutada por pacotes (BOCCI et al., 2010).

A tecnologia MPLS-TP utiliza, como entidades de transporte, Label Switched Paths (LSPs); Seções; e Pseudowires (PWs).

d) LSP (Label Switched Path)

Um **LSP** (Label Switched Path), de uma rede MPLS ou MPLS-TP, é uma sequência de n roteadores ($R_1, \dots, R_n$), através da qual os pacotes de mesmo rótulo (**label**) são roteados fazendo um caminho fixo (ou rota fixa), isto é, é uma sequência de n roteadores ($R_1, \dots, R_n$) nos quais as decisões de roteamento (de R_i para R_{i+1} onde $1 < i < n-1$) fazem com que os pacotes de mesmo rótulo sigam o mesmo caminho (ou a mesma rota) (ROSEN; VISWANATHAN, 2001).

Portanto, em um LSP de nível “m”:

- O roteador de ingresso R_1 do LSP acrescenta um rótulo à pilha de rótulos do pacote a ser transportado, fazendo com que essa pilha de rótulos tenha “m” níveis.
- Todos os roteadores intermediários R_i ($1 < i < n$) do LSP tomam suas decisões de roteamento exclusivamente por meio do rótulo de nível “m”.
- O roteador de saída R_n do LSP retira o rótulo inserido por R_1 . Depois disso, R_n toma sua decisão de roteamento pelo rótulo de nível m-1 da pilha de rótulos do pacote ou por qualquer outro método de roteamento.

Nas redes MPLS-TP, um LSP pode ser dos seguintes tipos (BOCCI et al., 2010):

- **Ponto-a-ponto unidirecional;**
- **Ponto-a-ponto bidirecional associado**, que consiste em dois LSPs unidirecionais distintos: um de A para B e outro de B para A;
- **Ponto-a-ponto bidirecional co-roteado**, que consiste em dois LSPs unidirecionais: um de A para B e outro de B para A, sendo que os dois componentes unidirecionais seguem exatamente o mesmo caminho em sentidos opostos, ou seja, seguem os mesmos nós e enlaces, resultando em um único caminho bidirecional);
- **Ponto-a-multiponto unidirecional**, que consiste em diversos LSPs ponto-a-ponto unidirecionais: cada LSP ponto-a-ponto unidirecional liga o nó de origem a um dos diversos nós de destino, ou seja, cada nó de destino é ligado ao nó de origem por um LSP ponto-a-ponto unidirecional distinto. Neste caso, como todos esses LSPs ponto-a-ponto unidirecionais estão associados a um determinado LSP ponto-a-multiponto unidirecional, todos os pacotes que saem do nó de origem

são rotulados com a identificação do LSP ponto-a-multiponto unidirecional e são automaticamente transmitidos em todos os LSPs ponto-a-ponto unidirecionais associados.

e) Seção MPLS-TP

Em um LSP de nível “ $m + 1$ ”, o roteador de ingresso R_1 desse LSP acrescenta um rótulo à pilha de rótulos do pacote a ser transportado, fazendo com que essa pilha de rótulos passe a ter “ $m + 1$ ” níveis, e o roteador de saída R_n desse LSP retira o rótulo inserido por R_1 , fazendo com que a pilha de rótulos do pacote volte a ter “ m ” níveis (se $m = 0$ então não há rotulamento de pacotes: neste caso, portanto, não existe um LSP e o roteamento dos pacotes não é baseado em rótulos).

Assim, considerando-se que o conjunto de LSPs de nível “ m ” provê o serviço de transporte ao LSP de nível “ $m + 1$ ”, então cada LSP de nível “ m ” na realidade é uma **seção MPLS-TP** do LSP de nível “ $m + 1$ ” (FROST; BRYANT; BOCCI, 2010). Observação: como não há LSP de nível 0, então um LSP de nível 1 não pode ser dividido em seções.

f) Caminho (ou Rota) de Transporte MPLS-TP

As denominações “Caminho de Transporte MPLS-TP” ou “Rota de Transporte MPLS-TP” têm o mesmo significado e correspondem a um LSP ou a um PW em ambiente MPLS-TP (NIVEN-JENKINS et al., 2009).

g) Domínio de Rede MPLS-TP

Um domínio de rede MPLS-TP representa um conjunto de entidades ou elementos de rede que são agrupados para um propósito ou por um motivo em particular, como por exemplo para unificar a subordinação (ou centralizar a responsabilidade) dos aspectos ou mecanismos de controle gerencial, controle administrativo, endereçamento, sobrevivência, etc (NIVEN-JENKINS et al., 2009).

h) Serviço Nativo de uma Rede MPLS-TP

O serviço nativo de uma rede MPLS-TP é o serviço de telecomunicações (conjunto de dados Ethernet, SDH, ATM, MPLS, MPLS-TP, etc.) que é transportado por essa rede (BOCCI et al., 2010).

i) Arquitetura em Planos das Redes MPLS-TP

As redes MPLS-TP são divididas em camadas arquiteturais denominadas “planos”: **Plano de Dados, Plano de Controle e Plano de Gerenciamento.**

- **Plano de Dados MPLS-TP**: camada arquitetural responsável pelas funções de encapsulamento e de transmissão dos pacotes de dados dentro de uma rede MPLS-TP (FROST; BRYANT; BOCCI, 2010).
- **Plano de Controle MPLS-TP**: camada arquitetural que provê métodos para estabelecer, remover e controlar os LSPs e PWs das redes MPLS-TP. Isso inclui o controle das atividades de OAM (Operação, Administração e Manutenção), controle do plano de dados e controle das funções de recuperação (ANDERSSON et al., 2011). O plano de controle, nas redes MPLS-TP, é opcional e separado do plano de dados. Uma falha no plano de controle não deve causar falhas no plano de dados. Quando existe, o plano de controle é responsável por prover dinamicamente os LSPs e os PWs das redes MPLS-TP. Quando não existe plano de controle, os LSPs e os PWs das redes MPLS-TP são criados estaticamente, pelos operadores, por meio de sistemas de gerenciamento de rede (Network Management Systems ou NMS) (BOCCI et al., 2010).
- **Plano de Gerenciamento MPLS-TP**: camada arquitetural responsável pelo gerenciamento da rede MPLS-TP, o que inclui, por exemplo, as atividades de configuração de todos os dispositivos da rede e a monitoração da operação e do desempenho da rede. Nas redes MPLS-TP, o plano de gerenciamento permite a criação estática, pelos operadores, dos LSPs e PWs. O gerenciamento de uma rede MPLS-TP deve ser separado ou

segregado do gerenciamento das redes de outras tecnologias e opera independentemente de qualquer outra camada (cliente ou servidora) de gerenciamento. Uma rede de gerenciamento MPLS-TP pode ser dividida em sub-redes por motivos de escalabilidade (separações geográficas ou balanceamento de carga) ou por motivos administrativos (LAM; MANSFIELD; GRAY, 2010).

j) Segmento MPLS-TP

Um segmento MPLS-TP é a parte de um LSP ou PW localizada sobre um simples link ou enlace. Um segmento concatenado MPLS-TP é um conjunto de vários seguimentos MPLS-TP contíguos e seus nós de interconexão.

Link ou enlace MPLS-TP é a conexão física ou lógica entre dois roteadores adjacentes. Um link pode fazer parte de nenhum, um ou vários LSPs ou PWs (NIVEN-JENKINS et al., 2009).

k) PseudoWire (PW)

Um **pseudowire (PW)** é um mecanismo que emula a existência de um “pseudo” cabo em uma rede de comutação de pacotes, ou seja, um PW transporta dados (sequência de bits, células, pacotes ou PDUs – *Protocol Data Units* –) de um determinado serviço de telecomunicações específico, por meio do encapsulamento desses dados dentro de uma rede de comutação de pacotes, de um roteador de origem (porta de entrada do PW) para um roteador de destino (porta de saída do PW), emulando assim a existência de um “pseudo” cabo entre esses dois roteadores (BRYANT, S.; PATE, 2005).

Em resumo, um PW encapsula os PDUs ou circuitos de dados (de um serviço de telecomunicações específico, como por exemplo Ethernet, SDH, ATM, etc.) que chegam ao roteador de entrada e transportam, até o roteador de saída, esses dados encapsulados por meio de túneis através da rede de comutação de pacotes.

Considerando-se que uma grande rede comutada a pacotes pode ser formada pela aglomeração de diversas outras redes (comutadas a pacotes) menores, com cada uma delas tendo seu próprio domínio de rede, um **segmento de**

PW é a parte de um PW de simples segmento ou de um PW de múltiplos segmentos que atravessa um túnel no interior de um determinado domínio de rede.

I) Tipos de Roteadores de uma Rede MPLS-TP

Um **CE** (Customer Edge) ligado a uma rede MPLS-TP é a entidade cliente que fornece ou recebe o tráfego de dados que entra ou sai de uma rede MPLS-TP.

Um **LSR** (Label Switching Router) de uma rede MPLS-TP é um roteador (de pacotes rotulados) que pertence a uma rede MPLS-TP. Pode ser de dois tipos: **Provider Edge (PE)** ou **Provider (P)** de uma rede MPLS-TP.

Um roteador **PE** (Provider Edge) de uma rede MPLS-TP é um **LSR** que encapsula o tráfego de dados (dos clientes) para ser transportado em um **LSP** de uma rede MPLS-TP. Esse encapsulamento pode ser feito pelo simples acréscimo de um rótulo à pilha de rótulos do pacote (fazendo com que esse PE se torne o R_1 de um novo LSP) ou pode requerer o uso de um PW.

Um PE existe na interface entre duas redes-em-camadas. No caso de um pseudowire de múltiplos segmentos, o PE pode ser do tipo **S-PE (Switching-PE)**, localizado entre dois segmentos do pseudowire de múltiplos segmentos) ou do tipo **T-PE (Terminating-PE)**, localizado nas extremidades do pseudowire de múltiplos segmentos).

Um roteador **P** (Provider) de uma rede MPLS-TP é um **LSR** que não tem a funcionalidade de PE em um LSP, ou seja, um roteador P de uma rede MPLS-TP apenas encaminha pacotes (ou seja, apenas provê o serviço de transporte), pois (ao contrário dos roteadores PE) não tem a funcionalidade de encapsular os dados dos clientes para transportá-los em um LSP.

Um **LER** (Label Edge Router) de uma rede MPLS-TP é um **LSR** localizado nas extremidades de um **LSP** MPLS-TP, isto é, é um LSR que pode acrescentar ou retirar rótulos da pilha de rótulos dos pacotes transportados.

2.3 ASPECTOS GERAIS DA TECNOLOGIA MPLS-TP

Nem todos os mecanismos ou capacidades da tecnologia MPLS são consistentes ou necessários para as operações de uma rede de transporte. Por outro lado, existem também características das redes de transportes que não são

plenamente suportadas pela tecnologia MPLS. A tecnologia MPLS-TP, que é um subconjunto da tecnologia MPLS, precisa combinar as capacidades existentes no MPLS com alguns mínimos mecanismos adicionais a fim de que possa ser utilizada para realizar o serviço de transporte.

A RFC-5654: “Requirements of an MPLS Transport Profile” (NIVEN-JENKINS et al., 2009) estabelece os requisitos das redes MPLS-TP: esses requisitos definem o comportamento que os mecanismos, dispositivos e procedimentos do MPLS-TP devem ter.

Ressalta-se que os LSPs MPLS-TP podem ser estabelecidos por meio de configuração estática ou dinâmica. A rede MPLS-TP e seus LSPs devem ser sempre totalmente controláveis mesmo na ausência de um plano de controle (NIVEN-JENKINS et al., 2009).

A tecnologia MPLS-TP pode ser utilizada para servir de base a redes de transporte de pacotes e, portanto, é aplicável a qualquer contexto de redes de pacotes (BOCCI et al., 2010).

2.3.1 Arquitetura Básica da Tecnologia MPLS-TP

A RFC-5921: “A Framework for MPLS in Transport Networks” (BOCCI et al., 2010) estabelece os seguintes elementos como sendo os componentes mínimos (ou arquitetura básica) de uma rede MPLS-TP:

- Um plano de dados MPLS.
- Um serviço de transporte de pacotes, provido por LSPs, PWs e seções MPLS-TP.
- Funções (proativas e sob-demanda) de OAM, para monitorar e diagnosticar a rede MPLS-TP.
- Planos de controle para LSPs e PWs, ou (na ausência de planos de controle) suporte para provisão e configuração estática dos LSPs e PWs.
- Mecanismos de proteção.
- Mecanismos de restauração, baseados em planos de controle (caso estes existam) ou baseados em funções de OAM ou de gerenciamento.
- Funções de gerenciamento.

A figura 2 abaixo ilustra um exemplo de relacionamento entre uma rede MPLS-TP e uma rede cliente MPLS ou MPLS-TP:

Figura 2 - Relacionamento entre uma rede MPLS-TP e sua rede cliente
Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

As figuras 3, 4, 5 e 6, a seguir, ilustram exemplos de arquiteturas MPLS-TP (respectivamente: PW de simples segmento; PW de múltiplos segmentos; LSP de simples seção; e LSP de múltiplas seções):

Figura 3 - Arquitetura MPLS-TP (PW de simples segmento)
Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

Figura 4 - Arquitetura MPLS-TP (PW de múltiplos segmentos)
 Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

Figura 5 - Arquitetura MPLS-TP (LSP de simples seção)
 Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

Figura 6 - Arquitetura MPLS-TP (LSP de múltiplas seções)
 Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

2.3.2 Funções de OAM (Operação, Administração e Manutenção)

Nas redes MPLS-TP, as funções de OAM são as responsáveis por verificar continuidade, conectividade e desempenho, ou para gerar, filtrar e gerenciar alarmes (locais ou remotos) de falhas, em quaisquer das suas entidades de transporte (LSPs, PWs ou seções). As funções de OAM MPLS-TP operam sem a necessidade de um plano de controle dinâmico, mas os pacotes de OAM recebem rótulos os associando a canais de controle.

Nas redes MPLS-TP as funções de OAM são também responsáveis pelas funções de gerenciamento de falhas (o que inclui a detecção e a localização das falhas) e de monitoração do desempenho (com medições de retardos e perdas de pacotes) de LSPs, PWs e seções MPLS-TP.

Nas redes MPLS-TP, quaisquer nós de um LSP ou de um PW (incluindo os nós PW S-PE) podem enviar pacotes de OAM. No entanto os pacotes de OAM só podem ser recebidos nos nós terminais (LSP endpoint ou PW T-PE endpoint) (BOCCI et al., 2010).

As redes MPLS-TP podem utilizar ou não planos de controle. O plano de controle MPLS-TP é baseado nos protocolos já existentes dos planos de controle MPLS e PW. A figura 7 abaixo mostra, para conexões MPLS-TP ponto-a-ponto (LSPs ou PWs), o relacionamento entre o plano de controle, o plano de gerenciamento, as funções de OAM, as funções de adaptação e as funções de transmissão.

Figura 7 - Contexto da Arquitetura do Plano de Controle MPLS-TP
Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

O Sistema de Gerenciamento de Rede (NMS) MPLS-TP pode ser centralizado ou distribuído. O Plano de Controle MPLS-TP é distribuído e pode ser transportado pela rede-em-camada servidora, por um LSP ou por um canal de controle.

Nas redes MPLS-TP, PWs de controle e manutenção são separados do túnel LSP de sinalização. A coordenação entre o controle dos LSPs e dos PWs ocorre nos nós terminais dos PWs. Os planos de controle dos PWs e dos LSPs são independentes e um pode ser empregado independente da existência do outro.

Nas redes MPLS-TP de múltiplas camadas, cada rede-em-camada utiliza seus próprios protocolos de controle, permitindo assim que diversos tipos e instâncias de protocolos de controle possam ser utilizados.

Os planos de controle MPLS-TP (quando empregados) provêm funções de sinalização, roteamento e engenharia de tráfego / determinação de caminhos. Em ambientes de múltiplos domínios, os planos de controle MPLS-TP podem empregar diferentes tipos de interfaces (com diferentes políticas de controle de troca de informações) nas fronteiras entre domínios.

Se necessário, o plano de controle MPLS-TP pode ativar as funções de OAM MPLS-TP para detectar e localizar falhas, de modo a restaurar um eventual caminho de transporte MPLS-TP em falha.

O plano de controle MPLS-TP possui suas próprias funções de sobrevivência, de modo a poder se recuperar de falhas e degradações. O plano de controle é logicamente desacoplado do plano de dados, de modo que uma falha no plano de controle não acarrete em falhas no plano de dados.

A configuração estática de um LSP ou de um PW (isto é, sem o suporte de um plano de controle) pode ser feita (pelos operadores da rede MPLS-TP) por meio da configuração direta dos PEs / LSRs ou via sistema de gerenciamento da rede. Um PW pode ser configurado estaticamente mesmo que o LSP que o suporta tenha sido configurado dinamicamente por um plano de controle, e o caminho de um LSP ou de um PW pode ser calculado dinamicamente, mesmo que o LSP ou o PW tenha sido configurado estaticamente (BOCCI et al., 2010).

2.3.3 Manutenção de Segmentos MPLS-TP

Um trecho ou porção MPLS-TP (ou seja, um segmento ou um segmento concatenado MPLS-TP) pode ser monitorado, protegido ou gerenciado por uma entidade denominada SPME (Sub-Path Maintenance Element).

Um SPME não transporta tráfego de dados diretamente das redes-em-camadas clientes e é estabelecido entre os nós terminais do trecho ou porção a ser monitorado, protegido ou gerenciado. Segundo a RFC-5921 (BOCCI et al., 2010), um LSR pode ser, por exemplo, roteador P de um LSP e, ao mesmo tempo, LER de um SPME. O tráfego (tanto de dados quanto de controle) do LSP é “tunelado” dentro do SPME. A figura 8 abaixo exemplifica a arquitetura de um SPME:

Figura 8 - SPME (Sub-Path Maintenance Element) ou Elemento de Manutenção de Segmentos MPLS-TP
Fonte: adaptação da RFC-5921 (BOCCI et al., 2010)

2.3.4 Gerenciamento de Redes MPLS-TP

A arquitetura de gerenciamento de redes MPLS-TP é definida na RFC-5950 “Network Management Framework for MPLS-based Transport Networks” (LAM; MANSFIELD, 2010) e seus requisitos estão estabelecidos na RFC-5951 “Network Management Requirements for MPLS-based Transport Networks” (LAM; MANSFIELD, 2010).

Nas redes MPLS-TP, o **sistema de gerenciamento de rede** (NMS ou Network Management System) gerencia os diversos **elementos de rede** (LSRs, LERs, PEs, S-PEs, T-PEs) que compõem a rede a ser gerenciada.

Cada **elemento da rede** possui uma **função de gerenciamento de equipamento** (EMF ou Equipment Management Function), que provê os meios pelos quais cada elemento é gerenciado pelo NMS.

O **canal de comunicação de gerenciamento** (MCC ou Management Communication Channel), fornecido pelo canal de controle, provê um canal para troca de informações de gerenciamento entre os elementos de rede.

As operações de manutenção de LSPs e PWs MPLS-TP independem da forma (estática ou dinâmica) pelas quais eles tenham sido criados. Segmentos MPLS-TP podem ser criados ou gerenciados de formas diferentes.

As **Funções de Gerenciamento de Falhas** (Fault Management Functions), presentes em cada elemento da rede, possibilitam as atividades de supervisão, detecção, validação, isolamento, correção e alarme das condições anormais das redes MPLS-TP.

As **Funções de Gerenciamento de Configuração** (Configuration Management Functions) controlam, identificam, coletam e inserem dados de configuração (de hardware e software) nos elementos da rede MPLS-TP. Também dão suporte às configurações das entidades de manutenção dos elementos da rede. Além disso, essas funções dão suporte também à configuração dos parâmetros de OAM.

As **Funções de Gerenciamento de Desempenho** (Performance Management Functions) existentes em cada elemento da rede dão suporte à avaliação e à divulgação de parâmetros de desempenho (como taxa de perdas de pacotes, retardos, etc.). Essas funções, que devem ser capazes de operar sob demanda ou proativamente, podem ser utilizadas para detectar e alarmar

Figura 10 - Modelo de Referência de Segurança 1 - Exemplo 1 (b)
 Fonte: adaptação da RFC-6941 (FANG et al., 2013)

- No **segundo modelo de referência de segurança**, o provedor não possui o controle total fim-a-fim da rede, pois compartilha esse controle com outros provedores de serviço, fazendo com que somente parte da rede MPLS-TP seja considerada como pertencente a uma “zona confiável”. As figuras 11 e 12 abaixo ilustram exemplos desse segundo modelo.

Figura 11 - Modelo de Referência de Segurança 2 - Exemplo 2 (a)
 Fonte: adaptação da RFC-6941 (FANG et al., 2013)

Figura 12 - Modelo de Referência de Segurança 2 - Exemplo 2 (b)
 Fonte: adaptação da RFC-6941 (FANG et al., 2013)

Segundo a RFC-6941 (FANG et al., 2013), as redes MPLS-TP podem sofrer diversos tipos de ataques, como manipulação indevida de rótulos, inserção de rótulos falsos, modificação, deleção ou replicação indevida de pacotes, etc.

Esses ataques podem causar o acionamento indevido de mecanismos de proteção, podem impossibilitar a restauração de LSPs ou podem provocar perdas de conectividade, além de outros tipos de falhas ou degradações em uma rede MPLS-TP.

Os alvos dos ataques às redes MPLS-TP podem ser o plano de dados, o plano de controle (se houver), o plano de gerenciamento, mais de um desses planos ou todos eles. Os ataques podem ser **externos** (originados de fora da zona confiável) ou **internos** (originados de dentro da zona confiável, ou seja, originados por entidades que têm acesso autorizado à rede e, acidental ou propositalmente, causam algum tipo de dano à rede).

As ameaças às redes MPLS-TP são diversas, como perda, alteração, inserção ou comprometimento de informações, geração de falsas mensagens de OAM, derrubada de LSPs, desvio de túneis MPLS-TP, ataques de DoS (Negação de Serviço), manipulação (coleta, modificação, inserção ou deleção) indevida de dados, etc.

As técnicas de defesa para redes MPLS-TP incluem uma grande diversidade de medidas, tais como autenticação, uso de infraestrutura isolada, verificação de conectividade, etc.

Ressalta-se, no entanto, que o assunto “segurança de redes MPLS-TP” é bastante amplo, engloba diversos aspectos (como vários tipos de ameaças e uma grande gama de técnicas defensivas) e foge ao escopo deste trabalho, sendo tratado em maiores detalhes pelas RFC-5920 (FANG, 2010) e RFC-6941 (FANG et al., 2013).

2.4 REQUISITOS DA TECNOLOGIA MPLS-TP

A RFC-5654 “Requirements of an MPLS Transport Profile” (NIVEN-JENKINS et al., 2009) especifica os requisitos das redes MPLS-TP, ou seja, os requisitos de comportamento para os mecanismos, dispositivos e procedimentos que constituem as redes MPLS-TP.

Existem, no entanto, outras RFCs que especificam, em maior nível de profundidade, os requisitos de algum outro aspecto em especial da tecnologia MPLS-TP:

- A RFC-5860 “Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks” (VIGOUREUX; WARD; BETTS, 2010) detalha os requisitos arquiteturais e funcionais dos mecanismos de OAM das redes MPLS-TP.
- A RFC-5951 “Network Management Requirements for MPLS-based Transport Networks” (LAM; MANSFIELD; GRAY, 2010) detalha os requisitos dos protocolos, mecanismos e procedimentos de gerenciamento das redes MPLS-TP.
- A RFC-7412 “Requirements for MPLS-TP Shared Mesh Protection” (WEINGARTEN et al., 2014) apresenta os requisitos básicos que devem ser atendidos por uma rede MPLS-TP que utilize proteção em malha compartilhada sem um Plano de Controle.

Os itens a seguir comentam, apenas de forma sintética, os requisitos listados na RFC-5654 (NIVEN-JENKINS et al., 2009), para que os principais aspectos abordados nessa RFC possam ser relacionados ao presente trabalho.

a) Requisitos Gerais do MPLS-TP

A RFC-5654 estabelece, nos seus requisitos de (1) a (29), os aspectos gerais para tecnologia MPLS-TP. Estes requisitos gerais definem as principais características do MPLS-TP, como o aproveitamento dos padrões do MPLS (no que se refere ao serviço de transporte), os tipos de tráfego suportado (ponto-a-ponto ou ponto-a-multiponto, bidirecional ou unidirecional), gerenciamento estático ou dinâmico, separação lógica entre os planos de controle e o plano de dados, etc.

b) Requisitos de Multicamadas do MPLS-TP

Os requisitos (30) a (35) da RFC-5654 tratam da capacidade das redes MPLS-TP utilizarem o conceito de redes-em-camadas, conforme explicado anteriormente neste trabalho.

c) Requisitos do Plano de Dados do MPLS-TP

Os requisitos do plano de dados do MPLS-TP (ou seja, os requisitos necessários para que uma rede MPLS-TP seja capaz de efetuar o serviço de transporte do tráfego de dados dos clientes) são estabelecidos nos requisitos (36) a (46) da RFC-5654.

d) Requisitos do Plano de Controle do MPLS-TP

Uma rede MPLS-TP pode ser controlada sem a existência de um plano de controle. No entanto, caso uma rede MPLS-TP utilize um plano de controle, este deverá atender aos requisitos (47) a (55) da RFC-5654. Esses requisitos estabelecem, por exemplo, a independência entre as topologias dos planos de dados e o plano de controle, o suporte aos mecanismos de OAM, aos mecanismos de recuperação e aos mecanismos de gerenciamento, etc.

e) Requisitos de Recuperação do MPLS-TP

A capacidade de sobrevivência é uma característica de importância crítica para as redes que se propõem a efetuar serviços confiáveis. Essas redes devem ter uma resiliência tal que lhes permitam rapidamente detectar falhas ou degradações e imediatamente restaurar os serviços a um nível pré-acordado (BOCCI et al., 2010).

Os requisitos de recuperação das redes MPLS-TP, por serem de maior relevância para o presente estudo, serão abordados neste tópico com um pouco mais de detalhes. Para tanto, a seguir serão resumidos os principais requisitos de recuperação para as redes MPLS-TP, correspondentes aos requisitos (56) a (109) da RFC-5654:

- O MPLS-TP deve prover mecanismos de proteção, aplicáveis a nós, enlaces, segmentos de caminhos (ou rotas) de transporte, segmentos concatenados de caminhos de transporte ou caminhos de transporte inteiros (fim-a-fim).
- O MPLS-TP deve prover mecanismos que garantam a recuperação da rede em menos de 50 ms, a partir do momento da detecção da falha, para redes de até 1.200 Km de extensão, e a proteção MPLS-TP deve atender a 100% do tráfego.
- Os mecanismos de recuperação devem ser aplicáveis a qualquer topologia e configuráveis para cada caminho de transporte da rede.
- Os mecanismos de proteção e os de restauração podem ser reversíveis ou não reversíveis.
- O MPLS-TP deve suportar os esquemas de proteção “1 + 1”, “1 : 1” e “1 : n”.
- Os mecanismos de recuperação devem estabelecer prioridade na ordem dos serviços a serem recuperados, podendo sacrificar os de menor prioridade em benefício da recuperação dos de maior prioridade.

- Os mecanismos de recuperação podem ser acionados a partir da indicação de falhas originados por outras camadas, pelos mecanismos de OAM, pelo plano de gerenciamento, pelo plano de controle (se houver) ou diretamente pelos operadores da rede.
- O plano de gerenciamento deve indicar a situação de todos os caminhos de transporte da rede e o histórico de todos os eventos de proteção (e seus respectivos motivos de acionamento).
- O plano de controle, se existir, deve suportar o estabelecimento e a manutenção de todas as entidades e funções de recuperação.
- O MPLS-TP pode (opcionalmente) suportar mecanismos de recuperação otimizados para topologias específicas (como por exemplo para topologias linear, em anel ou em malha), no entanto tais mecanismos devem ser interoperáveis com os mecanismos previstos para topologias genéricas (ou seja, para qualquer tipo de topologia), de modo a garantir a proteção de caminhos de transporte inteiros (fim-a-fim).

f) Requisitos de QoS (Quality of Service) para o MPLS-TP

As redes MPLS-TP devem atender aos requisitos mínimos de QoS, representados pelos requisitos (110) a (115) da RFC-5654, de modo a garantir que os acordos de níveis de serviços, estabelecidos com os clientes, possam ser alcançados.

Esses requisitos mínimos de QoS definem, em resumo, que as redes MPLS-TP devem: suportar diferentes serviços em diferentes tipos de tráfegos, garantir alocação de largura de banda flexível, suportar serviços sensíveis a retardos e a jitter (variações de retardos) e garantir tráfego de controle independentemente do volume do tráfego de dados.

2.5 APLICABILIDADE DA TECNOLOGIA MPLS-TP

A RFC-6965 “MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design” (FANG et al., 2013) trata com maiores detalhes da aplicabilidade da tecnologia MPLS-TP. Em resumo, pode se dizer que o MPLS-TP é uma nova tecnologia (de transporte de pacotes) que veio substituir as tradicionais tecnologias de transporte (SONET/SDH e TDM), oferecendo vantagens como alocação flexível da banda passante (o que proporciona um aproveitamento mais eficiente da banda), conexões com taxas flexíveis de transferência de dados e suporte a QoS para múltiplos serviços, com priorização de tráfego em caso de congestionamento.

As redes MPLS-TP, devido às suas características (principalmente de eficiência e custo), segundo Fang et al. (2013), vêm substituindo as redes legadas SONET/SDH, TDM (Time-Division Multiplexing) e ATM em diversos casos, como por exemplo nas redes de acesso e agregação às redes de transporte metropolitanas, nas redes ópticas de transporte de pacotes e nas redes de infraestrutura (ou backbones) das redes móveis.

Diversos foram os trabalhos acadêmicos publicados com o intuito de apresentar a tecnologia MPLS-TP e suas principais características e vantagens em relação a outras. A seguir são comentados alguns desses trabalhos.

Han et al. (2006) investigaram as potenciais vantagens do transporte baseado em pacotes por meio de uma comparação econômica quantitativa entre PTNs (Packet Transport Networks) e CTNs (Circuit Transport Networks). Os parâmetros econômicos utilizados na comparação foram o Custo de Aquisição (CapEx), o Custo de Operação (OpEx) e a Eficiência de Transporte. Os autores alcançaram os seguintes resultados: em relação às CTNs, as PTNs apresentaram um ganho de 18% de OpEx no 1º ano de testes, chegando a 24% no quarto ano. Considerando o transporte de todos os tipos de dados, as PTNs apresentaram um ganho de 48% de CapEx e de consumo de banda 70% menor em relação às CTNs. Alterando-se os dados para 25% TDM e 75% de todos os tipos, a vantagem das PTNs cai para 25% de CapEx e consumo de banda 57% menor em relação às CTNs. Os números encontrados pelo estudo demonstram a vantagem de se migrar para as PTNs e explicam o interesse comercial e industrial pelo desenvolvimento do MPLS-TP.

Huang et al. (2009) fazem um estudo abrangente dos requisitos das PTNs baseadas em MPLS-TP e da evolução histórica do esforço de padronização do

MPLS-TP. Ressalta-se que esse esforço de padronização ainda hoje permanece necessário.

Vaez-Ghaemi (2010) apresenta o MPLS-TP como sendo a nova geração de Redes de Transporte baseadas em Pacotes. O autor faz também um levantamento geral dos aspectos até então já definidos da tecnologia MPLS-TP, seus avanços em relação ao MPLS “puro” e seus recursos de sobrevivência de rede.

Hubbard (2011) apresenta uma pesquisa detalhada sobre diversos aspectos da tecnologia MPLS-TP, sua aplicabilidade, suas vantagens e seus desafios na época. Diversos fabricantes de roteadores nesse período (2011) já estavam, segundo o autor, produzindo e testando equipamentos capazes de utilizar o MPLS-TP, embora com algumas pequenas restrições. O autor também apresenta, nessa sua pesquisa, diversos exemplos de aplicações em que o uso do MPLS-TP traria melhor desempenho, assim como exemplos de equipamentos comerciais aprovados em testes de compatibilidade e de desempenho para uso em redes MPLS-TP.

Winter (2011) faz também um tutorial a respeito do MPLS-TP e conclui que, apesar de não estar ainda totalmente padronizada (principalmente em relação às soluções de sobrevivência), a tecnologia MPLS-TP (em 2011, quando o artigo foi publicado) já estava sendo utilizada como núcleo de diversos backbones de redes. O autor cita também a vantagem do menor custo do uso do MPLS-TP nas redes.

Como exemplo de aplicabilidade de redes MPLS-TP, Yan et al. (2010) apresentam uma avançada rede de satélites de baixa órbita baseada em MPLS-TP. Nessa rede, os satélites têm uma altitude que varia entre 500 e 2.000 km, viajam a uma velocidade típica de 20.000 km/h e não levam mais de 2 h para dar uma volta completa em torno da Terra. Os links inter-satélites são rápidos, mas os links entre os satélites e as estações terrenas são de baixa velocidade, provocando um “gargalo” nas comunicações entre a rede satélite e as estações terrestres. As ligações entre os satélites formam uma rede em malha de topologia altamente dinâmica (devido à rápida variação das posições dos satélites). Os autores estudam o comportamento do MPLS-TP nessa malha de topologia rapidamente mutante. Ao final, concluem que o MPLS-TP pôde prover a transmissão suave dos dados (sem grandes variações no fluxo de dados) e ao mesmo tempo garantir a QoS e as funções de OAM, apesar de (segundo os autores) ainda faltarem ser melhor discutidos aspectos como confiabilidade e segurança (security).

2.6 SÍNTESE DO CAPÍTULO

Neste capítulo foi apresentada uma visão geral da tecnologia MPLS-TP, procurando-se resumir as principais RFCs que abordam o assunto (preservando e ressaltando as padronizações nelas estabelecidas), de modo a, de forma introdutória, apresentar o tema e facilitar o entendimento dos capítulos posteriores deste trabalho. Também foram apresentados trabalhos acadêmicos que demonstram as potenciais vantagens do uso do MPLS-TP e explicam o interesse pelo seu desenvolvimento. Foi apresentado também (diferente dos diversos exemplos até então divulgados de uso do MPLS-TP como backbone de MANs e WANs) um exemplo de aplicação do MPLS-TP em uma rede satélite de baixa-órbita (interligando os satélites entre si e entre suas estações terrestres), de topologia altamente dinâmica, demonstrando a versatilidade de aplicações e uso do MPLS-TP.

3 SOBREVIVÊNCIA DE REDES MPLS-TP

A sobrevivência de uma rede, segundo Sprecher e Farrel (2011), é definida como sendo a capacidade dessa rede de recuperar sua taxa de entrega de dados após uma falha ou degradação do desempenho decorrente de erro, defeito ou ataque à rede.

As modernas redes de transporte, por sua vez, precisam ter características tais que as possibilitem rapidamente detectar falhas ou degradações na rede e imediatamente iniciar as medidas de recuperação necessárias, de modo a restabelecer prontamente os níveis de serviços acordados com os seus clientes. Os mecanismos de recuperação, portanto, é que garantem a sobrevivência da rede.

Em resumo, as características de sobrevivência de uma rede (isto é, as características dos seus mecanismos de detecção de falhas ou degradações e as características dos seus mecanismos de recuperação) é que determinam o nível de aplicabilidade dessa rede como uma moderna rede de transporte (SPRECHER; FARREL, 2011).

Este capítulo apresenta uma visão geral dos aspectos de sobrevivência da tecnologia MPLS-TP: seu arcabouço de sobrevivência, conforme descrito na RFC-6372: “MPLS-TP Survivability Framework” (SPRECHER; FARREL, 2011) e seus mecanismos de recuperação já aprovados: os de proteção linear, apresentados na RFC-6378: “MPLS Transport Profile (MPLS-TP) Linear Protection” (WEIGARTEN et al., 2011), e os de proteção linear em topologias em anel, apresentados na RFC-6974: “Applicability of MPLS Transport Profile for Ring Topologies” (WEIGARTEN et al., 2013). Ao final do capítulo são comentados alguns trabalhos acadêmicos relacionados à sobrevivência de redes MPLS-TP.

3.1 ARCABOUÇO DE SOBREVIVÊNCIA DA TECNOLOGIA MPLS-TP

A RFC-6372: “MPLS-TP Survivability Framework” (SPRECHER; FARREL, 2011) estabelece o arcabouço de sobrevivência para as redes MPLS-TP, ou seja, define elementos, tipos, métodos e considerações topológicas dos mecanismos de recuperação das redes MPLS-TP.

No ambiente MPLS-TP, as ações de recuperação, que visam reparar recursos ou redirecionar tráfegos, podem ser iniciadas automaticamente, a partir da detecção

de alguma falha ou degradação na rede, ou podem ser iniciadas por um operador (pelo plano de gerenciamento). As ações automáticas podem ser implementadas por mecanismos de OAM ou pela sinalização do plano de controle, caso seja utilizado um.

O arcabouço de sobrevivência das redes MPLS-TP descreve seus esquemas de recuperação e seus princípios de operação, estados de recuperação, “gatilhos” de acionamento de recuperação e troca de informações entre os elementos de suporte à recuperação.

Segundo esse arcabouço, o domínio de recuperação da tecnologia MPLS-TP oferece a possibilidade de escolha dos mecanismos de recuperação a serem utilizados, definição da granularidade pela qual o tráfego deve ser protegido e escolha do tipo específico de tráfego a ser protegido. Desta forma, a recuperação MPLS-TP pode prover diferentes níveis de proteção, para diferentes tipos de tráfego dentro do mesmo caminho, de acordo com os requisitos de cada serviço. No entanto, quanto maior for o grau de proteção requerido, maior será a quantidade de recursos consumidos.

O objetivo da flexibilidade descrita acima é proporcionar condições para que os operadores das redes MPLS-TP possam prover os mecanismos de proteção mais adequados, com razoável custo de recursos da rede, de acordo com os requisitos dos clientes (SPRECHER; FARREL, 2011).

3.1.1 Recuperação no Ambiente MPLS-TP

Os esquemas ou mecanismos de recuperação de uma rede MPLS-TP são aqueles dispositivos que, uma vez acionados (mediante, por exemplo, a detecção de falhas ou degradações na rede), tentam restabelecer o tráfego fim-a-fim, de acordo com os níveis de serviços pré-estabelecidos com os clientes. Os processos de recuperação podem ser acionados em caso de falha ou degradação de quaisquer das entidades de transporte (nós, enlaces, segmentos de rotas de transporte, segmentos concatenados de rotas de transporte ou rotas de transporte inteiras).

Os mecanismos de recuperação podem ser de **restauração** ou de **proteção** (MANNIE; PAPADIMITRIOU, 2006):

- **mecanismos de restauração:** são os mecanismos que efetivamente tentam restaurar os serviços da rede em caso de falha ou degradação. Usam qualquer capacidade disponível entre os nós e geralmente envolvem re-roteamento. As ações de restauração podem demorar até alguns segundos para serem concluídas, mas os resultados não são garantidos, pois pode não haver recursos disponíveis por ocasião do acionamento dessas ações.
- **mecanismos de proteção:** são os mecanismos que, por meio de comutação ou chaveamento, utilizam capacidades pré-definidas (ou pré-alocadas) em caso de falha ou degradação da rede. As entidades de proteção ficam reservadas (pré-alocadas) para serem utilizadas somente em caso de falha das entidades protegidas. Normalmente as ações de proteção são completadas em dezenas de milissegundos.

Os mecanismos de recuperação (restauração ou recuperação) podem ser **reversíveis** ou **não-reversíveis** e devem estabelecer a prioridade de recuperação dos serviços (os mais prioritários serão recuperados primeiro, de acordo com a capacidade disponível da rede).

As técnicas de recuperação podem ser otimizadas para diferentes topologias de redes MPLS-TP (topologias linear, em anel, em malha, etc.). No entanto, o uso dessas técnicas otimizadas não deve inibir ou prejudicar o uso de outras técnicas de recuperação em trechos adjacentes no mesmo caminho de transporte.

Os mecanismos de recuperação podem ser **unidirecionais** (somente o sentido afetado da rota de transporte é recuperado, mesmo que essa rota seja bidirecional) ou **bidirecionais** (os dois sentidos de uma rota de transporte são recuperados simultaneamente, mesmo que a falha tenha sido detectada em apenas um dos sentidos dessa rota).

Embora a arquitetura funcional dos mecanismos de proteção MPLS-TP possa ser aplicada tanto para LSPs quanto para PWs, a RFC-6372 se refere somente à proteção de LSPs e segmentos de LSPs (não tratando, portando, da proteção de PWs ou de segmentos de PWs).

A proteção de um PW MPLS-TP pode ser realizada pela proteção dos LSPs que dão suporte ao PW ou pela proteção da camada PW. No caso de ser realizada

proteção dos LSPs que dão suporte ao PW, entende-se que a proteção ao PW é operada na camada inferior.

A RFC-6372 relega a estudos futuros a definição dos mecanismos de recuperação pela camada PW (ou seja, dos mecanismos de recuperação dos PWs MPLS-TP). No entanto, ressalta que a recuperação de um PW pode ser provida pelo estabelecimento de um novo PW fim-a-fim em substituição ao PW em falha, e que deve existir também uma coordenação das ações de recuperação entre as camadas LSP e PW, de modo a se garantir que essas ações de recuperação sejam executadas em somente uma dessas camadas de cada vez.

A seguir são apresentadas as descrições gerais dos mecanismos que podem ser utilizados com propósitos de proteção nas redes MPLS-TP, segundo a RFC-6372:

a) Proteção a Nível de Enlace

A proteção a nível de enlace pode ser provida pela rede-em-camada inferior ou pela própria rede-em-camada do enlace. Não protege os nós de cada extremidade da entidade (enlace ou simples salto) a ser protegida. Para se proteger esses nós de cada extremidade devem ser usadas, em conjunto com a proteção a nível de enlace, a proteção de segmento ou a proteção fim-a-fim. A proteção a nível de enlace pode ser total (protegendo todo o tráfego da entidade de trabalho) ou parcial (protegendo somente uma parcela do tráfego da entidade de trabalho), e pode transportar tráfego extra quando ociosa.

b) Segmentos e Caminhos Alternativos

A proteção por meio de segmentos ou de caminhos alternativos é realizada por meio do pré-estabelecimento de entidades de proteção na mesma rede-em-camada da entidade protegida. É aplicável tanto para LSPs inteiros fim-a-fim quanto para segmentos de LSPs.

c) Túneis de Proteção

A proteção por meio de túneis é realizada por meio do pré-estabelecimento de entidades de proteção (denominadas túneis de proteção) que se localizam em redes-em-camadas diferentes daquela da

entidade protegida. Esses túneis podem prover proteção total (protegendo todo o tráfego da entidade de trabalho) ou parcial (protegendo somente uma parcela do tráfego da entidade de trabalho).

Nas redes MPLS-TP, as ações de recuperação são realizadas pelo plano de dados e podem ser iniciadas independentemente da forma pela qual a rede é configurada ou gerenciada, isto é, as ações de recuperação, realizadas no ambiente MPLS-TP pelo plano de dados, podem ser iniciadas pelo plano de controle (se houver um, pois é opcional), pelo plano de gerenciamento ou pelos mecanismos de OAM.

Em alguns esquemas de recuperação, como por exemplo na proteção bidirecional, se faz necessária uma coordenação entre os nós limítrofes (nós de borda) do domínio de recuperação para iniciar as ações de recuperação nas duas direções. Essa coordenação pode ser feita pelo plano de controle (se houver um) ou pelo plano de gerenciamento.

Relembra-se que, no ambiente MPLS-TP, as falhas e degradações na rede são detectadas pelas funções de OAM, responsáveis pela detecção e localização de falhas e pela monitoração do desempenho de LSPs, PWs e seções MPLS-TP. As falhas podem ser detectadas na própria rede-em-camada ou podem ser reportadas pela rede-em-camada inferior.

3.1.2 Escopos da Recuperação MPLS-TP

A RFC-6372 define os seguintes escopos de recuperação para as redes MPLS-TP:

a) Recuperação de Simples Salto

Um simples salto entre dois nós MPLS-TP vizinhos na mesma camada, denominado link ou enlace MPLS-TP, não deve ser confundido com um segmento simples MPLS-TP: um link ou enlace MPLS-TP pode fazer parte de nenhum, um ou vários LSPs ou PWs MPLS-TP, enquanto que um segmento simples MPLS-TP é a parte de um SLP ou PW que passa sobre um link ou enlace de uma rede MPLS-TP.

b) Recuperação de Segmento

A recuperação de um segmento MPLS-TP envolve o uso de um caminho alternativo para transporte do tráfego entre os nós terminais do segmento a ser recuperado. Se refere tanto à recuperação de um simples segmento MPLS-TP (simples salto ao longo do caminho de um LSP) quanto à recuperação de segmentos concatenados MPLS-TP (mais de um salto contínuo ao longo do caminho de um LSP).

De forma análoga, a recuperação de um **segmento PW** envolve a recuperação tanto de um PW de simples segmento quanto a recuperação de um PW de múltiplos segmentos. A RFC-6372 não trata da recuperação de segmento PW.

c) Recuperação Fim-a-Fim

A recuperação fim-a-fim envolve a recuperação de um LSP inteiro. Pode utilizar ou não algum dos nós intermediários ou links empregados no LSP original. A recuperação fim-a-fim é considerada um caso especial de recuperação de segmento, onde o segmento a ser recuperado é o caminho de transporte inteiro. Pode haver ocasiões em que a recuperação fim-a-fim não é possível, como por exemplo no caso de falhas nos nós terminais (nó de entrada ou nó de saída) do LSP, ou no caso de riscos compartilhados de falhas (devido a posição geográfica, recursos compartilhados, etc.).

Mais de um desses tipos de recuperação podem ser aplicados simultaneamente em um único LSP MPLS-TP.

Em um ambiente MPLS-TP, os esquemas de recuperação, por serem operados no plano de dados, podem envolver vários domínios de rede.

A RFC-6372 observa que a proteção de um LSP MPLS-TP contra falhas em um nó requer o uso de recuperação de segmento ou de recuperação fim-a-fim, enquanto que a proteção de um caminho de transporte contra falhas em um link requer o uso de recuperação de simples salto, recuperação de segmento ou recuperação fim-a-fim.

No caso de recuperação de redes multicamadas ou de recuperação de redes em múltiplos domínios (isto é, em domínios de recuperação aninhados), deve haver uma coordenação para se evitar condições de corrida nesse processo de recuperação (múltiplas camadas ou múltiplos domínios alocando recursos em resposta a uma mesma falha).

3.1.3 Graus de Recuperação MPLS-TP

Os graus de recuperação estão relacionados à velocidade com que o processo de recuperação será efetuado (e isso influencia a quantidade de dados perdidos) em caso de falhas na rede. Maiores graus de recuperação requerem pré-alocação de recursos para serem utilizados como caminhos de recuperação.

A RFC-6372 estabelece, abaixo listados, conceitos que (de acordo como forem ou não utilizados) podem impactar a velocidade da recuperação das redes MPLS-TP:

a) Proteção Dedicada

Na proteção dedicada, os recursos da entidade de proteção são reservados única e exclusivamente para uso do caminho de transporte a ser protegido.

b) Proteção Compartilhada

Na proteção compartilhada, as “m” entidades de proteção existentes são compartilhadas entre os “n” caminhos de transporte a serem protegidos (arquitetura de proteção “m : n”, na qual “m” ≥ 1 e “n” ≥ 1). Neste caso, após “m” falhas, os (“n”-“m”) caminhos restantes estarão desprotegidos. O MPLS-TP é obrigado a dar suporte somente à arquitetura “1 : n”, mas nada impede que, mesmo não sendo obrigado, dê suporte também à arquitetura “m : n”.

c) Tráfego Extra

É o tráfego que utiliza a capacidade ociosa de um determinado recurso de rede. O ambiente MPLS-TP não é obrigado a dar suporte a tráfego extra, mas nada impede que o tráfego extra exista. Quando um recurso de

proteção é requerido para atividades de proteção, qualquer tráfego extra que esteja utilizando esse recurso pode sofrer alta preempção (ser totalmente interrompido) ou baixa preempção (ter menor prioridade que o tráfego protegido, sem ser explicitamente descartado).

O tráfego extra não é suportado na proteção dedicada, mas pode existir em outros esquemas de proteção, como por exemplo na proteção compartilhada ou na proteção em túneis. O tráfego extra não é protegido (por definição), mas pode ser restaurado. A variação do tráfego extra (interrupção total ou degradação, dependendo do caso) pode ser detectada pelos mecanismos de OAM e ser reportada como uma falha (sob a perspectiva do tráfego extra), ou pode ser proativamente reportada por meio das sinalizações OAM ou do plano de controle.

Em caso de utilização da entidade de proteção, o tratamento do tráfego extra (interrupção ou degradação do mesmo) pode gerar uma troca adicional de mensagens nos planos de gerenciamento, de controle ou de dados. Essa troca adicional de mensagens pode retardar o processo de recuperação da rede e aumentar a complexidade do sistema de proteção. Portanto, há uma relação de compromisso entre as vantagens do uso do tráfego extra e suas desvantagens em caso de acionamento das entidades de proteção (retardo à recuperação da rede, overhead adicional na rede, aumento de complexidade e impacto aos serviços suportados pelo tráfego extra).

A RFC-6372 alerta que não se deve confundir tráfego extra com **tráfego de melhor esforço**, que é aquele que utiliza somente os recursos disponíveis, sem garantia de entrega e sem garantia de qualidade de serviços.

d) Restauração

Na ocorrência de falhas ou degradações na rede, caso os mecanismos de proteção não consigam restabelecer os serviços ou não estejam disponíveis, os mecanismos de restauração tentam (utilizando os recursos

de rede que estiverem disponíveis) restabelecer os serviços afetados. O processo de restauração requer o cálculo de novos caminhos e a ativação, por meio dos planos de controle ou de gerenciamento, de novos LSPs. Por envolver mais etapas, as atividades de restauração são mais demoradas que as atividades de proteção. Além disso, os processos de restauração podem não conseguir recuperar os serviços (aos níveis acordados com os clientes) devido à eventual indisponibilidade de algum dos recursos de rede necessários. LSPs de menor prioridade podem ser preemptados pelos LSPs de recuperação.

A restauração pode ser **pré-planejada**: os recursos para restauração podem ser pré-calculados ou mesmo pré-sinalizados antes do início do processo, mas nunca pré-alocados. O estabelecimento e a ativação dos LSPs de restauração só podem ocorrer após o início do processo de restauração.

e) Reversão

O processo de recuperação pode ser **reversível** ou **não-reversível** e esse comportamento quanto à reversão pode ser configurado para cada serviço ou para cada instância de recuperação.

3.1.4 Domínios de Recuperação MPLS-TP

Um domínio de recuperação, que pode ser tanto um domínio de proteção (relacionado a atividades de proteção) quanto um domínio de restauração (relacionado a atividades de restauração), se localiza entre os nós terminais de um elemento (simples salto, segmento ou caminho fim-a-fim inteiro) passível de ser recuperado. Os mecanismos de recuperação devem desempenhar suas atividades (de recuperação) dentro do seu respectivo domínio. Um domínio de proteção pode conter outros domínios de proteção dentro dele (domínios de proteção aninhados), mas não pode haver interseção apenas parcial entre domínios de proteção. Os nós terminais de um domínio de recuperação não são protegidos, a não ser que este domínio de recuperação esteja inserido dentro de um domínio de recuperação maior e seus respectivos nós terminais não sejam coincidentes.

Um caminho fim-a-fim inteiro, por exemplo, está contido dentro de um único domínio de recuperação, onde os LERs de entrada e de saída do LSP são os nós terminais do domínio de recuperação. No caso de uma entidade de proteção ponto-a-ponto, um LSP entra no domínio de proteção por um dos dois nós terminais (delimitadores do domínio de proteção) e sai pelo outro nó terminal. Já no caso de uma entidade de proteção unidirecional ponto-a-multiponto, existem três ou mais nós terminais delimitadores do domínio de proteção (um é o nó-raiz ou nó-fonte e os outros são os nós-folhas ou nós-sorvedouros).

3.1.5 Proteção de Redes MPLS-TP em Malha

Nas redes em malha (isto é, nas redes que tenham ligações arbitrárias entre seus nós), uma proteção possível de ser utilizada entre dois pontos da rede, segundo a RFC-6372, é a proteção linear, que pode proteger um nó, um simples salto, um segmento de transporte ou um caminho de transporte inteiro.

Em uma rede em malha, a proteção linear de um segmento de LSP é efetuada por meio de um SPME (Sub-Path Maintenance Element), descrito anteriormente.

De acordo com a RFC-6372, nas redes MPLS-TP em malha os caminhos de trabalho e seus respectivos caminhos de proteção não podem compartilhar nenhum link ou nó além dos nós terminais, ou seja, os caminhos de trabalho devem ser totalmente diversos dos seus respectivos caminhos de proteção. As redes MPLS-TP em malha suportam os seguintes tipos de proteção linear:

a) Proteção Linear “1 : n”

Na proteção linear “1 : n” em uma rede em malha, para se proteger “n” caminhos de trabalho existentes entre dois pontos, é alocado um único caminho de proteção, que deverá ser utilizado em caso de degradação ou falha em qualquer um dos “n” caminhos de trabalho protegidos ($n \geq 1$). Pode haver tráfego extra no caminho de proteção (aproveitando a capacidade ociosa do mesmo). A figura 13 ilustra um exemplo de proteção linear “1 : 2” entre dois nós de uma rede em malha:

Figura 13 - Exemplo de Proteção Linear “1 : 2” em uma rede em Malha
Fonte: adaptação da RFC-6372 (SPRECHER; FARREL, 2011)

b) Proteção Linear “1 + 1”

Na proteção linear “1 + 1” em uma rede em malha, uma entidade de proteção totalmente dedicada é alocada à entidade de trabalho a ser protegida. Nesta arquitetura “1 + 1”, no nó de origem o tráfego de dados do caminho de trabalho é simultânea e inteiramente copiado para o caminho de proteção, e o nó de destino seleciona um dos fluxos de dados que chegam, conforme exemplificado na figura 14 abaixo:

Figura 14 - Exemplo de Proteção Linear “1 + 1” em uma rede em Malha
Fonte: adaptação da RFC-6372 (SPRECHER; FARREL, 2011)

c) Proteção Linear Ponto-a-Multiponto (P2MP)

Nas redes em malha, as entidades de transporte ponto-a-multiponto possuem um nó de origem (nó-raiz ou nó-fonte) e diversos nós de destino (nós-folhas ou nós-sorvedouros), formando caminhos de transporte unidirecionais. No esquema de proteção “1 + 1” dessas entidades, cada caminho entre o nó-raiz e um dos nós-folhas é protegido da mesma

maneira que na proteção “1 + 1” ponto-a-ponto (uma entidade de proteção totalmente dedicada, com o tráfego de dados inteira e simultaneamente copiado).

No esquema de proteção “1 : 1” dessas entidades, para cada caminho de trabalho (entre o nó-raiz e um dos nós-folhas) é alocado um caminho de proteção, que deverá ser utilizado em caso de degradação ou falha do caminho de trabalho protegido.

A RFC-6372 não detalha o esquema de proteção “1 : n” para as entidades ponto-a-multiponto, embora o suporte a este esquema seja previsto na RFC-5654 (que trata dos requisitos das redes MPLS-TP).

d) Proteção em Malha Compartilhada

Na proteção em malha compartilhada, os recursos de proteção servem para proteger LSPs que não compartilhem nenhum dos seus nós terminais, isto é, na proteção em malha compartilhada dois ou mais LSPs distintos compartilham trechos do mesmo caminho de proteção, conforme exemplificado na figura 15 abaixo. Adicionalmente, o caminho de proteção pode transportar tráfego extra.

Figura 15 - Topologia de Proteção em Malha Compartilhada
Fonte: adaptação da RFC-6372 (SPRECHER; FARREL, 2011)

3.2 PROTOCOLO PARA COORDENAÇÃO DO ESTADO DE PROTEÇÃO LINEAR EM REDES MPLS-TP EM MALHA

A proteção linear de redes em malha pode necessitar de coordenação entre os seus nós terminais para ser realizada. A RFC-6378 “MPLS-TP Linear Protection”

(WEIGARTEN et al., 2011) apresenta um protocolo, denominado **PSC** (Protection State Coordination), para coordenação de estado de proteção linear, aplicável nos casos de proteção bidirecional “1 : 1” e proteção unidirecional ou bidirecional “1 + 1” de um caminho bidirecional.

Este protocolo PSC não é aplicável para a proteção unidirecional “1 : 1” ou para a proteção (unidirecional ou bidirecional) “1 : n”.

A proteção unidirecional “1 + 1”, embora não requeira coordenação entre seus nós terminais, pode utilizar o protocolo PSC para que um nó terminal avise o nó terminal oposto que um chaveamento ocorreu e para verificar a consistência das configurações. Isso pode ser útil no caso de proteção linear ponto-a-multiponto “1 + 1”, já que essa proteção é unidirecional por definição.

A arquitetura de funcionamento do protocolo PSC é a seguinte: uma **Unidade de Lógica de Requisição Local** processa as requisições de chaveamento que receber dos dispositivos de OAM, da rede-em-camada servidora, do plano de controle local (se for utilizado um), dos operadores externos e do temporizador de espera (que evita o chaveamento sucessivo em caso de falha intermitente). Após processar as requisições recebidas, a Unidade de Lógica de Requisição Local envia a requisição local de mais alta prioridade à **Unidade de Controle Lógico do PSC**, que faz a verificação cruzada dessa informação recebida localmente com a requisição recebida do PSC remoto (do nó oposto). De acordo com o resultado do processamento das informações recebidas, a Unidade de Controle Lógico do PSC determina as ações a serem tomadas pelo nó local, as mensagens a serem enviadas ao nó oposto e o status do domínio de proteção.

A figura 16 resume a Lógica do Controle de Coordenação do Chaveamento de Proteção do protocolo PSC:

Figura 16 - Lógica do Controle de Coordenação do Chaveamento de Proteção
Fonte: adaptação da RFC-6378 (WEIGARTEN et al., 2011)

3.3 APLICABILIDADE DE PROTEÇÕES MPLS-TP EM TOPOLOGIAS EM ANEL

A RFC-6372 não detalha arquiteturas ou mecanismos de proteção específicos para redes MPLS-TP em anel, mas a RFC-5654 (que trata dos requisitos das redes MPLS-TP) estabelece requisitos para a proteção em anel, compatíveis com os requisitos genéricos para recuperação de redes MPLS-TP.

A RFC-6974 “Applicability of MPLS-TP for Ring Topologies” (WEIGARTEN et al., 2013) propõe formas de aplicabilidade dos mecanismos de proteção MPLS, tanto local quanto fim-a-fim, em redes em anel MPLS-TP. No entanto, essa RFC aborda apenas a proteção em um anel simples, cujo domínio de proteção se localiza entre o nó de entrada no anel e o nó de saída, não tratando portanto da proteção de anéis interconectados ou de nós ou enlaces de interconexão de anéis.

A proteção de um anel simples é aplicável a um caminho de transporte ponto-a-ponto que pertence a um anel ou a um caminho de transporte ponto-a-multiponto cujos ramos (caminhos entre o nó-raiz e os nós-folhas) pertencem a um anel. As falhas podem ocorrer nos enlaces entre dois nós do anel ou nos nós do anel.

Basicamente, a proteção aplicável a topologias em anel simples MPLS-TP, segundo a RFC-6974, se resume a dois tipos: “**Wrapping**” e “**Steering**”.

- Na proteção “**Wrapping**” ponto-a-ponto, um nó do anel, ao perceber uma falha adiante (que tanto pode ser falha de enlace quanto falha de nó), faz o tráfego de dados se desviar (a partir desse nó que percebeu a falha) para o caminho de proteção, ou seja, o nó que percebeu a falha faz o chaveamento do tráfego para o caminho de proteção, que só volta a ser chaveado para o caminho de trabalho no nó que se segue à falha. No entanto, este tipo de proteção em anel faz com que alguns recursos de rede possam ser utilizados de forma duplicada (como nos links “A-B” e “E-F” do exemplo da figura 17 abaixo).

Figura 17 - Exemplo de Proteção “Wrapping” ponto-a-ponto em Anel Simples
Fonte: adaptação da RFC-6974 (WEIGARTEN et al., 2013)

- Na proteção “**Steering**” ponto-a-ponto, o chaveamento de proteção é sempre realizado pelo nó de entrada no anel e o caminho de proteção termina no nó de saída do anel (evitando-se, assim, o uso duplicado de links). Neste tipo de proteção se faz necessária a notificação da falha ao nó de entrada no anel. A figura 18 abaixo exemplifica a proteção “Steering” em um anel simples MPLS-TP.

Figura 18 - Exemplo de Proteção “Steering” ponto-a-ponto em Anel Simples
Fonte: adaptação da RFC-6974 (WEIGARTEN et al., 2013)

No caso de proteção ponto-a-multiponto em anéis simples MPLS-TP, as proteções “Wrapping” e “Steering” preservam seus respectivos comportamentos aplicados na proteção ponto-a-ponto, com as devidas adaptações.

Na proteção “Wrapping” ponto-a-multiponto o chaveamento de proteção é sempre realizado pelo nó anterior à falha e chaveado de volta ao caminho de trabalho no nó que se segue à falha, tal como na proteção “Wrapping” ponto-a-ponto. Depois disso o tráfego retoma seu fluxo normal e é chaveado para as respectivas saídas. Nesse tipo de proteção também ocorrem casos de recursos de rede utilizados de forma duplicada (como nos links “A-B”, “C-D”, “D-E” e “E-F” do exemplo da figura 19 abaixo).

Figura 19 - Exemplo de Proteção “Wrapping” ponto-a-multiponto em Anel Simples
Fonte: adaptação da RFC-6974 (WEIGARTEN et al., 2013)

Para melhorar o desempenho da proteção “Wrapping” ponto-a-multiponto, a RFC-6974 define a proteção “ROM-Wrapping” (Ring Optimized Multipoint Wrapping). Nessa proteção, cada nó tem previamente estabelecido seu caminho de proteção em caso de falha à sua frente no caminho de trabalho. Por exemplo, na figura 20 abaixo, o LSP de trabalho é definido pela sequência de nós B – A – E – E – D – C

(onde os nós de saída estão sublinhados). Nesse exemplo, usando a proteção “ROM-Wrapping”, cada nó teria previamente configurado seu caminho de backup (a partir dele mesmo até o último nó de saída, no sentido oposto ao do caminho de trabalho), para ser utilizado em caso de falha à sua frente pelo caminho de trabalho, conforme abaixo:

caminho de backup do nó A => A – B – C – D – E – F

caminho de backup do nó B => B – C – D – E – F

caminho de backup do nó C => C

caminho de backup do nó D => D – E – F – A – B – C

caminho de backup do nó E => E – F – A – B – C

caminho de backup do nó F => F – A – B – C – D – E

A vantagem da proteção “ROM-Wrapping”, em relação à proteção “Wrapping”, é que ela usa menos recursos de redes, pois apresenta um menor número de recursos usados em duplicidade. Por exemplo, na figura 20 abaixo, a proteção “ROM-Wrapping”, devido à falha no link “E-F”, provoca a duplicação de uso apenas dos links “A-B” e “A-F”.

Figura 20 - Exemplo de Proteção “ROM-Wrapping” em Anel Simples
Fonte: adaptação da RFC-6974 (WEIGARTEN et al., 2013)

No caso de proteção “Steering” ponto-a-multiponto em anéis simples MPLS-TP, o comportamento é análogo ao da proteção “Steering” ponto-a-ponto: o chaveamento de proteção é sempre realizado pelo nó de entrada no anel e o caminho de proteção termina no último nó de saída do anel (evitando-se, assim, o uso duplicado de links). A figura 21 abaixo exemplifica a proteção “Steering” ponto-a-multiponto em um anel simples MPLS-TP. Nesse exemplo, devido à falha no link “E-F”, o nó de entrada B duplica os caminhos, transferindo ao mesmo tempo um fluxo

de dados no caminho de trabalho e outro no caminho de proteção, evitando deste modo o uso duplicado de links.

Figura 21 - Exemplo de Proteção “Steering” ponto-a-multiponto em Anel Simples
Fonte: adaptação da RFC-6974 (WEIGARTEN et al., 2013)

3.4 TRABALHOS RELACIONADOS

Dongyun-Zhou e Subramaniam (2000) apresentam uma visão geral das técnicas (até então) utilizadas para se alcançar sobrevivência nas tradicionais redes ópticas, e como essas técnicas estavam, naquela época, evoluindo para prover sobrevivência nas novas gerações de redes. Segundo eles, os algoritmos de restauração, por serem dinâmicos (buscarem os caminhos alternativos somente após a ocorrência das falhas nos caminhos de trabalho), são muito complicados e o tempo de restauração é muito maior que o tempo de chaveamento do tráfego para os caminhos pré-estabelecidos de proteção. Ainda segundo eles, a proteção compartilhada utiliza os recursos da rede muito mais eficientemente que a proteção dedicada.

Makam et al. (1999) propuseram um modelo de recuperação para redes MPLS no qual o último nó antes da falha avisa ao nó inicial para que o tráfego seja desviado na origem, conforme ilustrado na figura 22 abaixo.

Figura 22 - Modelo de Makam
Fonte: adaptação de Makam et al. (1999)

Tentando minimizar a perda de pacotes que ocorria nesse modelo proposto por Makam (citado acima), Haskin e Krishnan (2000) propuseram um modelo semelhante, no qual o tráfego MPLS é chaveado de volta no último nó antes da falha. A proposta deles diminuía a perda de pacotes, mas aumentava o uso de recursos de rede, conforme exemplificado na figura 23 abaixo.

Figura 23 - Modelo de Haskin e Krishnan
Fonte: adaptação de Haskin e Krishnan (2000)

Hundessa e Pascual (2001) propuseram um modelo otimizado em relação a estes dois anteriores: os nós entre a falha e o nó origem armazenariam os pacotes do fluxo de ida enquanto estivessem recebendo um fluxo de volta, retransmitindo-os de volta após o término do fluxo de volta (sem repassá-los adiante no caminho de ida). O nó origem, ao receber um fluxo de volta, interromperia o envio (pelo caminho inicial), retransmitiria por um novo caminho os pacotes recebidos de volta e, após isso, transmitiria o restante dos pacotes já pelo novo caminho.

Já a RFC-4090 “Fast Reroute Extensions to RSVP-TE for LSP Tunnels” (PAN; SWALLOW; ATLAS, 2005) estabelece o modelo conhecido como “MPLS Fast Reroute um-para-um”, no qual para cada nó é pré-selecionado um caminho backup até o segundo nó seguinte (com exceção do penúltimo nó, cujo backup só poderia ser até o primeiro nó seguinte), conforme ilustrado na figura 24 abaixo. A proteção “ROM-Wrapping”, mostrada anteriormente, foi baseada no modelo “MPLS Fast Reroute um-para-um”. A técnica “fast reroute” é aquela na qual os caminhos de proteção são alocados para a proteção local de segmentos de caminhos (PETERSSON, 2005).

Figura 24 - Modelo MPLS Fast Reroute um-para-um
Fonte: adaptação da RFC-4090 (PAN; SWALLOW; ATLAS, 2005)

Hundessa e Domingo (2002) propuseram melhorias em relação ao modelo “MPLS Fast Reroute um-para-um” acima, apresentando o modelo “MPLS Fast Reroute um-para-um com merging”, no qual os caminhos de backup um-para-um, quando se cruzam, os de maior tamanho (em número de saltos) se “mesclam” com os de menor tamanho. A figura 25 abaixo ilustra um exemplo desse modelo, no qual o caminho de backup 1 (de 4 saltos) se mescla com o caminho de backup 2 (de 3 saltos), passando a ter 5 saltos.

Figura 25 - Modelo MPLS Fast Reroute um-para-um com merging
Fonte: adaptação de Hundessa e Domingo (2002)

Kosta, Thaker e Nagar (2011) apresentaram uma comparação, mediante rigorosos estudos, entre os desempenhos dos modelos “Makam”, “Haskin”, “Fast Reroute um-para-um” e “Fast Reroute um-para-um com merging”. Em relação ao parâmetro “perdas de pacotes”, os resultados foram os seguintes: o melhor desempenho foi o do modelo “Haskin”, seguido dos modelos “Fast Reroute um-para-um”, “Fast Reroute um-para-um com merging” e “Makam”, nessa ordem. Em relação ao parâmetro “tempo total de recuperação”, a ordem dos resultados foi a seguinte (do melhor para o pior desempenho): “Fast Reroute um-para-um”, “Fast Reroute um-para-um com merging”, “Haskin” e “Makam”. Em relação ao parâmetro “uso de recursos pré-alocados”, o melhor avaliado foi o modelo “Makam”, e os demais modelos ficaram (nesse parâmetro) empatados em segundo lugar. Em relação ao parâmetro “desordenamento de pacotes durante a restauração”, os melhores modelos foram os seguintes (em ordem decrescente de desempenho): “Makan” (apesar de apresentar o maior índice de perda de pacotes), “Fast Reroute um-para-um com merging”, “Fast Reroute um-para-um” e “Haskin”. Em suma, verifica-se que há uma solução de compromisso entre os modelos empregados e os quatro parâmetros estudados.

O estudo acima demonstra que, de acordo com o tipo de tráfego a ser transportado pela rede (e seus respectivos requisitos de QoS), o esquema de

recuperação empregado pode impactar no desempenho global da rede em caso de necessidade de recuperação mediante a ocorrência de falhas. Nesse sentido, se faz importante ressaltar o estudo de Cao et al. (2010), que demonstra que uma rede de transporte MPLS-TP suporta tráfegos de múltiplas classes e características, tais como VoIP, streaming de dados (HDTV/SDTV, Vídeo-on-Demand - VoD, P2P), TDM, Ethernet, PDH, SDH, ATM, FR (Frame-Relay), etc.; e que, por isso, o tráfego de pacotes em um backbone MPLS-TP tem uma distribuição “self-similar”.

Wang, Sahasrabuddhe e Mukherjee (2002) investigaram três escopos básicos de restauração (de segmento simples, de segmentos concatenados e fim-a-fim), e concluíram que a restauração de segmentos concatenados tem (em termos de uso dos recursos da rede) desempenho melhor que a restauração de simples segmento, e que a restauração fim-a-fim, por sua vez, tem desempenho melhor que a de segmentos concatenados, conforme exemplificado na figura 26 abaixo.

Figura 26 - Restauração de segmentos e fim-a-fim

Fonte: adaptação de Wang, Sahasrabuddhe e Mukherjee (2002)

Ho, Tapolcai e Cinkler (2004) demonstram que o uso de proteção compartilhada de segmentos em redes em malha é vantajoso em relação a outros tipos de proteção, devido à possibilidade de oferecer tempos de recuperação menores e garantidos e ao fato de que uma maior possibilidade de compartilhamento de recursos pode oferecer proteção a um maior número de segmentos.

Os estudos de Hue-Fen et al. (2010), Hua et al. (2010) e Huifeng e Yuefeng (2011) propõem a adoção de mecanismos de alarme antecipado de falhas, segundo os quais os caminhos de restauração seriam pré-calculados por ocasião da ocorrência de um alarme antecipado: neste caso, os caminhos de restauração pré-calculados seriam estabelecidos e ativados somente após as falhas tiverem sido

efetivamente confirmadas. Haveria então, portanto, um ganho de tempo devido ao pré-cálculo antecipado dos caminhos de restauração a serem utilizados. A dificuldade, nessa abordagem, recai sobre a capacidade efetiva desses mecanismos em prover alarmes realmente antecipados das falhas, ou seja, em prover o alarme em um tempo antecipado tal que permita finalizar o pré-cálculo do caminho de restauração antes da ocorrência propriamente dita da falha.

Roy et al. (2014) compararam o uso de esquemas de proteção em malha compartilhada em relação ao esquema de proteção 1+1 em serviços de alta prioridade (tempo de proteção ≤ 50 ms). Eles concluíram que, mesmo para serviços críticos de alta prioridade, a proteção em malha compartilhada pode atender dentro do tempo (≤ 50 ms), a um custo menor, principalmente em caso de falhas múltiplas.

Tendo em vista que as redes de transporte legadas em geral utilizam a infraestrutura física de anéis interconectados e são baseadas na comutação de circuitos, ou mais especificamente na tecnologia SONET/SDH (HAN et al., 2006), alguns estudos foram feitos tentando-se empregar o MPLS-TP nessas redes legadas, de modo a se reduzir o custo de evolução. Sob essa abordagem, Zhang et al. (2009), Zhang, Berger e Ruepp (2010) e Zhang et al. (2011) propõem esquemas de proteção para prover serviços multicast MPLS-TP usando topologias de proteção de anéis interconectados. O estudo deles mostra um intensivo uso de recursos empregando-se topologias de proteção em anel, demonstrando que tais mecanismos de proteção são menos eficientes (quanto ao uso de recursos) que a proteção em malha compartilhada.

Yoshikane e Tsuritani (2014) fazem, em redes ópticas de mais de 100 Gbps, um estudo comparativo de custos de utilização de recursos de redes entre proteções dedicadas e proteções em malha compartilhada. A partir da avaliação comparativa realizada, baseada nas topologias dos EUA, da Europa e do Japão, eles demonstram que a proteção em malha compartilhada é mais eficiente em termos de utilização dos recursos de fibra óptica das redes.

3.5 SÍNTESE DO CAPÍTULO

Neste capítulo foi apresentada uma visão geral dos aspectos de sobrevivência da tecnologia MPLS-TP, seu arcabouço de sobrevivência e seus mecanismos de recuperação padronizados por meio de RFCs: os de proteção linear

e os de proteção linear em topologias em anel. Ao final do capítulo foram comentados alguns trabalhos acadêmicos relacionados à sobrevivência de redes MPLS-TP. O assunto, no entanto (apesar da importância das características de sobrevivência das redes MPLS-TP para se tornarem a base das modernas redes de transporte), não está plenamente consolidado, o que possibilita ainda a realização de uma grande gama de estudos a ele relacionados, sob diversas abordagens. Dos trabalhos analisados, ressalta-se a recorrente demonstração de que a proteção em malha compartilhada apresenta, segundo o parâmetro de uso dos recursos de rede, melhor eficiência do que a (até então tradicional) proteção dedicada.

4 ESTABELECIMENTO DE LSPs EM REDES MPLS-TP EM MALHA

Conforme visto nos capítulos anteriores, apesar dos backbones de algumas redes legadas ainda utilizarem redes em anéis interconectados, a tendência atual é de que essas redes migrem para estruturas em malhas. Além disso, os principais backbones de redes do mundo, atualmente, têm topologia física em malha, conforme demonstram as figuras 27 e 28 abaixo.

Figura 27 - Backbone MPLS Norte-Americano
Fonte: Yang et al. (2015)

Figura 28 - Backbone MPLS Europeu
Fonte: Maesschalck et al. (2003)

Nas redes em malha baseadas na tecnologia MPLS-TP com proteção em malha compartilhada, durante o estabelecimento de um LSP, os caminhos de trabalho devem ser criados concomitantemente com seus respectivos caminhos de proteção, de acordo com a RFC-7412 (WEINGARTEN et al., 2014), e não podem compartilhar nenhum nó ou link intermediário. LSPs novos também não podem deslocar ou remover LSPs de mesma prioridade já estabelecidos anteriormente (apesar de poderem fazer isso com os de menor prioridade), de acordo com a RFC-6372 (SPRECHER; FARREL, 2011).

Este capítulo apresenta a dificuldade de se estabelecer LSPs em uma rede MPLS-TP em malha, comenta alguns trabalhos acadêmicos a respeito desse assunto e explica os métodos de estabelecimento de LSPs que foram comparados, mediante simulações, no presente estudo. As simulações e respectivos resultados serão apresentados no próximo capítulo desta Tese de Doutorado.

4.1 DIFICULDADE PARA SE ESTABELEECER LSPs EM REDES EM MALHA

O estabelecimento de LSPs em uma rede MPLS-TP em malha pode não ser simples, dependendo da complexidade da rede e do número de LSPs já estabelecidos anteriormente nessa rede inteira. Por exemplo, o uso dos caminhos mais curtos entre dois nós por diferentes LSPs pode sobrecarregar alguns links, enquanto outros ficam sub-utilizados. Num pior caso, os links sobrecarregados podem se tornar congestionados. Se um caminho de trabalho passa por links congestionados (cujo nó de entrada pode atrasar a transmissão, devido à formação de filas, ou pode até mesmo descartar pacotes), seu desempenho será pior do que se passasse por links não congestionados. No caso de uma falha que afete um caminho de trabalho, seu respectivo caminho de proteção será utilizado. Se o correspondente caminho de proteção pré-selecionado, quando usado, passar por links congestionados, também terá pior desempenho do que se utilizasse um link alternativo não congestionado.

Em uma rede MPLS-TP, os LSPs são normalmente criados uma a um, sem informação de qual será a demanda futura. Por isso, quanto mais sobrecarregados forem os links, maior a chance deles eventualmente se tornarem congestionados devido à ocorrência de picos ou ao aumento gradativo da demanda. Portanto, quanto mais balanceado for o uso da rede (ou seja, quanto menos sobrecarregados

forem os links), maior será a capacidade de essa rede suportar um posterior acréscimo do tráfego devido ao aumento (gradual ou em picos) da carga dos LSPs já existentes ou ao estabelecimento de novos LSPs.

4.1.1 Problema NP-Completo

O uso eficiente dos recursos da rede, no estabelecimento de LSPs, pode aumentar a capacidade de uma rede MPLS-TP de absorver o aumento da demanda dos serviços por ela providos. Entretanto, os estudos de Ou et al. (2003) e (2006) demonstram que o problema de se encontrar, em uma rede em malha, um par elegível de caminho de trabalho e respectivo caminho de proteção para a instauração (de forma otimizada na rede) de um novo LSP, considerando-se a existência dos LSPs já estabelecidos, é NP-Completo. Em outras palavras, o problema seria muito mais simples se não fosse necessário se considerar também os LSPs já existentes na rede.

4.1.2 Caminhos em “Trap”

Outro óbice existente é a dificuldade de se encontrar caminhos de trabalho e respectivos caminhos de proteção totalmente não coincidentes (isto é, que compartilham somente os nós terminais) devido à ocorrência de caminhos em “trap”, que são os caminhos que impedem a existência, entre dois pontos, de um par de caminhos que não se cruzam.

No exemplo mostrado na figura 29 abaixo, o caminho em “trap” 1-2-7-8 não pode ser utilizado como caminho de trabalho, pois isso impediria a existência de um correspondente caminho de proteção totalmente não coincidente (isto é, que não compartilha nós ou links intermediários com o caminho de trabalho).

LSP 1-8 em “trap”:

Caminho de trabalho em “trap”: **1-2-7-8**
(neste caso, seria impossível se estabelecer caminhos de trabalho e de proteção que não se cruzem)

LSP 1-8 normal (sem “trap”):

Caminho de trabalho: **1-2-3-5-8**
Caminho de proteção: **1-4-6-7-8**

Figura 29 - Exemplo de Caminho em “Trap”

Fonte: o autor

O problema dos caminhos em “trap” surgiu a partir da busca de pares de caminhos (de trabalho e de proteção) totalmente não coincidentes nos estudos de Xu, Xiong e Quiao (2003), Xu et al. (2003) e Guo et al. (2006). Nos dois primeiros estudos, os autores propuseram soluções ao problema por meio de Programação Linear Inteira. A dificuldade, nesse caso, reside na alta complexidade da Programação Linear Inteira empregada. No terceiro estudo, os autores apresentam uma solução por meio de iterações sucessivas para o cálculo dos k-ésimos caminhos mais curtos. O problema desse método de solução (proposto no último estudo citado) é que, na medida em que o valor de k aumenta, aumenta também a complexidade dos cálculos iterativos.

Shen e Grover (2005) demonstram que em redes em malha densamente conectadas o problema dos caminhos em “trap” é impactante, e em redes em malha pouco conectadas esse problema se torna bastante severo. Neste caso (de redes em malha pouco conectadas), segundo o estudo realizado por eles, a abordagem de solução ao problema dos caminhos em “trap” por meio de busca iterativa se mostra satisfatória.

4.1.3 Cálculo Centralizado ou Distribuído

Outro aspecto a ser avaliado é de que forma os caminhos são calculados: se de forma centralizada ou distribuída. Martinez, Casellas e Muñoz (2011) apresentaram um estudo que discute as características de um plano de controle que efetue os cálculos dos caminhos (de trabalho e de proteção) dos LSPs em uma rede MPLS-TP em malha. Para validar o estudo eles realizaram um teste laboratorial para o provisionamento dinâmico (ou seja, para cálculo dos caminhos de restauração) de LSPs bidirecionais em uma rede MPLS-TP em malha. O provisionamento dinâmico computava os caminhos mais curtos e escolhia, dentre eles, o que possuísse o link de maior capacidade ociosa. O referido teste laboratorial media o tempo de execução do cálculo computacional dos caminhos quando o mesmo era realizado de forma distribuída (em cada nó) e quando era realizado de forma centralizada (por meio de uma entidade centralizadora denominada PCE – Path Computation Element – ou Elemento de Computação de Caminho), e comparava os resultados. Os autores concluíram, mediante os resultados obtidos nos testes por eles realizados,

que ambas as estratégias (centralizada ou distribuída) tinham desempenhos similares quanto ao tempo de execução.

Outro estudo, muito mais amplo, desse assunto foi apresentado por Paolucci et al. (2013). Eles realizaram uma extensa e profunda pesquisa sobre os PCEs, entidades de rede dedicadas exclusivamente para o processo de cálculo dos caminhos de trabalho, de proteção e de restauração. Nesse estudo eles sintetizam (a partir dos dados coletados pela pesquisa por eles realizada) uma série de motivos para a utilização das entidades centralizadoras PCEs, como por exemplo:

- algoritmos intensivos para cálculo de caminhos requerem altos recursos de CPU, que só podem ser suportados pelas unidades dedicadas centralizadoras PCEs;
- limitação (e algumas vezes impossibilidade) das unidades distribuídas para efetuar o cálculo dos caminhos nos casos de redes de múltiplos domínios, nos de redes de múltiplas áreas ou nos de redes de múltiplas camadas;
- impossibilidade das unidades distribuídas antigas (legadas) de efetuar os cálculos dos caminhos; e
- facilidade das unidades dedicadas centralizadoras PCEs em prover sincronismo de serviços, como por exemplo no estabelecimento de VPNs.

Os autores também alertam que o cálculo de caminhos em grandes redes requer um tratamento cuidadoso dependendo do tipo dos serviços utilizados pelas conexões. Em particular, quando uma otimização global é considerada, serviços que continua e dinamicamente requeiram o provisionamento de LSPs podem ser responsáveis por uma alocação de recursos ineficiente.

Outro aspecto a ser ressaltado, segundo essa pesquisa, é que em uma rede em malha, unidades dedicadas centralizadoras PCEs podem auxiliar na obtenção de maiores taxas de compartilhamento de recursos e, assim, melhorar a utilização dos recursos da rede. A pesquisa faz também comentários detalhados a respeito de 10 trabalhos acadêmicos sobre o uso de PCEs nos processos de proteção e restauração de redes em malha, segundo os quais a forma como forem usadas as unidades dedicadas centralizadoras PCEs pode aumentar significativamente o tráfego de mensagens de controle e o tempo de restauração das redes.

O estudo de Paolucci et al. (2013) também apresenta, com riqueza de detalhes e de exemplos, aspectos sobre o uso de unidades dedicadas centralizadoras PCEs em redes de múltiplos domínios, em redes de múltiplas áreas,

em redes de múltiplas camadas e em redes hierárquicas. Os altos níveis de amplitude, profundidade e detalhamento da pesquisa apresentada servem de respaldo para os seus resultados. Segundo essa pesquisa, na maioria dos estudos o uso dos PCEs visa reduzir a quantidade de recursos de rede a ser alocada para caminhos de proteção. Além disso, concluem os autores, em destaque, que a proteção em malha compartilhada se mostra o mais promissor dos mecanismos de proteção (PAOLUCCI et al., 2013).

Portanto, apesar dos estudos de Martinez, Casellas e Muñoz (2011) indicarem que as abordagens centralizada ou distribuída (para o cálculo dos caminhos) apresentam desempenhos similares quanto ao tempo de execução, o estudo de Paolucci et al. (2013) demonstra uma série de vantagens (mediante certos cuidados) do uso de unidades dedicadas centralizadoras PCEs (ou seja, vantagens da abordagem centralizada) e que a proteção em malha compartilhada é o mecanismo que proporciona a melhor utilização dos recursos da rede e, por isso, é (segundo esses autores) o mais promissor dos mecanismos de proteção.

Ressalta-se, no entanto, que há uma solução de compromisso entre a forma como se é utilizado um PCE na rede, o tráfego de mensagens de controle e o tempo de restauração das redes, e isso pode impactar ou dificultar a decisão quanto à abordagem (centralizada ou distribuída) de cálculo dos caminhos.

4.1.4 Métrica a Ser Utilizada

A métrica mais comum e normalmente utilizada nos cálculos de rotas ou caminhos em redes é o número de saltos. No entanto, em redes MPLS-TP em malha, o uso dessa métrica pode não ser vantajoso. Por exemplo, o uso de caminhos com o menor número de saltos entre dois nós por diferentes LSPs pode sobrecarregar alguns links, enquanto outros ficam sub-utilizados.

Outra métrica que poderia ser utilizada em redes MPLS-TP em malha, sem se considerar o número de saltos, é a carga total em cada caminho (considerando-se a carga de um link como sendo a quantidade de tráfego suportado pelo link, somando-se todos os LSPs que passam por esse link; e carga total de um caminho como sendo a soma de todas as cargas suportadas por todos os links do caminho). Essa métrica evitaria a ocorrência de links sobrecarregados, mas criaria caminhos mais longos. Estes caminhos mais longos, por sua vez, passariam por uma maior

quantidade de nós e links e, portanto, estariam sujeitos a um maior número de falhas e, também, sua carga (pelo caminho inteiro) impactaria na carga de um maior número de links, elevando assim o tráfego total da rede.

O seguinte exemplo pode elucidar o entendimento acima: supondo-se uma rede, conforme mostrado na figura 30 abaixo, onde as cargas em cada link, em Gbps, estão representadas por números, o caminho entre os nós B e C seria B-A-D-F-G-H-E-C (considerando-se como métrica a carga total do caminho). Estabelecendo-se um novo LSP de 1Gbps nesse caminho entre os nós B e C, a carga total da rede representada na figura abaixo se elevaria de 20 para 27 Gbps. Se nesse exemplo fosse utilizada a métrica de número de saltos para a escolha do caminho B-C, a carga total da rede representada na figura se elevaria de 20 para 21 Gbps. Quanto maior for a carga total na rede, maior poderá ser a possibilidade de ocorrência de nós congestionados ou o impacto em caso de falhas na rede.

Figura 30 - Exemplo 1 de cargas em uma rede em malha
Fonte: o autor

Outro parâmetro que poderia ser utilizado (para a escolha de caminhos) seria a capacidade residual de cada link (isto é, a diferença entre a capacidade do link e sua carga). Mas isso também geraria os seguintes impasses: para a escolha de caminhos, deve ser considerada a maior capacidade residual do caminho, a maior soma das capacidades residuais do caminho, a média das capacidades residuais do caminho ou outros parâmetros?

Figura 31 - Exemplo 2 de cargas em uma rede em malha
Fonte: o autor

No exemplo mostrado na figura 31 acima, onde as cargas de cada link, em Gbps, estão representadas por números e considerando-se nesse exemplo hipotético a capacidade máxima de cada link = 10 Gbps, qual seria o melhor caminho para se estabelecer um LSP entre os nós A e B? Os caminhos (representados pelas cargas dos seus respectivos links) 5-5-5, 1-10-1, 2-9-2 e 9-1-9 estão empatados com o menor número de saltos. O caminho 1-10-1, que apresenta dois links com a maior capacidade individual da rede, já não pode receber nenhum LSP novo (pois um de seus links já está na sua capacidade máxima). A tabela 4.1 abaixo mostra alguns parâmetros dessa rede exemplificada acima:

Tabela 4.1 - Exemplo de cargas e capacidades residuais de links de rede em malha
Fonte: o autor

Caminho (indic. links)	Soma das cargas	Média das cargas	Capacidades residuais indiv.	Maior capacid. residual indiv.	Soma capacid. residual indiv.	Média capac. residual indiv.
5-5-5	15	$15/3 = 5,0$	5-5-5	5	15	$15/3 = 5,0$
1-10-1	12	$12/3 = 4,0$	9- 0 -9	9	18	$18/3 = 6,0$
2-9-2	13	$13/3 = 4,3$	8-1-8	8	17	$17/3 = 5,7$
9-1-9	19	$19/3 = 6,3$	1-9-1	9	11	$11/3 = 3,7$
3-4-2-4-3	16	$16/5 = 3,2$	7-6-8-6-7	8	34	$34/5 = 6,8$

Conforme pode ser observado no exemplo acima, não se deve utilizar um critério único para a escolha dos caminhos, pois também pode haver outras restrições (como um link já saturado). Por exemplo, se o critério for a menor carga total do caminho, nessa ilustração em análise o percurso a ser escolhido seria justamente aquele que já não pode receber novos LSPs (pois o caminho 1-10-1 já tem um link na sua capacidade máxima).

No problema exemplificado em tela, poderia ser adotado (como critério para a escolha de caminhos) o parâmetro de menor carga total dos caminhos viáveis (isto é, dos caminhos que não possuem links já saturados) que estejam empatados com o menor número de saltos. Nesse critério, seria escolhido o caminho 2-9-2 para a alocação do novo LSP. Caso o critério de escolha fosse a maior capacidade residual individual (dentre os caminhos viáveis), o LSP recairia obre o caminho 9-1-9. Caso a escolha do caminho fosse feita pelo critério de maior capacidade residual média (dentre os caminhos viáveis), a opção seria o caminho 3-4-2-4-3, mas se, nesse critério, fossem considerados somente os percursos empatados com o menor número de saltos, a escolha seria então pelo caminho 2-9-2.

Uma questão importante a ser observada é a seguinte: concomitante com a escolha do caminho de trabalho de um LSP, deve ser também estabelecido um caminho de proteção totalmente não coincidente (evitando-se eventuais caminhos em “trap”), e os critérios para a escolha desses caminhos (de trabalho e de proteção) devem ser os mesmos. Nesse exemplo em tela, considerando-se o critério de maior capacidade residual média (dentre os caminhos viáveis e empatados com o menor número de saltos), o LSP A-B seria estabelecido sobre o caminho de trabalho 2-9-2 e teria alocado, para ser seu caminho de proteção, o percurso 5-5-5.

Ressalta-se, no entanto, que a escolha dos caminhos de trabalho e de proteção de um determinado LSP deve levar em conta também toda a rede, ou seja, deve ser considerado o impacto que determinada escolha terá sobre os demais LSPs estabelecidos na rede, pois dependendo das escolhas (de caminhos) feitas, em caso de ocorrência de falhas na rede poderão ser afetadas grandes (ou pequenas) parcelas desses LSPs.

4.2 TRABALHOS RELACIONADOS

Muitos foram os trabalhos publicados relacionados ao estabelecimento de caminhos em redes em malha que teoricamente poderiam, de alguma forma, contribuir para o presente estudo. Nesse sentido, a seguir são comentados aqueles considerados mais relevantes para esta Tese de Doutorado.

Iraschko, MacGregor e Grover (1998) afirmam que os dois maiores problemas no projeto de redes em malha com requisitos de sobrevivência são: 1) determinar a escolha ótima na rede em malha para alocação de caminhos de proteção; e 2) combinar a otimização da escolha do caminho de trabalho com a alocação ótima dos caminhos de proteção. Eles propuseram uma metodologia, baseada em Programação Linear Inteira, para se determinar a capacidade mínima que os links de uma rede em malha deveriam ter para suportar a restauração da rede em caso de falhas simples de links. Eles também concluem que os mecanismos de recuperação das redes em malha se tornam mais eficientes quando o problema é definido sob uma abordagem de recuperação fim-a-fim.

Segundo Kodialam e Lakshman (2000), um dos mais comuns algoritmos de roteamento utilizados em redes de computadores é o MHA (Minimum Hop Algorithm)

que utiliza como métrica a contagem do número de saltos e escolhe como rotas possíveis as de menor valor.

De acordo com Walkowiak (2007), outro muito comum algoritmo de roteamento aplicado em redes é o SPF (Shortest Path First), que utiliza uma métrica qualquer, normalmente o número de saltos.

Esses dois algoritmos (MHA e SPF) têm como principais vantagens a simplicidade de programação e a rapidez de execução, mas ambos têm a desvantagem de concentrar o tráfego nas rotas de menor custo, saturando alguns links mesmo na existência de outros menos utilizados. Uma forma de melhorar o desempenho deles é considerar também a capacidade residual dos links, tentando diminuir a ocorrência de saturação precoce de alguns deles (KODIALAM; LAKSHMAN, 2000), (WALKOWIAK, 2007).

Kodialam e Lakshman (2000) propõem um algoritmo de escolha de caminhos MPLS denominado MIRA (Minimum Interference Routing Algorithm), segundo o qual na escolha dos caminhos, por meio de Programação Linear Inteira, são evitados os links considerados “críticos” (aqueles que podem interferir com potenciais futuros caminhos). No entanto, esse algoritmo proposto apresenta duas desvantagens: apresenta uma alta complexidade computacional e uma utilização desbalanceada dos recursos da rede.

Kodialam e Lakshman (2000) citam também o WSP (Widest Shortest Path), algoritmo que é uma variação do MHA e que considera, na escolha dos caminhos MPLS, aquele que possuir a maior soma das capacidades residuais dos links que o compõem.

Szeto, Boutaba e Iraqui (2002 e 2002) apresentam a proposta de um algoritmo de escolha de caminhos MPLS denominado DORA (Dynamic Online Routing Algorithm), que por meio de Programação Linear Inteira procura melhor balancear a utilização dos recursos da rede. Os autores do algoritmo proposto demonstram, pelos resultados dos seus estudos, que o DORA obtém maior eficiência no cálculo dos caminhos de restauração que os algoritmos SPF e MIRA, apesar da sua também alta complexidade computacional, similar à do MIRA.

Outro algoritmo proposto para escolha de caminhos MPLS é o LIOA (Least Interference Optimization Algorithm), apresentado por Bagula, Botha e Krzesinski (2004). O algoritmo proposto LIOA é baseado no SPF e na capacidade residual dos links da rede. Segundo seus autores, o LIOA apresenta complexidade

computacional similar à do SPF e supera em eficiência, em caso de falha simples de links na rede, os algoritmos SPF, CSPF (Constrained-SPF: variação do SPF que impõe restrições ao uso de alguns links), MHA e MIRA.

El-Darieby, Petriu e Rolia (2002) propõem um protocolo distribuído hierárquico para determinação de caminhos MPLS, segundo o qual a rede inteira é dividida em camadas hierárquicas, onde cada camada (por meio de um PCE próprio) realiza o cálculo dos caminhos MPLS no seu nível, e ao final são determinados os pontos de interseção entre cada camada, encontrando-se assim o caminho inteiro na rede. Os autores desse protocolo distribuído hierárquico acreditam que o proposto paralelismo computacional pode reduzir o tempo total para estabelecimento do caminho completo na rede.

Seguindo essa idéia, Kodialam, Lakshman e Sengupta (2004) apresentam o conceito de roteamento em duas fases, em que o tráfego (direcionado para qualquer nó) é inicialmente distribuído para nós intermediários, para só então ser direcionado para o nó de destino final.

Por outro lado, Shen e Grover (2005) demonstram que, em redes em malha, o emprego de esquemas que consideram a rede como um todo (e não apenas partes dela) pode mais eficientemente utilizar a capacidade compartilhada de proteção da rede.

Walkowiak (2007) propõe um algoritmo de escolha de caminhos MPLS para entrega de serviços anycast (isto é, entrega de pacotes no nó mais próximo de um determinado grupo de nós). A idéia do algoritmo proposto é a de que as informações seriam replicadas em servidores espalhados pela rede e os clientes poderiam escolher de qual servidor (a critério dos clientes) seria mais apropriado recebê-las. A transmissão anycast poderia reduzir o tráfego na rede e, assim, tentar evitar a ocorrência de congestionamentos. Essa proposta é uma espécie de variação do algoritmo de roteamento em duas fases.

Kodialam e Lakshman (2009) melhoram o esquema de roteamento em duas fases, provendo resiliência contra falhas de links por meio do estabelecimento de caminhos de proteção “1 : n” fim-a-fim em duas fases. Nesse novo esquema proposto, um caminho de trabalho entre os nós A e B continua tendo duas fases, e podem existir vários caminhos de trabalho entre esses nós A e B, todos de duas fases. O caminho de proteção (também de duas fases) será acionado em caso de

falha em algum dos caminhos de trabalho (segundo, portanto, o esquema de proteção “1 : n”).

Kim et al. (2007) propõem um algoritmo de escolha de caminhos MPLS baseado em algoritmos genéticos. As simulações realizadas pelos autores indicam que, para redes muito grandes, o algoritmo genético proposto consegue superar, em questão de tempo de cálculo dos caminhos, o algoritmo CSPF.

Kotti, Hamza e Bouleimen (2007) apresentam a proposta de um algoritmo de escolha de caminhos MPLS denominado BCRA (Bandwidth Constrained Routing Algorithm), que tenta balancear a carga nos links, diminuir o tamanho dos caminhos e minimizar o custo de cada caminho. No BCRA os links que suportam carga acima da carga média da rede são considerados links críticos, e quanto mais links críticos um caminho possuir, mais crítico é considerado esse caminho. O BCRA estabelece “pesos” aos links e aos caminhos, e calcula os caminhos de menor “peso” utilizando o SPF.

Alidad, Mahdavi e Hashmi (2009) também propõem um algoritmo de escolha de caminhos MPLS, denominado BGLC (Bandwidth Guarantee with Low Complexity), baseado no BCRA. O algoritmo BGLC estabelece índices de criticidade para cada link, de acordo com sua respectiva carga, e elimina do cálculo de novos caminhos os links cuja carga ultrapasse um determinado valor pré-estabelecido. Em questão de tempo de cálculo de caminhos, os autores do BGLC o compararam com os algoritmos MHA, WSP, BCRA e MIRA, sendo que o referido algoritmo (BGLC) só não foi mais rápido para o cálculo dos caminhos que o MHA (que, apesar de ser rápido, no entanto sobrecarrega alguns links deixando a rede desbalanceada).

Jamhour e Penna (2012) propõem, para redes em malha MPLS-TP com proteção em malha compartilhada e com suporte à preempção, um modelo de escolha de caminhos baseado na estimativa de disponibilidade dos links de proteção. Nesse modelo, um algoritmo de planejamento de recursos de proteção calcula a capacidade de proteção mínima necessária para atingir o estado desejado de disponibilidade de todos os caminhos protegidos, e atribui prioridades para os caminhos de proteção. Os testes efetuados pelos autores desse modelo indicam que, em situações específicas, a utilização de prioridades de proteção distintas permite alcançar um nível desejado de proteção, com economia da largura de banda. Nesse estudo, no entanto, os caminhos de proteção preemptados (deslocados para dar lugar a outros de maior prioridade) que não puderem

preemptar outros caminhos de menor prioridade são bloqueados, isto é, o processo de recuperação não é usado nestes casos, aumentando, assim, a ocorrência de LSPs interrompidos na rede em malha.

4.3 COMPARAÇÃO DE MÉTODOS DE ESTABELECIMENTO DE CAMINHOS

As RFCs que padronizam a tecnologia MPLS-TP estipulam que, em uma rede em malha com proteção em malha compartilhada, os caminhos de trabalho e de proteção devem ser definidos concomitantemente por ocasião da criação de um LSP, mas devido à dificuldade de se resolver esse problema de forma otimizada para a rede como um todo (conforme mostrado anteriormente no atual estudo), por enquanto essas RFCs ainda não determinaram um modelo padronizado para o estabelecimento desses caminhos.

Portanto, o problema de escolha conjunta de caminhos de trabalho e de proteção de um LSP, considerando todos os LSPs de uma determinada rede MPLS-TP em malha, precisa ser melhor estudado.

Visando contribuir para o estudo da solução otimizada em rede desse problema, sem a pretensão, no entanto, de esgotar-se o assunto, o presente trabalho realizou uma comparação, mediante simulações, de 3 métodos de estabelecimento de caminhos.

Segundo Calle, Marzo e Urra (2004), a carga da rede é um aspecto crucial a ser considerado na escolha do caminho de proteção, assim como a distância (em número de saltos). Portanto, tendo como base esta afirmação e os demais aspectos apresentados até aqui no presente trabalho, foram escolhidos 3 métodos de escolha de caminhos para serem comparados.

A comparação foi realizada (em ambiente simulado) medindo-se o impacto na carga da rede decorrente da aplicação de cada um dos métodos de escolha de caminhos, ou seja, medindo-se a carga na rede após o estabelecimento de todos os LSPs da rede, de acordo com cada um dos métodos avaliados.

Após a instauração de todos os LSPs, foi também necessário medir a carga na rede após a ocorrência de falhas, para se avaliar a capacidade de sobrevivência da rede de acordo com os caminhos escolhidos: no caso das falhas, foram empregadas duas heurísticas de recuperação, para se avaliar a distribuição de carga na rede resultante após as falhas.

Em todas as ocasiões (com ou sem falhas), juntamente com a medição da carga na rede, foi verificado também o tamanho médio de cada LSP resultante (em número de saltos). No caso de falhas, foi também apurado o número máximo de LSPs afetados em cada uma das falhas, de acordo com o método de escolha de caminhos empregado.

Neste item são apresentados os métodos de escolha de caminhos que foram comparados e as heurísticas de recuperação empregadas. As simulações e respectivos resultados serão apresentados e comentados adiante, no próximo capítulo deste trabalho.

4.3.1 Métodos (de Escolha de Caminhos) que Foram Comparados

Conforme já informado anteriormente, foram designados 3 métodos de escolha de caminhos para serem comparados. Para efeito de simulação, foi considerado que os cálculos eram sempre realizados de forma centralizada, por um PCE único na rede. Seguindo-se as recomendações de Calle, Marzo e Urra (2004), anteriormente mencionadas, a escolha dos métodos priorizou os aspectos de carga nos links e tamanho dos LSPs, conforme a seguir detalhado. Ressalta-se que, para que fosse investigado tão somente o impacto da escolha do método de determinação de caminhos, não foram estabelecidos limites para a capacidade máxima de carga de cada link (e por isso não foi utilizado o parâmetro de capacidade residual nessas avaliações).

1º método (método “estático”):

No 1º método selecionado, a escolha dos caminhos depende única e exclusivamente do número de saltos entre os nós terminais (nós de origem e de destino) do caminho: o caminho com o menor número de saltos é o escolhido. Em caso de empate, a escolha é feita aleatoriamente entre os caminhos empatados. Este 1º método (que corresponde ao MHA, citado anteriormente) procura somente minimizar o tamanho dos caminhos, sem se importar em balancear a carga dos mesmos. Para efeito de nomenclatura, neste trabalho este método passará a ser denominado de método estático de determinação de caminhos, pois para ser estabelecido, o caminho depende somente que sejam definidos seus nós terminais (informação que é estática),

para que seja escolhida a rota de menor tamanho, independentemente dos demais caminhos já anteriormente estabelecidos na rede. Portanto, este método não considera os demais LSPs já estabelecidos na rede.

2º método (método “espalhado”):

No 2º método selecionado, a escolha dos caminhos depende única e exclusivamente da carga total do caminho entre seus nós terminais: o caminho com a menor carga total é o escolhido, independentemente do seu tamanho (em número de saltos). Em caso de empate, a escolha é feita aleatoriamente entre os caminhos empatados. Este 2º método procura somente balancear a carga dos caminhos, sem se importar em minimizar o tamanho dos mesmos. Para efeito de nomenclatura, neste trabalho este método passará a ser denominado de método espalhado de determinação de caminhos, pois para ser estabelecido, o caminho escolhe a rota de menor carga total entre seus nós terminais, e essa rota escolhida pode não ser a de menor tamanho. Portanto, este método considera os demais LSPs já estabelecidos na rede.

3º método (método “dinâmico”):

No 3º método selecionado, a escolha dos caminhos depende do número de saltos entre os nós terminais do caminho e também da carga suportada em cada um dos links pelos quais o caminho passa: o caminho com o menor número de saltos e com a menor carga total é o escolhido. Em caso de empate, a escolha é feita aleatoriamente entre os caminhos empatados. Neste caso, considera-se carga de um link = quantidade de tráfego suportado pelo link, somando-se todos os caminhos que passam por esse link na mesma direção; e carga total de um caminho = soma de todas as cargas suportadas por todos os links do caminho. Este 3º método procura balancear a carga e ao mesmo tempo minimizar o tamanho dos caminhos. Para efeito de nomenclatura, neste trabalho este método passará a ser denominado de método dinâmico de determinação de caminhos, pois para ser estabelecido, o caminho depende que sejam definidos seus nós terminais e também a carga dos links pelos quais ele passa: essa informação (a carga de cada link) depende dos demais caminhos já anteriormente estabelecidos na rede e é

uma informação dinâmica, pois depende da ordem sequencial na qual o caminho está sendo instaurado na rede. Portanto, este método considera os demais LSPs já estabelecidos na rede.

4.3.2 Heurísticas de Recuperação Empregadas

Nesta seção são apresentadas as heurísticas de recuperação empregadas nas simulações (para se avaliar o desempenho da rede após a ocorrência de falhas, de acordo com os métodos utilizados para a escolha dos caminhos) e são feitas algumas considerações importantes a serem observadas.

Foram aplicadas duas heurísticas de recuperação em caso de falhas na rede:

1ª heurística de recuperação (heurística “+pp”):

Na 1ª heurística de recuperação, o processo de recuperação ocorre da seguinte maneira: se o caminho de trabalho é afetado por alguma falha na rede, o nó de origem tenta redirecionar o tráfego desse caminho afetado para o seu caminho de proteção correspondente. Se esse caminho de proteção também tiver sido afetado pelas falhas, um caminho de restauração é procurado. Esta 1ª heurística é o procedimento padrão de recuperação da tecnologia MPLS-TP para proteção em malha compartilhada. Para efeito de nomenclatura, neste trabalho esta heurística de recuperação passará a ser denominada de heurística “+pp”, devido a utilizar os caminhos de proteção (“Protection Paths”).

2ª heurística de recuperação (heurística “-pp”):

Na 2ª heurística de recuperação, se o caminho de trabalho é afetado por alguma falha na rede, o nó de origem ignora o caminho de proteção e imediatamente procura encontrar um caminho de restauração (para redirecionar o tráfego do caminho afetado para ele). Para efeito de nomenclatura, neste trabalho esta heurística de recuperação passará a ser denominada de heurística “-pp”, devido a não utilizar os caminhos de proteção (“Protection Paths”).

Importante observar que os caminhos de trabalho e os caminhos de proteção não compartilham nenhum link ou nó intermediário, enquanto que os caminhos de restauração podem ou não compartilhar links ou nós com os caminhos de trabalho a que buscam restaurar.

Importante observar também que, diferentemente do estabelecimento dos caminhos de trabalho e de proteção, que são feitos antecipadamente (por ocasião do estabelecimento do LSP), o caminho de restauração só pode ser estabelecido após a ocorrência de alguma falha. Um caminho de restauração entre os pontos A e B é escolhido entre os caminhos disponíveis (que interligam esses pontos A e B) após a ocorrência de falhas. Neste estudo, o caminho de restauração, para ser escolhido, pode considerar o menor número de saltos entre A e B, a menor carga total entre A e B, ou ambos (número de saltos e carga entre A e B), de acordo com o método utilizado para a determinação dos caminhos.

Os caminhos de proteção e os de restauração podem envolver rotas maiores (isto é, com maior número de saltos) que os caminhos de trabalho atendidos por eles, causando um maior consumo de banda a um maior número de links. Portanto, as escolhas do método de determinação de caminhos e da heurística de recuperação afetam diretamente a carga da rede.

Neste estudo os LSPs são todos unidirecionais, portanto a carga de um link físico em uma direção pode ser completamente diferente da carga neste mesmo link na direção oposta. Lembra-se que a carga de um link é a soma da carga de todos os caminhos ativos (de trabalho, de proteção ou de restauração) que passam por esse link (ou seja, que o compartilham) na mesma direção.

Conforme já comentado, a carga de um caminho é a soma da carga de todos os links pelos quais o caminho passa. Portanto, quando a rede está sem falhas, o cálculo da carga total de um caminho não envolve grande complexidade. No entanto, quando ocorrem falhas na rede, o cálculo da carga na rede pode não ser simples, pois será necessário realocar todos os LSPs afetados pelas falhas antes de se calcular a carga resultante na rede. No entanto, esta realocação de LSPs também depende da carga existente na rede, por isso é importante o uso de um simulador.

4.4 SÍNTESE DO CAPÍTULO

Neste capítulo foram comentados aspectos relacionados à dificuldade de se estabelecer LSPs em uma rede MPLS-TP em malha, foram citados e comentados alguns trabalhos acadêmicos a respeito do estabelecimento de LSPs e foram também explicados os métodos de estabelecimento de LSPs e as heurísticas de recuperação que foram comparadas, mediante simulações, no presente estudo.

5 SIMULAÇÕES E RESULTADOS

Neste capítulo são apresentados o simulador, a abordagem utilizada para se evitar os caminhos em “trap”, os cenários de simulação e os resultados alcançados. São também realizados comentários a respeito dos resultados obtidos.

5.1 SIMULAÇÕES

Neste tópico são tratados aspectos relacionados às simulações efetuadas.

5.1.1 Simulador

O simulador utilizado foi desenvolvido, utilizando-se Linguagem C, pelo próprio autor deste trabalho.

O software de desenvolvimento utilizado foi o "Eclipse IDE for C/C++ Developers", versão “Mars.1 Release (4.5.1) / Build id: 20150924-1200”.

O microcomputador utilizado para as simulações foi um laptop Samsung, modelo R440, com processador Intel i3 M350, de 2,27Ghz, memória principal de 4,0 GB e sistema operacional Windows 7 – versão Home Premium, de 64 bits.

5.1.2 Abordagem para Evitar Caminhos em “Trap”

Na programação das simulações, a abordagem utilizada para se evitar os caminhos em “trap” foi a seguinte: na busca de caminhos entre dois pontos quaisquer de uma rede, caso (de acordo com a métrica utilizada) o “menor” caminho encontrado seja um caminho em “trap” e existam outros caminhos entre os dois pontos, a solução empregada foi aumentar-se temporariamente os “pesos” do referido caminho em “trap” encontrado (em “steps” reguláveis, apenas enquanto o caminho em “trap” persistir), até que um outro caminho existente passe a ser mais “vantajoso” e “conquiste” o título de “menor” caminho. Caso o novo caminho seja também um caminho em “trap”, o processo se repete até que um caminho normal (“não-trap”) seja encontrado ou não existam mais caminhos entre os dois pontos avaliados. Esta abordagem mostrou-se bastante simples de ser programada e

computacionalmente muito rápida de ser executada, sem falhas. A seguir são mostrados exemplos elucidativos dessa abordagem.

1º exemplo: na figura 32 abaixo, na qual a “carga” de cada link está representada por números, deseja-se encontrar o “menor” caminho (ou seja, o caminho de menor carga total) entre os pontos A e H. O caminho em “trap” A-B-G-H é encontrado. As cargas dos links desse caminho são temporária e gradativamente aumentadas (conforme exemplificado na figura) até que um outro caminho “conquiste” o posto de “menor” caminho. Nesse 1º exemplo, após o aumento temporário das cargas do caminho em “trap”, são encontrados dois caminhos (entre os pontos A e H) que não se cruzam: A-B-C-E-H e A-D-F-G-H.

Figura 32 - Exemplo 1 de Abordagem para Evitar Caminhos em “Trap”
Fonte: o autor

2º exemplo: na figura 33 a seguir, na qual a “carga” de cada link está representada por números, deseja-se encontrar o “menor” caminho entre os pontos A e F. O caminho em “trap” A-B-C-D-E-F é encontrado. As cargas dos links desse caminho são temporária e gradativamente aumentadas (conforme exemplificado na figura) até que um outro caminho “conquiste” o posto de “menor” caminho. Nesse 2º exemplo, após o aumento temporário das cargas do caminho em “trap”, são encontrados dois caminhos (entre os pontos A e F) que não se cruzam: A-B-F e A-C-D-F (sendo este último o caminho de menor carga total ao término do processo).

Figura 33 - Exemplo 2 de Abordagem para Evitar Caminhos em “Trap”
Fonte: o autor

Ressalta-se que, na pesquisa bibliográfica efetuada, não foi encontrada nenhuma abordagem semelhante, de tão simples implementação via programação e computacionalmente tão rápida de ser executada.

5.1.3 Cenários de Simulação

O simulador utilizado suporta a simulação de nenhuma, uma ou múltiplas falhas de links, de nós ou ambos. As falhas simuladas eram sempre do tipo “cable cut” (interrompendo totalmente o tráfego nos dois sentidos, se fosse falha de link, ou deixando um nó totalmente inoperante, se fosse falha de nó), por serem o pior caso de falhas.

O caminho mais curto (em termos de número de saltos, de carga total ou ambos) era sempre calculado por um algoritmo Dijkstra modificado, e todos os caminhos de trabalho e respectivos caminhos de proteção eram sempre não coincidentes (compartilhando apenas os nós terminais), evitando-se caminhos em “trap” (utilizando-se a técnica descrita acima).

De acordo com os caminhos (de trabalho, de proteção ou de restauração) de todos os LSPs ativos da rede, o simulador calcula a carga em cada link da rede, o tamanho (em número de saltos) e a densidade de tráfego (carga total do caminho dividido pelo número de saltos do caminho) de cada um dos caminhos ativos na rede, o número de LSPs afetado a cada falha na rede, etc.

Os resultados das simulações dependem do arranjo inicial dos LSPs (seus caminhos de trabalho e os correspondentes caminhos de proteção, de acordo com o método empregado de escolha de caminhos), das falhas, da heurística de

recuperação utilizada, dos caminhos de restauração porventura utilizados e da carga de cada LSP na rede.

Foram utilizadas 4 topologias de redes: a) 10-nós/14-links; b) 16-nós/23-links; c) 17-nós/25-links; e d) 26-nós/39-links, conforme mostrado na figura 34 abaixo. Essas topologias não representam nenhuma rede real em especial, pois foram estabelecidas aleatoriamente, para que fossem realizadas as simulações propostas como “prova de conceito” no presente estudo.

Figura 34 - Topologias de redes em malha utilizadas nas simulações
Fonte: o autor

Para cada conjunto de simulações de uma rede, foi estabelecido um, e somente um, LSP entre cada par de nós na rede, totalizando $n \times (n - 1)$ LSPs em cada rede simulada (onde n = número de nós da rede). Desta forma, nas 4 redes simuladas, foram estabelecidos respectivamente ($10 \times 9 = 90$), ($16 \times 15 = 240$), ($17 \times 16 = 272$) e ($26 \times 25 = 650$) LSPs.

Nas simulações, um caminho de A para B pode ser diferente do caminho inverso, de B para A, ou seja, os caminhos A-B e B-A podem compartilhar ou não nós e links intermediários.

Nas simulações, com o intuito de se facilitar os cálculos, todos os LSPs ativos tinham uma carga de 1 Gbps e, para que não houvesse preempção, todos os LSPs ativos tinham a mesma prioridade.

Foram simulados os três métodos de escolha de caminhos e as duas heurísticas de recuperação, totalizando seis diferentes configurações de comportamento para cada rede.

Todos os conjuntos de configurações de rede foram avaliados exhaustivamente (considerando todas as falhas possíveis), conforme mostrado na tabela 5.1 abaixo, com respectivamente: falha nenhuma (1 simulação por rede); falha de 1 link; falha de 2 links; falha de 1 nó; falha de 1 nó e 1 link; e falha de 1 nó e 2 links. A rede de 26-nós/39-links foi simulada, por exemplo, $6 \times 21.087 = 126.522$ vezes.

Tabela 5.1 - Número de simulações de falhas de rede
Fonte: o autor

Número de simulações de falhas de rede		REDE			
		10 nós 14 links	16 nós 23 links	17 nós 25 links	26 nós 39 links
Conjunto de Falhas	0 nó 0 link	1	1	1	1
	0 nó 1 link	14	23	25	39
	0 nó 2 links	91	253	300	741
	1 nó 0 link	10	16	17	26
	1 nó 1 link	140	368	425	1.014
	1 nó 2 links	910	4.048	5.100	19.266
Total de simulações		1.166	4.709	5.868	21.087

5.2 RESULTADOS

Neste tópico são tratados aspectos relacionados aos resultados alcançados. Os dados mostrados nas tabelas e figuras adiante demonstram o impacto dos métodos de escolha de caminhos e das heurísticas de recuperação sobre as quatro

redes simuladas, com e sem falhas, nos seis comportamentos avaliados nas simulações.

5.2.1 Densidade Média de Tráfego dos LSPs (em Gbps/salto)

Na tabela 5.2 abaixo pode ser observado que os métodos “dinâmico” e “espalhado” de determinação (ou escolha) de caminhos causam uma redução na densidade média de tráfego dos LSPs (em Gbps/salto) em comparação com o método “estático”. Observa-se, também, que em redes sem falhas a heurística de recuperação é irrelevante.

Tabela 5.2 - Densidade média de tráfego dos LSPs (em Gbps/salto)

Fonte: o autor

Conjunto de falhas =>		0 nó 0 link	0 nó 1 link	0 nó 2 links	1 nó 0 link	1 nó 1 link	1 nó 2 links
10-nós 14-links	estático + pp	8,054	8,489	9,772	7,731	8,815	9,724
	estático – pp	8,054	8,698	10,015	7,864	8,990	9,880
	dinâmico + pp	7,226	8,157	9,462	7,415	8,534	9,505
	dinâmico – pp	7,226	8,007	9,430	7,283	8,503	9,524
	espalhado + pp	7,406	8,207	9,463	7,420	8,534	9,498
	espalhado – pp	7,406	8,093	9,427	7,314	8,491	9,494
16- nós 23-links	estático + pp	16,268	17,509	19,282	16,802	18,445	20,100
	estático – pp	16,268	17,345	19,175	16,655	18,374	20,118
	dinâmico + pp	15,290	16,877	18,738	16,154	17,897	19,628
	dinâmico – pp	15,290	16,559	18,383	15,908	17,634	19,417
	espalhado + pp	15,648	17,204	18,957	16,428	18,076	19,722
	espalhado – pp	15,648	16,812	18,547	16,126	17,773	19,493
17- nós 25-links	estático + pp	17,952	18,588	20,139	17,832	19,287	20,887
	estático – pp	17,952	18,749	20,464	18,067	19,651	21,329
	dinâmico + pp	16,077	17,493	19,150	16,840	18,372	20,036
	dinâmico – pp	16,077	17,189	18,892	16,583	18,181	19,965
	espalhado + pp	16,499	17,934	19,521	17,239	18,677	20,253
	espalhado – pp	16,499	17,483	19,083	16,807	18,330	20,061
26- nós 39-links	estático + pp	37,445	38,563	40,929	37,989	40,375	43,002
	estático – pp	37,445	38,400	40,812	37,986	40,436	43,179
	dinâmico + pp	33,585	35,759	38,370	35,273	37,852	40,596
	dinâmico – pp	33,585	34,856	37,110	34,422	36,734	39,459
	espalhado + pp	35,067	36,857	39,200	36,204	38,538	41,101
	espalhado – pp	35,067	35,899	37,910	35,297	37,427	40,044

Para as redes maiores, em caso de falhas na rede, a heurística de recuperação “-pp” (isto é, que não usa os caminhos de proteção) tem resultados melhores (em termos de densidade média de tráfego) em relação aos resultados da heurística oposta “+pp”. Observa-se, também, que quanto maior é a rede simulada, maior (a uma alta taxa) é a densidade média de tráfego. Relembra-se que, quanto maior o número de nós na rede simulada, maior o número de LSPs (por exemplo: 10 nós = 90 LSPs; 16 nós = 240 LSPs; 17 nós = 272 LSPs; e 26 nós = 650 LSPs).

Os resultados mostrados na tabela 5.2 acima seguem a mesma tendência, e todas as redes têm comportamentos similares. Para evitar gráficos repetitivos, será mostrado, na figura 35 abaixo, apenas o gráfico relacionado à rede de 26-nós/39-links, que apresenta as maiores diferenças entre os seis comportamentos avaliados.

Figura 35 - Densidade média de tráfego (Gbps/salto) da rede de 26-nós/39-links
Fonte: o autor

5.2.2 Tamanho Médio dos LSPs (em Número de Saltos)

A tabela 5.3 abaixo mostra que, para o parâmetro “tamanho médio dos LSPs”, em número de saltos, os métodos “dinâmico -pp” e “estático -pp” têm os mesmos resultados, os métodos “dinâmico +pp” e “estático +pp” têm resultados similares e o método “espalhado”, como esperado, apresenta os valores mais altos.

A heurística “-pp”, em geral, também tem resultados melhores (menores LSPs, em média) quando comparada à heurística “+pp”.

Tabela 5.3 - Tamanho médio dos LSPs (em número de saltos)

Fonte: o autor

Conjunto de falhas =>		0 nó 0 link	0 nó 1 link	0 nó 2 links	1 nó 0 link	1 nó 1 link	1 nó 2 links
10-nós 14-links	estático + pp	2,067	2,175	2,312	2,128	2,257	2,363
	estático – pp	2,067	2,175	2,312	2,128	2,257	2,363
	dinâmico + pp	2,067	2,198	2,332	2,156	2,275	2,373
	dinâmico – pp	2,067	2,175	2,312	2,128	2,257	2,363
	espalhado + pp	2,133	2,225	2,342	2,172	2,283	2,377
	espalhado – pp	2,133	2,206	2,326	2,150	2,269	2,369
16- nós 23-links	estático + pp	2,642	2,789	2,908	2,782	2,895	3,000
	estático – pp	2,642	2,736	2,846	2,731	2,841	2,955
	dinâmico + pp	2,642	2,785	2,906	2,776	2,893	3,001
	dinâmico – pp	2,642	2,736	2,846	2,731	2,841	2,955
	espalhado + pp	2,750	2,867	2,967	2,853	2,950	3,044
	espalhado – pp	2,750	2,817	2,907	2,804	2,897	2,997
17- nós 25-links	estático + pp	2,765	2,866	2,959	2,855	2,945	3,038
	estático – pp	2,765	2,840	2,928	2,830	2,918	3,014
	dinâmico + pp	2,765	2,875	2,971	2,866	2,957	3,048
	dinâmico – pp	2,765	2,840	2,928	2,830	2,918	3,014
	espalhado + pp	2,846	2,945	3,026	2,931	3,005	3,083
	espalhado – pp	2,846	2,898	2,968	2,880	2,954	3,040
26- nós 39-links	estático + pp	3,557	3,651	3,738	3,657	3,747	3,842
	estático – pp	3,557	3,619	3,692	3,626	3,705	3,798
	dinâmico + pp	3,557	3,665	3,759	3,675	3,768	3,863
	dinâmico – pp	3,557	3,619	3,692	3,626	3,705	3,798
	espalhado + pp	3,735	3,819	3,887	3,819	3,887	3,959
	espalhado – pp	3,735	3,755	3,796	3,748	3,800	3,872

A figura 36 abaixo mostra os resultados deste parâmetro (tamanho médio dos LSPs) nas simulações para a rede de 26-nós/39-links. As demais redes seguem a mesma tendência.

Figura 36 - Tamanho médio dos LSPs (em número de saltos)
da rede de 26-nós/39-links
Fonte: o autor

5.2.3 Número Máximo de LSPs Afetados em Caso de Falhas na Rede

A tabela 5.4 abaixo mostra que os métodos “dinâmico” e “espalhado” apresentam os melhores resultados com respeito ao parâmetro “número máximo de LSPs afetados em caso de falhas na rede”, principalmente para grandes redes.

Tabela 5.4 - Número máximo de LSPs afetados em caso de falhas na rede
Fonte: o autor

Conjunto de falhas =>		0 nó 1 link	0 nó 2 links	1 nó 0 link	1 nó 1 link	1 nó 2 links
10-n 14-l	estático	28	40	42	56	64
	dinâmico	21	36	36	53	63
	espalhado	21	38	39	55	64
16-n 23-l	estático	52	98	92	126	154
	dinâmico	45	87	90	123	156
	espalhado	46	90	84	124	157
17-n 25-l	estático	66	110	90	138	162
	dinâmico	48	83	80	123	151
	espalhado	47	83	80	125	153
26-n 39-l	estático	122	229	184	283	379
	dinâmico	99	190	167	251	334
	espalhado	103	199	174	263	336

As heurísticas de recuperação “+pp” e “-pp” são irrelevantes neste caso, pois o parâmetro é medido antes das medidas de recuperação.

Importante observar que, em caso de falhas, alguns dos LSPs afetados podem não ser recuperados, devido seus nós terminais se tornarem inalcançáveis devido às falhas na rede. O número de LSPs irrecuperáveis independe do método empregado para seleção de caminhos.

A figura 37 abaixo mostra os resultados do parâmetro “número máximo de LSPs afetados em caso de falhas na rede” na simulação da rede de 26-nós/39-links. A tendência apresentada por essa rede é similar às apresentadas pelas demais redes simuladas.

Figura 37 - Número máximo de LSPs afetados em caso de falhas na rede 26-nós/39-links

Fonte: o autor

5.2.4 Sumário dos Resultados

A tabela 5.5 abaixo apresenta um resumo dos resultados das simulações para a rede de 26-nós/39-links. Este resumo permite melhor visualizar o impacto dos diversos métodos de determinação de caminhos e das heurísticas de recuperação sobre a rede em questão. A tendência verificada nos resultados apresentados nessa

tabela, referente à rede de 26-nós/39-links, é a mesma nas simulações das demais redes. Portanto, o resumo abaixo reflete também o comportamento das demais redes.

Tabela 5.5 - Resumo dos resultados das simulações da rede 26-nós/39-links

Fonte: o autor

Conjunto de Falhas	parâmetro	Estático	Dinâmico	Espalhado
0 nó 0 link (sem falha)	Densidade média de tráfego (Gbps/salto)	37,445	33,585	35,067
	Tamanho médio dos LSPs (número de saltos)	3,557	3,557	3,735
		Estático+pp	Dinâmico+pp	Espalhado+pp
1 nó 2 links (pior caso simulado)	Densidade média de tráfego (Gbps/salto)	43,002	40,596	41,101
	Tamanho médio dos LSPs (número de saltos)	3,842	3,863	3,959
	Número máximo de LSPs afetados	379	334	336
		Estático-pp	Dinâmico-pp	Espalhado-pp
	Densidade média de tráfego (Gbps/salto)	43,179	39,459	40,044
	Tamanho médio dos LSPs (número de saltos)	3,798	3,798	3,872
	Número máximo de LSPs afetados	379	334	336

Foram testados 3 métodos para determinação de caminhos:

- a) o método denominado neste trabalho de “estático”, que considera somente o aspecto tamanho dos LSPs em termos de número de saltos e não faz balanceamento de carga (pois não considera os demais LSPs já estabelecidos na rede);

- b) o método denominado neste trabalho de “espalhado”, que faz somente balanceamento da carga (considerando, portanto, os demais LSPs já estabelecidos na rede), mas não se preocupa com o tamanho dos caminhos em termos de número de saltos; e
- c) o método denominado neste trabalho de “dinâmico”, que faz um meio termo entre os dois extremos: procura diminuir o tamanho dos LSPs e ao mesmo tempo procura fazer algum balanceamento de carga (considerando, portanto, os demais LSPs já estabelecidos na rede).

As heurísticas de recuperação denominadas neste trabalho de “+pp” e “-pp” foram introduzidas para se avaliar a rede resultante (de acordo com o arranjo dos LSPs estabelecidos na rede mediante cada método de escolha de caminhos) em caso de falhas.

Segundo os resultados obtidos, o método denominado neste trabalho de “dinâmico” consegue diminuir não só a densidade de tráfego na rede, como reduz também o número máximo de LSPs afetados em caso de falhas na rede. Além disso, esse método não aparenta ser complicado de ser implementado na prática.

A heurística de recuperação “-pp” apresentou melhores resultados que a outra heurística de recuperação testada, a “+pp” (que é a forma padronizada do MPLS-TP). No entanto, é importante ser ressaltado que o tempo de se calcular um caminho de restauração (heurística “-pp”) é muito superior ao tempo de se “chavear” o tráfego de um caminho de trabalho para seu caminho de proteção correspondente (heurística “+pp”). Portanto, o uso da heurística “-pp” só será vantajoso em ambientes que não requeiram tempo de resposta rápido ou quando o tempo de cálculo de um caminho de restauração for substancialmente reduzido.

5.3 SÍNTESE DO CAPÍTULO

Neste capítulo foram apresentados aspectos relacionados ao simulador empregado no presente estudo, os cenários de simulação e os resultados alcançados. Foi apresentada também a abordagem utilizada para se evitar os caminhos em “trap” nas simulações, que pode contribuir para trabalhos futuros.

Foram também realizados comentários a respeito dos resultados obtidos, que podem ser relevantes na busca dos melhores métodos de se estabelecer caminhos de LSPs em redes MPLS-TP em malha, redes estas que aparentam ser a tendência das modernas redes de transporte.

O próximo capítulo apresenta as conclusões deste trabalho.

6 CONCLUSÕES

O presente trabalho estudou aspectos relacionados ao estabelecimento de LSPs em redes MPLS-TP em malha, que utilizem como mecanismo de proteção esquemas de proteção em malha compartilhada.

Conforme visto no decorrer do trabalho, ainda não foram definidas medidas padronizadas para o estabelecimento desses LSPs, dada a dificuldade de se resolver esse problema de forma otimizada para a rede como um todo.

De modo a avaliar, de acordo com a aplicação de métodos de escolha de caminhos, o impacto no uso dos recursos da rede (considerando tanto a rede sem falhas quanto com falhas), foram testados três métodos de determinação de caminhos: um que prioriza somente o tamanho do caminho (em número de saltos) sem considerar os demais LSPs já estabelecidos na rede (portanto, sem efetuar o balanceamento de carga), denominado neste trabalho de método estático de escolha de caminhos; um segundo método, que prioriza somente o balanceamento de carga (portanto, considerando os demais LSPs já estabelecidos na rede), sem se importar com o tamanho dos caminhos, denominado neste trabalho de método espalhado de determinação de caminhos; e um terceiro método, denominado neste trabalho de método dinâmico de determinação de caminhos, que procura fazer um pouco das duas coisas: tanto tenta diminuir o tamanho do caminho quanto tenta também efetuar algum balanceamento de carga (considerando, portanto, os demais LSPs já estabelecidos na rede).

Nas simulações, os melhores resultados (em termos de uso dos recursos da rede) foram alcançados pelo método dinâmico, que tenta fazer um meio termo entre os dois paradigmas (carga e tamanho dos caminhos). Em segundo lugar, nesse parâmetro de uso da rede, ficou o método espalhado. Esses dois métodos consideram os LSPs já estabelecidos na rede para a escolha dos seus caminhos na rede. Em último lugar, no parâmetro de uso dos recursos da rede, ficou o método estático de escolha de caminhos, que não considera os LSPs já estabelecidos na rede para a escolha dos seus caminhos.

No caso de redes sem falhas, o método dinâmico reduziu a densidade média de tráfego em torno de 10% em relação ao método estático, enquanto que o método espalhado reduziu a densidade média do tráfego em torno de 6% em relação ao método estático.

Também foram acrescentadas heurísticas de recuperação, para avaliar (após o arranjo dos LSPs segundo cada método de escolha de caminhos) o desempenho da rede resultante em caso de falhas.

O método dinâmico conseguiu não só diminuir a carga média na rede (em aproximadamente 10% em relação ao método estático), assim como também diminuir (em torno de 11%, no pior caso de falhas, na maior rede simulada) o número máximo de LSPs afetados em caso de falhas na rede. Tudo isso foi alcançado apenas pela maneira de se arranjar (ou de se estabelecer) os LSPs na rede.

Os resultados das simulações efetuadas demonstram o quanto um simples melhor arranjo dos caminhos, levando-se em conta os demais LSPs já estabelecidos na rede, pode contribuir para uma redução no uso dos recursos da rede e no número máximo de LSPs afetados em casos de falhas.

Pelos resultados, observa-se que devem ser considerados, para a determinação de novos caminhos, os caminhos mais curtos que consigam fazer um melhor balanceamento da carga. Este simples procedimento consegue, inclusive, melhorar também as características de sobrevivência da rede, pois mesmo no pior caso simulado (falha simultânea de 1 nó e 2 links), o método dinâmico mostrou-se com melhores resultados no uso dos recursos da rede e no número máximo de LSPs afetados pelas falhas, seguido de perto pelo método espalhado.

Neste trabalho foi necessário também vencer o desafio do problema dos caminhos em “trap”, cuja solução até então se mostrava complexa e de alto custo computacional.

Em suma, o presente estudo acrescenta informações que podem ser utilizadas na busca da melhor solução global para o estabelecimento de LSPs em redes MPLS-TP em malha.

6.1 CONTRIBUIÇÕES

A principal contribuição provida por este trabalho foi a comparação entre os impactos à rede e à sobrevivência da rede (em caso de falhas) da forma como são estabelecidos os LSPs na rede MPLS-TP, considerando-se somente o tamanho dos caminhos, somente o balanceamento de carga ou um meio termo entre esses dois extremos. Foi demonstrado que considerar-se os demais LSPs já instalados na rede

proporciona um melhor uso dos recursos da rede em relação a não considerá-los, e que o balanceamento da carga juntamente com o tamanho dos caminhos (método dinâmico) proporciona resultados melhores do que se forem consideradas somente as cargas, independentemente dos tamanhos dos caminhos.

Como contribuição secundária, foi apresentada uma abordagem de solução simples e de baixo custo computacional ao problema dos caminhos em “trap”, até então inédita segundo a bibliografia pesquisada.

6.2 TRABALHOS FUTUROS

Como trabalhos futuros, sugere-se:

- a) aperfeiçoar a forma de balanceamento de carga efetuado pelo método denominado dinâmico utilizado neste trabalho, de modo a se melhorar ainda mais o uso global dos recursos da rede;
- b) nas simulações, aplicar prioridade aos LSPs, permitindo a ocorrência de preempção, de acordo com os requisitos da tecnologia MPLS-TP; e
- c) limitar a capacidade dos links, de modo a se acrescentar o parâmetro “capacidade residual” à equação do problema de se estabelecer LSPs em redes MPLS-TP em malha.

REFERÊNCIAS

- ALIDADI, A.; MAHDAVI, M.; HASHMI M.R., **A New Low-Complexity QOS Routing Algorithm for MPLS Traffic Engineering**, Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15-17; Kuala Lumpur Malaysia, p. 205-210, dez, 2009.
- ANDERSSON, L. et al., **MPLS Transport Profile (MPLS-TP) Control Plane Framework**, IETF RFC-6373, 2011.
- BAGULA, B. A.; BOTHA, M.; KRZESINSKI, A. E., **Online Traffic Engineering: the Least Interference Optimization Algorithm**. In Proceedings of IEEE International Conference on Communications ICC 2004, Paris, 2004.
- BELLER, D.; SPERBER, R.; **MPLS-TP – The New Technology for Packet Transport Network**. 2 DFN Forum, vol. 149, p. 81-92, 2009.
- BOCCI et al., **A Framework for MPLS in Transport Networks**, IETF RFC-5921, 2010.
- BRYANT, S., **An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge**, IETF RFC-5659, 2009.
- BRYANT, S.; PATE, P., **Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture**, IETF RFC-3985, 2005.
- CALLE, E.; MARZO, J. L.; URRÁ, A., **Protection performance components in MPLS networks**, Computer Communications, Volume 27, Issue 12, p. 1220-1228, jul, 2004.
- CAO, C. et al., **Packet-Level Optimization for Transnission Performance Improvement of Internet-Bound Traffic in a MPLS-TP Network**. Journal of Optical Communication Networks, vol. 2, No. 11, p. 991-999, nov, 2010.
- DONGYUN-ZHOU; SUBRAMANIAM, S., **Survivability in optical networks**, in Network, IEEE, vol.14, no.6, p.16-23, nov/dez 2000.
- EL-DARIEBY, M.; PETRIU, D.; ROLIA, J., **A Hierarchical Distributed Protocol for MPLS path creation**. In: Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on. IEEE, p. 920-926, 2002.
- FANG, L. et al., **MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design**, IETF RFC-6965, 2013.
- _____, **MPLS Transport Profile (MPLS-TP) Security Framework**, IETF RFC-6941, 2013.
- FANG, L., **Security Framework for MPLS and GMPLS Network**, IETF RFC-5920, 2010.

FROST, D.; BRYANT, S.; BOCCI, M., **MPLS Transport Profile Data Plane Architecture**, IETF RFC-5960, 2010.

GUO, L.; CAO, J.; YU, H.; LI, L., **Path-based routing provisioning with mixed shared protection in WDM mesh networks**. Lightwave Technology, Journal of, v. 24, n. 3, p. 1129-1141, 2006.

HAN, S; O'CONNOR, D.; YUE, W.; HAVALA, P., **Next-generation packet-based transport networks economic study**, Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference. OFC, 2006.

HASKIN, D.; KRISHNAN, R., **A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute**, IETF draft-haskin-mpls-fast-reroute-05.txt, 2000.

HO, P.; TAPOLCAI, J.; CINKLER, T., **Segment Shared Protection in Mesh Communications Networks with Bandwidth Guaranteed Tunnels**. IEEE/ACM Transactions on Networking, vol. 12, No. 6, p. 1105-1118, dez, 2004.

HUA, Y. et al. **Active-Fault-Alarm Based Dynamic Temporary Protection Mechanism for MPLS-TP Optical Networks**. In: Network Infrastructure and Digital Content, 2010 2nd IEEE International Conference on. IEEE, p. 911-915, 2010.

HUANG, F.; YI, X.; ZHANG, H.; GONG, P., **Key requirements of packet transport network based on MPLS-TP**; Communications and Photonics Conference and Exhibition (ACP), 2009 Asia, nov, 2009.

HUBBARD, S., **MPLS-TP in Next-Generation Transport Networks**. White paper, Light Reading/Heavy Reading MPLS-TP Initiative, 2011.

HUE-FEN, B. et al. **Active-fault-alarm Based Pre-restoration Mechanism in MPLS-TP Optical Network**. The Journal of China Universities of Posts and Telecommunications, v. 17, n. 3, p. 97-103, 2010.

HUIFENG, B.; YUEFENG, J., **Active Dynamic Pre-Protection Mechanism for MPLS-TP Network**. In: China High Technology Letters, v. 17, n. 4, p. 354-359, dez, 2011.

HUNDESSA, L.; DOMINGO, J., **Reliable and fast Rerouting Mechanism for a Protected Label Switch Path**. Proceedings of the IEEE GLOBECOM 02, nov, 2002.

HUNDESSA, L.; PASCUAL, J., **Fast Rerouting Mechanism for a Protected Label Switch Path**, Proceedings of the IEEE International Conference on Computer Communications 01; out, 2001.

IEEE 802.3 Ethernet Working Group, <http://www.ieee802.org/3/>

IEEE 802.3bs 400Gb/s Ethernet Task Force, <http://www.ieee802.org/3/bs/index.html>

IRASCHKO, R.; MACGREGOR, H.; GROVER, W. D., **Optimal Capacity Placement for Path Restoration in STM or ATM Mesh-Survivable Networks**, IEEE/ACM Transactions on Networking, Vol. 6, No. 3, jun, 1998.

ITU-T 16, **Optical Transport Networks & Technologies Standardization Work Plan, Issue 16**, set, 2012.

ITU-T G.707, **Network node interface for the synchronous digital hierarchy (SDH)**, 2007.

JAMHOUR, E.; PENNA, M., **A State-Based Availability Model to Shared Mesh Protection in MPLS-TP Networks with Preemption Support**. In: Network Operations and Management Symposium (NOMS), 2012 IEEE. p. 926-932, 2012.

KIM, S. W.; YOUN, H. Y.; CHOI, S. J.; SUNG, N. B., **GAPS: The Genetic Algorithm-based Path Selection Scheme for MPLS Network**, in Information Reuse and Integration, 2007. IRI 2007. IEEE International Conference on, p. 570-575, 13-15/ ago, 2007.

KODIALAM, M.; LAKSHMAN, T. V., **Garanteed Performance Routing of Unpredictable Traffic With Fast Path Restoration**, IEEE/ACM Transactions on Networking, vol. 17, No. 5, out, 2009.

_____, **Minimum Interference routing with applications to MPLS traffic engineering**, in Proceedings of INFOCOM, p. 884-893, 2000.

KODIALAM, M.; LAKSHMAN, T. V.; SENGUPTA, S., **Efficient and Robust Routing of Highly Variable Traffic**, In Proceedings of Third Workshop on Hot Topics in Networks (HotNets-III), nov, 2004.

KOSTA, Y.; THAKER, M.; NAGAR, B., **Performance Comparison of Rerouting Schemes of Multi Protocol Label Swithing Network**. ACEEE International Journal on Control Systems and Instrumentation, Vol. 02, No. 01, fev, 2011.

KOTTI, A.; HAMZA, R.; BOULEIMEN, K., **Bandwidth Constrained Routing Algorithm for MPLS traffic Engineering**, Networking and Services, ICNS. Third International Conference on, 19-25/jun, 2007.

LAM, K.; MANSFIELD, S.; GRAY, E., **Network Management Framework for MPLS-based Transport Networks**, IETF RFC-5950, 2010.

_____, **Network Management Requirements for MPLS-based Transport Networks**, IETF RFC-5951, 2010.

MAESSCHALCK, S. et al., **Pan-European Optical Transport Networks: An Availability-based Comparison**, Photonic Network Communications, 5:3, p. 203-225, 2003.

MAKAM, S.; SHARMA, V.; OWENS, K.; HUANG, C., **Protection / Restoration of MPLS Networks**, IETF draft-makam-mpls-protection-00.txt, 1999.

MANNIE, E.; PAPADIMITRIOU, D., **Analysis of Generalized Multi-Protocol Label Switching (GMPLS) – based Recovery Mechanisms (including Protection and Restoration)**, IETF RFC-4428, 2006.

MARTINEZ, R.; CASELLAS, R.; MUÑOZ, R., **Lab Trial of a GMPLS controlled MPLS-TP Packet Transport Network with Source/PCE Path Computations**. In: Optical Communication (ECOC), 2011 - 37th European Conference and Exhibition on. IEEE, p. 1-3, 2011.

NIVEN-JENKINS et al., **Requirements of an MPLS Transport Profile**, IETF RFC-5654, 2009.

OISHI, T.; TAKASE, M.; SAKAMOTO, K.; ENDO, H.; **Implementation of packet transport system using MPLS-TP technologies**, Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on , p. 1-6, 15-18/jun, 2010.

OU, C.; ZHANG, J.; ZANG, H.; SAHASRABUDDHE, L. H.; MUKHERJEE, B., **Online algorithms for shared-path protection in WDM mesh networks**. Department of Computer Science, University of California, Davis, Tech. Rep. CSE-2002-6, jun, 2006.

_____, **Near-optimal approaches for shared-path protection in WDM mesh networks**. In Communications, 2003. ICC'03. IEEE International Conference on (Vol. 2, pp. 1320-1324). IEEE, 2003.

PAN, P.; SWALLOW, G.; ATLAS, A., **Fast Reroute Extensions to RSVP-TE for LSP Tunnels**, IETF RFC-4090, 2005.

PAOLUCCI, F.; CUGINI, F.; GIORGETTI, A.; SAMBO, N.; CASTOLDI, P., **A Survey on the Path Computation Element (PCE) Architecture**. IEEE Communications Surveys & Tutorials, 2013.

PETERSSON, J. M., **MPLS Based Recovery Mechanisms**. Master Thesis. University of Oslo, maio, 2005.

ROSEN, E.; VISWANATHAN, A., **Multiprotocol label switching architecture**, IETF RFC 3031, 2001.

ROY, S.; BALASUBRAMANIAN, S.; GOWDA, P.B.V.; KOTA, S.A., **Doing more with less: Multiple-link failure resiliency using shared mesh protection**, in Advanced Networks and Telecommunications Systems (ANTS), 2014 IEEE International Conference on , vol., no., pp.1-3, 14-17; dez, 2014.

SHEN, G.; GROVER, W., **Survey and Performance Comparison of Dynamic Provisioning Methods for Optical Shared Backup Path Protection**, in Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on, p. 1310-1319, Vol. 2, out, 2005.

SPRECHER, N.; FARREL, A., **MPLS Transport Profile (MPLS-TP) Survivability Framework**, IETF RFC-6372, 2011.

SZETO, W.; BOUTABA, R.; IRAQUI, Y., **DORA: Efficient Routing for MPLS Traffic Engineering**, Journal of Network and Systems Management, vol. 10, No. 3, p. 309-325, set, 2002.

_____, **Dynamic Online Routing Algorithm for MPLS Traffic Engineering**. Lectures Notes in Computer Science, LNCS 2345, p. 936-946, 2002.

UTSTARCOM; **MPLS-TP based Packet Transport Networks**. UTStarCom. Alameda, Estados Unidos. CP-WP-MPLS-TP PTN-1109, 2009.

VAEZ-GHAEMI, R., **Next-Generation Packet-Based Transport Networks (PTN)**. JDSU white paper. NEXTGENPTN.WP.TFS.TM.AE, nov, 2010.

VIGOUREUX, M.; WARD, D.; BETTS, M., **Requirements for Operations Administration, and Maintenance (OAM) in MPLS-Transport Networks**, IETF RFC-5860, 2010.

Virtual Network Index – VNI, **The Zettabyte Era: Trends and Analysis**, White Paper, CISCO Public Document, 2015. Disponível em:

<http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html>

Acesso em: 28 dez 2015.

WALKOWIAK, K., **Survivable Routing of Unicast and Anycast Flows in MPLS Networks**, in Next Generation Internet Networks, 3rd EuroNGI Conference on, p. 72-79, 21-23/maio, 2007.

WANG, J.; SAHASRABUDDHE, J.; MUKHERJEE, B., **Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signaling**, IEEE Communications Magazine, vol. 40, no. 11, p. 80-87, nov, 2002.

WEIGARTEN et al. **Applicability of MPLS Transport Profile for Ring Topologies**, IETF RFC-6974, 2013

_____, **MPLS Transport Profile (MPLS-TP) Linear Protection**, IETF RFC-6378, 2011.

_____, **Requirements for MPLS-TP Shared Mesh Protection**, IETF RFC-7412, 2014.

WINTER, R.; **The Coming Age of MPLS**; Proceedings of IEEE Communications Magazine, p. 78-81, 2011.

XU, D.; XIONG, Y.; QUIAO, C., et al., **Trap avoidance and protection schemes in networks with shared risk link groups**, J. Lightw. Technol., vol. 21, no. 11, p. 2683–2693, nov, 2003.

XU, D.; XIONG, Y.; QUIAO, C., **Novell algorithms for shared segment protection**, IEEE J. Sel. Areas Commun., vol. 21, no. 8, p. 1320-1331, out, 2003.

YAN, X. et al., **An advanced LEO satellite network model based on MPLS-TP**, Advanced Intelligence and Awareness Internet (AIAI 2010), 2010 International Conference on, 2010.

YANG, H.; ZHANG, J.; ZHAO, Y.; JI, Y.; WU, J.; LIN, Y.; HAN, J.; LEE, Y., **Performance evaluation of multi-stratum resources integrated resilience for software defined inter-data center interconnect**, Opt. Express 23, p. 13384-13398, 2015.

YOSHIKANE, N.; TSURITANI, T., **Comparative cost analysis of optical networks with shared mesh protection in the beyond-100-Gb/s networks era**, in Optical Fiber Communications Conference and Exhibition (OFC), p.1-3, 9-13/mar, 2014.

ZHANG, J. et al. **Protection for MPLS-TP Multicast Services**. In: Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on. IEEE, 2009. p. 297-304, 2009.

_____, **Two Novel Tunnel-based Ring Protection Switching for MPLS-TP Multicast Services**. In: Telecommunications (ICT), 2011 18th International Conference on. IEEE, 2011. p. 458-462, 2011.

ZHANG, J.; BERGER, M.; RUEPP, S., **Flow-based End-to-End OAM Functions for the Multicast Service on the MPLS-TP Ring Network**, IEEE ICC 2010 Proceedings, 2010.

ZHANG, Z. et al. **Demonstration of Transport and Protection Schemes in a Multi-service Testbed for MPLS-TP Networks**. In: Photonics and Optoelectronics (SOPO), 2011 Symposium on. IEEE, p. 1-4, 2011.

APÊNDICE A – Cópia de Artigo Científico Publicado

Proceed. of the 13th International Conference on Data Networks, Communications and Computers 2015 p. 65-71.

Recent Advances on Systems, Signals, Control, Communications and Computers

LSP placement in an MPLS-TP mesh network with shared mesh protection mechanism

CLÁUDIO ROBERTO FERREIRA COSTA, WAGNER LUIZ ZUCCHI
Escola Politécnica – Departamento de Engenharia de Sistemas Eletrônicos
Universidade de São Paulo – USP
São Paulo – SP
BRAZIL
ferreiracosta@usp.br, wzucchi@lps.usp.br

Abstract: - The LSP path selection in an MPLS-TP mesh network is a problem whose solution is crucial to performance and survivability of that network. This paper evaluates three methods to select LSP paths, combined with two recovery heuristics, in order to indicate the most appropriate method, among them, to be used in MPLS-TP mesh networks with shared mesh protection mechanism. The recovery heuristics were applied to evaluate, in case of failures, the resultant network after the recovery of the LSPs. The simulation results demonstrate the impact of the methods and heuristics used.

Key-Words: - LSP placement, mesh network, MPLS-TP, shared mesh protection mechanism, survivability

1 Introduction

In the MPLS-TP (*Multi-Protocol Label Switching-Transport Profile*) environment, a path between two points or nodes in the network is called LSP (*Label Switched Path*). The route selected to the LSP pass through (with the network without failures) is called *working path*. To minimize the time to find a new path for the LSP in the event of network failures that affect its working path, an alternative route, called *protection path*, is also chosen jointly with the working path selection. Therefore, the establishment of an LSP involves selecting a pair of paths: the working path and its corresponding protection path.

The LSP placement in a mesh network may not be simple, depending on the complexity of the network and the number of established LSPs in the entire mesh network. For example, the use of shortest paths from different LSPs can overlap some links, causing congestion on those links, while other links are underutilized. If the selected working path passes through congested links, its performance will be worse than if it uses alternative paths less loaded. In the event of network failures affecting the LSP working path, its corresponding protection path is used. If the pre-selected protection path, when used, passes through congested links, it will also have a worse performance than if it uses an alternative path less loaded.

Thus, in an MPLS-TP network, the selection of the working path and the respective protection path of the LSPs can directly affect the performance of these LSPs.

The use of efficient LSPs (e.g., passing through less loaded paths) improves the performance of services provided by the MPLS-TP network. Furthermore, the problem of finding an eligible pair of working and protection paths under shared mesh protection for a new LSP arrival, with respect to existing LSPs in the network, is NP-complete [1][2].

This paper aims to evaluate some methods to select LSP paths in mesh networks, according to the load (bandwidth; amount of traffic) faced by each selected path (which consequently affects its performance), in order to indicate the most appropriate path selection method, among those tested, to be used in MPLS-TP mesh networks with shared mesh protection mechanism. The most appropriate method, in this case, is one that provides LSPs facing minor loads (consequently more efficient LSPs) and whose resultant network has the lowest number of affected LSPs in the event of network failures.

The remaining of this paper is organized as follows. The section 2 introduces a simple background review about the theme. The section 3 presents a brief overview of previous work. Section 4 presents the network recovery heuristics used in this paper and some considerations about the network load. Section 5 presents the simulation scenarios. Section 6 presents our simulation results and respective analysis. Finally, the Section 7 presents the conclusion and future work.

that, in the second and third methods, the paths are placed one by one, and the choice of a path depends on the choices of the previous paths, while in the first method the selection of a path does not depend on the other paths.

We consider the following assumptions in this paper: (1) Each working path has one, and only one, pre-allocated corresponding protection path. (2) Each working path and its respective protection path have the same endpoints, but do not share network physical links or intermediary nodes. (3) The network links may be simultaneously shared by working, protection and restoration paths belonging to different LSPs. (4) The links failures are always “cable cut” type. (5) All LSPs have equal priority, so there is no preemption and the links are utilized on the first come first served rule. (6) All LSPs are unidirectional, so the LSP X-Y (from node X to node Y) may use different physical links from the LSP Y-X, i.e., the path from X to Y may not be the inverse of the path from Y to X.

3 Related Works

Some research works have been performed on MPLS-TP mesh network recovery. For example: the study in [4] discuss the characteristics of the implemented GMPLS (Generalized Multi-Protocol Label Switching) control plane architecture for MPLS-TP along with the path computation algorithm, and presents the conducted lab trial to validate and evaluate the GMPLS control plane for the dynamic provisioning of bidirectional MPLS-TP LSPs in a mesh network, comparing either distributed (source-based) or centralized (Path Computation Element – PCE-based) path computation. The dynamic provisioning computes the shortest path cost in the mesh network and selects the higher unused bandwidth link in the feasible paths. The dynamic provisioning used in [4], in fact, is the restoration process and the focus of that study is the runtime of the calculation, according to the location (centralized or distributed) where the calculation is performed. The authors conclude that both strategies (centralized or distributed based path computation) perform similarly considering the runtime.

In [5] the authors propose a state-based availability model for shared mesh protection in MPLS-TP mesh networks with preemption support. In their model, a protect resource planning algorithm computes the minimum spare capacity required to achieve the desired availability of all protected paths, as well as the strategy for assigning priorities to the protection paths. The model tests

indicate that, in specific scenarios, the use of distinct protection priorities permits to achieve a desired level of protection with bandwidth economy. In that study, however, the preempted protection paths that can not preempt other lower priority paths are blocked, i.e., the restoration process is not used, thereby increasing the occurrence of disrupted LSPs in the mesh network.

The authors of [6] propose two novel protection schemes to provide efficient and reliable MPLS-TP multi-service using interconnected ring topologies in a mesh network. The study shows an intensive use of resources using ring protection topologies in mesh networks, demonstrating that such mechanism is less efficient in resource use than the shared mesh protection.

The study in [7] proposes a point-to-multipoint protection schemes to MPLS-TP mesh networks using interconnected ring topologies. In one scheme proposed, instead of be used one direction as working path and the other direction as protection path, the two are used as working paths and protect each other when there is a failure, enhancing the efficiency of network resource usage. This reinforces the thesis that, in mesh networks, the shared protection is more efficient in the use of resources than other types of protection.

4 Recovery Heuristics and Network Load

In this section we present the network recovery heuristics used in this paper and also some considerations about the network load calculation.

After the placement of the LSPs, it is necessary to test the resultant network without and with failures. In order to compare the resulting network performance after failures, we applied two recovery heuristics in case of network failures. In the first recovery heuristic, the recovery activation follows this sequence: if the working path fails, then it tries to switch the data traffic over its respective predefined protection path; but, if the protection path has also been affected by failures, then a restoration path is sought. Note that this recovery heuristic is the standard in MPLS-TP shared mesh protection mechanisms.

In the second recovery heuristic, if the working path is affected by failures, the protection path is not used; instead this, the restoration path is immediately sought. In this situation, observe that, differently from a working path and its protection path that do not share any link or intermediate node (i.e., they share only the end points), a restoration

path can also share links or intermediate nodes with the working path recovered by it.

Please note that, unlike the establishment of the working and protection paths, which are laid down in advance, the restoration paths can be established only after the failure occurrences. In our paper, the restoration path of an LSP S-D is chosen from the best paths (that interconnect the nodes S and D) available after the failures, considering the lowest number of hops, the lowest path load or both, depending on the path selection method used.

Observe that the protection and restoration paths may involve longer routes than the working paths served by them, causing greater bandwidth consumption at a higher number of links. So, the path choice method and the recovery heuristic used affect directly the load of the network and, consequently, its performance (due the delay of a link be impacted by the load of this link). The links (through which these working, protection or restoration paths pass) support the load of the LSP attended by them. The total load that a link supports is the sum of the loads of all paths (of all active LSPs in the network) that share this link. Note that the LSPs are unidirectional, so the load of a physical link in one direction may be completely different of the load of this same physical link in the opposite direction.

When the mesh network is without failures, the load calculation on each link does not involve great complexity. The load supported by each link (when the mesh network operates normally, without failures) is the sum of the load of all active working paths that share the link (considering that, in the network without failures, all LSPs have only working paths activated). However, in case of network failures, the network load calculation may be not simple (because it is necessary to reroute all LSPs affected by the failures before calculating the resulting load on the network, but this rerouting also depends on the existing network load), therefore it is helpful to use a simulator.

5 Simulation Scenarios

We have developed a simulator, where we can set up the mesh network and simulate the occurrence of none, single or multiple failures on nodes, links or both. The link failures (in our paper) are always type "cable cut", because we consider that it is the worst case. In our simulator, the shortest paths (in number of hops, load or both metrics) are determined by a modified Dijkstra algorithm and all working paths and their respective protection paths are set disjoint,

avoiding the trap paths (e.g., in Fig 2, the LSP 1 to 8 cannot use the path 1-2-7-8 as the working path, because that trap path does not allow the existence of a disjoint protection path). The trap paths were defined in [8][9].

Fig. 2 example of trap path with 'number of hops' metric

According the working, protection and restoration paths of all active LSPs in the MPLS-TP mesh network that use the *shared mesh protection* mechanism, our simulation calculates the resultant load of each link in the entire network, the traffic density faced by each resultant LSP (i.e., the sum of the total load of all links which the LSP passes through, divided by the LSP number of hops), the number of hops of each resultant LSP, the number of affected LSPs due the network failures, etc. It is important to observe that the simulation results depend on the predetermined arrangement of LSPs (the working paths and their respective protection paths), the failures, the recovery heuristics used, the (when necessary, if there are) found restoration paths and the load of each LSP in the network.

Fig. 3 topology of the simulated mesh networks

We have used 4 mesh networks in our simulation: a) 10-nodes/14-links; b) 16-nodes/23-links; c) 17-nodes/25-links; and d) 26-nodes/39-links, as shown in Fig. 3. For each set of simulations of a network, we have established one, and only one, unidirectional LSP between each pair of nodes, totaling $n \times (n - 1)$ LSPs in each simulated network (where n = number of network nodes); thus, we had 90, 240, 272 and 650 LSPs in the 4 simulated networks, respectively. In the simulations, a LSP "A-B" (from node A to node B) may be different from the inverse LSP "B-A", i.e., the LSPs "A-B" e "B-A" can share or not intermediary nodes. In all simulations, in order to facilitate the analysis of the results, the load of each LSP was 1Gbps and all LSPs had the same priority level.

We simulated the three methods of path selection and the two recovery heuristics previously explained, totaling six different behavior

configurations for each network. All network set of configurations was evaluated exhaustively (considering all possibilities of a specific set of failures), as shown in the Table 1, with respectively no failure (1 simulation by network); 1 link failure; 2 link failures; 1 node failure; 1 node and 1 link failures; and 1 node and 2 link failures. The 26-nodes/39-links network, for example, was simulated $6 \times 21.087 = 126.522$ times.

Table 1: number of network failure simulations for each network behavior configuration

number of network failure simulations	NETWORK			
	10 nodes 14 links	16 nodes 23 links	17 nodes 25 links	26 nodes 39 links
0 node 0 link	1	1	1	1
0 node 1 link	14	23	25	39
0 node 2 links	91	253	300	741
1 node 0 link	10	16	17	26
1 node 1 link	140	368	425	1.014
1 node 2 links	910	4.048	5.100	19.266
Total of simulations	1.166	4.709	5.868	21.087

The first method of to select paths (a static method that considers only the number of hops between the terminal nodes), when using the protection paths in case of failures (i.e., in the first recovery heuristic), we call “static + pp”; and when not using the protection paths (in the second recovery heuristic), we call “static – pp”. The second method of to choose paths (a dynamic method that considers the number of hops and also the load between the terminal nodes), according to the recovery heuristics used, we call “dynamic + pp” and “dynamic – pp”. The third method of to select paths (a dynamic method that considers only the load between the terminal nodes and that, therefore, can result in longer paths, with more hops) we call “spread + pp” and “spread – pp”, respectively, according to the use or not of the protection paths.

6 Simulation Results

The data shown in the following tables and figures demonstrate the impact of the path selection and the recovery heuristic in the four simulated networks, with and without failures, in the six behaviors evaluated in the simulations.

As can be seen in Table 2, the evaluated “dynamic” and “spread” methods to select paths cause a reduction of the average of the LSP traffic density (in Gbps/hop) when compared with the

“static” (standard of MPLS-TP) method. Note that, in a network without failures, the recovery heuristics are not relevant.

Table 2: average of the LSP traffic density (in Gbps/hop)

Set of failures =>	0 node 0 link	0 node 1 link	0 node 2 links	1 node 0 link	1 node 1 link	1 node 2 links
10-nodes 14-links	static + pp	8,054	8,489	9,772	7,731	8,815
	static – pp	8,054	8,698	10,015	7,864	8,990
	dynamic + pp	7,226	8,157	9,462	7,415	8,534
	dynamic – pp	7,226	8,007	9,430	7,283	8,503
	spread + pp	7,406	8,207	9,463	7,420	8,534
	spread – pp	7,406	8,093	9,427	7,314	8,491
16-nodes 23-links	static + pp	16,268	17,509	19,282	16,802	18,445
	static – pp	16,268	17,345	19,175	16,655	18,374
	dynamic + pp	15,290	16,877	18,738	16,154	17,897
	dynamic – pp	15,290	16,559	18,383	15,908	17,634
	spread + pp	15,648	17,204	18,957	16,428	18,076
	spread – pp	15,648	16,812	18,547	16,126	17,773
17-nodes 25-links	static + pp	17,952	18,588	20,139	17,832	19,287
	static – pp	17,952	18,749	20,464	18,067	19,651
	dynamic + pp	16,077	17,493	19,150	16,840	18,372
	dynamic – pp	16,077	17,189	18,892	16,583	18,181
	spread + pp	16,499	17,934	19,521	17,239	18,677
	spread – pp	16,499	17,483	19,083	16,807	18,330
26-nodes 39-links	static + pp	37,445	38,563	40,929	37,989	40,375
	static – pp	37,445	38,400	40,812	37,986	40,436
	dynamic + pp	33,585	35,759	38,370	35,273	37,852
	dynamic – pp	33,585	34,856	37,110	34,422	36,734
	spread + pp	35,067	36,857	39,200	36,204	38,538
	spread – pp	35,067	35,899	37,910	35,297	37,427

To the largest networks, in case of network failures, the recovery heuristic “– pp” (i.e., that no use the protection paths) has better performance than the opposite recovery heuristic “+ pp” in this parameter. Observe also that the larger is the simulated network, the greater (at a high rate) is the resultant average of the LSP traffic density by hop. Remember that in the larger simulated networks there are a greater number of LSPs (e.g., 10 nodes = 90 LSPs; 16 nodes = 240 LSPs; 17 nodes = 272 LSPs and 26 nodes = 650 LSPs).

The results shown in Table 2 follow the same trend, so the graphics with the simulation results (related to the average of the LSP traffic density in Gbps/hop) of all networks would be very similar. In order to visually highlight the impact of the methods and heuristics used, but avoiding being repetitive, in Fig. 4 we show only the simulation results on the 26-nodes/39-links network (which presents the biggest differences between the results on the six behaviors evaluated).

Fig. 4 average of the LSP traffic density (in Gbps/hop) in the simulated network of 26nodes/39links

The Table 3 shows that, to the parameter “average of the LSP number of hops”, the “dynamic – pp” and “static – pp” methods have the same results, the “dynamic + pp” and “static + pp” methods have similar results and that the “spread” method, as expected, presents higher values. The recovery heuristic “– pp”, in general, also has a better performance in this parameter than when compared with the recovery heuristic “+ pp”. The Fig. 5 standouts the results of this parameter on the 26-nodes/39-links network simulations.

Table 3: average of LSP number of hops

Set of failures =>		0 node 0 link	0 node 1 link	0 node 2 links	1 node 0 link	1 node 1 link	1 node 2 links
10-nodes 14-links	static + pp	2,067	2,175	2,312	2,128	2,257	2,363
	static – pp	2,067	2,175	2,312	2,128	2,257	2,363
	dynamic + pp	2,067	2,198	2,332	2,156	2,275	2,373
	dynamic – pp	2,067	2,175	2,312	2,128	2,257	2,363
	spread + pp	2,133	2,225	2,342	2,172	2,283	2,377
	spread – pp	2,133	2,206	2,326	2,150	2,269	2,369
16-nodes 23-links	static + pp	2,642	2,789	2,908	2,782	2,895	3,000
	static – pp	2,642	2,736	2,846	2,731	2,841	2,955
	dynamic + pp	2,642	2,785	2,906	2,776	2,893	3,001
	dynamic – pp	2,642	2,736	2,846	2,731	2,841	2,955
	spread + pp	2,750	2,867	2,967	2,853	2,950	3,044
	spread – pp	2,750	2,817	2,907	2,804	2,897	2,997
17-nodes 25-links	static + pp	2,765	2,866	2,959	2,855	2,945	3,038
	static – pp	2,765	2,840	2,928	2,830	2,918	3,014
	dynamic + pp	2,765	2,875	2,971	2,866	2,957	3,048
	dynamic – pp	2,765	2,840	2,928	2,830	2,918	3,014
	spread + pp	2,846	2,945	3,026	2,931	3,005	3,083
	spread – pp	2,846	2,898	2,968	2,880	2,954	3,040
26-nodes 39-links	static + pp	3,557	3,651	3,738	3,657	3,747	3,842
	static – pp	3,557	3,619	3,692	3,626	3,705	3,798
	dynamic + pp	3,557	3,665	3,759	3,675	3,768	3,863
	dynamic – pp	3,557	3,619	3,692	3,626	3,705	3,798
	spread + pp	3,735	3,819	3,887	3,819	3,887	3,959
	spread – pp	3,735	3,755	3,796	3,748	3,800	3,872

Fig. 5 average of LSP number of hops in the simulated network of 26nodes/39links

The Table 4 shows that the “dynamic” and “spread” methods achieved the best results with respect to the parameter “highest number of affected LSPs in case of network failures”, especially for the larger networks. The recovery heuristics “– pp” and “+ pp” are not relevant in this case, because the parameter is measured before the recovery actions. Please note that some of the affected LSPs may not be recovered (because of nodes which may have become unreachable due to the failures of the network). The number of unrecoverable LSPs due node failures is independent of the path selection

method used. The Fig. 6 standouts the results of this parameter on the 26-nodes/39-links network simulations.

Table 4: highest number of affected LSPs in case of network failures

Set of failures =>		0 node 1 link	0 node 2 links	1 node 0 link	1 node 1 link	1 node 2 links
10-n 14-l	static	28	40	42	56	64
	dynamic	21	36	36	53	63
	spread	21	38	39	55	64
16-n 23-l	static	52	98	92	126	154
	dynamic	45	87	90	123	156
	spread	46	90	84	124	157
17-n 25-l	static	66	110	90	138	162
	dynamic	48	83	80	123	151
	spread	47	83	80	125	153
26-n 39-l	static	122	229	184	283	379
	dynamic	99	190	167	251	334
	spread	103	199	174	263	336

Fig. 6 highest number of affected LSPs in case of network failures in the simulated network of 26-nodes/39-links

The Table 5 summarizes the findings for the simulated network of 26-nodes/39-links, also in order to better show, using this example, the impact on network performance of the path selection methods and recovery heuristics used.

Table 5 summary of the 26-nodes/39-links network simulation results

Failures set	parameter	Static	Dynamic	Spread
0 node 0 link (without failure)	average of the LSP traffic density (Gbps/hop)	37,445	33,585	35,067
	average of the LSP number of hops	3,557	3,557	3,735
1 node 2 links (worst case simulated)	Static +pp	43,002	40,596	41,101
	average of the LSP traffic density (Gbps/hop)	43,002	40,596	41,101
	average of the LSP number of hops	3,842	3,863	3,959
	highest number of affected LSPs	379	334	336
	Static -pp	43,179	39,459	40,044
	average of the LSP traffic density (Gbps/hop)	43,179	39,459	40,044
	average of the LSP number of hops	3,798	3,798	3,872
	highest number of affected LSPs	379	334	336

7 Conclusion

The results achieved in this paper, taken together, indicate that the “dynamic” method of path selection performs best both for networks without failures as for networks with failures, mainly for the larger networks. It reduces not only the traffic density in the network, but also the number of affected LSP in case of network failures. Moreover, apparently the use of the “dynamic” method tested in this paper does not require great efforts. Regarding the recovery heuristics tested, the “– pp” recovery heuristic shows, in general, better performance (in terms of traffic density and number of hops) than the other tested recovery heuristic “+ pp” (which is the standard recovery procedure on MPLS-TP networks). It is very important to observe, however, that the time to calculate a restoration path is much longer than the time to switch the data traffic to a previously allocated protection path. Thus, the use of heuristic “– pp” only will be advantageous when its calculation time has already been substantially reduced. As future work, we will be studying the use of priorities among LSPs, with preemption, in the problem of the LSP placement in MPLS-TP mesh networks with the shared mesh protection mechanism.

References:

- [1] C. Ou, J. Zhang, H. Zang, L. H. Sahasrabudde, and B. Mukherjee, *Online algorithms for shared-path protection in WDM mesh networks*. Department of Computer Science, University of California, Davis, Tech. Rep. CSE-2002-6.
- [2] C. Ou, J. Zhang, H. Zang, L. H. Sahasrabudde, and B. Mukherjee, *Near-optimal approaches for shared-path protection in WDM mesh networks*. In Communications, 2003. ICC'03. IEEE International Conference on (Vol. 2, pp. 1320-1324). IEEE.
- [3] N. Sprecher, and A. Farrel, *MPLS Transport Profile (MPLS-TP) Survivability Framework*, RFC-6372, September 2011.
- [4] Ricardo Martinez, Ramon Casellas, and Raúl Muñoz, *Lab Trial of a GMPLS controlled MPLS-TP Packet Transport Network with Source/PCE Path Computations*. In: Optical Communication (ECOC), 2011 37th European Conference and Exhibition on. IEEE, 2011. p. 1-3.
- [5] Edgard Jamhour, and Manoel Camillo Penna, *A State-Based Availability Model to Shared Mesh Protection in MPLS-TP Networks with Preemption Support*. In: Network Operations and Management Symposium (NOMS). IEEE, 2012. p. 926-932.
- [6] Zhihui Zhang, Yongjun Zhang, and Wanyi Gu, *Demonstration of Transport and Protection Schemes in a Multi-service Testbed for MPLS-TP Networks*. In: Photonics and Optoelectronics (SOPO), 2011 Symposium on. IEEE, 2011. p. 1-4.
- [7] Jiang Zhang, Sarah Ruepp, Michael S. Berger, and Henrik Wessing, *Protection for MPLS-TP Multicast Services*. In: Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on. IEEE, 2009. p. 297-304.
- [8] D. Xu, Y. Xiong, and C. Quiao, *Novell algorithms for shared segment protection*, IEEE J. Sel. Areas Commun., vol. 21, no. 8, pp. 1320-1331, Oct. 2003.
- [9] Lei Guo, Jin Cao, Hongfang Yu and Lemin Li. *Path-based routing provisioning with mixed shared protection in WDM mesh networks*. Lightwave Technology, Journal of, v. 24, n. 3, p. 1129-1141, 2006.