UNIVERSIDADE FEDERAL RURAL DO SEMIÁRIDO
UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE
CURSO DE MESTRADO EM CIÊNCIA DA COMPUTAÇÃO

MÁRIO JORGE LIMEIRA DOS SANTOS

AVALIAÇÃO DO PROTOCOLO DE GERENCIAMENTO DE ENLACE EM UM PLANO DE CONTROLE EM REDES ÓTICAS DINÂMICAS

MOSSORÓ - RN
2012

MARIO JORGE LIMEIRA DOS SANTOS

AVALIAÇÃO DO PROTOCOLO DE GERENCIAMENTO DE ENLACE EM UM PLANO DE CONTROLE EM REDES ÓTICAS DINÂMICAS

Dissertação apresentada ao Mestrado em Ciência da Computação, associação ampla entre a Universidade do Estado do Rio Grande do Norte e a Universidade Federal Rural do Semi-Árido, para a obtenção do título de Mestre em Ciência da Computação.

Orientador: PROF. DR. IGUATEMI EDUARDO DA FONSECA - UFPB

MOSSORÓ - RN
2012

MÁRIO JORGE LIMEIRA DOS SANTOS

AVALIAÇÃO DO PROTOCOLO DE GERENCIAMENTO DE ENLACE EM UM PLANO DE CONTROLE EM REDES ÓTICAS DINÂMICAS

Dissertação apresentada ao Mestrado em Ciência da Computação para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em 02/05/2012

BANCA EXAMINADORA

Prof. Dr. Iguatemi Eduardo da Fonseca (Orientador)
Universidade Federal da Paraíba - UFPB

Prof. Dr. Hélcio Wagner da Silva
Universidade Federal Rural do Semi-Árido - UFERSA

Prof. Dr. Luiz Gonzaga de Queiroz Silveira Júnior
Universidade Federal do Rio Grande do Norte - UFRN

Aos meu pais, Maria do Rosário e José Praxedes dos Santos.

Agradecimentos

Agradeço a Deus pela saúde, pela força de vontade que me faz seguir em frente e pelas bençãos e graças alcançadas.

Agradeço aos meu pais pelo suporte e pelo amor incondicional.

Agradeço à minha namorada Luana Dantas, pelo amor, o apoio, o carinho, a amizade e companheirismo sempre.

Agradeço ao meu orientador, professor Iguatemi Eduardo pelas orientações e ajuda indispensável para a realização deste trabalho.

Agradeço aos colegas de mestrado e ao bolsista PIBIC Bruno Ramon, pela convivência, a troca de experiência e os momentos de estudo que contribuíram para chegar até aqui.

Agradeço aos professores do mestrado com que convivi e com quem muito aprendi, e a secretária do mestrado, Rosita.

Agradeço à UERN e a UFERSA pela oportunidade e pela infra-estrutura disponibilizadas.

Agradeço ao IFCE Campus Limoeiro do Norte, na pessoa de seus diretores, pela compreensão e apoio.

Agradeço também aos meus amigos e familiares pela compreensão e pelos bons momentos.

Enfim, agradeço a todos que de alguma forma contribuíram para que eu chegasse ao final de mais essa importante etapa na minha vida.

Obrigado a todos!

Resumo

Neste trabalho foram propostas e avaliadas funções de descoberta de recursos e de topologia para o protocolo de gerenciamento de enlace (LMP), como parte do plano de controle GMPLS (*Generalized Multi-Protocol Label Switching*) em redes óticas dinâmicas transparentes. Os objetivos são trazer a fase de descoberta e manutenção do mapa de recursos da rede para a fase de planejamento e demonstrar que mesmo com a adição de parâmetros de Engenharia de Tráfego ao LMP e modificações nas mensagens de gerenciamento do canal de controle, o estabelecimento dos canais de controle pode ser realizado em tempos na faixa de segundos para os cenários de rede testados. Para as avaliações, foram implementadas duas versões do LMP, a primeira com acréscimo de parâmetros como comprimento de onda e uma característica da fibra, além do identificador de porta local. A segunda versão respeitou estritamente o tamanho das mensagens e o conteúdo dos cabeçalhos dos objetos LMP, e incluiu os parâmetros comprimento de onda e o Identificador de porta local. O desempenho das funções foi avaliado nas duas versões implementadas por meio de experimentos computacionais que comprovaram que as funções propostas são capazes de estabelecer os canais de controle em tempos na faixa de segundos. Foram medidos o tempo médio de conexão dos nós a todos os seus vizinhos e o número médio de mensagens *Config* enviadas para um nó conectar-se a seus vizinhos. Os resultados dos experimentos mostraram que com o aumento do número de nós, a versão estendida do LMP mostrou-se um pouco mais eficiente nos nós com menos vizinhos. Entretanto, nos nós com maior número de vizinhos, no cenário de testes com maior número de nós, a versão padrão do LMP se mostrou-se um pouco mais vantajosa. Com base nos resultados, foi possível comprovar que em cenários com diferentes números de nós, o algoritmo estabeleceu a conexão completa do plano de controle em tempo de segundos de maneira automatizada.

Palavras-chave: LMP, GMPLS, Descoberta de topologia, Descoberta de vizinhos.

Abstract

In this work was proposed and evaluated functions of resource and topology discovery for the Link Management Protocol (LMP), as part of the GMPLS control plane for transparent dynamic optical networks. The goals are to bring the network resource map discovery and maintenance phase for the planning phase and demonstrate that even with the addition of Traffic Engineering parameters in the LMP and changes in management messages of the control channel, the establishment of control channels could be achieved in times ranging from seconds in the network scenarios tested. Two versions of LMP were implemented, the first one with the addition of parameters such as wavelength and a fiber parameter, also the local port identifier. The second version is strictly complied with the message size and content of the LMP objects headers, and included the parameters wavelength and the local port identifier. The performance of the functions was evaluated, in both implemented versions, by means of computational experiments that proved that the proposed functions are able to establish control channels in times ranging from seconds. It was measured the average time of connection of the nodes to all its neighbors and the average number of Config messages sent to a node connect to its neighbors. The results showed that increasing the number of nodes, the extended version of LMP proved to be a little more efficient with fewer neighbors. However, nodes with more neighbors, in the test scenario with a larger number of nodes, the standard version of the LMP proved to be somewhat more advantageous. Based on the results, the experiments suggest that in scenarios with different numbers of nodes, the algorithm established connections of the control plane in times of seconds in an automated manner.

Keywords: LMP, GMPLS, Topology discovery, Neighbor discovery.

Lista de Siglas

BCid	Bearer Channel identifier
BER	Bit Error Rate
CCid	Control Channel Identifier
CD	Chromatic Dispersion
CR-LDP	Constraint-Based Routing Label Distribution Protocol
DCN	Data Communication Network
DRAGON	Dynamic Resource Allocation in GMPLS Optical Networks
DWDM	Dense Wavelength Division Multiplexing
FSC	Fiber Switching Capable
FSM	Finite State Machine
G-LSP	Generalized Label Switched Path
GMPLS	Generalized Multi-Protocol Label Switching
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISC	Interface Switching Capable
ISIS-TE	Intermediate System to Intermediate System with Traffic Engineering extensions
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
L2SC	Layer 2 Switching Capable
LMP	Link Management Protocol
LSA	Link State Advertising
LSC	Label Switching Capable
LSP	Label Switching Path
LSR	Label Switched Router

MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MPLS-TE	Multiprotocol Label Switching - Traffic Engineering
OADM	Optical Add/Drop Multiplexer
OBS	Optical Burst Switching
OEO	Optical-Eletrical-Optical
OIF	Optical Internetworking Forum
OLT	Optical Line Terminal
OSC	Optical Supervisory Channel
OSPF-TE	Open Shortest Path First - Traffic Engineering
OXC	Optical CrossConnect
PDG	Polarization dependent gain
PDL	Polarization-dependent loss
PMD	Polarization Mode Dispersion
PSC	Package Switching Capable
QoS	Quality of Service
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RWA	Routing and Wavelength Assignment
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
SPF	Shortest Path First
TDMC	Time Division Multiplexing Capable
TWC	Tunable Wavelength Converter
UDP	User Datagram Protocol
WDM	Wavelength Division Multiplexing

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

Desde a fabricação da primeira fibra ótica de baixa-perda em 1970, a possibilidade de uma rede de comunicação totalmente ótica tem instigado pesquisadores e provedores de serviço. (STERN *et al.*, 2009).

As fibras óticas são amplamente empregadas hoje como base para os mais variados tipos de redes de comunicação (RAMASWAMI; SIVARAJAN, 2002). A tecnologia de transmissão por fibra tem evoluído ao longo das últimas décadas para oferecer taxas de transmissão cada vez mais altas para distâncias cada vez mais longas.

Ao longo da última década com o crecimento do acesso à banda larga, a demanda por aplicações baseadas na *internet* tem aumentado continuamente. O que levou fabricantes de equipamentos, empresas de comunicação e provedores de serviço a juntarem-se em torno do desenvolvimento das comunicações óticas em rede para tornar as redes óticas comercialmente viáveis em custo e desempenho (STERN *et al.*, 2009). A comercialização de largura de banda foi introduzida como uma maneira de melhorar a utilização de fibras e desse modo otimizar os lucros. Uma operadora com capacidade de transmissão ociosa pode vender essa capacidade para uma outra operadora com excesso de demanda. Esse tipo de troca requer sofisticadas ferramentas de controle e gerenciamento para reconfiguração da rede (STERN *et al.*, 2009). As necessidades atuais de largura de banda nas redes de comunicação em função do contínuo crescimento do tráfego de dados e da heterogeneidade desse tráfego tem demandado um grande esforço de pesquisa para melhor aproveitamento das redes óticas (ABBADE *et al.*, 2009). O foco da comunidade de pesquisa em redes óticas tem sido a organização, controle, gerenciabilidade, sobrevivência, padronização e efetividade de custo, o que reflete a maturidade das tecnologias óticas e o reconhecimento de que as redes óticas são o único meio que pode suportar as demandas atuais e futuras por largura de banda. Questões de alto nível como a padronização de técnicas de gerenciamento e controle em redes com equipamentos de múltiplos fabricantes estão contribuindo para a eficácia das redes óticas.

De maneira geral, uma rede de grande porte requer complexos sistemas de gerenciamento e controle e elementos de rede inteligentes para monitoramento de desempenho, reconfiguração da rede e recuperação de falhas (STERN *et al.*, 2009). Esses elementos e sistemas complexos estão convergindo para um plano de controle que emgloba protocolos para sistemas de gerenciamento propostos para redes óticas.

Alguns dos problemas, em geral relacionados ao planejamento de rede, que podem ser resolvidos pelo plano de controle são a minimização do "custo" da rede em relação a largura de banda dos enlaces entre os nós na rede, e também o problema da descoberta

da topologia da rede a fim de minimizar os custos de transmissão (MUKHERJEE, 2006). Conforme vão sendo adicionados novos nós na rede ou novas demandas de tráfego, o plano de controle deve reorganizar a topologia de modo a atender as novas demandas estabelecidas levando em consideração a topologia atual e a capacidade de cada enlace.

As características e requisitos dos serviços suportados pelas redes óticas são extremamente diversos em termos de conectividade, largura de banda, desempenho, sobrevivência, custo, entre outras características. Foi feito um esforço de padronização por parte de órgãos internacionais especializados e empresas fabricantes de equipamentos de rede, para desenvolver um plano de controle unificado baseado na suíte de protocolos conhecida como GMPLS. Trata-se de uma versão generalizada do MPLS (*Multiprotocol Label Switching*) proposta pela Força tarefa para a engenharia da *Internet* (IETF - *Internet Engineering Task Force*), que adicionalmente oferece suporte às redes com outros tipos de comutação que não as de pacotes, como as redes óticas sincronas (SONET - *Synchronous Optical Network*) , que comutam a informação a partir de intervalos de tempo e as redes com a tecnologia de multiplexagem por divisão de comprimento de onda (WDM - *Wavelength Division Multiplexing*) que realizam o chaveamento de conexões utilizando comprimentos de onda (PERROS, 2005). O padrão GMPLS tem sido amplamente aceito como a melhor solução para o desenvolvimento de um plano de controle para redes óticas chaveadas por comprimento de onda (MUNOZ *et al.*, 2009).

O GMPLS proporciona a automação da operação de rede em ambientes envolvendo diferentes redes interconectadas, por meio de elementos de gerência de rede, provisão de conexões e implementação de engenharia de tráfego. Além disso, deve prover proteção e recuperação de maneira rápida e automática em toda a rede (STERN *et al.*, 2009).

As principais funções do plano de controle são: descoberta de vizinhos, sinalização e roteamento. Na arquitetura GMPLS, essas funções são implementadas por extensões melhoradas dos protocolos do MPLS-TE (*Multi-Protocol Label Switching - Traffic Engineering*) , que são: o protocolo de reserva de recursos com Engenharia de tráfego (RSVP-TE - *Resource Reservation Protocol - Traffic Engineering*), protocolo de sinalização para configurar conexões fim-a-fim habilitadas à qualidade; o OSPF-TE (*Open Shortest Path First - Traffic Engineering*), para disseminação automática de informações de topologia e recursos da rede; e o protocolo de gerenciamento de enlace (LMP - *Link Management Protocol*) para descoberta e verificação de enlace e suas propriedades (MUNOZ *et al.*, 2009).

1.1 Motivação

Visando alcançar a automatização do processo de reorganização das redes óticas GMPLS transparentes, o foco deste trabalho está no já citado LMP. O LMP é um protocolo de descoberta automatizada de vizinhos e permite a rede criar e manter bancos de dados de estados das portas e conexões, e da topologia, com o objetivo de realizar atribuição de nós-portas entre nós vizinhos.

Durante as pesquisas bibliográficas foram identificados alguns trabalhos correlatos recentes na literatura científica que abordam as funções de descoberta de vizinhos e de topologia do LMP e a descoberta de recursos em geral, nas redes óticas transparentes.

No trabalho realizado por (SHIOMOTO *et al.*, 2009), os autores propõem um método de descoberta de vizinhos utilizando um módulo chamado *trunk* acoplado a todos os elementos de chaveamento ótico. Esse módulo realiza troca de mensagens de teste entre nós vizinhos para identificar os endereços de interfaces desses nós. A função de descoberta de vizinhos neste trabalho também tem como objetivo evitar as tarefas de configuração manual da rede. No trabalho citado foi avaliado o tempo gasto até a identificação de todos os endereços das interfaces dos nós.

A descoberta automática de recursos em redes GMPLS transparentes é proposta em (PERELLO *et al.*, 2007). A tarefa de descoberta é feita através de extensões do LMP que realizam a função de descoberta do plano de transporte das redes totalmente óticas. A função de descoberta do plano de controle em redes óticas transparentes é implementada em uma rede em que a topologia do plano de controle é igual a topologia do plano de transporte, usando mensagens LMP. Os autores avaliam duas estratégias de descoberta para o plano de transporte, chamadas descoberta sequencial (SD) e descoberta paralela (PD). Em cada uma dessas estratégias é avaliado no plano de transporte o parâmetro tempo total para a descoberta dos recursos, calculado em função do número de enlaces de dados entre os nós e em função do número de nós que compõem a rede. Para as avaliações foi usado um ambiente de testes (*testbed*) com topologia em anel e uma rede com diferentes topologias em malha.

O trabalho descrito em (ÁRTICO, 2011) teve como objetivo a implementação do LMP na linguagem de programação C e a sua integração ao pacote de software de código aberto para plano de controle em redes óticas do projeto chamado DRAGON (*Dynamic Resource Allocation in GMPLS Optical Networks*) (DRAGON, 1999-2012). Foram realizados testes em laboratório com as funções de estabelecimento, manutenção e gerenciamento do canal de controle.

Em (PERELLO *et al.*, 2009) os autores propõem dois esquemas para diminuir a probabilidade de perda por rajada na camada de chaveamento ótico por rajada (OBS

-*Optical Burst Switching*), em um cenário de redes heterogêneas, que combina os benefícios do circuito ótico e as tecnologias de chaveamento por rajada. Os autores chamam atenção para a viabilidade de usar informação de estado de recursos para decisões de roteamento na camada OBS. Eles procuram mostrar que o mecanismo de disseminação das informações de estado torna-se crucial para todo o desempenho da camada OBS. Em um dos dois esquemas propostos, os dados a respeito do estado dos nós são incluídos nas mensagens *Hello* do protocolo LMP, que são trocadas entre nós vizinhos na camada de controle a cada 150ms, com o objetivo de diminuir o *overhead* de mensagens de controle. Como um dos resultados obtidos, os autores identificaram que a disseminação de informações de estados de recursos baseada no protocolo LMP mostrou-se favorável para rajadas curtas e médias, provendo melhor probabilidade de perda ao passo que introduz um baixo *overhead* de controle.

Em (LEE *et al.*, 2009) os autores demonstraram o monitoramento de desempenho do enlace usando uma extensão do LMP em um ambiente de testes (*testbed*) de rede totalmente ótica com quatro nós. Múltiplos parâmetros do enlace importantes para o cálculo de rotas puderam ser monitorados dinamicamente no plano de controle GMPLS.

A proposta do presente trabalho tem como um dos diferenciais, o fato de que a descoberta de vizinhos e seus recursos é feita de maneira dinâmica com o protocolo LMP executando em cada nó simultaneamente sem a necessidade do uso de módulos adicionais. Outro característica deste trabalho deve-se ao fato do plano de controle manter um "Banco de dados", com as informações sobre os recursos da rede à disposição do algoritmo de roteamento e atribuição de comprimento de onda (RWA). Essa base de dados se dá na forma de uma matriz de tráfego, com uma riqueza maior de informações coletadas pela função de descoberta de recursos do protocolo LMP. Esse conhecimento prévio de informações da rede tais como comprimentos de onda disponíveis em cada nó, parâmetros de Engenharia de tráfego, tais como dispersão de modo de polarização (PMD) da fibra, largura de banda ociosa, entre outras, acarreta na diminuição da necessidade de mensagens de anúncio de recursos (*flooding*) por parte das funções de RWA e sinalização do plano de controle, o que diminui o *overhead* gerado pelo tráfego dessas mensagens na rede. No presente trabalho são avaliados os parâmetros de tempo total para descoberta de recursos e o número de mensagens trocadas até que todos os nós da rede estejam conectados aos seus vizinhos.

1.2 Objetivos

1.2.1 Objetivo Geral

O objetivo principal deste trabalho é desenvolver as funções de descoberta de vizinhos e de topologia para o LMP de modo que a topologia da rede possa ser criada e modificada de forma automatizada. O trabalho será desenvolvido considerando o cenário de redes óticas dinâmicas transparentes. As funções do LMP desenvolvidas nesse trabalho visam facilitar o aprovisionamento automático de conexões no tipo de rede já citado, tornando o planejamento e configuração dessas redes menos dispendioso, permitindo assim a migração do planejamento e configuração manuais de rede com atraso de tempo de dias, para um planejamento automatizado dessas redes.

1.2.2 Objetivos Específicos

Para que o objetivo geral deste trabalho seja atingindo, os seguintes objetivos específicos foram estabelecidos:

- Levantamento bibliográfico do estado da arte dos trabalhos de pesquisa, desenvolvimento e testes do protocolo LMP, identificando trabalhos correlatos.
- Desenvolvimento de um ambiente de testes em software, que possibilitasse o registro dos dados para geração de resultados numéricos.
- Desenvolvimento das funções de descoberta de topologia e de recursos, estabelecimento de canais de controle e da função de armazenamento e disponibilização das informações dos nós, do protocolo LMP para serem utilizadas no ambiente de testes.

1.3 Metodologia

A metodologia utilizada no desenvolvimento desse trabalho de pesquisa consistiu das seguintes etapas:

- Revisão bibliográfica: Nesta fase foi feita uma revisão de artigos que tratam das pesquisas em Redes Óticas transparentes, Plano de Controle GMPLS, os protocolos que o compõem com foco no LMP e suas funções para o gerenciamento do canal de controle.
- Criação do ambiente de testes para as funções a serem desenvolvidas.

- Desenvolvimento das funções de descoberta de recursos e de estabelecimento de canais de controle do protocolo LMP para gerência do canal de controle no plano de controle GMPLS em redes óticas dinâmicas transparentes;

- Avaliações: Definição de variáveis a serem consideradas no trabalho. Teste do funcionamento das funções do protocolo com registro dos dados numéricos medidos. Organização dos dados e interpretação dos resultados.

1.4 Organização do documento

O restante deste documento está organizado da seguinte forma: o Capítulo 2 trata da camada ótica das redes de transporte atuais e sua relação com as redes clientes. Faz uma explanação sobre as redes óticas e um tipo especial dessas redes, as chamadas redes óticas transparentes e apresenta o plano de controle nas redes óticas. O Capítulo 3 explica em detalhes como trabalha o plano de controle desenvolvido sobre a arquitetura GMPLS nas redes óticas. O Capítulo 4 mostra em detalhes o algoritmo e as funções desenvolvidas, demonstra como foi montado o ambiente para testes, a forma como esses foram realizados e os resultados obtidos a partir desses testes. O Capítulo 5 apresenta as conclusões do trabalho e indica trabalhos futuros.

2 A camada ótica e as redes clientes

Com o rápido avanço das tecnologias da informação no início do Século XXI tem havido uma crescente demanda pelos serviços de comunicação que podem ser fornecidos com essas tecnologias. Em geral esses serviços de comunicação, que englobam música, jogos interativos, compartilhamento de arquivos, voz e vídeo, são voltados para a *internet* e a *web*. Essa demanda por serviços de informação e comunicação continua a crescer em um ritmo cada vez maior. Por baixo de todos esses serviços existe uma infraestrutura de comunicação global baseada em fibra ótica (STERN *et al.*, 2009). Esta seção trata da comunicação ótica em rede, mostrando os componentes dessa comunicação e elucidando o conceito de transparência em redes óticas. Faz um apanhado das redes clientes, tratando da sua interação com a camada ótica e apresenta o plano de controle nas redes óticas.

2.1 Visão Geral

A clássica visão em camadas das redes de comunicação necessita de algumas modificações para manipular a variedade de redes e protocolos que estão proliferando atualmente. Um modelo em camadas mais realístico para as redes atuais empregaria múltiplas pilhas de protocolos residindo umas no topo das outras. Cada pilha incorpora muitas subcamadas, que podem prover funções semelhantes as tradicionais camadas física, de enlace e de rede (RAMASWAMI *et al.*, 2010).

A introdução da chamada segunda geração das redes óticas, que veremos a seguir, adiciona uma outra camada para a hierarquia de protocolos, a tão chamada camada ótica. A camada ótica é uma camada servidora que provê serviços para outras camadas clientes. Essa camada ótica provê caminhos óticos (chamados de *lightpaths* ou caminhos chaveados por rótulos (LSP - *Label Switching Path*)) para uma variedade de camadas clientes. Exemplos de camadas clientes residindo sobre uma camada de rede ótica de segunda geração incluem as camadas IP (*Internet Protocol*), *Ethernet*, e a SONET/SDH (*Synchronous Digital Hierarchy*) (RAMASWAMI *et al.*, 2010).

Para as redes SONET, *Ethernet* ou IP operando sobre a camada ótica, os LSPs são simplesmente substituições para as conexões físicas de fibra entre terminais SONET ou roteadores IP. Dependendo das capacidades da rede, o LSP pode ser pensado como um serviço chaveado por circuito. Esse serviço LSP pode ser usado para suportar conexões de alta velocidade para uma variedade de redes (RAMASWAMI *et al.*, 2010).

A camada ótica multiplexa múltiplos LSPs dentro de uma única fibra e permite que LSPs individuais sejam extraídos eficientemente de um sinal composto em nós da

rede. Essa camada incorpora sofisticadas técnicas de recuperação de serviço e também técnicas de gerenciamento (RAMASWAMI *et al.*, 2010).

2.2 Redes Óticas

No início das últimas décadas do século XX enormes quantidades de fibra ótica foram instaladas por todo o mundo. Inicialmente as fibras foram usadas em enlaces de transmissão ponto-a-ponto como substituto direto aos cabos de cobre, com as fibras terminando em equipamentos eletrônicos. Vale ressaltar que fibras por si só não formam redes até que elas sejam interconectadas em uma arquitetura devidamente estruturada. Atualmente, as arquiteturas adequadas para redes óticas envolvem complexas combinações de dispositivos óticos e eletrônicos (STERN *et al.*, 2009).

Quando se fala em redes óticas, considera-se duas gerações. Na primeira geração, a fibra ótica foi usada essencialmente para prover capacidade de transmissão. As fibras óticas provêem valores menores de taxa de erro de bits (BER - *Bit Error Rate*) e maiores capacidades de transmissão em relação a cabos metálicos. Todas as funções de chaveamento e outras funções "inteligentes" eram manipuladas pelos dispositivos eletroeletrônicos (RAMASWAMI; SIVARAJAN, 2002). Exemplos da primeira geração das redes óticas são as redes SONET e as redes SDH.

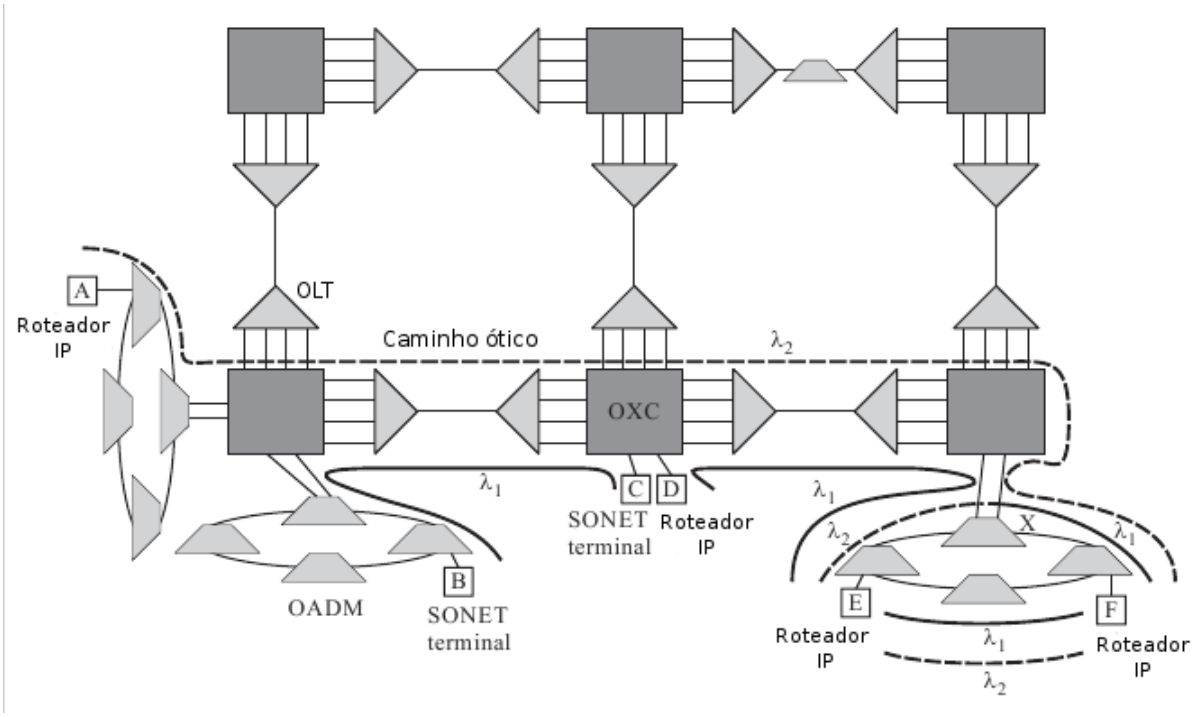
Atualmente presencia-se a implementação da segunda geração das redes óticas, na qual algumas das funções de roteamento, chaveamento e "inteligência" estão se movendo para a camada ótica (RAMASWAMI *et al.*, 2010). Segundo (MUKHERJEE, 2006), o conceito chave em projetar redes de comunicação ótica a fim de explorar a enorme largura de banda das fibras é introduzir concorrência entre múltiplas transmissões dos clientes na arquitetura da rede e nos protocolos. Nas redes de comunicação ótica atuais, essa concorrência é provida de acordo com o seu comprimento de onda ou frequência, utilizando a tecnologia de multiplexação conhecida como WDM.

A tecnologia WDM foi desenvolvida por operadores de redes de telecomunicações do mundo todo, basicamente para comunicação ponto-a-ponto. Nessa tecnologia, o espectro de transmissão ótica é dividido em um número de comprimentos de onda ou bandas de frequência não sobrepostos, com cada comprimento de onda suportando um único canal de comunicação operando numa determinada taxa de transmissão. Desse modo, o WDM permite que múltiplos canais coexistam em uma única fibra (MUKHERJEE, 2006). Desde a década de noventa, a implementação das redes WDM por operadores de redes de comunicação tem aumentado cada vez mais em todo o mundo. A próxima geração da *Internet* está empregando redes óticas baseadas em WDM, conduzindo às redes IP sobre WDM.

As redes óticas são capazes de prover mais funções do que apenas a transmissão ponto-a-ponto. As principais vantagens são os ganhos obtidos pela incorporação de algumas das funções de chaveamento e roteamento, que eram realizadas pelos dispositivos eletroeletrônicos, na parte ótica da rede (RAMASWAMI *et al.*, 2010). Por exemplo, conforme as taxas de transmissão de dados vão ficando cada vez maiores, torna-se mais difícil para os dispositivos eletrônicos processarem os dados. Nas redes óticas de primeira geração, a parte eletrônica de um nó manipula não somente todos os dados destinados a este nó, mas também todos os dados que estão passando através do nó em direção a outros nós na rede. Os dados que estão atravessando um nó podem ser roteados através do domínio ótico, de modo que a carga sobre a camada eletrônica no nó seria significativamente reduzida (RAMASWAMI *et al.*, 2010). Esse é um dos fatores chave para a segunda geração das redes óticas. A arquitetura de uma rede de segunda geração é mostrada na Figura 1. Essa rede é chamada de rede chaveada por comprimento de onda. A rede provê caminhos óticos para seus clientes, que podem ser representados por roteadores IP ou terminais SONET/SDH. Os caminhos óticos são conexões óticas transportadas fim-a-fim de um nó fonte a um nó de destino sobre um comprimento de onda em cada enlace intermediário (RAMASWAMI *et al.*, 2010). Em nós intermediários na rede, os LSPs são roteados e chaveados de um enlace para outro enlace. Em alguns casos, LSPs podem ser convertidos de um comprimento de onda para outro comprimento de onda ao longo da sua rota. Diferentes LSPs em uma rede roteada por comprimento de onda podem usar o mesmo comprimento de onda contanto que não compartilhem qualquer enlace comum. Isso permite o mesmo comprimento de onda ser reusado espacialmente em diferentes partes da rede (RAMASWAMI *et al.*, 2010).

Como visto na Figura 1, os elementos chave que permitem a comunicação ótica em rede são o terminal ótico de linha (OLT), o multiplexador ótico de entrada e derivação (OADM) e a chave ótica (OXC). Um OLT multiplexa múltiplos comprimentos de onda dentro de uma única fibra e demultiplexa um conjunto de comprimentos de onda presentes em uma única fibra, em fibras separadas. OLTs são usados nos fins de um enlace WDM ponto-a-ponto. Um OADM capta sinais em múltiplos comprimentos de onda e seletivamente descarta alguns desses comprimentos de onda localmente enquanto permite que outros passem. Ele também seletivamente adiciona comprimentos de onda para o sinal de saída composto. Um OADM tem duas portas linha em que os sinais WDM compostos estão presentes e um número de portas locais em que comprimentos de onda individuais são descartados e adicionados. Um OXC basicamente realiza uma função similar, mas em escala maior. Um OXC tem um grande número de portas e é capaz de chavear comprimentos de onda de uma porta para outra. Ambos OADMs e OXCs podem incorporar capacidades de conversão de comprimento de onda

Figura 1: Uma rede WDM chaveada por comprimento de onda, mostrando OLTs, OADMs e OXCs.
(RAMASWAMI *et al.*, 2010).



(RAMASWAMI *et al.*, 2010).

Redes óticas baseadas na arquitetura descrita já estão sendo implementadas. OLTs tem sido amplamente implementados por aplicações ponto-a-ponto. OADMs são atualmente usados em redes de longas distâncias e em redes metropolitanas. OXCs estão começando a ser implementados primeiramente em redes de longas distâncias por causa das capacidades maiores nessas redes (RAMASWAMI *et al.*, 2010).

2.3 Redes Óticas Transparentes

O desenvolvimento tecnológico atual tem mostrado que as fibras óticas são ótimos meios para transmissão, porém, o desenvolvimento de *switches* totalmente óticos tem indicado que o chaveamento ótico ainda tem muito a se desenvolver. (MUKHERJEE, 2006). Nas redes óticas a transmissão é feita pelo meio óptico se utilizando de fibras, porém, o chaveamento pode ser ótico, elétrico ou ainda híbrido.

Os avanços tecnológicos recentes na concepção de dispositivos óticos parecem tornar possível, em breve, a construção de redes WDM totalmente óticas (MUKHERJEE, 2006). Em uma rede totalmente ótica a conversão ótica-eletrica-ótica (OEO) não é usada nos nós intermediários de uma conexão, resultando em uma potencial redução de custos para construir a rede.

Como foi visto anteriormente, em uma rede WDM chaveada por comprimento de onda, o tráfego de dados é transportado via um canal ótico chamado *lightpath*, viajando através dos nós da rede interconectados por fibras óticas (MUKHERJEE, 2006).

Em uma rede opaca, a transmissão de dados ocorre sobre enlaces ponto-a-ponto de modo que o sinal é regenerado em cada nó intermediário ao longo de um *lightpath* via conversão OEO. A necessidade por alta capacidade de transporte foi cumprida pela implementação da técnica de WDM. Porém, os custos operacionais desses sistemas ponto-a-ponto podem ser muito altos, principalmente devido a grande quantidade de regeneradores necessários nos nós de uma rede em escala nacional (MUKHERJEE, 2006). O custo pode ser reduzido em uma rede chamada "translucente" (RAMAMURTHY *et al.*, 1999), na qual a funcionalidade de regeneração é empregada somente em alguns nós em vez de em todos os nós da rede. Mas o objetivo final de redução dos dispositivos eletrônicos leva a uma tendência no desenvolvimento de redes óticas totalmente transparentes (WILLNER *et al.*, 2000).

Em uma rede ótica transparente, um sinal que é transmitido permanece no domínio ótico pelo LSP inteiro. Desse modo, a rede transparente pode eliminar as dispendiosas conversões OEO. (MUKHERJEE, 2006).

Dois dos principais objetivos de projeto das redes totalmente óticas são a extensibilidade e a modularidade. Extensibilidade é definida como a propriedade de que mais elementos de rede podem ser sempre adicionados à rede sem que, no entanto, seu desempenho seja prejudicado de maneira proporcional. Modularidade é definida como a propriedade de que apenas um nó necessita ser adicionado de uma vez. Além dessas duas características, as redes totalmente óticas se destinam a suportar um alto grau de reuso de comprimentos de onda. Essa característica permite que comprimentos de onda sejam usados muitas vezes em diferentes lugares por toda a rede de forma que os sinais enviados nos mesmos comprimentos de onda nunca interfiram uns nos outros (MAIER, 2008).

O principal problema com as redes transparentes vem do fato de que a qualidade de um sinal ótico degrada conforme ele viaja através de muitos componentes óticos ao longo do LSP. O tamanho físico de uma rede transparente é determinado principalmente pelos efeitos das deficiências físicas tais como atenuação, ruído, *crosstalk*, dispersão cromática e dispersão de modo de polarização (CD/PMD), efeitos não lineares, ganho e perda dependentes de polarização (PDL/PDG), e assim por diante (TOMKOS, 2002). Um maior detalhamento desses efeitos pode ser encontrado em (FONSECA, 2005). A PMD é abordada em detalhes em (SERGEY; MERRION, 2006). Tais efeitos e características presentes no meio ótico devem ser considerados ao implementar redes totalmente óticas. Devido a essas restrições, a transparência pode ser

alcançada somente em redes de grande porte ou em partes menores dessas redes. Em outras palavras, grandes redes totalmente óticas podem necessitar serem divididas em muitas subredes, em que cada subrede é capaz de prover transparência (MAIER, 2008).

Um LSP pode ser oticamente amplificado, manter seu comprimento de onda atribuído não modificado, ou, alternativamente ter seu comprimento de onda alterado ao longo do caminho. Se cada LSP tiver que ficar em um só comprimento de onda atribuído, é dito que a configuração dos LSPs na rede satisfaz a restrição de continuidade de comprimento de onda. Essa restrição torna mais difícil prover LSPs, levando a um aumento da probabilidade de bloqueio. Para melhorar o desempenho das redes totalmente óticas em relação a probabilidade de bloqueio, os OXCs podem ser equipados com conversores de comprimento de onda adicionais. A capacidade de conversão de comprimento de onda adicionada ajuda a diminuir a probabilidade de bloqueio nas redes totalmente óticas, uma vez que a restrição de continuidade de comprimento de onda pode ser omitida, e adicionam flexibilidade à rede. (MAIER, 2008). Entende-se como flexibilidade a propriedade de se ajustar dinamicamente às mudanças de tráfego e/ou condições da rede a fim de melhorar o seu desempenho. Usando conversores de comprimento de onda sintonizáveis (TWCs), a flexibilidade das redes totalmente óticas pode ser aumentada. Semelhante a conversores de comprimento de onda convencionais, TWCs podem ter uma natureza totalmente ótica ou ótico eletrônica (MAIER, 2008).

Empregando TWCs nos nós intermediários, é possível tornar a rede inteira uma rede reconfigurável. Reconfigurabilidade é uma propriedade das redes que permite o reroteamento e o balanceamento da carga de tráfego em resposta às mudanças no tráfego e/ou falhas na rede (MAIER, 2008).

Redes totalmente óticas reconfiguráveis podem ser usadas para conceber poderosas infraestruturas de telecomunicações, mas também dão origem a alguns novos problemas. Dado o fato de que os elementos da rede são reconfiguráveis, esses elementos tem que encontrar sua configuração ótima sobre um dado cenário de tráfego e prover a melhor política de reconfiguração na presença de mudanças na carga de tráfego, falhas e atualizações na rede (GOLAB; BOUTABA, 2004). Além disso, o gerenciamento e controle de redes totalmente óticas reconfiguráveis é de suma importância a fim de garantir sua adequada e eficiente operação e também para tornar essas redes comercialmente viáveis (WAGNER *et al.*, 1996).

As funções de controle são necessárias para configurar, modificar e derrubar LSPs através da rede ótica por meio da configuração de transmissores sintonizáveis, receptores, conversores de comprimento de onda, OADMs e OXCs reconfiguráveis ao longo do caminho. As funções de gerenciamento são necessárias para monitorar as redes óticas

e garantir sua operação adequada por meio do isolamento e diagnóstico de falhas e disparando mecanismos de recuperação a fim de alcançar uma maior sobrevivência contra falhas nos enlaces e nos nós (MAIER, 2008).

Em redes de comunicação existentes, nas quais cada nó tem acesso a todo o tráfego passante, as informações de controle podem ser transportadas junto com o tráfego regular, o chamado controle *in-band*. Em redes óticas transparentes a situação é completamente diferente já que os nós não intermediários podem ser oticamente ignorados e assim impedidos de acessar os comprimentos de onda correspondentes. Portanto, em redes óticas transparentes um canal de controle separado é tipicamente alocado para transportar informação de controle e gerenciamento (MAIER, 2008). Esse canal é chamado de canal supervisório ótico (OSC). O OSC pode ser usado para distribuir informações de gerenciamento e controle para todos os nós na rede. Esse dispositivo permite o controle centralizado ou distribuído dos elementos de rede reconfiguráveis.

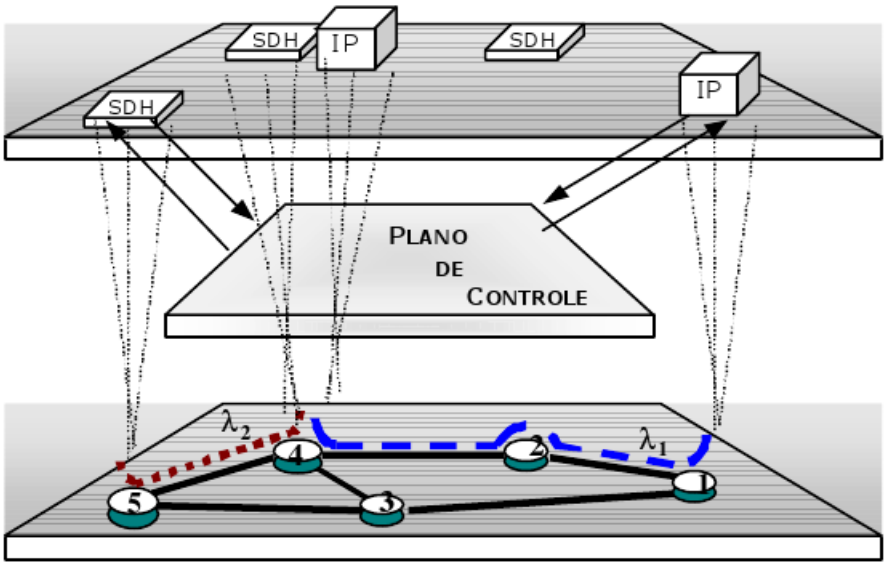
2.4 Redes Clientes

Como já foi dito anteriormente, as redes óticas provêem caminhos óticos para uma variedade de outras redes, chamadas redes clientes. Tradicionalmente, um caminho ótico era caracterizado pelo par (rota, comprimento de onda); entretanto, numa visão com múltiplos clientes distintos, os caminhos óticos em uma rede ótica transparente podem possuir características diferentes dependendo da aplicação e/ou da rede cliente que os está solicitando. Desse modo, além de uma rota e um comprimento de onda, para uma melhor adequação, é necessário que o caminho ótico possua também atributos de QoS associados à sua criação num contexto de rede transparente (FONSECA, 2005). Exemplos de redes clientes que se utilizam das redes óticas como são as redes IP e SONET/SDH.

Para viabilizar o provimento de caminhos óticos que levem em consideração os atributos de QoS peculiares a cada rede cliente, deve existir uma entidade que se encarregue da interconexão entre as redes clientes e a rede ótica (FONSECA, 2005). Tal entidade é denominada plano de controle, A Figura 2.4 ilustra o plano de controle como interface entre a rede ótica e as redes clientes.

Em síntese, o plano de controle é responsável por configurar conexões dinamicamente na rede. O plano de controle das redes óticas será visto em mais detalhes na seção 2.5.

Figura 2: O plano de controle como interface entre a rede ótica e as redes clientes. (FONSECA, 2005).



2.5 Plano de Controle das Redes Óticas

Nas redes óticas atuais, as diferentes técnicas de chaveamento, tais como chaveamento por fibra e chaveamento por comprimento de onda, trabalham no chamado plano de dados das redes óticas. O plano de dados engloba todos os mecanismos e técnicas de chaveamento necessárias para enviar e encaminhar dados da origem ao destino. A fim de trabalhar adequadamente, o plano de dados deve ser gerenciado por um plano de controle (MAIER, 2008). Em termos gerais, o plano de controle é responsável por configurar e fazer com que as técnicas de chaveamento trabalhem de uma maneira coordenada e eficiente na rede ótica. Ele pode ser implementado na camada de acesso ao meio (MAC) da rede ótica a fim de evitar colisões de *frames* de dados em cada canal de comprimento de onda. O plano de controle também pode ser implementado na camada de rede para rotear e estabelecer conexões óticas da origem ao destino (MAIER, 2008).

A idéia de um plano de controle em uma rede ótica introduz vantagens significativas, incluindo o rápido aprovisionamento de conexões, a rápida recuperação em caso de uma falha, e a introdução de engenharia de tráfego para alocar dinamicamente recursos de rede para conexões aprovisionadas visando otimizar o desempenho da rede (STERN *et al.*, 2009). Entre os objetivos da engenharia de tráfego estão, atender os requisitos de QoS, distribuição de fluxos de tráfego para utilizar os recursos da rede de maneira ótima e assegurar que os acordos de nível de serviço sejam satisfeitos (STERN *et al.*, 2009). Para prover uma conexão entre dois nós em uma rede de transporte ótica, uma rota com recursos suficientes para acomodar a conexão tem que ser encontrada

e os nós através dos quais a conexão é estabelecida têm que ser configurados apropriadamente (STERN *et al.*, 2009). Existe um consenso emergente de que o melhor caminho para alcançar isso é adaptar protocolos de plano de controle desenvolvidos para a camada lógica da rede, tais como o MPLS, para o ambiente das redes óticas. Desenvolvido pela IETF, o MPLS basicamente estende conceitos e protocolos das redes IP para ampliar as funcionalidades dessas e de outras redes chaveadas por pacotes. A primeira iniciativa em direção às redes óticas pelo IETF foi dado em 1999 com a criação de uma extensão do MPLS chamado MPλS. (STERN *et al.*, 2009) Esse protocolo foi ampliado para o MPLS generalizado (GMPLS) para dar suporte a dispositivos que realizam chaveamento usando *slots* de tempo, comprimento de onda e espaço (MANNIE, 2004).

Existem três principais funções do plano de controle: descoberta de vizinhos, sinalização e roteamento. A descoberta de vizinhos determina a conectividade dos elementos da rede para todos os seus elementos de rede vizinhos. A sinalização estabelece o caminho para os agentes de controle comunicarem-se entre si para prover e manter conexões fim-a-fim na rede. O roteamento inclui duas funções de controle separadas: a descoberta de topologia e de recursos e o cálculo de rotas. A primeira função envolve a descoberta de todos os recursos na rede e a descoberta da topologia da rede, que é realizada através da troca de informações sobre os recursos disponíveis e a topologia entre os nós e seus agentes de controle (STERN *et al.*, 2009). Uma quarta importante função do plano de controle é o gerenciamento de recursos, que envolve a representação e o acompanhamento dos recursos locais disponíveis para serem usados no cálculo de rotas.

De acordo com (STERN *et al.*, 2009), as funções do plano de controle aqui apresentadas podem ser implementadas usando um dos seguintes paradigmas:

- Controle centralizado: Um controlador central comunica-se com cada elemento da rede que é usado para funções de controle.
- Controle distribuído: Todas as funções do plano de controle são distribuídas entre os elementos da rede individualmente.
- Controle Híbrido: Algumas funções do plano de controle são centralizadas e algumas são distribuídas entre os elementos da rede. Por exemplo, a descoberta de recursos e o cálculo de rotas pode ser implementado de forma centralizada, enquanto o o estabelecimento da rota pode ser implementado de forma distribuída.

A adoção das funções e protocolos de sinalização e roteamento baseadas no protocolo IP tem recebido uma grande atenção da indústria e da academia visando construir

um plano de controle centrado em IP, em que os clientes IP são capazes de dinamicamente configurar, modificar e derrubar LSPs ponto-a-ponto (RAJAGOPALAN *et al.*, 2000). A comunicação em rede envolvendo diferentes camadas entre as redes totalmente óticas e os clientes IP tornou-se o próximo passo na evolução em se projetar redes óticas flexíveis e resilientes, levando as chamadas redes IP/WDM (MAIER, 2008). De acordo com (MAIER, 2008), para tais redes, os seguintes modelos de interconexão foram propostos:

- Modelo Par (*Peer*): No modelo par, redes IP e redes óticas são consideradas uma rede integrada com um plano de controle unificado. Nesse modelo, os elementos de rede, tanto IP, quanto óticos, agem como pares sem qualquer diferença entre eles.

- Modelo Sobreposto (*Overlay*): O modelo sobreposto prevê que redes IP e redes óticas operam independentes umas das outras. Nesse modelo, redes IP e redes óticas executam seus próprios protocolos de roteamento e sinalização, respectivamente. As interfaces entre esses tipos de rede necessitam ser padronizadas.

- Modelo interdominio ou aumentado: Nesse modelo, tanto as redes IP, quanto as redes óticas tem suas próprias instâncias de roteamento, porém as informações de acesso dos roteadores IP geograficamente distribuídos passa pela rede ótica em direção aos clientes IP. Desse modo, o modelo interdomínio pode ser visto como estando entre o modelo par e o modelo sobreposto, com os domínios ótico e eletrônico interagindo até certo ponto.

Várias organizações de padronização e parte da indústria tem trabalhado para padronização de um plano de controle para as redes óticas que permita a interoperabilidade entre redes de múltiplas operadoras e plataformas de diferentes fabricantes (BENJAMIN *et al.*, 2001). Os padrões resultantes permitirão que usuários finais e operadores de rede controlem dinamicamente conexões fim-a-fim através de redes óticas. Os principais atores envolvidos no processo de padronização são a União Internacional de Telecomunicação (ITU-T - *International Telecommunication Union - Telecommunication Standardization Sector*, a já citada IETF e o OIF (*Optical Internetworking Forum*).

3 GMPLS como plano de controle para Redes Óticas

No capítulo 2 viu-se que foi criada uma versão generalizada do protocolo MPLS chamada de GMPLS. Essa suíte de protocolos permite a migração do plano de controle MPLS para redes óticas chaveadas por comprimento de onda (MANNIE, 2004) e também para outros tipos de rede, criando a ideia de um plano de controle unificado (PAPADIMITRIOU *et al.*, 2006). Este capítulo apresenta e descreve como deve funcionar o plano de controle GMPLS para redes óticas.

3.1 Visão geral

A ideia principal por trás do GMPLS é de definir um Plano de Controle comum para diferentes tipos de tecnologias de rede (MAIER, 2008), como mostrado na Figura 3. Em outras palavras, a premissa do GMPLS é que um rótulo pode ser generalizado para ser qualquer coisa que seja suficiente para identificar um fluxo de tráfego (PALMIERI, 2008). Desse modo, o GMPLS suporta rótulos adaptados à tecnologias de rede arbitrárias na camada física (STERN *et al.*, 2009). Por exemplo, para uma rede chaveada por comprimento de onda, o rótulo poderia estar associado ao comprimento de onda, e para uma rede chaveada por fibra os rótulos poderiam ser vinculados a números de portas. Desse modo, a rede passa a ser uma combinação de camadas lógicas, cada uma responsável por trabalhar com uma determinada tecnologia de transporte. A integração destas camadas oferece uma visão unificada da topologia (SANTOS *et al.*, 2009).

Figura 3: Plano de Controle comum para diferentes tipos de redes com chaveamento óptico.
(MAIER, 2008).

O MPLS possui especificações dos planos de controle e de dados, porém, o GMPLS somente se preocupa com o plano de controle. O GMPLS suporta aprovisionamento de canais óticos em tempo real, incluindo roteamento dinâmico, emprega versõees estendidas dos esquemas de sinalização e roteamento desenvolvidos para engenharia

de tráfego no MPLS e suporta gerenciamento de enlace, uma nova função que não foi definida no MPLS (STERN *et al.*, 2009).

3.1.1 Interfaces GMPLS

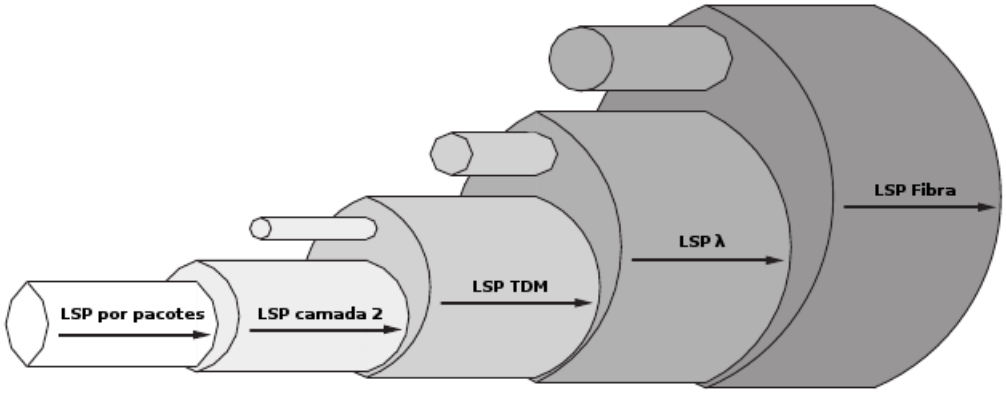
O GMPLS é capaz de operar sobre uma ampla faixa de dispositivos de rede heterogêneos, como roteadores IP/MPLS, elementos de rede SONET/SDH, `switches` ATM, elementos de rede ótica como OXCs e OADMs. Todos esses dispositivos de rede representam roteadores chaveados por rótulos (LSR) que realizam diferentes tipos de chaveamento. Os diferentes tipos de LSRs utilizados nas redes GMPLS podem ser categorizados por sua interface com capacidade de chaveamento (ISC) (MAIER, 2008). De acordo com (MANNIE, 2004), essas interfaces podem ser subdivididas em classes: interfaces capazes de chavear pacotes (**PSC**); interfaces capazes de chavear frames/células (**L2SC**); interfaces capazes de multiplexar por divisão de tempo (**TDMC**); interfaces capazes de chavear comprimentos de onda(lambda)/bandas de frequência (**LSC**); e interfaces capazes de chavear fibras (**FSC**).

É importante notar que, em redes GMPLS, é possível estabelecer um LSP apenas entre e através de interfaces do mesmo tipo. Todavia, LSPs estabelecidos entre pares de elementos de rede com diferentes ISCs podem ser aninhados um dentro do outro dando origem a o que é chamado de Hierarquia de LSPs (MAIER, 2008).

3.1.2 Hieraquia LSP

Uma hierarquia de LSPs pode ser entendida como uma hierarquia de encaminhamento que pode ser construída entre LSRs generalizados com as mesmas interfaces com capacidade de chaveamento (MAIER, 2008). Como mostrado na Figura 4, a hierarquia de LSPs GMPLS é baseada nas diferentes capacidades de chaveamento das interfaces dos LSRs (MAIER, 2008). No topo dessa hierarquia estão os nós que têm interfaces FSC, seguidas por nós que têm interfaces LSC, seguidas por nós que têm interfaces TDMC e seguidas por nós que têm interfaces PSC (PALMIERI, 2008). Como visto, essa hierarquia forma os chamados túneis LSP. Esse princípio de "tunelamento" é válido para todos os domínios GMPLS, em que LSPs de ordem superior podem ser vistos como túneis LSP para LSPs de ordem inferior aninhados (MAIER, 2008). Segundo (PALMIERI, 2008), o aninhamento de LSPs entre tipos de interfaces aumenta a flexibilidade na definição de serviço e torna possível para provedores de serviço operarem uma rede GMPLS para entregar tanto serviços empacotados, quanto serviços não empacotados.

Figura 4: Hierarquia de LSPs do GMPLS.
(IOVANNA *et al.*, 2003).



3.1.3 O rótulo generalizado

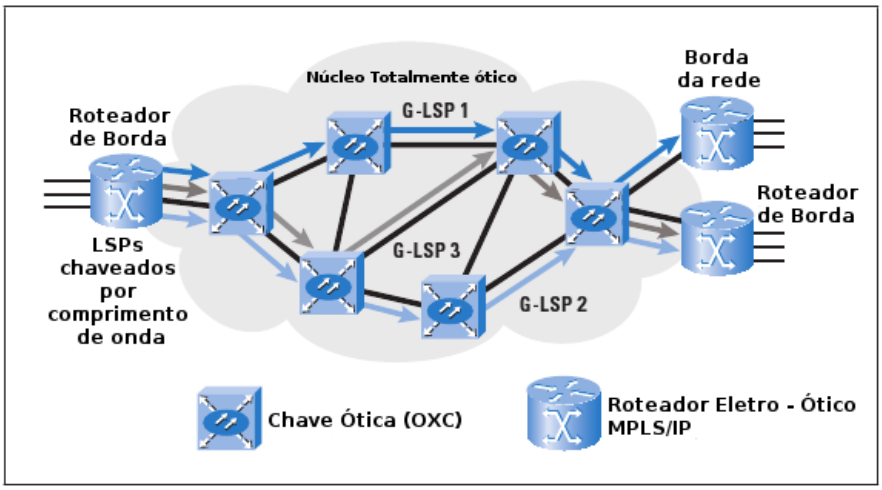
Conforme (PALMIERI, 2008), o GMPLS define muitos novos tipos de rótulo, os chamados objetos de rótulo generalizado. Em geral, esses objetos incluem a requisição de rótulo generalizado, o rótulo generalizado por si só, o controle explícito do rótulo e a *flag* de proteção. Como já falado anteriormente nesse trabalho, os rótulos generalizados podem ser utilizados para representar pacotes, células, divisões de tempo, comprimentos de onda entre outros.

Com o rótulo GMPLS sendo derivado do rótulo MPLS, ele herda algumas características deste e agrega novas características. Para que fosse possível embarcar informações específicas da tecnologia de chaveamento utilizada, (por exemplo, comprimento de onda ou fibras) dentro da estrutura de tráfego de pacotes, novas características foram adicionados a estrutura do rótulo MPLS. Esses rótulos incluem indicadores específicos que representam comprimentos de onda, agrupamentos de fibras, ou portas de fibras e são distribuídos para os nós através de sinalização GMPLS *out-of-band* (PALMIERI, 2008). A sinalização GMPLS *out-of-band* dá origem ao problema de separação do canal de controle. Basicamente, conforme explica (PALMIERI, 2008), no MPLS, a informação de controle é encontrada no rótulo, que é diretamente ligado a carga útil dos dados. Porém, quando se envia a informação de controle *out-of-band*, o rótulo é separado dos dados que se estão tentando controlar. Ainda segundo (PALMIERI, 2008), o GMPLS provê um meio de identificar canais de dados explicitamente. Essa habilidade permite que as mensagens de controle sejam associadas a um determinado fluxo de dados, seja um comprimento de onda, uma fibra ou um agrupamento de fibras. Esse processo de sinalização é mostrado em detalhes posteriormente neste trabalho.

3.1.4 LSPs Generalizados

De acordo com (PALMIERI, 2008) a principal característica dos LSPs no GMPLS que os difere dos LSPs do MPLS é o fato de que no GMPLS um LSP pode ser estabelecido de forma bidirecional. Os requisitos para o LSP bidirecional são os mesmos nos dois sentidos, e é estabelecido para ambas as direções com apenas uma mensagem de sinalização, permitindo reduções no tempo de configuração do LSP. Em um ambiente ótico, um OXC traduz a atribuição de rótulo em uma atribuição de comprimento de onda correspondente e configura um LSP generalizado (G-LSP) usando suas interfaces de controle local com outros dispositivos de chaveamento (PALMIERI, 2008). A Figura 3.1.4 abaixo ilustra alguns G-LSPs em uma rede ótica.

Figura 5: G-LSPs em uma rede ótica.
(PALMIERI, 2008).



Uma outra característica muito útil do empacotamento é a capacidade de manipular múltiplos enlaces vizinhos. O processo de agregação de enlace (que será visto posteriormente) trata o tráfego desses enlaces como um único enlace. Para que enlaces vizinhos sejam agrupados, eles devem ser do mesmo tipo e devem ter os mesmos requisitos de Engenharia de Tráfego. Esses requisitos reduzem a quantidade de anúncios que necessitam ser mantidos na rede, aumentando assim a estensibilidade do plano de controle (PALMIERI, 2008).

3.2 Componentes do GMPLS

O serviço fundamental oferecido pelo plano de controle GMPLS é o aprovisionamento dinâmico de conexões fim-a-fim (PALMIERI, 2008). Para tanto, o GMPLS é dividido em componentes principais que são as funções de gerenciamento de enlace, roteamento, e sinalização.

O gerenciamento de enlace inclui a descoberta de vizinhos e o gerenciamento de mecanismos de sinalização para provimento de conexões e recuperação de falhas. Essas são funções básicas fundamentais a todos os outros aspectos da operação da rede (STERN *et al.*, 2009). O LMP é o protocolo responsável por essas funções e será visto em detalhes posteriormente nesse trabalho.

A função de roteamento engloba a descoberta de recursos, descoberta de topologia, e o cálculo de rotas. Os principais protocolos que comumente são usados para implementar a função de roteamento do GMPLS são o OSPF-TE e o ISIS-TE (*Intermediate System to Intermediate System with Traffic Engineering extensions*) (STERN *et al.*, 2009).

A função de sinalização é usada para o estabelecimento de conexão (aprovisionamento) e recuperação de falhas. O protocolo RSVP-TE é comumente usado para implementar sinalização em GMPLS (STERN *et al.*, 2009).

Essas funções, da forma como foram colocadas, tem uma relação cliente-servidor com a função precedente. A função de sinalização se utiliza da descoberta de topologia e do cálculo de rotas realizados pela função de roteamento para o aprovisionamento de conexões. Por sua vez, a função de roteamento se utiliza das informações da descoberta de vizinhos, realizada pela função de gerenciamento de enlace, para construir uma figura global da rede no momento atual. As funções de roteamento e sinalização são abordadas em detalhes nos Apêndices A e B respectivamente.

3.3 Gerenciamento de Enlace

No contexto do GMPLS, um par de nós pode ser conectado por dezenas de fibras, e cada fibra pode ser usada para transmitir centenas de comprimentos de onda, no caso de uma tecnologia como a DWDM (*Dense Wavelength Division Multiplexing*) seja utilizada. Para permitir a comunicação entre nós para fins de roteamento, sinalização e gerenciamento de enlace, canais de controle devem ser estabelecidos entre os pares de nós (MANNIE, 2004).

Nas redes GMPLS, o plano de controle é separado do plano de dados. Dessa forma, os canais de controle usados para trocar mensagens do plano de controle GMPLS existem independente dos enlaces que eles gerenciam. O LMP é o meio usado no GMPLS para implementar descoberta de vizinhos, gerenciamento do canal de controle, agrupamento de enlaces e isolamento de falhas. Este protocolo foi especificado para estabelecer e manter os canais de controle *in-band* ou *out-of-band* entre nós vizinhos e para gerenciar os enlaces de dados com engenharia de tráfego entre eles (MAIER, 2008). É importante salientar que em uma rede ótica transparente, somente o controle *out-of-band* é possível (STERN *et al.*, 2009).

Como dito anteriormente, as principais funções do LMP no GMPLS envolvem a determinação de conectividade entre nós através de um procedimento de descoberta de vizinhos e a implementação desse procedimento junto com suas funções relacionadas. Para que seja possível a identificação de um elemento de rede vizinho, o LMP implementa mensagens *Hello* de configuração e de manutenção do canal de controle. O monitoramento do canal de controle é realizado pela troca de mensagens *Hello* em um intervalo de tempo especificado para assegurar que a sessão LMP esteja operacional (STERN *et al.*, 2009).

Um outro importante conceito no LMP é o agrupamento de enlaces. O agrupamento de enlaces é uma técnica usada para combinar muitos enlaces paralelos que tenham as mesmas propriedades para propósitos de roteamento dentro de um grupo lógico único chamado "*link TE*", juntando um par de nós vizinhos. Isso é importante para simplificar a troca de informações em protocolos de roteamento quando um grande número de enlaces estão envolvidos (STERN *et al.*, 2009).

O agrupamento minimiza a quantidade de informação que é trocada na rede pelo protocolo de roteamento, por anunciar somente o *link TE* agrupado como uma representação de todos os enlaces que o compõem. Como apenas o *link TE* é anunciado, um método para identificar os enlaces componentes desse agrupamento é ainda necessário para propósitos de roteamento. Isso é feito no LMP via uma verificação no enlace e um mecanismo de sumarização das informações do enlace (STERN *et al.*, 2009). O processo de verificação de enlace utiliza um mapeamento de identificadores (ID) em ambos os fins de um enlace componente para determinar qual será usado para um dado LSP. Também é usado para verificar a conectividade física dos enlaces componentes. O processo de sumarização de enlace agrupa os IDs em cada fim de componentes individuais para criar um ID do *link TE*. Ele também correlaciona as propriedades do enlace entre elementos de rede vizinhos (STERN *et al.*, 2009).

De acordo com (MAIER, 2008), o LMP é projetado para completar quatro tarefas: (1) Gerenciamento do canal de controle, (2) Correlação de propriedade de enlace, (3) Verificação de conectividade do enlace, e (4) Gerenciamento de falha. Em redes GMPLS, as tarefas de gerenciamento do canal de controle e correlação de propriedade do enlace são obrigatórias no LMP, enquanto que a verificação de conectividade do enlace e o gerenciamento de falha são opcionais (MANNIE, 2004). A seguir, uma breve descrição de cada uma dessas funções:

- **Gerenciamento do canal de controle**

  Um canal de controle entre dois nós vizinhos é um par de interfaces mutuamente alcançáveis que são usadas para permitir a comunicação entre esses nós. Um canal de controle pode ser um comprimento de onda ou fibra separados, um

enlace *Ethernet*, ou um túnel IP através de uma rede de gerenciamento separada (MAIER, 2008). Canais de controle existem independentemente de *links TE*, e podem ser usados para trocar informações do Plano de Controle GMPLS tais como informações de sinalização, roteamento, e de gerenciamento de enlace (MANNIE, 2004).

São usadas quatro mensagens LMP para o estabelecimento e manutenção do canal de controle, as mensagens *Config*, *ConfigAck*, *ConfigNack* e a mensagem *Hello*.

No LMP, um ou mais canais de controle podem ser ativados entre dois nós. Uma vizinhança ou adjacência LMP é formada entre dois nós que suportem as mesmas capacidades. Um canal de controle pode ser configurado explicitamente ou de forma manual ou selecionado automaticamente. Atualmente o LMP assume que os canais de controle são estabelecidos automaticamente, enquanto a configuração das capacidades do canal de controle pode ser dinamicamente negociada (MANNIE, 2004).

A ativação do canal de controle começa com uma troca para negociação de parâmetros, usando mensagens *Config*, *ConfigAck* e *ConfigNack*. As mensagens são construídas com os parâmetros do LMP, que podem ser negociáveis ou não (essa característica é identificada pelo *bit* N no cabeçalho do objeto). Os parâmetros negociáveis podem ser inseridos para que vizinhos LMP concordem com determinados valores. Os não-negociáveis são usados para o anúncio dos valores específicos que não precisam ou não permitem negociação (ÁRTICO, 2011).

Logo que o canal de controle for ativado entre dois nós, o protocolo *Hello* será usado para manter a conectividade do canal e detectar falhas rapidamente, enviando mensagens *Hello* (ÁRTICO, 2011).

- **Correlação de propriedade de enlace**

  Quando agrupamentos de enlaces ocorrem, o plano de controle GMPLS necessita de uma maneira para verificar que todos os requisitos de Engenharia de Tráfego são similares entre enlaces ou nós vizinhos (PALMIERI, 2008). No LMP, a troca de correlação de propriedade de enlace é usada para agregar múltiplos enlaces transportando dados, e trocar, correlacionar, ou mudar parâmetros de *links TE* (MANNIE, 2004). Isso permite a adição de enlaces componentes para um agrupamento de enlaces, mudar a largura de banda reservável de um enlace, mudar de identificadores de porta, ou mudar de identificadores de componentes em um agrupamento (MANNIE, 2004). Em suma, a correlação de propriedade de enlace faz uso de uma troca de mensagens entre dois nós vizinhos e é definida por *links TE* para assegurar que ambos os fins (local e remoto) de um dado *link TE* sejam do mesmo tipo (MAIER, 2008).

- **Verificação de conectividade de enlace**

  Como já foi citado, a verificação de conectividade de enlace é um procedimento opcional que pode ser usado para verificar a conectividade física de enlaces transportando dados, assim como identificar os enlaces que são usados na sinalização GMPLS (MANNIE, 2004).

  O procedimento de verificação consiste de enviar mensagens de teste *in-band* sobre os enlaces transportando dados (MAIER, 2008). É importante notar que a mensagem de teste é a única mensagem LMP que é transmitida sobre o enlace transportando dados e que mensagens *Hello* continuam sendo trocadas no canal de controle durante o processo de verificação de enlace (MANNIE, 2004). No LMP, enlaces de transporte de dados são testados na direção de transmissão como se fossem unidirecionais. Dessa forma, no LMP, é possível que nós vizinhos troquem mensagens de teste simultaneamente em ambas as direções (MANNIE, 2004).

  O processo de verificação inicia com um nó notificando um nó vizinho de que irá iniciar enviando uma mensagem de teste através de um determinado enlace de dados, ou através de enlaces componentes de um determinado agrupamento (MANNIE, 2004). No último caso, os identificadores de enlaces agrupados, local e remoto, são transmitidos ao mesmo tempo para realizar a associação do enlace componente com os seus identificadores de enlace agrupado (MANNIE, 2004).

- **Gerenciamento de Falhas**

  Todas as redes de comunicação estão sujeitas a falhas, as quais podem impedir sua operação e funcionamento. Em redes óticas elas podem ocorrer em enlaces, elementos de comutação ou mesmo nos canais de controle (SANTOS *et al.*, 2009).

  O gerenciamento de falhas permite que a rede "sobreviva" a falhas em nós e enlaces (MAIER, 2008). Esse tipo de gerenciamento é um importante requisito do ponto de vista operacional. Ele inclui normalmente: detecção, localização, e notificação de falhas. A detecção de falhas deve ser manipulada na camada mais próxima da falha. Em redes totalmente óticas, essa é a camada ótica, onde a detecção de falha pode ser realizada, por exemplo, por meio de medidas de perda de luz (MAIER, 2008). Quando uma falha ocorre e é detectada, um operador necessita saber onde aconteceu e um nó fonte pode necessitar ser notificado a fim de realizar algumas ações (MANNIE, 2004).

  Vale salientar que a localização de falhas pode também ser usada para dar suporte a alguns mecanismos locais de proteção/restauração (MANNIE, 2004).

  O isolamento da falha é particularmente importante e mais difícil no caso das redes transparentes. Nessas redes a falha se propaga de volta à origem da trans-

missão através de múltiplos nós, assim sendo, não é uma tarefa fácil isolar sua localização (STERN *et al.*, 2009).

No LMP, para localizar uma falha entre dois nós vizinhos em um enlace TE, o nó que detectou a falha informa seu nó vizinho sobre a falha, enviando uma mensagem de controle à frente. Quando o nó localizado à frente recebe a notificação da falha, ele correlaciona a falha à interface correspondente para determinar se a falha é entre os dois nós vizinhos (MAIER, 2008).

Os estados e a lógica de operação de um canal de controle LMP são definidos por uma máquina de estados finitos (MEF) (LANG, 2005). Conforme (LANG, 2005) um canal de controle LMP pode assumir um dos estados descritos abaixo:

- *Down*: Esse é o estado inicial do canal de controle. Nesse estado nenhuma mensagem LMP está sendo enviada e não está sendo feita nenhuma tentativa de ativar o canal de controle. Normalmente nesse estado configura-se os parâmetros iniciais de forma manual.
- *ConfSnd*: Nesse estado o canal de controle está realizando negociação de parâmetros. O nó fica enviando periodicamente uma mensagem *config* e esperando o seu vizinho responder ou com uma mensagem *configAck* ou com uma mensagem *configNack*.
- *ConfRcv*: Nesse estado o canal de controle está realizando negociação de parâmetros. O nó está aguardando parâmetros de configuração aceitáveis do nó remoto.
- *Active*: Nesse estado o nó envia periodicamente uma mensagem *Hello* e fica esperando para receber uma mensagem *Hello* válida.
- *Up*: O canal de controle está em estado operacional. O nó envia e recebe mensagens *Hello* válidas.
- *GoingDown*: Um canal de controle pode ir para esse estado por causa de uma ação administrativa.

Como é possível notar, cada estado corresponde a uma certa condição do canal de controle e é normalmente associado a um tipo de mensagem LMP específica que é periodicamente transmitida para um nó vizinho.

Assim como os estados do canal de controle, a lógica de operação desse canal também é descrita na forma de máquina de estados finitos e eventos. Eventos do

canal de controle são gerados por protocolos de mais baixo nível e módulos de software, também por rotinas de processamento de pacotes e máquinas de estados finitos de *links TE* associados (LANG, 2005). Cada evento tem um número correspondente e um nome simbólico. No LMP existem 17 eventos possíveis, são eles: (1) evBringUp, (2) evCCDn, (3) evConfDone, (4) evConfErr, (5) evNewConfOK, (6) evNewConferr, (7) evContenWin, (8) evContenLost, (9) evAdminDown, (10) evNbrGoesDn, (11) evHelloRcvd, (12) evHoldTimer, (13) evSeqNumErr, (14) evReconfig, (15) evConfRet, (16) evHelloRet e (17) evDownTimer. As descrições detalhadas de cada evento e das máquinas de estado podem ser vistas em (LANG, 2005).

No LMP existem 20 tipos de mensagens e cada tipo tem um número correspondente de 1 a 20. Essas mensagens são mostradas na Tabela 1.

Número da mensagem	**Tipo da mensagem**
1	*Config*
2	*ConfigAck*
3	*ConfigNack*
4	*Hello*
5	*BeginVerify*
6	*BeginVerifyAck*
7	*BeginVerifyNack*
8	*EndVerify*
9	*EndVerifyAck*
10	*Test*
11	*TestStatusSucess*
12	*TestStatusFailure*
13	*TestStatusAck*
14	*LinkSummary*
15	*LinkSummaryAck*
16	*LinkSummaryNack*
17	*ChannelStatus*
18	*ChannelStatusAck*
19	*ChannelStatusRequest*
20	*ChannelStatusResponse*

Tabela 1: Tipos de mensagens do LMP

No capítulo 4, é feita uma descrição mais detalhada das mensagens LMP responsáveis pelo gerenciamento do canal de controle.

3.4 Considerações

Uma nova classe de dispositivos versáteis de chaveamento ótico endereçáveis por IP está surgindo, operando em conformidade com um plano de controle comum baseado em GMPLS para suportar muitos recursos de Engenharia de Tráfego em modernas infraestruturas óticas transparentes (PALMIERI, 2008).

Um plano de controle padronizado para essas redes óticas é essencial para prover o aprovisionamento de conexões e a recuperação de falhas automatizados em um ambiente que em geral é multi-domínio e com equipamentos de múltiplos fabricantes (STERN *et al.*, 2009). O GMPLS tem um grande potencial para reduzir significativamente os custos dessas redes (MAIER, 2008).

A principal vantagem do GMPLS é o fato de ele ser baseado em protocolos já existentes e amplamente implementados, ao passo que simplificam o gerenciamento da rede e as tarefas ligadas à Engenharia de Tráfego, que podem ser realizadas de uma maneira única em ambos os domínios, ótico e de dados. Além do mais, o GMPLS oferece um arcabouço de funções que podem acomodar futuras expectativas em relação a maneira como as redes trabalharão no futuro e a maneira como os serviços serão providos aos clientes. É inevitável a tendência de um plano de controle GMPLS unificado, onde todos os elementos de rede trabalham como pares para estabelecer caminhos óticos automaticamente através da rede (PALMIERI, 2008). Porém, o plano de controle padronizado é ainda um trabalho em progresso dentro de várias organizações industriais e corpos de padronização (STERN *et al.*, 2009).

4 Testes e Resultados

No Capítulo 2, foi visto que a implementação de um plano de controle visa permitir a migração do planejamento e configuração manuais de rede para redes de transporte automatizadas. Atualmente, as implementações do plano de controle de redes óticas são baseadas principalmente na suíte de protocolos definida sobre a arquitetura do GMPLS (MUNOZ *et al.*, 2009).

No Capítulo 3, mostrou-se que o GMPLS permite a migração do plano de controle MPLS para redes óticas chaveadas por comprimento de onda (MANNIE, 2004) e também para outros tipos de rede, criando a idéia de um plano de controle unificado.

As funções de gerenciamento de enlace do GMPLS incluem a descoberta de vizinhos e o gerenciamento de mecanismos de sinalização para provimento de conexões e recuperação de falhas. Essas são funções básicas fundamentais a todos os outros aspectos da operação da rede (STERN *et al.*, 2009). O padrão LMP, como protocolo automatizado de descoberta de vizinhos, permite a rede criar e manter bancos de dados de estados das portas e conexões, e da topologia, com o objetivo de realizar descoberta e atribuição de nós-portas entre nós vizinhos. Após o LMP ser executado e as associações de nós-portas serem verificadas, a topologia de rede pode ser criada automaticamente por um sistema de gerenciamento centralizado ou de forma distribuída (ELLINAS *et al.*, 2004).

O LMP é executado entre nós vizinhos e foi projetado para prover quatro funções básicas para o par de nós: gerenciamento do canal de controle, verificação de conectividade de enlace, correlação de propriedade do enlace e isolamento de falhas (LANG, 2005). Um requisito para o LMP é que cada enlace tenha associado a ele um canal de controle bi-direcional.

Em uma rede ótica transparente, somente o controle *out-of-band* é possível (Separação do plano de controle do plano de transporte). Nas redes óticas GMPLS transparentes, em função dessa separação dos planos de controle e transporte, os canais de controle usados para trocar mensagens do plano de controle GMPLS existem independente dos enlaces que eles gerenciam.

Na implementação realizada, a separação do plano de controle do plano de transporte é feita em cada dispositivo de chaveamento ótico através da escolha de um número fixo de portas destinadas a canais de controle, e o restante das portas destinadas a transmissão dos dados. Para que seja feito o processo de estabelecimento dos canais de controle, considera-se que já foi configurado um circuito físico ou lógico entre o nó e seus vizinhos. Cada nó já tem configurado os identificadores locais das

portas destinadas tanto para controle como à transmissão de dados, além de outros parâmetros iniciais como a largura de banda e os comprimentos de onda disponíveis para transmissão. Dessa forma essas informações ficam à disposição do protocolo LMP executando em cada nó.

O LMP requer que os endereços dos canais de controle sejam configurados em cada nó. Além dos endereços dos nós e das portas pertencentes a estes, os parâmetros de configuração e Engenharia de Tráfego, tais como largura de banda e comprimentos de onda também devem ser configurados. Em geral essa configuração é feita manualmente e pode demorar dias, dependendo do tamanho da rede. É possível ter mais de um canal de controle entre um par de nós vizinhos, contudo, para que seja estabelecida uma adjacência LMP, no mínimo um canal de controle precisa estar ativo. O estabelecimento desses canais de controle é feito através da troca de mensagens LMP entre os nós. O formato detalhado e conteúdo de todas as mensagens LMP estão descritas em (LANG, 2005).

São usadas quatro mensagens LMP para o estabelecimento e manutenção do canal de controle, as mensagens *Config*, *ConfigAck*, *ConfigNack* e a mensagem *Hello*. Essas mensagens são detalhadas na subseção 4.1.

4.1 As mensagens LMP

Em (LANG, 2005), é definido que as mensagens LMP são transportadas usando o Protocolo de Datagrama do usuário (UDP - *User Datagram Protocol*) e o protocolo utiliza a porta 701. Além dos cabeçalhos padrão do UDP e do protocolo IP, as mensagens LMP tem um cabeçalho comum que segue o formato apresentado na Figura 6.

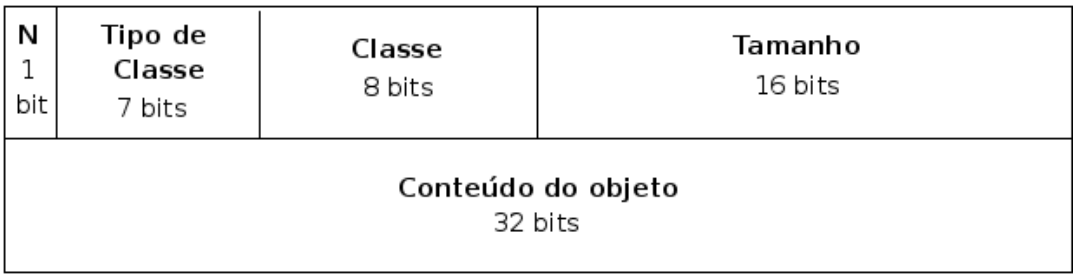
Figura 6: Cabeçalho comum LMP.
Adaptado de (LANG, 2005).

Versão 4 bits	**(Reservado)** 12 bits	***Flags*** 8 bits	**Tipo de mensagem** 8 bits
Tamanho da mensagem 16 bits		**(Reservado)** 16 bits	

As mensagens LMP são construídas usando objetos. Cada objeto tem um nome e também é identificado por sua classe e pelo tipo da sua classe. Os objetos LMP podem ser negociáveis ou não negociáveis. Objetos negociáveis podem ser usados para que os dispositivos de rede negociem sobre determinados valores de parâmetros. Por sua vez, objetos não negociáveis são usados para o anúncio de valores específicos que podem ou

não permitirem negociação (LANG, 2005). A Figura 7 mostra o formato de um objeto LMP e o tamanho de cada campo que o constitui em *bits*.

Figura 7: Formato do objeto LMP.
Adaptado de (LANG, 2005).



Tendo em vista que o objetivo deste trabalho é implementar e avaliar as funções propostas que auxiliam no estabelecimento e manutenção do canal de controle, apenas as mensagens relativas a negociação de parâmetros e gerenciamento do canal de controle foram implementadas. São elas, a mensagem *Config* (Tipo de mensagem = 1), a mensagem *ConfigAck* (Tipo de mensagem = 2), a mensagem *ConfigNack* (Tipo de mensagem = 3) e a mensagem *Hello* (Tipo de mensagem = 4). Segue uma breve descrição dessas mensagens, mostrando quais objetos LMP as compõem:

- Mensagem *Config*

  A mensagem *Config* é usada na fase de negociação do LMP. Essa mensagem é composta de objetos LMP de acordo com o seguinte formato:

  Mensagem *Config* ::= <Cabeçalho comum> <LOCAL_CCID>
  <ID_mensagem> <LOCAL_NO_ID> <CONFIG>

- Mensagem *ConfigAck*

  A mensagem *ConfigAck* é usada para aceitar a recepção da mensagem *Config* e indicar o acordo sobre todos os parâmetros. O formato dessa mensagem é mostrado abaixo:

  Mensagem *ConfigAck* ::= <Cabeçalho comum> <LOCAL_CCID>
  <LOCAL_NO_ID> <CCID remoto> <Mensagem_ID_ACK>
  <ID_NO_REMOTO>

  Os conteúdos dos objetos CCID remoto, Mensagem_ID_ACK e ID_NO_REMOTO devem ser obtidos da mensagem *Config* que está sendo aceita.

- Mensagem *ConfigNack*

  A mensagem *ConfigNack* é usada para aceitar a recepção da mensagen *Config* e indicar desacordo sobre parâmetros não negociáveis ou para propor outros valores para parêmetros negociáveis. O formato dessa mensagem é apresentado a seguir:

  Mensagem *ConfigNack* ::= <Cabeçalho comum> <LOCAL_CCID> <LOCAL_NO_ID> <CCID remoto> <Mensagem_ID_ACK> <ID_NO_REMOTO> <CONFIG>

  Os conteúdos dos objetos CCID remoto, Mensagem_ID_ACK e ID_NO_REMOTO devem ser obtidos da mensagem *Config* que está sendo negativamente aceita.

- Mensagem *Hello*

  A mensagem *Hello* é usada para a manutenção do canal de controle. O formato da mensagem *Hello* é mostrado abaixo:

  Mensagem *Hello* ::= <Cabeçalho comum> <LOCAL_CCID> <Hello>

Como pode ser visto, segundo a RFC 4204 (LANG, 2005), sem levar em conta os cabeçalhos UDP e IP, o tamanho da mensagem *Config* é de no máximo 40 *Bytes*. O tamanho da mensagem *ConfigAck* é de no máximo 48 *Bytes*. A mensagem *ConfigNack* tem o tamanho máximo de 56 *Bytes* e a mensagem *Hello* tem o tamanho máximo de 24 *Bytes*.

4.2 Algoritmo Implementado

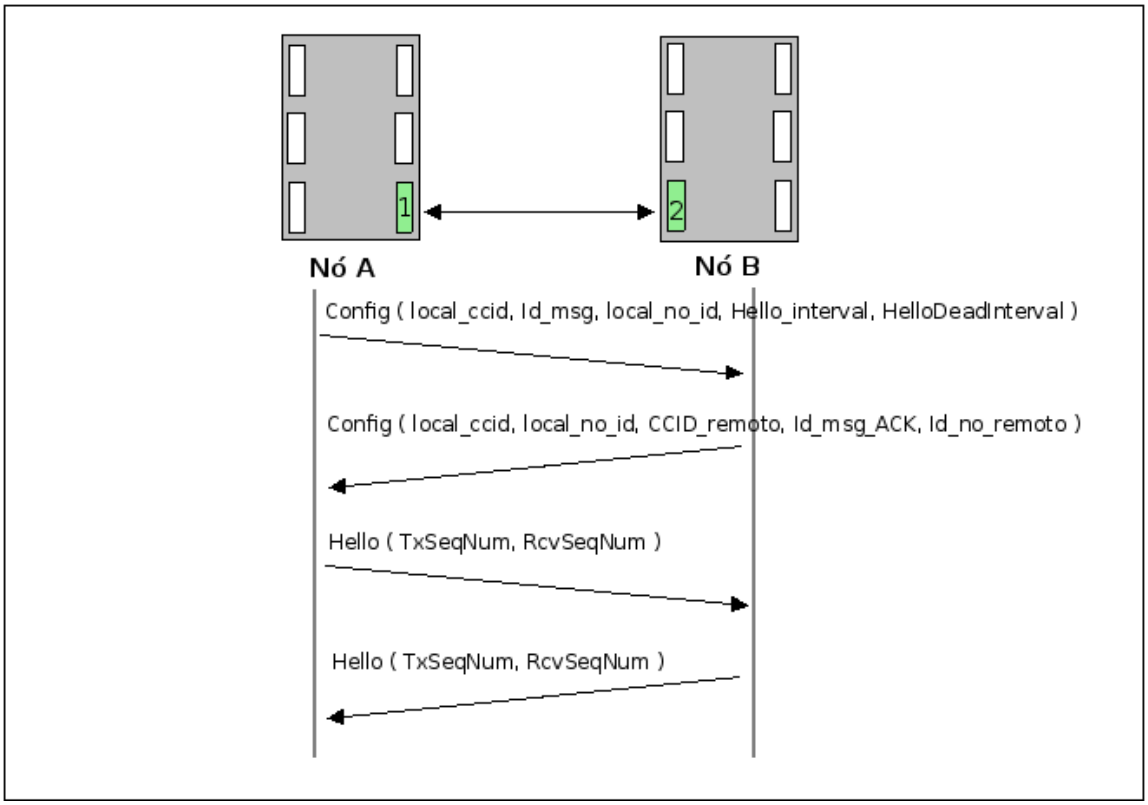
Como visto anteriormente, a ativação do canal de controle começa com uma troca para negociação de parâmetros, usando mensagens *Config*, *ConfigAck* e *ConfigNack*. As mensagens são construídas com os parâmetros do LMP, que podem ser negociáveis ou não. Os parâmetros negociáveis podem ser inseridos para que vizinhos LMP concordem com determinados valores. Os não-negociáveis são usados para o anúncio dos valores específicos que não precisam ou não permitem negociação.

O procedimento corrente de descoberta de vizinhos adotado no LMP padrão requer uma considerável quantidade de intervenção manual e não é aplicável a comutadores totalmente óticos transparentes. A adaptação de protocolos de descoberta para comutadores transparentes ainda é uma tarefa complexa, primariamente devido a implementação limitada desses comutadores em redes operacionais.

Uma vez que um canal de controle foi configurado entre dois nós vizinhos, um protocolo *Hello* será usado para estabelecer e manter a conectividade entre os nós e para detectar falhas no enlace. O protocolo *Hello* consiste de duas fases: uma fase de negociação e uma fase de manutenção do canal de controle, chamada *keep-alive*. A fase de negociação só é iniciada quando o enlace está no estado ***down***, e é usada para trocar identificadores de Canal de Controle (CCIds) e acordar os parâmetros usados na fase de manutenção. A fase de manutenção consiste em uma rápida e leve troca de mensagens pertencentes ao protocolo *Hello* (LANG, 2005).

A troca de mensagens durante o processo de estabelecimento do canal de controle no LMP pode vista na Figura 8.

Figura 8: Troca de mensagens para o estabelecimento do canal de controle LMP.



No presente trabalho foram implementadas duas versões do LMP. Na primeira versão proposta, denominada LMP-e, as mensagens padrão LMP foram modificadas e passaram a usar os seguintes parâmetros na fase de negociação: os CCids locais, o *HelloInterval*, o *HelloDeadInterval*, o comprimento de onda a ser utilizado no canal de controle e um identificador da porta local (LPId). Foi incluído também um parâmetro de Engenharia de tráfego, tal como uma característica inerente a fibra. O endereço do nó na rede é enviado junto com cada mensagem. O parâmetro *HelloInterval* indica a frequência com que mensagens LMP *Hello* devem ser enviadas e é medido em milisegundos. O *HelloDeadInterval* indica quanto um dispositivo deve esperar para

receber uma mensagem *Hello* antes de declarar um canal de controle como "morto". Esse parâmetro também é medido em milisegundos. Os parâmetros dessa fase são estabelecidos usando três mensagens: uma mensagem *HelloConfig*, uma mensagem *HelloConfigAck* e uma mensagem *HelloConfigNack* (LANG, 2005). Além de acrescentar parâmetros inexistentes nas mensagens padrão LMP, na implementação do LMP-e, não foram respeitadas os tamanhos dos campos com os parâmetros nas mensagens e por conseguinte o tamanho das mensagens também não foi restrito. Nessa versão do LMP, o cabeçalho comum LMP e os cabeçalhos dos objetos também não foram implementados e o tamanho das mensagens *Config, ConfigAck, ConfigNack* e *Hello* implementadas foi modificado com a inclusão dos parâmetros já anteriomente citados.

Na segunda versão do LMP desenvolvida, denominada LMP-strict, as quatro mensagens responsáveis pelo gerenciamento do canal de controle foram implementadas seguindo estritamente os tamanhos recomendados em (LANG, 2005). O cabeçalho comum LMP e todos os objetos componentes das mensagens incluindo seus cabeçalhos foram implementados seguindo a recomendação. Nessa versão, os parâmetros comprimento de onda a ser utilizado no canal de controle e identificador de porta local não estão presentes nas mensagens e são disponibilizados apenas pela função que reúne as informações do nó na forma de uma matriz de tráfego/estado dos enlaces. Já o endereço do nó na rede além de disponibilizado por essa função, também é enviado junto com cada mensagem no cabeçalho UDP que encapsula a mensagem LMP.

Um dos principais objetivos de comparar as duas abordagens é para identificar se os parâmetros do nó passados nas mensagens no LMP-e aumentam o *overhead* de controle de forma significativa para interferir no tempo de estabelecimento dos canais de controle em relação ao LMP-strict.

O algoritmo para a troca de mensagens usado nas duas abordagens do protocolo foi o mesmo e pode ser descrito da seguinte forma: para iniciar o processo de negociação, um nó que está num estado **down** envia uma mensagem *HelloConfig* contendo o CCId para o canal de controle, o seu endereço de rede, o identificador da porta local e os parâmetros *HelloInterval* e *HelloDeadInterval* propostos. No caso do LMP-strict a mensagem *HelloConfig* poderá também conter informações de Engenharia de tráfego e Qos, como largura de banda do canal e a PMD da fibra. O nó também inicia um *timer* local que é usado para retransmissões no caso de mensagens perdidas. Quando uma mensagem *HelloConfig* é recebida em um nó, uma mensagem *HelloConfigAck* será transmitida se os valores de *HelloInterval* e *HelloDeadInterval* forem aceitáveis. Caso contrário, o nó rejeitará os parâmetros enviando uma mensagem *HelloConfigNack*. Essa mensagem deverá ser usada para notificar o nó remoto sobre quais valores são aceitáveis para os parâmetros negociados. Quando um nó enviou ou recebeu uma mensagem *HelloConfigAck*, ele pode começar a enviar mensagens *Hello* (fase *keep-alive*). Uma vez

que ambos os nós tenham enviado e recebido uma mensagem *Hello*, o enlace passa a estar no estado **up**. Após o estabelecimento dos canais de controle, o nó montará um banco de dados que contém as informações de quais vizinhos o nó mantém conexão, quais as portas ligadas a quais portas desses vizinhos, os comprimentos de onda utilizados nessas ligações e as informações de Engenharia de tráfego e Qualidade de Serviço. A união dos vários bancos de dados dos nós deve gerar um mapa do estado atual da topologia da rede, isso pode ser feito por uma entidade de controle centralizada, ou de forma distribuída, quando do estabelecimento de conexões pelas camadas de protocolo superiores no GMPLS.

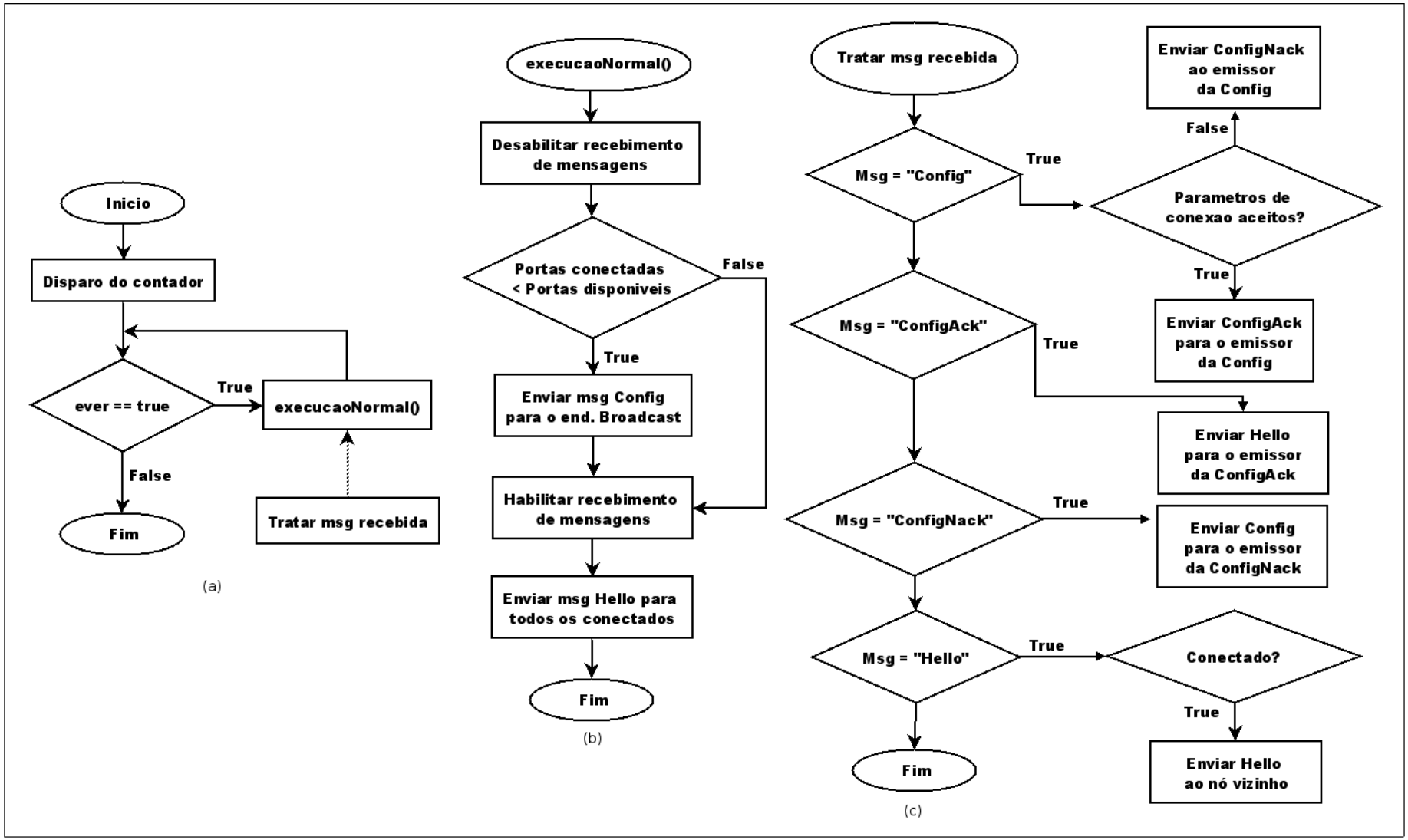
Como parte do LMP, visando atender a função de correlação de propriedades de enlace, deve-se usar as mensagens *LinkSummary*, *LinkSummaryAck* e *LinkSummaryNack*. Essas mensagens devem ser transmitidas a fim de ajustar certos parêmetros do enlace. Por exemplo, adicionar canais de transporte para um enlace, mudar um identificador de canal de transporte (*Bearer Channel identifier* (BCid)) ou mudar o mecanismo de proteção de um canal. No algoritmo proposto, essa mensagem poderia servir também para informar a um enlace vizinho mudanças nos requisitos de Engenharia de Tráfego e QoS. Essas mensagens podem ser trocadas a qualquer hora desde que o enlace esteja no estado *up* e não esteja no processo de verificação de enlace (LANG, 2005). Neste trabalho essas mensagens não foram implementadas. Somente o estabelecimento das conexões e a criação do mapa da rede é considerado.

O algoritmo básico, a função principal de execução e a função de tratamento do recebimento das mensagens do protocolo LMP desenvolvidas neste trabalho podem ser representados pelo fluxograma na Figura 9.

O algoritmo possui duas funções principais. A função mostrada na Figura 9(b) é responsável pela manutenção das conexões já ativas, ou seja, o envio de mensagens LMP *Hello* em tempos já acordados no ato da conexão dos nós, definido no *HelloInterval*. Também é responsável pelo envio de mensagens LMP *Config* ao endereço de *broadcast* da rede, a fim de descobrir novos vizinhos. A segunda função trata as mensagens recebidas, como podemos ver na Figura 9(c).

Quando uma mensagem é recebida por um nó ela é analisada pela função, dependendo de seu tipo, ela serve ou para estabelecer uma conexão nova, ou para confirmar que uma conexão ainda está ativa. Para que uma conexão seja estabelecida, alguns parâmetros devem ser acordados entre os nós. Além dos parâmetros referentes aos intervalos de tempo, presentes nas duas versões do LMP, na primeira versão também podem ser negociados os parâmetros relacionados a aspectos físicos como comprimento de onda e características da fibra e, alternativamente, relacionados a QoS como largura de banda disponível, entre outros.

Figura 9: Algoritmo Básico e funções detalhadas.



Caso ambos os nós aceitem os parâmetros negociados, eles se conectam e passam a trocar mensagens LMP *Hello* para manutenção do canal de controle. Caso os parâmetros não sejam aceitos, novas mensagens são trocadas buscando uma configuração que satisfaça a necessidade de ambos os nós. Caso os nós não possuam as características necessárias naquele momento, a conexão é recusada.

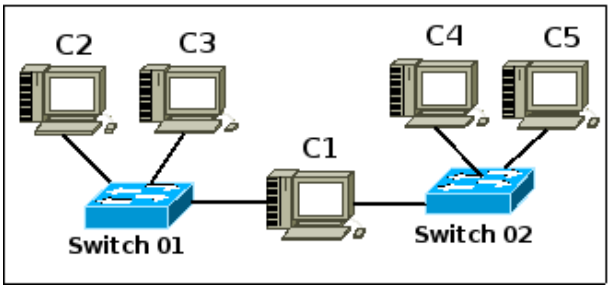
Uma terceira função proposta e implementada em ambas as abordagens do protocolo desenvolvido faz a atualização e armazenamento dos dados dos nós na forma de uma matriz de tráfego com uma maior riqueza de parâmetros tais como o identificador da porta que o nó está utilizando, o estado do canal de controle de acordo com os estados possíveis no LMP, o comprimento de onda utilizado e o endereço do nó vizinho a que o nó local está conectado. O conjunto dessas informações de cada nó na rede pode ser utilizado para o cálculo e atribuição de rotas/comprimentos de onda pelo Algoritmo de RWA. A manutenção desses dados sempre atualizados, pode diminuir a necessidade de anúncios (*flooding*) por parte de protocolos de roteamento enlace-estado como o OSPF-TE que se utiliza desse recurso. Dessa forma pode-se alcançar um menor *overhead* de mensagens de anúncios de estado dos enlaces. Um esquema de inclusão de informações de anúncio de estados de enlace nas mensagens LMP pode ser visto em (PERELLO *et al.*, 2009). No entanto, a redução do número de mensagens de anúncio de estado do enlace nos protocolos de RWA não foi testada nesse trabalho.

4.3 Ambiente de testes

O ambiente de testes criado para o desenvolvimento desse trabalho utilizou-se de cinco computadores e dois *switches ethernet*, representando o plano de transporte da rede ótica. Essa topologia física é apresentada na Figura 10. Os computadores possuem sistema operacional *GNU/Linux Ubuntu* 10.04. Os testes com as implementações das funções propostas foram realizados em laboratório e não foram usados simuladores de rede já existentes, tais como *Network Simulator* (NS) (CALIFORNIA, 2011) e OMNET++ (OMNET, 2011), o ambiente de testes e as funções do LMP foram desenvolvidos de maneira estruturada utilizando a linguagem C, o que aproxima a implementação das funções de uma implementação real em dispositivos de chaveamento de rede. O ambiente foi montado e os testes realizados no Laboratório de Sistemas e Infraestrutura de Comunicação (LASIC) da Universidade Federal Rural do Semi-Árido - UFERSA, localizada na cidade de Mossoró, RN, Brasil.

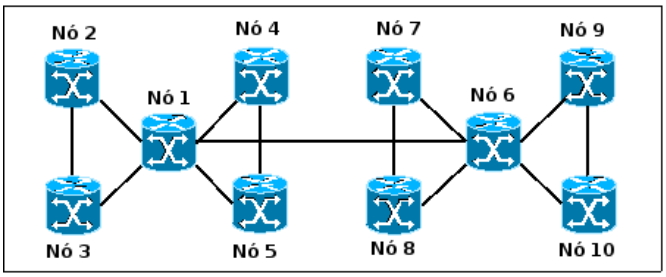
Esse ambiente de testes foi utilizado para simular duas topologias de redes óticas. A primeira rede é composta por 10 nós e a segunda por 15 nós óticos. Essas topologias são mostradas nas Figuras, 11(a) e 11(b). Para efeito de testes, foram simulados nós com apenas 4 portas dedicadas a canais de controle. Para simular a comunicação entre

Figura 10: Topologia Física

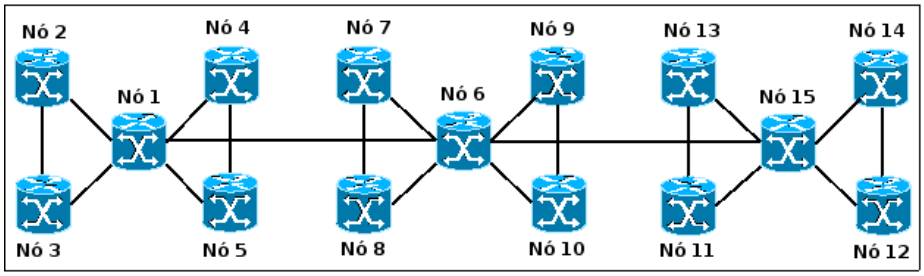


os nós foram usados *Sockets* UDP e a descoberta de vizinhos foi realizada de maneira automática utilizando-se como estratégia o envio de mensagens *HelloConfig* para o endereço de *broadcast* da rede. Os parâmetros medidos nos testes foram: o tempo que os nós levaram para conectar a todos os seus vizinhos através do LMP, parâmetro esse representado pela variável *Tc*, e o número de mensagens enviadas por cada nó até a conexão ser estabelecida com todos os seus vizinhos, representado pela variável *m*. O número de nós em cada teste é representado pela variável *n*.

Figura 11: Topologias Virtuais



(a) topologia com dez nós



(b) topologia com quinze nós

Na topologia da Figura 11(a) composta por 10 nós, os nós 1 e 6 têm 4 vizinhos cada (apesar da conexão direta, eles não trocam informações para estabelecimento de canal de controle) e os demais nós têm 2 vizinhos cada. A Figura 11(b), mostra rede com topologia composta por 15 nós, os nós 1, 6 e 15 têm 4 vizinhos cada e o restante dos nós

têm dois vizinhos cada.

4.4 Resultados

A Figura 12 mostra o tempo médio de conexão dos nós com dois vizinhos nos testes realizados com o LMP-e na rede com topologia de 10 nós. Esse parâmetro foi calculado nas duas versões do protocolo com uma média aritmética simples, seguindo a fórmula $MTc = \frac{\sum_{i=1}^{n} Tc_i}{n}$. Logo abaixo é apresentado o tempo médio de conexão dos nós com dois vizinhos na topologia com 10 nós utilizando o LMP-strict. Esses dados podem ser observados na Figura 13.

Figura 12: Tempo médio de conexão dos nós com 2 vizinhos na rede com topologia de 10 nós - LMP-e.

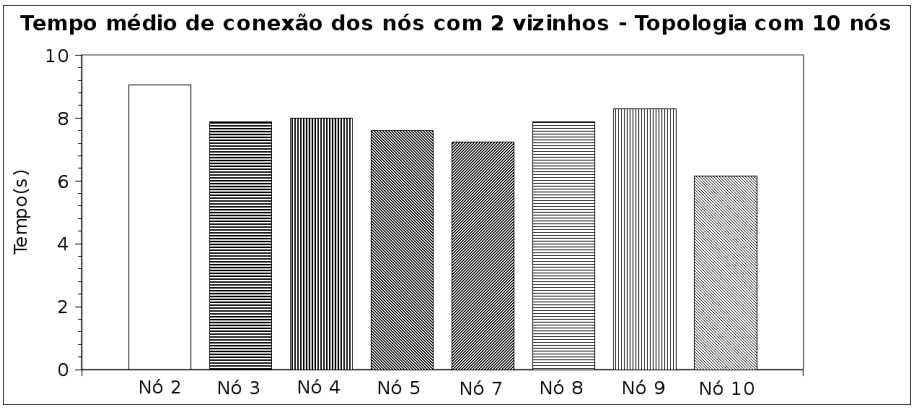


Figura 13: Tempo médio de conexão dos nós com 2 vizinhos na rede com topologia de 10 nós - LMP-strict.

Observando as Figuras 12 e 13, é possível ver que os nós 8 e 10 apresentaram tempo médio de conexão a seus vizinhos durante o estabelecimento dos canais de controle menor no LMP-e, que teve parâmetros adicionais nas mensagens, em relação ao LMP-strict, que seguiu o padrão estrito do tamanho das mensagens.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 2	9,059	8,368	2,938
Nó 3	7,868	9,280	3,094
Nó 4	7,991	5,542	2,391
Nó 5	7,612	5,078	2,288
Nó 7	7,234	2,338	1,553
Nó 8	7,871	7,546	2,790
Nó 9	8,285	4,703	2,202
Nó 10	6,147	4,874	2,242

Tabela 2: Tempo médio de conexão, variância e desvio padrão dos nós com dois vizinhos. Topologia com 10 nós executando LMP-e.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 2	8,056	5,803	2,409
Nó 3	5,940	2,872	1,695
Nó 4	6,938	3,717	1,928
Nó 5	7,205	5,610	2,369
Nó 7	6,423	4,465	2,113
Nó 8	7,993	3,457	1,859
Nó 9	5,644	3,589	1,894
Nó 10	7,948	1,488	1,220

Tabela 3: Tempo médio de conexão, variância e desvio padrão dos nós com dois vizinhos. Topologia com 10 nós executando LMP-s.

As Tabelas 2 e 3 mostram o tempo médio de conexão, a variância e o desvio padrão dos nós com dois vizinhos nos testes com as duas versões implementadas do LMP na topologia com 10 nós.

A Figura 14 apresenta a média do número de mensagens enviadas por cada nó com 2 vizinhos até a conexão com estes, utilizando o LMP-e. Esse parâmetro também foi calculado com uma média aritmética simples para as duas abordagens do protocolo. Na Figura 15, é apresentado o número médio de mensagens enviadas pelos nós com 2 vizinhos na rede com topologia de 10 nós, executando o LMP-strict.

Com base nos gráficos das Figuras 14 e 15, é possível notar que a média do número de mensagens enviadas pelos nós nas duas abordagens do LMP permanece estável para os nós com 2 vizinhos, com pequena variação para mais ou para menos em alguns nós. Os nós 5 e 10 apresentaram número médio de mensagens enviadas menor no LMP-e.

Figura 14: Média do número de mensagens enviadas pelos nós com 2 vizinhos cada, na rede com topologia de 10 nós - LMP-e.

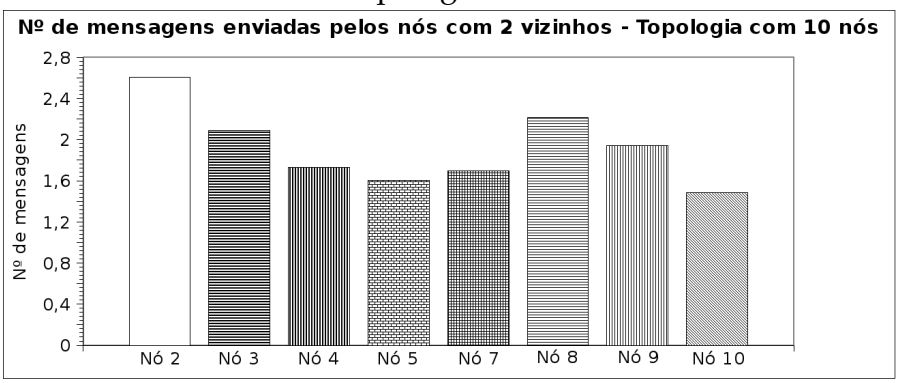
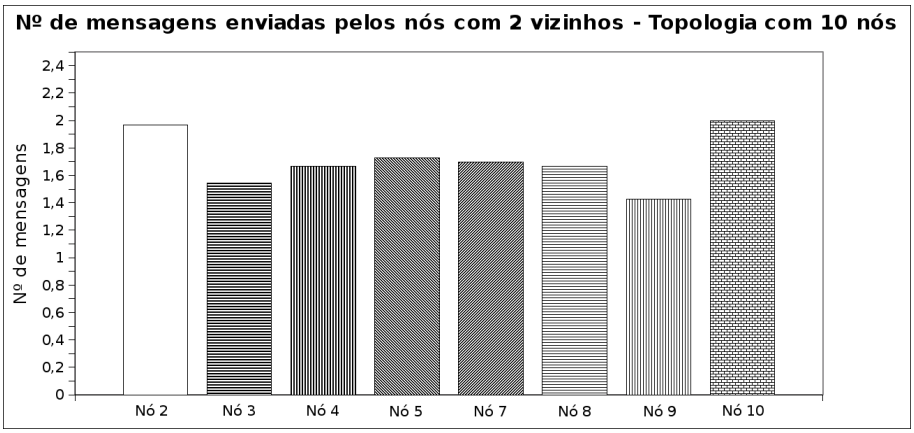


Figura 15: Média do número de mensagens enviadas pelos nós com 2 vizinhos cada, na rede com topologia de 10 nós - LMP-strict.



As Tabelas 4 e 5 mostram o número médio de mensagens enviadas por cada nó até a conexão com seus vizinhos, a variância e o desvio padrão dessa medida, dos nós com dois vizinhos nos testes com as duas versões implementadas do LMP na topologia com 10 nós.

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	2,606	0,481	0,704
Nó 3	2,091	1,295	1,156
Nó 4	1,727	0,198	0,452
Nó 5	1,606	0,360	0,609
Nó 7	1,697	0,211	0,467
Nó 8	2,212	1,137	1,083
Nó 9	1,939	0,239	0,496
Nó 10	1,485	0,310	0,566

Tabela 4: Número médio de mensagens enviadas, variância e desvio padrão dos nós com dois vizinhos. Topologia com 10 nós executando LMP-e.

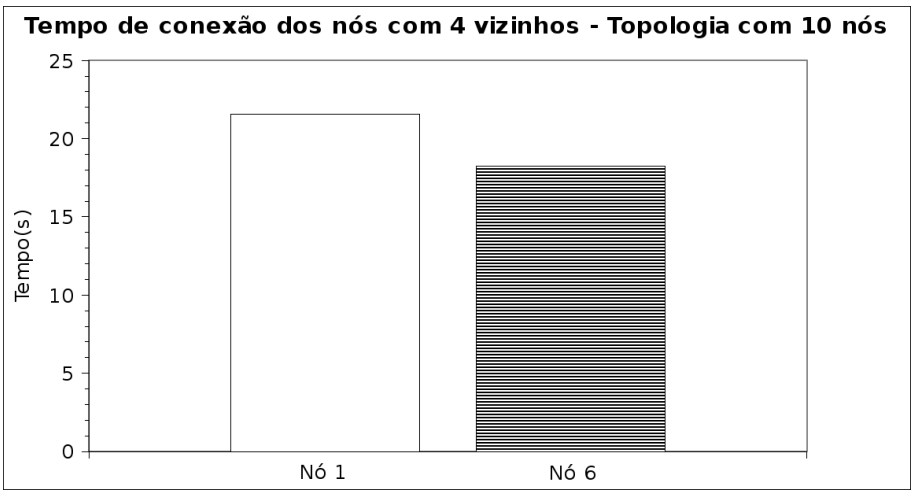
As Figuras 16 a 19 mostram as mesmas grandezas avaliadas anteriormente, dessa

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	1,970	0,405	0,637
Nó 3	1,545	0,318	0,564
Nó 4	1,667	0,229	0,479
Nó 5	1,727	0,330	0,574
Nó 7	1,697	0,530	0,728
Nó 8	1,667	0,292	0,540
Nó 9	1,424	0,252	0,502
Nó 10	2,000	0,125	0,354

Tabela 5: Número médio de mensagens enviadas, variância e desvio padrão dos nós com dois vizinhos. Topologia com 10 nós executando LMP-s.

vez para os nós com 4 vizinhos, ainda na rede com topologia de 10 nós para as duas implementações do protocolo. A Figura 16 mostra o tempo médio dos nós com 4 vizinhos executando o LMP-e. Na Figura 17 é possível ver o mesmo parâmetro para os nós com 4 vizinhos operando com o LMP-strict.

Figura 16: Tempo médio de conexão dos nós com 4 vizinhos na rede com topologia de 10 nós - LMP-e

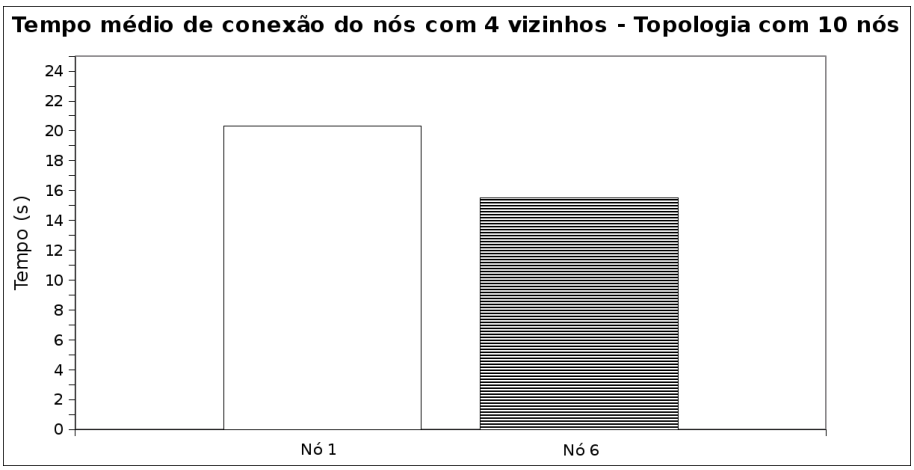


Comparando os gráficos mostrados nas Figuras 16 a 17 é possível notar que no cenário com 10 nós, os nós que tinham 4 vizinhos obtiveram tempo médio de conexão maior na abordagem LMP-e. O nó 1 teve seu tempo médio de conexão 1 segundo maior em relação aos testes com a segunda versão do LMP e o nó 6 obteve um tempo médio de conexão maior em aproximadamente 2,5 segundos no LMP-e em detrimento do LMP-strict.

As Tabelas 6 e 7 mostram o tempo médio de conexão, a variância e o desvio padrão dos nós com quatro vizinhos nos testes com as duas versões implementadas do LMP na topologia com 10 nós.

A Figura 18 apresenta a média do número de mensagens enviadas pelos nós com 4 vizinhos executando o LMP-e na topologia com 10 nós. Logo abaixo, a Figura

Figura 17: Tempo médio de conexão dos nós com 4 vizinhos na rede com topologia de 10 nós - LMP-strict



Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 1	21,553	13,459	3,730
Nó 6	18,232	14,441	3,860

Tabela 6: Tempo médio de conexão, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 10 nós executando LMP-e.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 1	20,318	2,087	1,444
Nó 6	15,497	13,226	3,637

Tabela 7: Tempo médio de conexão, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 10 nós executando LMP-s.

19 mostra o mesmo parâmetro para os nós com 4 vizinhos executando na mesma topologia, porém, com o LMP-strict.

Nos gráficos apresentados nas Figuras 18 e 19 mostra-se que a média do número de mensagens enviadas em ambos os nós se manteve estável nos testes realizados com as duas versões do LMP. Na LMP-e proposto, o nó 1 enviou em média 0,6 mensagens a mais do que no LMP-strict proposto. O nó 6 teve a média de mensagens enviadas um pouco menor na LMP-e com média de 1,8 mensagens enviadas enquanto no LMP-strict esse nó enviou em média 2 mensagens até a conexão com seus vizinhos.

As Tabelas 8 e 9 mostram o número médio de mensagens enviadas por cada nó até a conexão com seus vizinhos, a variância e o desvio padrão dessa medida, dos nós com quatro vizinhos nos testes com as duas versões implementadas do LMP na topologia

Figura 18: Média do número de mensagens enviadas pelos nós com 4 vizinhos na rede com topologia de 10 nós - LMP-e.

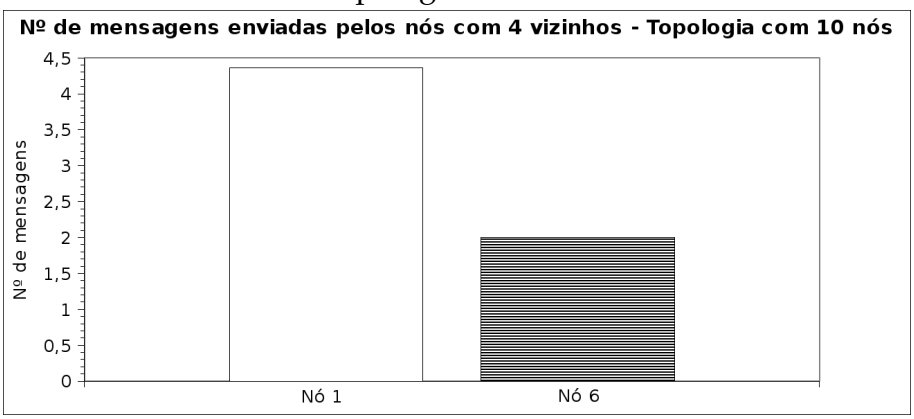
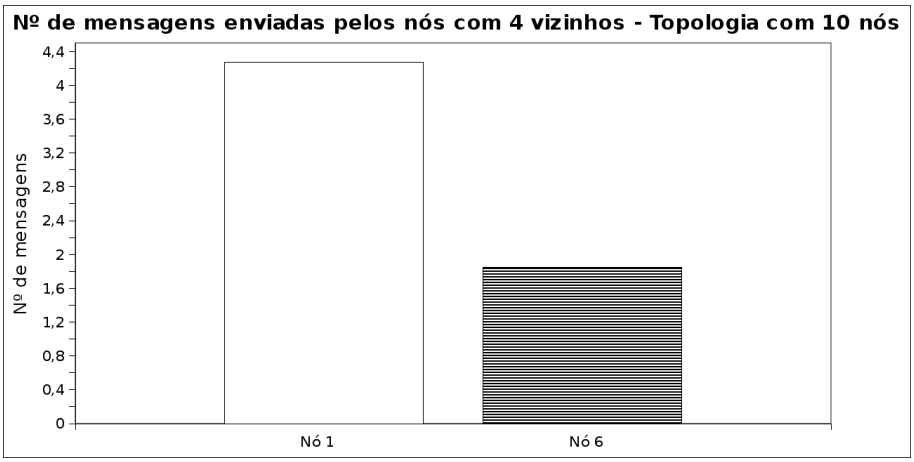


Figura 19: Média do número de mensagens enviadas pelos nós com 4 vizinhos na rede com topologia de 10 nós - LMP-strict.



Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 1	4,364	1,262	1,141
Nó 6	2,000	0,727	0,866

Tabela 8: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 10 nós executando LMP-e.

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 1	4,273	0,267	0,517
Nó 6	1,848	0,695	0,834

Tabela 9: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 10 nós executando LMP-s.

com 10 nós.

Nas Figuras 20 e 21, são mostrados os tempos médios de conexão dos nós com 2 vizinhos para a topologia com 15 nós executando o LMP-e e o LMP-strict respectiva-

mente.

Figura 20: Tempo médio de conexão dos nós com 2 vizinhos na rede com topologia de 15 nós - LMP-e.

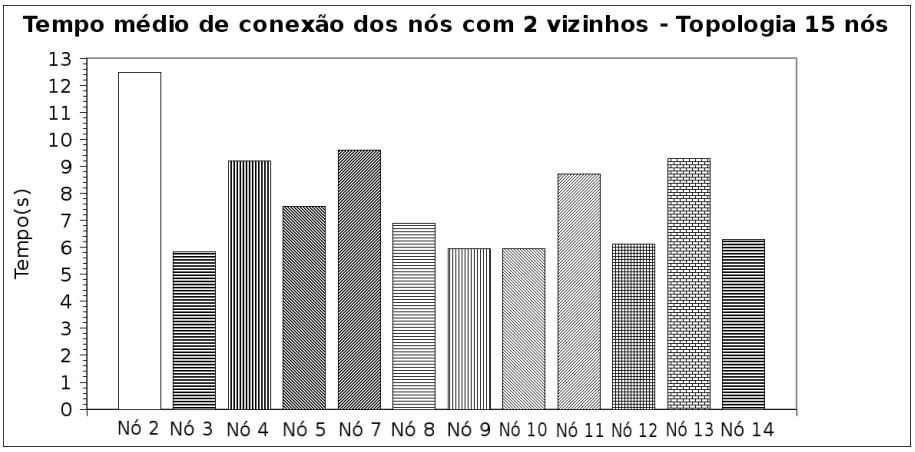
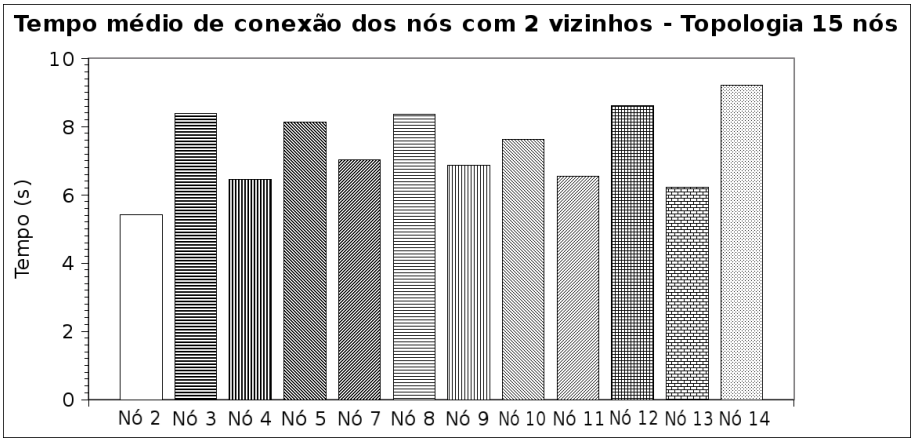


Figura 21: Tempo médio de conexão dos nós com 2 vizinhos na rede com topologia de 15 nós - LMP-strict.



Os gráficos das figuras 20 e 21 mostram que 7 dos 12 nós com 2 vizinhos tiveram tempos médios de conexão menores nos testes com o LMP-e na topologia com 15 nós em relação aos testes com o LMP-strict na mesma topologia, enquanto os outros 5 nós tiveram tempo médio de conexão menor nos testes com o LMP-strict. Os nós 3, 5, 8, 9, 10, 12 e 14 tiveram seus tempos médios menores aproximadamente 2,3, 0,5, 1, 1, 1,8, 2,6, 3,2 segundos respectivamente no LMP-e em relação aos tempos nos testes com o LMP-strict.

As Tabelas 10 e 11 mostram o tempo médio de conexão, a variância e o desvio padrão dos nós com dois vizinhos nos testes com as duas versões implementadas do LMP na topologia com 15 nós.

A Figura 22 apresenta a média do número de mensagens enviadas pelos nós com 2 vizinhos na rede com topologia de 15 nós executando o LMP-e. Na Figura 23 é

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 2	12,483	9,080	3,060
Nó 3	5,836	1,995	1,430
Nó 4	9,204	6,754	2,640
Nó 5	7,516	5,931	2,470
Nó 7	9,597	6,472	2,580
Nó 8	6,885	5,277	2,330
Nó 9	5,954	2,671	1,660
Nó 10	8,712	4,766	2,220
Nó 11	6,111	3,697	1,950
Nó 12	9,288	3,460	1,890
Nó 13	6,290	3,178	1,810
Nó 14	10,392	5,427	2,370

Tabela 10: Tempo médio de conexão, variância e desvio padrão dos nós com 2 vizinhos. Topologia com 15 nós executando LMP-e.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 2	5,423	1,693	1,301
Nó 3	8,390	1,934	1,391
Nó 4	6,463	3,873	1,968
Nó 5	8,125	2,330	1,526
Nó 7	7,035	5,759	2,400
Nó 8	8,351	9,546	3,090
Nó 9	6,873	5,686	2,384
Nó 10	7,615	3,988	1,997
Nó 11	6,551	3,981	1,995
Nó 12	8,609	2,293	1,514
Nó 13	6,233	4,697	2,167
Nó 14	9,210	1,820	1,349

Tabela 11: Tempo médio de conexão, variância e desvio padrão dos nós com 2 vizinhos. Topologia com 15 nós executando LMP-s.

mostrado o número médio de mensagens enviadas por cada nó com 2 vizinhos na mesma topologia com 15 nós e executando o LMP-strict.

Os gráficos apresentados nas Figuras 22 e 23 demonstram que houve menor número médio de mensagens enviadas por 6 nós nos testes com a implementação do LMP-e em relação ao LMP-strict e houve aumento do número médio de mensagens enviadas nos outros 6 nós do cenário apresentado. O nós que apresentaram menor número médio de mensagens enviadas no LMP-e foram os nós 3, 5, 8, 9, 12 e 14 com o número médio de mensagens enviadas menor em aproximadamente 0,9, 0,25, 0,35, 0,35, 0,25,

Figura 22: Média do número de mensagens enviadas pelos nós com 2 vizinhos cada, na rede com topologia de 15 nós - LMP-e.

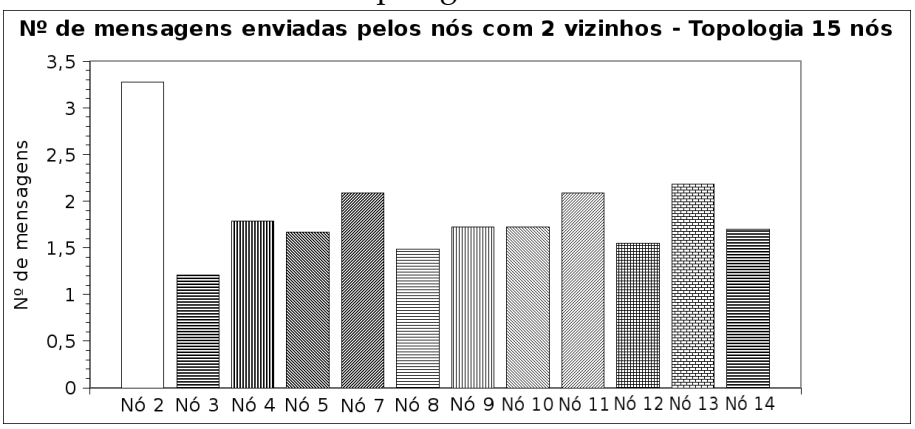
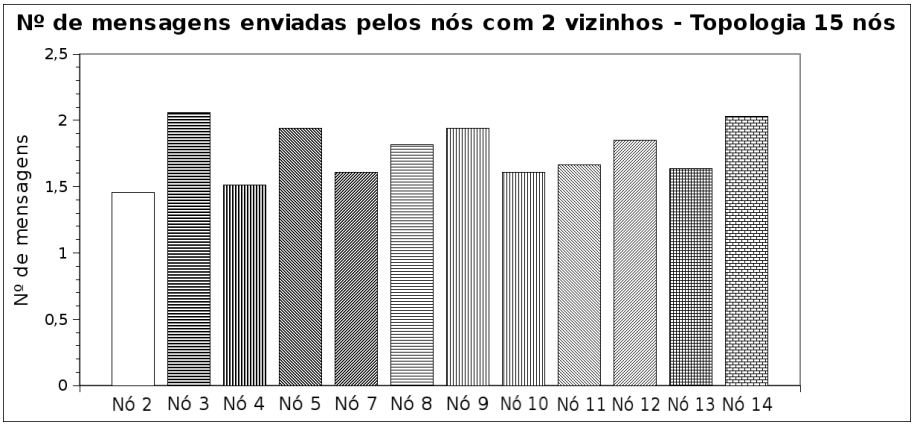


Figura 23: Média do número de mensagens enviadas pelos nós com 2 vizinhos cada, na rede com topologia de 15 nós - LMP-strict.



0,5 mensagens respectivamente.

As tabelas 12 e 13 mostram o número médio de mensagens enviadas por cada nó até a conexão com seus vizinhos, a variância e o desvio padrão dessa medida, dos nós com dois vizinhos nos testes com as duas versões implementadas do LMP na topologia com 15 nós.

A Figura 24 mostra o tempo médio de conexão dos nós com 4 vizinhos na topologia com 15 nós executando o LMP-e. A Figura 25 mostra o mesmo parâmetro da figura anterior, para os nós com 4 vizinhos na mesma topologia, mas executando o LMP-strict.

Com base nos gráficos das Figuras 24 e 25, pode-se notar que nos testes realizados com o LMP-strict houve redução no tempo médio de conexão dos 3 nós com 4 vizinhos em relação a implementação do LMP-e. O nó 1 teve redução de aproximadamente 6 segundos, o nó 6 teve redução de aproximadamente 2 segundos e o nó 15 teve seu tempo médio de conexão reduzido em aproximadamente 2 segundos no seu tempo médio de conexão com seus vizinhos.

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	3,273	1,410	1,206
Nó 3	1,212	0,167	0,415
Nó 4	1,788	0,349	0,600
Nó 5	1,667	0,404	0,646
Nó 7	2,091	0,446	0,678
Nó 8	1,485	0,250	0,508
Nó 9	1,727	0,320	0,574
Nó 10	2,091	0,507	0,723
Nó 11	1,545	0,248	0,506
Nó 12	2,182	0,209	0,465
Nó 13	1,697	0,272	0,529
Nó 14	2,424	0,305	0,561

Tabela 12: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 2 vizinhos. Topologia com 15 nós executando LMP-e.

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	1,455	0,256	0,506
Nó 3	2,061	0,121	0,348
Nó 4	1,515	0,320	0,566
Nó 5	1,939	0,184	0,429
Nó 7	1,606	0,309	0,556
Nó 8	1,818	0,591	0,769
Nó 9	1,939	0,621	0,788
Nó 10	1,606	0,309	0,556
Nó 11	1,667	0,292	0,540
Nó 12	1,848	0,133	0,364
Nó 13	1,636	0,301	0,549
Nó 14	2,030	0,030	0,174

Tabela 13: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 2 vizinhos. Topologia com 15 nós executando LMP-s.

Figura 24: Tempo médio de conexão dos nós com 4 vizinhos na rede com topologia de 15 nós - LMP-e.

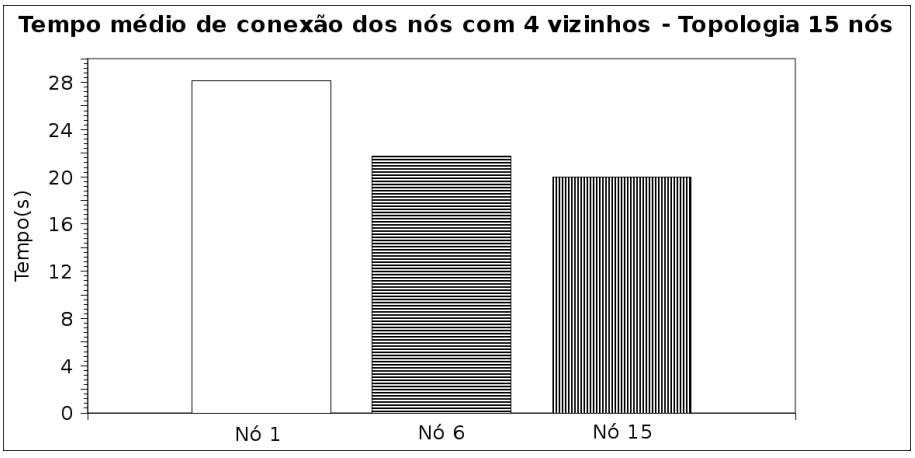
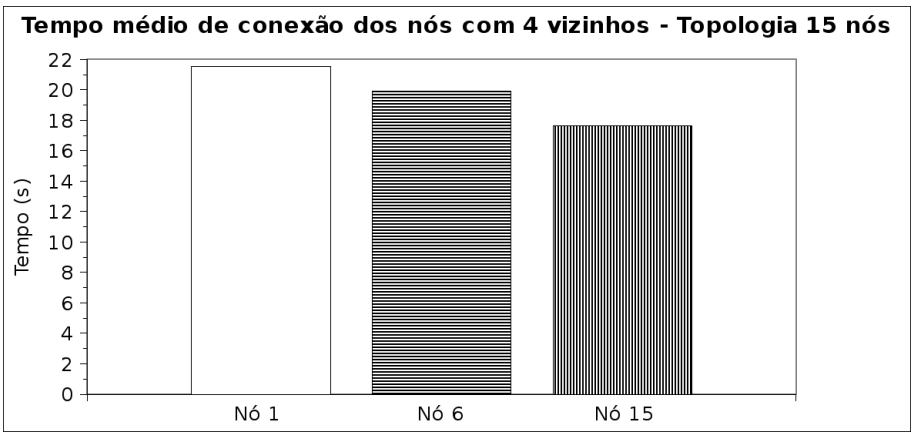


Figura 25: Tempo médio de conexão dos nós com 4 vizinhos na rede com topologia de 15 nós - LMP-strict.



As Tabelas 14 e 15 mostram o tempo médio de conexão, a variância e o desvio padrão dos nós quatro vizinhos nos testes com as duas versões implementadas do LMP na topologia com 15 nós.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 1	28,117	15,407	3,990
Nó 6	21,763	14,170	3,820
Nó 15	19,987	12,556	3,540

Tabela 14: Tempo médio de conexão, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 15 nós executando LMP-e.

Nós	Tempo médio de conexão de cada nó (s)	Variância	Desvio Padrão
Nó 1	21,542	4,210	2,052
Nó 6	19,900	2,693	1,641
Nó 15	17,657	17,164	4,143

Tabela 15: Tempo médio de conexão, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 15 nós executando LMP-s.

O número médio de mensagens enviadas pelos nós com 4 vizinhos para conexão com estes na rede com topologia de 15 nós e executando o LMP-e é apresentado na Figura 26. Por sua vez, o número médio de mensagens enviadas pelos nós com 4 vizinhos na rede com topologia de 15 nós, executando o LMP-strict é mostrado na Figura 27.

No cenário apresentado nos gráficos das Figuras 26 e 27, comparando os testes com as duas versões do LMP, no LMP-e, apenas o nó 15 apresentou um número médio de

Figura 26: Média do número de mensagens enviadas pelos nós com 4 vizinhos cada, na rede com topologia de 15 nós - LMP-e.

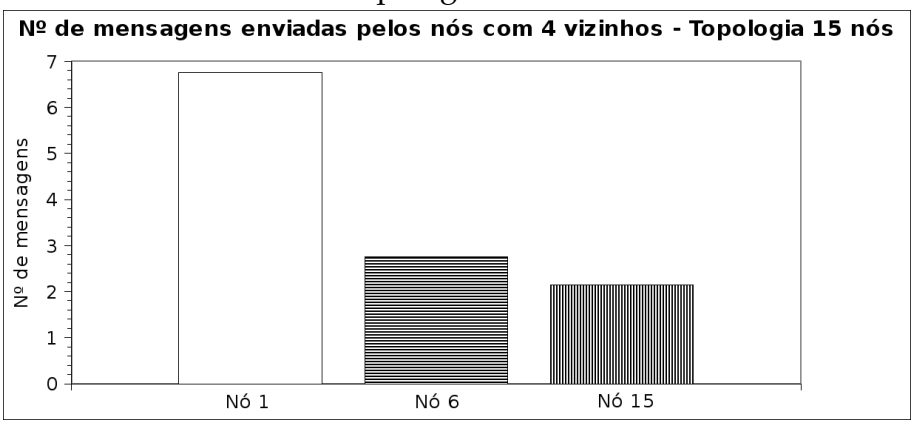
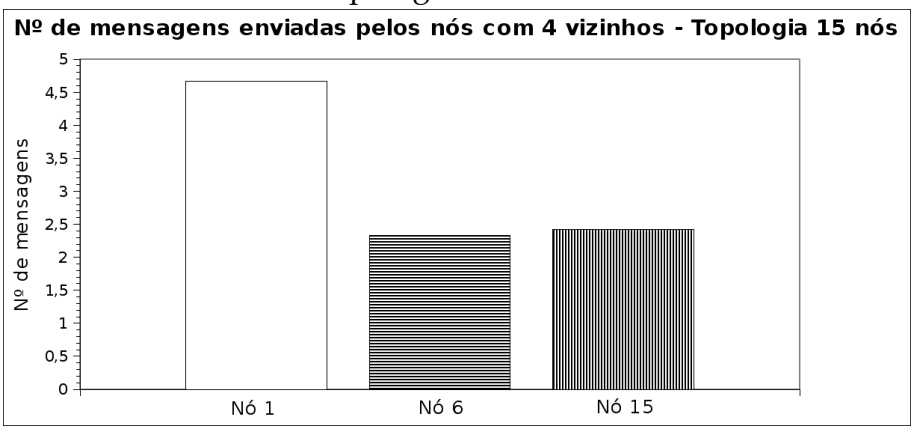


Figura 27: Média do número de mensagens enviadas pelos nós com 4 vizinhos cada, na rede com topologia de 15 nós - LMP-strict.



mensagens enviadas até a conexão com seus vizinhos menor em relação ao LMP-strict. Esse nó enviou em média 0,3 mensagens a menos executando o LMP-e. Os nós 1 e 6 enviaram em média aproximadamente 2 e 0,5 mensagens a menos respectivamente.

As Tabelas 16 e 17 mostram o número médio de mensagens enviadas por cada nó até a conexão com seus vizinhos, a variância e o desvio padrão dessa medida, dos nós com quatro vizinhos nos testes com as duas versões implementadas do LMP na topologia com 15 nós.

Com a análise dos gráficos obtidos foi possível notar que no cenário com 10 nós não houve grandes ganhos em relação aos tempos médios e nem em relação as mensagens enviadas, em qualquer das versões desenvolvidas. Houve algumas exceções onde cada versão se mostrou um pouco mais eficiente que a outra. Já quando aumentado o número de nós para 15, o LMP-e, mesmo com a adição de parâmetros, mostrou-se um pouco mais eficiente nos nós com dois vizinhos, tanto nos tempos médios de conexão, quanto no número médio de mensagens enviadas para conexão dos nós a seus vizinhos. Já nos nós que tinham 4 vizinhos, na topologia com 15 nós, o LMP-strict se

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	3,273	1,410	1,206
Nó 3	1,212	0,167	0,415
Nó 4	1,788	0,349	0,600
Nó 5	1,667	0,404	0,646
Nó 7	2,091	0,446	0,678
Nó 8	1,485	0,250	0,508
Nó 9	1,727	0,320	0,574
Nó 10	2,091	0,507	0,723
Nó 11	1,545	0,248	0,506
Nó 12	2,182	0,209	0,465
Nó 13	1,697	0,272	0,529
Nó 14	2,424	0,305	0,561

Tabela 16: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 15 nós executando LMP-e.

Nós	Número médio de mensagens de cada nó	Variância	Desvio Padrão
Nó 2	1,455	0,256	0,506
Nó 3	2,061	0,121	0,348
Nó 4	1,515	0,320	0,566
Nó 5	1,939	0,184	0,429
Nó 7	1,606	0,309	0,556
Nó 8	1,818	0,591	0,769
Nó 9	1,939	0,621	0,788
Nó 10	1,606	0,309	0,556
Nó 11	1,667	0,292	0,540
Nó 12	1,848	0,133	0,364
Nó 13	1,636	0,301	0,549
Nó 14	2,030	0,030	0,174

Tabela 17: Número médio de mensagens enviadas, variância e desvio padrão dos nós com 4 vizinhos. Topologia com 15 nós executando LMP-s.

mostrou mais eficiente tanto nos tempos médios de conexão, quanto no número médio de mensagens enviadas.

5 Conclusões e Trabalhos Futuros

No presente trabalho, foram propostas funções de descoberta de topologia e de recursos do protocolo LMP. Essas funções possibilitam o fornecimento de informações aos nós, informações essas que são importantes para o estabelecimento de canais de controle nesse protocolo atuando em redes óticas GMPLS dinâmicas. Essas funções foram desenvolvidas e testadas em duas versões do LMP. A primeira versão foi implementada com acréscimo de parâmetros como comprimento de onda e uma característica da fibra, além do identificador de porta local. A segunda versão respeitou estritamente o tamanho das mensagens e o conteúdo dos cabeçalhos dos objetos LMP. O desempenho das funções foi avaliado nas duas versões implementadas por meio de experimentos computacionais que comprovaram que as funções propostas são capazes de estabelecer os canais de controle em tempos na faixa de segundos. Foram medidos o tempo médio até a conexão dos nós a seus vizinhos e o número médio de mensagens *Config* enviadas até para um nó conectar-se a seus vizinhos.

O estabelecimento dos canais de controle foi realizado em todos os cenários de testes propostos, com tempos na faixa dos segundos em vez de horas como se tem normalmente num ambiente de configuração manual. Também foi proposta e desenvolvida uma função que disponibiliza o mapa dos recursos de cada nó para o uso do algoritmo de alocação de comprimento de onda da suíte GMPLS. Essa função disponibiliza em ambas as versões do LMP desenvolvidas informações como o identificador da porta que o nó está utilizando, o estado do canal de controle de acordo com os estados possíveis no LMP, o comprimento de onda utilizado e o endereço do nó vizinho a que o nó local está conectado.

Com base nos resultados obtidos nos testes com topologias de redes óticas com 10 e 15 nós, foi possível comprovar que em cenários com diferentes números de nós, o algoritmo estabeleceu a conexão completa do plano de controle em tempo de segundos de maneira automatizada.

Como trabalhos futuros, pretende-se desenvolver a função de tratamento de falhas no plano de controle e avaliar como este trataria a reconexão da rede e alocação de recursos em função do tempo no mesmo cenário testado neste trabalho ou em um ambiente de simulação por software. Também objetiva-se a integração do algoritmo desenvolvido às demais funções do plano de controle GMPLS.

Referências

ABBADE, M.; MARCONI, J.; CASSIOLATO, R.; ISHIZUCA, V.; FONSECA, I.; FRAGNITO, H. Field-trial evaluation of cross-layer effect caused by all-optical wavelength converters on ip network applications. *Lightwave Technology, Journal of*, v. 27, n. 12, p. 1816 –1826, june15, 2009. ISSN 0733-8724.

ÁRTICO, A. F. R. *Implementação do protocolo LMP de gerência de enlace em redes GMPLS ópticas.* Dissertação (Mestrado) — UNIVERSIDADE ESTADUAL PAULISTA, São José do Rio Preto, SP, Brasil, Fevereiro 2011.

ASHWOOD-SMITH, P.; BERGER, L. *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions*. IETF, January 2003. RFC 3472 (Proposed Standard). (Request for Comments, 3472). Updated by RFCs 3468, 4201. Disponível em: <http://www.ietf.org/rfc/rfc3472.txt>.

AWDUCHE, D.; BERGER, L.; GAN, D.; LI, T.; SRINIVASAN, V.; SWALLOW, G. *RSVP-TE: Extensions to RSVP for LSP Tunnels*. IETF, December 2001. RFC 3209 (Proposed Standard). (Request for Comments, 3209). Updated by RFCs 3936, 4420, 4874, 5151, 5420. Disponível em: <http://www.ietf.org/rfc/rfc3209.txt>.

BENJAMIN, D.; TRUDEL, R.; SHEW, S.; E., K. Optical services over the intelligent optical network. *Communications Magazine, IEEE*, v. 39, p. 73 – 78, Sep 2001. ISSN 0163-6804.

BERGER, L. *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*. IETF, January 2003. RFC 3471 (Proposed Standard). (Request for Comments, 3471). Updated by RFCs 4201, 4328, 4872. Disponível em: <http://www.ietf.org/rfc/rfc3471.txt>.

BERGER, L. *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*. IETF, January 2003. RFC 3473 (Proposed Standard). (Request for Comments, 3473). Updated by RFCs 4003, 4201, 4420, 4783, 4874, 4873, 4974, 5063, 5151, 5420. Disponível em: <http://www.ietf.org/rfc/rfc3473.txt>.

CALIFORNIA, U. of S. *The Network Simulator*. 2011. Disponível em: <http://www.isi.edu/nsnam/ns/>. Acesso em: 29 Novembro 2011.

DRAGON. *DRAGON - Dynamic Resource Allocation in GMPLS Optical Networks*. 1999–2012. Disponível em: <http://dragon.maxgigapop.net>.

ELLINAS, G.; LABOURDETTE, J.-F.; WALKER, J.; CHAUDHURI, S.; LIN, L.; GOLDSTEIN, E.; BALA, K. Network control and management challenges in opaque networks utilizing transparent optical switches. *Communications Magazine, IEEE*, v. 42, n. 2, p. S16 – S24, feb. 2004. ISSN 0163-6804.

FONSECA, I. E. da. *Uma Abordagem para Aprovisionamento e Diferenciação de QoS Óptico na Presença de FWM em Redes Ópticas Transparentes*. Tese (Doutorado) — Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação., abril 2005.

GOLAB, W.; BOUTABA, R. Policy-driven automated reconfiguration for performance management in wdm optical networks. *Communications Magazine, IEEE*, v. 42, n. 1, p. 44 – 51, jan. 2004. ISSN 0163-6804.

IOVANNA, P.; SABELLA, R.; SETTEMBRE, M. A traffic engineering system for multi-layer networks based on the gmpls paradigm. *Network, IEEE*, v. 17, n. 2, p. 28 – 37, mar. 2003. ISSN 0890-8044.

LANG, J. *Link Management Protocol (LMP)*. IETF, October 2005. RFC 4204 (Proposed Standard). (Request for Comments, 4204). Disponível em: <http://www.ietf.org/rfc/rfc4204.txt>.

LEE, J. H.; YOSHIKANE, N.; TSURITANI, T.; OTANI, T. Optical link performance monitoring using extended link management protocol for transparent optical networks. In: *Optical Fiber Communication - incudes post deadline papers, 2009. OFC 2009. Conference on*. [S.l.: s.n.], 2009. p. 1 –3.

MAIER, M. *Optical Switching Networks*. 1. ed. [S.l.]: Cambridge University Press, 2008. ISBN 978-0-521-86800-6.

MANNIE, E. *Generalized Multi-Protocol Label Switching (GMPLS) Architecture. RFC 3945*. United States: RFC Editor, 2004.

MUKHERJEE, B. *Optical WDM Networks (Optical Networks)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006. ISBN 0387290559.

MUNOZ, R.; MARTÍNEZ, R.; CASELLAS, R. Challenges for gmpls lightpath provisioning in transparent optical networks: wavelength constraints in routing and signaling. *Comm. Mag.*, IEEE Press, Piscataway, NJ, USA, v. 47, n. 8, p. 26–34, 2009. ISSN 0163-6804.

OMNET. *OMNet++ Network Simulator Framework*. 2011. Disponível em: <http://www.omnetpp.org>. Acesso em: 29 Novembro 2011.

PALMIERI, F. Gmpls control plane services in the next-generation optical internet. In: *The Internet Protocol Journal*. [S.l.]: Ole J. Jacobsen, Cisco., 2008. v. 11, n. 3.

PAPADIMITRIOU, D.; BERDE, B.; MARTINEZ, R.; ORDAS, J.; THEILLAUD, R.; VERBRUGGE, S. Generalized multi-protocol label switching (gmpls) unified control plane validation. *ICC'06. IEEE International Conference on Communications*, Istanbul, v. 6, p. 2717 – 2724, December 2006. ISSN 8164-9547.

PERELLO, J.; ESCALONA, E.; SPADARO, S.; COMELLAS, J.; JUNYENT, G. Resource discovery in ason/gmpls transport networks. *Communications Magazine, IEEE*, v. 45, n. 10, p. 86 –92, october 2007. ISSN 0163-6804.

PERELLO, J.; SPADARO, S.; COMELLAS, J.; JUNYENT, G. Burst contention avoidance schemes in hybrid gmpls-enabled obs/ocs optical networks. In: *Optical Network Design and Modeling, 2009. ONDM 2009. International Conference on*. [S.l.: s.n.], 2009. p. 1 –6.

PERROS, H. G. *Connection-oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks*. [S.l.]: John Wiley & Sons, 2005. ISBN 0470021632.

RAJAGOPALAN, B.; PENDARAKIS, D.; SAHA, D.; RAMAMOORTHY, R. S.; BALA, K. Ip over optical networks: Architectural aspects. *Communications Magazine, IEEE*, v. 38, p. 94 – 102, Sep 2000. ISSN 0163-6804.

RAMAMURTHY, B.; FENG, H.; DATTA, D.; HERITAGE, J.; MUKHERJEE, B. Transparent vs. opaque vs. translucent wavelength-routed optical networks. In: *Optical Fiber Communication Conference, 1999, and the International Conference on Integrated Optics and Optical Fiber Communication. OFC/IOOC '99. Technical Digest*. [S.l.: s.n.], 1999.

RAMASWAMI, R.; SIVARAJAN, K. N. *Optical Networks: A Practical Perspective*. 2. ed. [S.l.]: Morgan Kaufmann, 2002. ISBN 1-55860-655-6.

RAMASWAMI, R.; SIVARAJAN, K. N.; SASAKI, G. H. *Optical Networks: A Practical Perspective*. 3. ed. [S.l.]: Morgan Kaufmann, 2010. ISBN 978-0-12-374092-2.

SANTOS, G. C.; D., S. F.; OLIVEIRA, J. C. R. F.; A., M. R.; SALVADOR, M. R.; ROMERO, M. A.; M., M. Aprovisionamento automático de circuitos Ópticos protegidos via plano de controle gmpls considerando restrições de camada física. *XXVII Simpósio Brasileiro de Telecomunicações*, Anais do XXVII Simpósio Brasileiro de Telecomunicacões. SBRT'09, Blumenau, SC, Brasil, 2009.

SERGEY, T.; MERRION, E. *An Introduction to the Fundamentals of PMD in Fibers*. Corning Incorporated, July 2006. Disponível em: <http://www.corning.com/docs/opticalfiber/WP5071.pdf>.

SHIOMOTO, K.; SHIMIZU, K.; HAYASHI, R.; INOUE, I. Gmpls-based optical circuit switch with neighbor auto-discovery mechanism. In: *INFOCOM Workshops 2009, IEEE*. [S.l.: s.n.], 2009. p. 1 –6.

STERN, T. E.; ELLINAS, G.; BALA, K. *Multiwavelength Optical Networks: Architectures, design, and control*. 2. ed. [S.l.]: Cambridge University Press, 2009. ISBN 978-0-521-88139-5.

TOMKOS, I. Transport performance of wdm metropolitan area transparent optical networks. In: *Optical Fiber Communications Conference*. Optical Society of America, 2002. p. WW3. Disponível em: <http://www.opticsinfobase.org/abstract.cfm?URI=OFC-2002-WW3>.

WAGNER, R. E.; ALFERNESS, R. C.; SALEH, A. M.; GOODMAN, M. S. Monet: multiwavelength optical networking. *Journal of Lightwave Technology*, IEEE Aerospace and Electronic Systems Society, v. 14, p. 1349–1355, Jun 1996. ISSN 0733-8724.

WILLNER, A. E.; C., C. M.; H., A. O.; YONG-WON, S.; DENIZ, G. Key building blocks for all-optical networks(special issue on advanced internetworking based on photonic network technologies). *IEICE transactions on communications*, The Institute of Electronics, Information and Communication Engineers, v. 83, n. 10, p. 2166–2177, October 2000. ISSN 09168516. Disponível em: <http://ci.nii.ac.jp/naid/110003218532/en/>.

APÊNDICE A - Roteamento em GMPLS

Os protocolos de roteamento baseados no GMPLS atualmente usados para o plano de controle das redes óticas são baseados naqueles que foram usados com sucesso por décadas nas redes IP. Nesse intuito, GMPLS provê o arcabouço para estender a aplicabilidade dos protocolos de roteamento IP "tradicionais" para vários tipos de redes óticas (STERN *et al.*, 2009). O protocolo de roteamento OSPF e seus melhoramentos é o mais representativo para o GMPLS, por ser o mais amplamente usado em implementações GMPLS atuais (STERN *et al.*, 2009).

Para facilitar o estabelecimento de LSPs, os LSRs necessitam de mais informações sobre os enlaces do que as providas pelas redes que usam protocolos de roteamento IP. As extensões de roteamento TE permitem não somente a descoberta de topologia convencional, mas também a descoberta de recursos no domínio de roteamento explorando o mecanismo de anúncio de estado do enlace (LSA), advindo dos protocolos de roteamento OSPF/IS-IS (MAIER, 2008). Através desse mecanismo, cada LSR dissemina nos seus LSAs as informações de recursos de seus *links TE* locais através do canal ou canais de controle. Além de informações de recursos TE, LSRs podem também anunciar informações de recursos óticos, incluindo valor de comprimento de onda e restrições físicas. Porém, informações de roteamento sobre a camada ótica aumentam a quantidade de informação necessária a ser distribuída em LSAs, levando a aumentar o tempo de distribuição e configuração (MAIER, 2008).

Uma maneira de evitar o problema da escalabilidade é executar o protocolo de roteamento de estado do enlace somente em redes totalmente óticas de tamanho geográfico limitado, as chamadas "ilhas de transparência". Em cada ilha de transparência, todas as rotas tem qualidade de sinal ótico adequado e desse modo, o anúncio de informação de recursos óticos pode ser negligenciada (MAIER, 2008).

Os LSAs permitem que todos os LSRs em um dado domínio de roteamento adquiram e atualizem uma figura coerente da rede. Essa figura da rede é referida como o **Banco de Dados de estado de enlace**. As informações desse banco de dados são usadas pelos LSRs para o cálculo de rotas.

Cálculo de rotas

Protocolos de roteamento necessitam determinar um "bom" ou "ótimo" caminho através de uma rede para cada conexão requisitada (STERN *et al.*, 2009).

Enquanto os protocolos de roteamento com extensões TE são padronizados pelas redes GMPLS, o cálculo de rotas é tipicamente proprietário e desse modo permite a fabricantes buscarem diversas estratégias, e diferenciarem seus produtos (MAIER, 2008).

Os algoritmos que foram originalmente usados para o cálculo de rotas em redes IP, e são atualmente usados no GMPLS, são todos variantes de métodos para encontrar caminhos mais curtos através de grafos (STERN *et al.*, 2009). Do ponto de vista do controle da rede, o algoritmo de cálculo de rotas é apenas uma pequena parte do problema de roteamento como um todo. Uma outra questão fundamental é onde

o algoritmo é implementado em uma rede e que informação ele necessita. Outra informação importante é que algoritmos de caminho mais curto (SPF) são adaptados somente à redes opacas. Roteamento em redes transparentes é mais complexo e requer diferentes técnicas (STERN *et al.*, 2009). Vale ressaltar que o roteamento discutido aqui em termos de algoritmos de caminho mais curto é aquele feito de forma dinâmica, em que a rede já está em operação com um número de conexões ativas, e novas conexões estão sendo aprovisionadas sequencialmente.

A comutação de LSPs é comumente referida como o problema de roteamento e atribuição de comprimento de onda (RWA). O problema de RWA é normalmente decomposto em dois subproblemas separados: (1) seleção de rotas e (2) atribuição de comprimento de onda (MAIER, 2008). É importante notar que decompor o problema RWA em dois subproblemas separados é bem suportado para cálculo de LSPs em redes óticas chaveadas por comprimento de onda que empregam conversores de comprimento de onda. Se conversores de comprimento de onda não estão disponíveis, o cálculo de LSPs torna-se sensívelmente mais complexo devido a chamada "restrição de continuidade de comprimento de onda". Essa restrição impõe que um dado LSP deve ser estabelecido usando o mesmo comprimento de onda em todos os enlaces pertencentes ao caminho selecionado. Devido a essa restrição, o problema de cálculo de LSPs não pode ser decomposto em subproblemas de seleção de rota e atribuição de comprimento de onda (MAIER, 2008). Além do caso especial do cálculo de LSPs em redes óticas chaveadas por comprimento de onda, em redes GMPLS as rotas precisam ser calculadas para qualquer ISC. Em geral, o cálculo de rotas é realizado executando um algoritmo de roteamento SPF sobre um grafo ponderado. Esse grafo é construído usando a informação de *link TE* presente no banco de dados de estado de cada LSR (MAIER, 2008).

Protocolos de roteamento de caminho mais curto baseiam-se em algoritmos que utilizam topologia de rede global ou parcial e informações do enlace para calcular uma rota, e elas podem ser calculadas de forma centralizada ou de forma distribuída em cada nó da rede. Em GMPLS, informações de topologia e estado de enlace são originadas do procedimento de descoberta de vizinhos usando o LMP. Algoritmos de roteamento que necessitam de conhecimento global da rede são chamados algoritmos "estado de enlace" porque o estado de todos os enlaces conectados a rede devem ser conhecidos a priori para o cálculo de rotas. O OSPF determina o caminho mais curto usando o algoritmo de *Dijkstra* (STERN *et al.*, 2009).

O OSPF é um protocolo de roteamento estado de enlace distribuído. A palavra *open* indica que o protocolo é aberto ao público e não proprietário (STERN *et al.*, 2009).

Seguem algumas características que de acordo com (STERN *et al.*, 2009) tornam vantajosa a utilização do OSPF:

- Separação lógica da rede em áreas de roteamento hierárquicas para controle e eficiência;
- Resposta rápida a mudanças com baixa sobrecarga;
- Autenticação de atualizações de roteamento.

APÊNDICE B - Sinalização em GMPLS

Um protocolo de sinalização é necessário para aprovisionar, manter, recuperar, e excluir conexões em uma rede. A sinalização GMPLS é um meio para transportar a informação de aprovisionamento (porta escolhida, canal) de um nó para o próximo ao longo do caminho escolhido (STERN *et al.*, 2009).

Para implementar um protocolo de sinalização, uma rede de comunicação de dados (DCN) é necessária para transportar mensagens de sinalização entre os nós da rede. Redes de sinalização podem ou não estar associadas com o plano de dados ótico (STERN *et al.*, 2009).

Depois do cálculo de uma rota apropriada, como visto no item anterior, a sinalização é usada para estabelecer o LSP (MAIER, 2008). Para o estabelecimento do LSP, o protocolo de sinalização se faz necessário também para trocar informações de controle entre os nós, para distribuir rótulos e reservar recursos ao longo do caminho (PALMIERI, 2008). Os protocolos padronizados para sinalização GMPLS adequados para o plano de controle são o RSVP-TE (BERGER, 2003b) e o CR-LDP (*Constraint-Based Routing Label Distribution Protocol*) (ASHWOOD-SMITH; BERGER, 2003). Esses protocolos são usados para configurar os LSPs, e podem ser usados para modificá-los e atualizá-los. Claramente, o suporte ao aprovisionamento e recuperação de LSPs dentro de uma rede fotônica consistindo de elementos de rede heterogêneos impõe novos requisitos para os protocolos de sinalização, como tempo curto de configuração, suporte a LSPs bidirecionais, rápida detecção e notificação de falha, e rápida recuperação do LSP (PALMIERI, 2008).

Sinalização GMPLS provê um número de características vantajosas. Entre outras, permite que um rótulo seja sugerido por um LSR à frente. Embora o rótulo sugerido possa ser sobrescrito por um LSR anterior (MAIER, 2008). Ambos os protocolos RSVP-TE e CR-LDP podem ser usados para reservar um único comprimento de onda para um LSP se o comprimento de onda for conhecido com antecedência. Esses protocolos também podem ser modificados para incorporar funções de seleção de comprimento de onda no processo de reserva (PALMIERI, 2008). No RSVP-TE, mas não no CR-LDP, a mensagem *Notify* foi definida com o objetivo de informar LSRs não adjacentes de falhas relacionadas a LSPs. As mensagens *Notify* podem ser direcionadas a qualquer LSR além do LSR imediatamente posterior ou anterior (MAIER, 2008).

No GMPLS, as mensagens de sinalização podem conter informações tais como requisitos de QoS para o tráfego transportado e requisições de rótulos para atribuí-los em nós intermediários que reservam os recursos apropriados para o caminho (PALMIERI, 2008).

RSVP-TE com melhorias para suporte ao GMPLS

O papel do RSVP em sua versão original foi introduzir mecanismos no transporte IP para executar requisitos de QoS para fluxos de tráfego bem definidos, chamados ”sessões”. Quando estendido para redes óticas e outros tipos de rede operando sob o GMPLS, as propriedades do RSVP são modificadas para adaptar-se aos tipos de conexões encontradas nessas redes e para criar uma clara separação entre os planos de

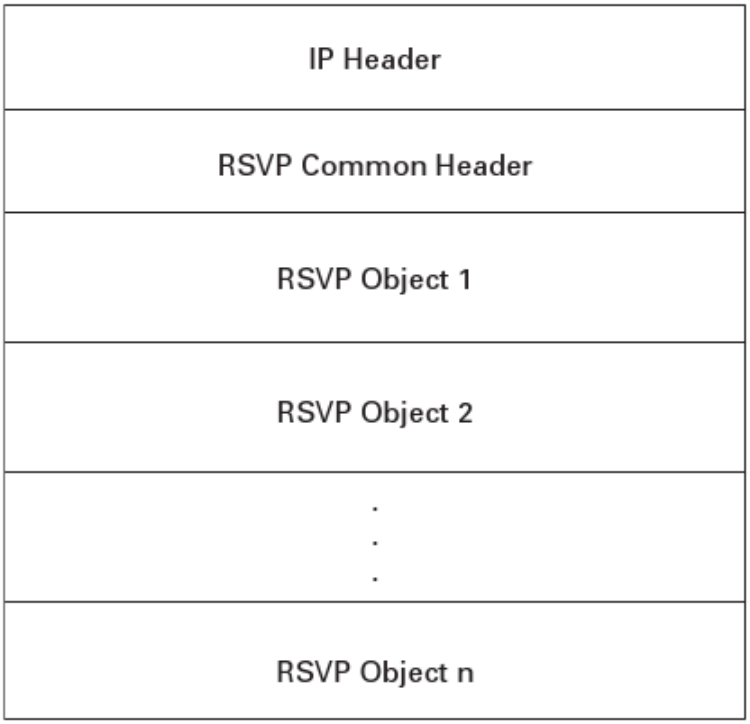
controle e de transporte (STERN *et al.*, 2009).

Existem quatro entidades básicas no RSVP: (1) *sessions* (o fluxo de tráfego), (2) *messages* (a informação de sinalização transportada) (3) *objects* (transportados na carga útil da mensagem), e (4) *states* (armazenados nos roteadores IP) (STERN *et al.*, 2009).

O protocolo RSVP utiliza sete tipos de mensagens: *(1) Path, (2) Resv, (3) PathErr, (4) ResvErr, (5) PathTear, (6) ResvTear, e (7) ResvConf* (STERN *et al.*, 2009).

A Figura 5 mostra o formato de uma mensagem RSVP.

Figura 28: Formato da mensagem RSVP.
(STERN *et al.*, 2009).



No cabeçalho comum RSVP, um campo *message type* identifica o tipo de mensagem. Os principais objetos RSVP são:

1.*Session*: Identifica um fluxo de tráfego;

2.*Sender Template*: Identifica o emissor do fluxo;

3.*Sender Tspec*: Identifica as características do fluxo de tráfego;

4.*Flowspec*: Descreve a requisição de reserva;

5.*Filterspec*: Descreve os pacotes para uma sessão específica que se submeterá à manipulação de QoS específica nos nós no caminho daquela sessão.

A informação carregada nesses objetos é armazenada nos bancos de dados dos roteadores IP na forma de *states Path* e *Resv* para assegurar o processamento apropriado para os pacotes no fluxo de tráfego passando pelo roteador (STERN *et al.*, 2009).

RSVP-TE foi criado para adaptar o RSVP à sistemas envolvendo chaveamento de rótulo. RSVP-TE suporta requisição e atribuição de rótulos para o estabelecimento de LSPs, a especificação de uma rota explícita, da largura de banda e de outras características para um LSP, e a associação de LSPs relacionados (STERN *et al.*, 2009).

De acordo com (STERN *et al.*, 2009), os novos objetos definidos em RSVP-TE para acomodar as novas características descritas acima são:

- *Label object request*: usado para requisitar um rótulo para o túnel LSP sendo configurado.
- *Label object*: O rótulo que foi atribuído em resposta a uma requisição de rótulo é transportado na mensagem *Resv*.
- *Explicit route object*: Transportado na mensagem *Path* durante o estabelecimento do LSP
- *Record route object*: Registro de todos os nós no caminho do nó fonte ao nó destino. Também transportado na mensagem *Path*.
- *Tunnel identification*: Identifica o túnel LSP e seu nó de saída. Transportado no objeto *session*.
- *Session attribute object*: Descreve parâmetros diferentes de QoS para uma sessão. É transportado na mensagem *Path*.

Em RSVP-TE, um protocolo *Hello* é definido entre LSRs vizinhos com o propósito explícito de rapidamente detectar falhas nos nós (AWDUCHE *et al.*, 2001). Se uma mensagem Hello não é recebida em um período de tempo predefinido, então um LSR considera que seu vizinho falhou. Ele pode então realizar a ação apropriada, tal como relatar a falha para a camada de gerenciamento.

Em suma, as principais extensões ao protocolo RSVP-TE para adaptar a sinalização em uma rede ótica tratam da manipulação de muitas tecnologias de base, configuração de rotas para conexões bidirecionais, e a independência entre os planos de controle e de dados (STERN *et al.*, 2009).

Como já foi visto, redes óticas podem acomodar uma variedade de técnicas e tecnologias de chaveamento e multiplexação. Para ser adaptado ao GMPLS, o RSVP-TE deve ser capaz de suportar o conceito de rótulo generalizado para estabelecer LSPs em qualquer camada arquitetural em uma rede (BERGER, 2003a). Pensando nisso, de acordo com (STERN *et al.*, 2009), novos objetos são definidos no GMPLS RSVP-TE como segue:

- *Generalized label request object*: Substitui o *label object request* no RSVP-TE e transporta as seguintes informações: tipo de codificação do LSP, tipo de chaveamento, ID protoclo generalizado (tipo de carga útil), pontos finais fonte e destino, e largura de banda da conexão. É transportado na mensagem *Path*.
- *Generalized label object*: Substitui o *label object* do RSVP-TE. É transportado na mensagem *Resv*.

- *Suggested label object*: Permite que um nó à frente "sugira" para o nó anterior qual rótulo generalizado retonar na fase de resposta para evitar atrasos durante a mesma. Esse objeto é transportado na mensagem *Path*.

- *Upstream label object*: O rótulo selecionado pelo nó à frente para a direção reversa da conexão. É transportado na mensagem *Path* e é usado para conexões bidirecionais.

- *Label set object*: Usado por um nó à frente para controlar a seleção de rótulos pelos nós anteriores a ele. É transportado na mensagem *Path*.

- *Acceptable set object*: Gerado por um nó quando este não pode aceitar um rótulo específico. É transportado em *PathErr, ResvErr* e em mensagens de notificação.

- *Protection information object*: Indica o tipo de proteção em cada enlace no caminho. É transportado na mensagem *Path*.

- *Administrative status object*: usado para sinalizar ações administrativas tais como testar uma conexão.

- *Interface identification object*: Identifica o enlace de dados em que rótulos estão sendo atribuídos.

- *Notification request object*: Indica o endereço para o qual uma notificação de falha deve ser enviada.