UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA

ANTONIO DE CAMPOS SACHS

REDE AUTO-ORGANIZADA UTILIZANDO CHAVEAMENTO DE PACOTES ÓPTICOS

São Paulo
2011

ANTONIO DE CAMPOS SACHS

REDE AUTO-ORGANIZADA UTILIZANDO CHAVEAMENTO DE PACOTES ÓPTICOS

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Doutor em Engenharia

São Paulo

2011

ANTONIO DE CAMPOS SACHS

REDE AUTO-ORGANIZADA UTILIZANDO CHAVEAMENTO DE PACOTES ÓPTICOS

Tese apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Doutor em Engenharia

Área de Concentração: Sistemas Digitais

Orientadora: Profa. Dra. Tereza Cristina Melo de Brito Carvalho

São Paulo

2011

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

São Paulo, 21 de junho de 2011.

Assinatura do autor _____

Assinatura do orientador _____

Sachs, Antonio de Campos.
Rede auto-organizada utilizando chaveamento de pacotes ópticos / A. C. Sachs. -- ed.rev.-- São Paulo, 2011.
190 p.

Tese (Doutorado) – Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Comunicação óptica. 2. Fibras ópticas. 3. Computabilidade e complexidade. I. Universidade de São Paulo. Departamento de Engenharia Elétrica. II. T.

DEDICATÓRIA

Para Maria José e Paulo

AGRADECIMENTOS

Aos colegas do CPqD que juntos comigo durante 26 anos se revezaram trabalhando, aprendendo e descobrindo conteúdos tecnológicos que também fazem parte desta tese.

À Profa. Dra. Tereza Cristina Melo de Brito Carvalho pela orientação e grande apoio despendido desde o início deste trabalho.

Aos colegas, professores e funcionários do LARC (Laboratório de Arquitetura e Redes de Computadores) do PCS (Departamento de Engenharia de Computação e Sistemas Digitais) da EPUSP (Escola Politécnica da Universidade de São Paulo) pelas proveitosas discussões e pelo apoio incondicional durante todo o desenvolvimento do trabalho.

Aos Profs. Antonio Sandro Verri, José Kleber da Cunha Pinto e demais professores e funcionários do LME (Laboratório de Microeletrônica) do PSI (Departamento de Engenharia de Sistemas Eletrônicos) da EPUSP, pelas contribuições e por colocarem à disposição equipamentos e laboratórios para caracterização do protótipo de chave óptica rápida.

Aos professores do LTA (Laboratório de Linguagem e Técnicas Adaptativas) do PCS da EPUSP, Prof. Dr. João José Neto e Prof. Dr. Ricardo Luis de Azevedo da Rocha pelas sugestões, e apoio durante o desenvolvimento do trabalho.

Ao colega Lucas Pauli Simões pelo especial auxílio com as simulações, parte fundamental para validação do modelo analítico apresentado na tese.

Ao colega Carlos Magno Baptista Lopes pelas valorosas discussões que serviram de estímulo para continuidade do trabalho.

Aos membros da banca de qualificação Prof. Dr. José Roberto Amazonas, Profa. Dra. Regina Melo Silveira e Profa. Dra. Tereza Cristina Melo de Brito Carvalho pelas valorosas contribuições e pelo direcionamento que deram a esta tese.

Aos amigos da empresa Optolink pelas idéias e contribuições inseridas no protótipo de chave óptica rápida.

À Fundação de Amparo à Pesquisa do Estado de São Paulo, pelo apoio financeiro para a montagem de um protótipo de chave óptica rápida no projeto KyaTera.

RESUMO

A tecnologia de chaveamento de pacotes ópticos comumente utiliza componentes muito complexos, relegando sua viabilidade para o futuro. A utilização de pacotes ópticos, entretanto, é uma boa opção para melhorar a granularidade dos enlaces ópticos, bem como para tornar os processos de distribuição de banda muito mais eficientes e flexíveis. Esta tese propõe simplificações nas chaves ópticas que além de tornarem o pacote óptico viável para um futuro mais próximo, permitem montar redes ópticas complexas, com muitos nós, que operam de maneira auto-organizada. A rede proposta nesta tese não possui sinalização para reserva ou estabelecimento de caminho. As rotas são definidas pacote a pacote, em tempo real, durante o seu percurso, utilizando roteamento por deflexão. Com funções muito simples realizadas localmente, a rede ganha características desejáveis como: alta escalabilidade e eficiente sistema de proteção de enlace. Estas características desejáveis são tratadas como funções da rede que emergem de funções realizadas em cada um dos nós de rede individualmente. A tese apresenta um modelo analítico estatístico, validado por simulação, para caracterização da rede. No sistema de proteção contra falhas, os cálculos realizados para redes com até 256 nós mostram que o aumento do número médio de saltos ocorre apenas para destinos localizados no entorno da falha. Para demonstrar a viabilidade de construção de chave óptica rápida simplificada utilizando somente componentes já disponíveis no mercado foi montado um protótipo, que mostrou ter um tempo de chaveamento inferior a dois nanossegundos, sendo compatível com as operações de chaveamento de pacotes ópticos.

Palavras Chave: complexidade, auto-organização, redes ópticas, chaveamento de pacotes ópticos, escalabilidade.

ABSTRACT

The Optical Packet Switching (OPS) technology usually involves complex and expensive components relegating its application viability to the future. Nevertheless the OPS utilization is a good option for improving the granularity at high bit rate transmissions, as well as for operation involving flexibility and fast bandwidth distribution. This thesis proposes simplifications on optical switching devices that besides getting closer future viability enable the deployment of highly scalable and self-organized complex network architecture. The proposed network operates without resources reservation or previous path establishment. The routes are defined packet-by-packet in a real time deflection routing procedure. With simple local functions the network starts to operate with desirable performance characteristics such as high scalability and automatic protection system. Those desirable performance characteristics are treated as Emerging Functions. For the network characterization it is presented a statistical analytical model validated by simulation. In the automatic protection functions investigation the results for a 256 nodes network showed that the mean number of hops enhancement occurs only around the failure neighborhood. To demonstrate the switch viability, a prototype was fabricated utilizing components already available in the market. The switching time obtained was below two nanoseconds showing compatibility with the optical packet switching technology.

Keywords**:** complexity, self-organization, optical network, optical packet switching, scalability.

LISTA DE ABREVIATURAS

3G	Terceira Geração de Telefonia Móvel
3R	*Re-amplification, Re-shaping, Re-timing* (Recuperação da Amplitude, Formato e Relógio)
ACTS	*Advanced Communications Technologies and Services* (Tecnologias de Comunicações e Serviços Avançados)
AD	*Add and Drop* (Inserção e Derivação)
ADD-DROP	*Add and Drop* (Inserção e Derivação)
APC	*Angle Physical Contact* (Contato Físico em Ângulo)
ASIC	*Application-Specific Integrated Circuit* (Circuito Integrado para Aplicações Específicas)
ATM	*Asynchronous Transfer Mode* (Modo de Transmissão Assíncrono)
ATM-PON	*ATM-Passive Optical Network* (Rede Óptica Passiva com ATM)
BNC	*Bayonet Neill-Concelman Connector* (Conector Neill-Concelman tipo Baioneta)
BS	*Broadcast-and-Select* (Espalha e Seleciona)
bps	bit/s (bites por segundo)

BUONA	*Bottom-Up Organized Network Architecture* (Arquitetura de Rede Organizada de Baixo Para Cima)
CAPEX	*Capital Expenditure* (Custo de Investimento)
DAVID	*Data And Voice Integration over DWDM* (Integração de Dados e Voz sobre DWDM)
DIO	Distribuidor Interno Óptico
DLF	*Delay Line Fiber* (Fibra de Retardo)
DLV	*Digital Low Voltage* (Sistema Digital de Baixa Voltagem)
DWDM	*Dense Wavelength Division Multiplexing* (Multiplexação por Comprimento de Onda Denso)
EDFA	*Erbium Doped Fiber Amplifier* (Amplificador a Fibra Dopada com Érbio)
EPON	*Ethernet Passive Óptical Network* (Rede Óptica Passiva com Ethernet)
FILO	*First In Last Out* (Primeiro que Chega é o Último Que Sai)
FP7	*Seventh Framework Program* (Sétimo Programa Quadro)
FPGA	*Field-Programmable Gate Array* (Arranjo de Transistores, Programável em Campo)
FTTH	*Fiber To The Home* (Fibra até a Casa)
Gbps	*Gb/s* (Gigabit por Segundo)

GEth	*Gigabit Ethernet*
GLIF	*Global Lambda Integrated Facility* (Infraestrutura para Integração Global de Comprimentos de Onda)
GMPLS	*Generalized Multi-Protocol Label Switching* (Generalização do Chaveamento por Troca de Etiqueta no transporte de Múltiplos Protocolos)
G-PON	*Gigabit Passive Optical Network* (Rede Óptica Passiva de Gigabites)
GSa/s	*Giga Samples per second* (Um Bilhão de Amostras por segundo)
HORNET	*Hybrid Opto-electronic Ring Network* (Rede Optoeletrônica Híbrida em Anel)
ICT	*Information and Communication Technologies* (Tecnologias de Informação e Comunicação)
IETF	*Internet Engineering Task Force* (Força Tarefa de Engenharia da Internet)
IMOC	*International Microwave and Optoelectronics Conference* (Conferência Internacional de Microondas e Optoeletrônica)
InGaAsP	Índio, Gálio, Arsênio e Fósforo
InP	Fosfeto de Índio
INPI	Instituto Nacional de Propriedade Industrial

IP	*Internet Protocol* (Protocolo da Internet)
IST	*Information Society Technologies* (Tecnologias da Sociedade da Informação)
ITU	*International Telecommunication Union* (União Internacional para Telecomunicação)
ITU-T	*Telecommunication Standardization Sector of ITU* (Setor de Padronização em Telecomunicações do ITU)
KEOPS	*Keys to Optical Packet Switching* (Princípos para o Chaveamento de Pacotes Ópticos)
LCD	*Liquid Cristal Display* (Tela de Cristal Líquido)
MEMS	*Micro Electro-Mechanical System* (Sistema Eletro-Mecânico Micrométrico)
MPLS	*Multi Protocol Label Switching* (Chaveamento por Troca de Etiqueta no transporte de Múltiplos Protocolos)
NFOEC	*National Fiber Optic Engeneers Conference* (Conferência Nacional de Engenheiros de Fibra Óptica)
NP	*Non-deterministic Polynomial* (Polinomial Não Determinístico)
NUDESA	NÚmero DE SAltos
OBS	*Optical Burst Switching* (Chaveamento de Rajadas de Pacotes Ópticos)
OCDM	*Optical Code Division Multiplexing* (Multiplexação Óptica

por Divisão de Código)

OCDMA *Optical Code Division Multiple Access* (Múltiplo Acesso Óptico por Divisão de Código)

OFC *Optical Fiber Communication Conference* (Conferência de Comunicações por Fibras Ópticas)

OMEGA *Optical Metro network for Emerging Gigabit Applications* (Rede Óptica metropolitana para aplicações emergentes de Gigabites por segundo)

OPEX *OPerational EXpenditures* (Despesas com Operação)

OPS *Optical Packet Switching* (Chaveamento de Pacotes Ópticos)

OSI *Open Systems Interconnection* (Interconexão de Sistemas Abertos)

OXC *Optical Cross Connect* (Conexão Cruzada Óptica)

PB *Peta Bytes* (Um quatrilhão de Bytes)

PCF *Photonic Cristal Fiber* (Fibra de Cristais Fotônicos)

PhC *Photonic Cristal* (Cristais Fotônicos)

PON *Passive Optical Network* (Rede Óptica Passiva)

RF *Radio Frequency* (Freqüência de Rádio)

RFC *Request For Comment* (Requisição para Comentário)

SDH *Synchronous Digital Hierarchy* (Hierarquia Digital

	Síncrona)
SERDES	*Serializer/Deserializer* (Serializador/Desserializador)
SFP	*Small Form-factor Pluggable* (Formato de Pequena Escala Plugável)
SMA	*SubMiniature version A* (Sub-miniatura versão A)
SOA	*Semiconductor Optical Amplifier* (Amplificador Óptico de Semicondutor)
SPINet	*Scalable Photonic Integrated Network* (Rede Fotônica Integrada com escalabilidade)
Tbps	Tb/s (Terabites por segundo)
TCP	*Transmission Control Protocol* (Protocolo de Controle de Transmissão)
TEC	*Thermo Electric Cooler* (Resfriador termo-elétrico)
TTL	*Time-To-Live* (Tempo de Vida)
WDM	*Wavelength Division Multiplexing* (Multiplexação por Divisão de Comprimentos de Onda)
WDM-PON	*WDM-Passive Optical Network* (Rede Óptica Passiva com Multiplexação por Divisão de Comprimentos de Onda)

LISTA DE FIGURAS E TABELAS

Figura 1: Esquema de chaveamento de comprimento de onda (ROCHA, 2003)..... 11

Figura 2: GLIF_Leste da América do Norte. Fonte: (GLIF, 2008)..... 12

Figura 3: GLIF_América do Sul. Fonte: (GLIF, 2008)..... 13

Figura 4: Arquitetura de chave óptica rápida do projeto KEOPS que utiliza conceito de BS (*Broadcast-and-Select*)..... 18

Figura 5: Arquitetura de chave óptica rápida do projeto DAVID 20

Figura 6: Cristal fotônico (PhC – *Photonic Cristal*) sobre InGaAsP (SHINYA, 2008). 24

Figura 7: Dispositivo utilizando PhC que pode ser estabilizada no estado "1" ou "0" conforme estímulos ópticos (SHINYA, 2008)..... 25

Figura 8: Principais funções presentes em uma chave de pacotes ópticos..... 33

Figura 9: Exemplo de uma arquitetura de chave óptica e de funções usualmente utilizadas para o processo de chaveamento de pacotes ópticos. 34

Figura 10: Dados OVUM dos enlaces DWDM: capacidade(Gbps); tráfego IP (PB/mês) e custo (US$/Gbps/km)..... 36

Figura 11: Esquema de deflexão de pacotes sem armazenamento óptico. Quebra do paradigma *"Store-And-Forward"*..... 40

Figura 12: Esquema de inserção sem colisão..... 41

Figura 13: Esquema de sinalização localizada. 52

Figura 14: Rede do tipo *Manhattan Street* com 16 nós..... 54

Figura 15: Rede do tipo *Manhattan Street* com 16 nós - Topologia Resultante depois da falha de um enlace horizontal (tipo "rua") 54

Figura 16: Mapa de Manhattan com ruas horizontais e avenidas verticais. Fonte: GoogleMaps (GOOGLE, 2008) 55

Figura 17: Numeração de portas da rede *Manhattan Street* por quarteirão..... 56

Figura 18: Montagem da matriz de conexão ***c*** para rede de 4 nós. 61

Figura 19: Árvore adaptativa para cálculo da matriz de caminhos preferenciais..... 63

Figura 20: Tempo para calcular o caminho mais curto em função do número de nós de rede 64

Figura 21: Cálculo da probabilidade de ocupação *Poc* 68

Figura 22: Topologia *Manhattan Street* com 9 nós..... 73

Figura 23: Número médio de saltos em função da carga no enlace. Comparação entre modelos analíticos (curvas contínuas) e simulação (pontos com barras de erro) 78

Figura 24: Número médio de saltos em função da carga para rede *Manhattan Street* com N nós. 79

Figura 25: Mapa do número médio de saltos para 256 destinos dispostos em 16 linhas e 16 colunas. 81

Figura 26: Número médio de saltos com ou sem falha. 84

Figura 27: Aumento relativo do número de saltos depois da falha em função do número de nós..... 84

Figura 28: Número médio de saltos com falha, sem falha e com aviso de falha ao vizinho mais próximo. 86

Figura 29: Segregação dos efeitos da falha 88

Figura 30: Rede NFSNET utilizada como referência para protocolos de roteamento. Fonte: (NFSNET, 2008)..... 91

Figura 31: Adaptação em Huston e Pittsburgh da rede NFSNET. Um único nó, com 4 enlaces bidirecionais, pode ser representado por 4 chaves 2x2..... 91

Figura 32: Rede NFSNET com 42 nós que utilizam apenas chaves 2x2. 92

Figura 33: Rede NFSNET com indicação dos números das portas de cada nó de rede..... 94

Figura 34: Tabelas de portas preferenciais em primeira opção (a) e segunda opção (b). 95

Figura 35: Rede NFSNET com 14 nós 2x2, 3x3 e 4x4 comparada com rede MS com 16 nós 2x2..... 96

Figura 36: Dispositivo SOA montado na placa de teste do fabricante. Figura retirada do manual de operação (INPHENIX). 100

Figura 37: Protótipo montado com os módulos Fonte, Controle, SOA, Acoplador, Conversor de Mídia e Transceiver, mostrados respectivamente da esquerda para a direita. 103

Figura 38: Montagem mecânica em caixa de 19 polegadas e placa do SOA com transistores de chaveamento BFG35. 106

Figura 39: Parâmetros do dispositivo SOA, modelo IPSAD1302 de fabricação INPHENIX, utilizado no protótipo (Tradução do manual de operação). 107

Figura 40: *Transceiver* 1000Base-LX 10G comercializado pela ZyXEL. Figura disponibilizada em: http://www.zyxelguard.com/SFP-LX-10.asp Obtida em: 31 de agosto de 2010..... 110

Figura 41: Bancada para caracterização do protótipo 110

Figura 42: Caracterização do tempo de resposta do transceiver 111

Figura 43: Sinais elétricos utilizados na caracterização. 112

Figura 44: Avaliação do tempo de resposta do fotodetector. 112

Figura 45: Caracterização do tempo de resposta da chave óptica rápida. 113

Figura 46: Avaliação do tempo de resposta da chave óptica rápida..... 114

Figura 47: Tempo de resposta de Chaves ópticas MEMS (MURAKAMI, 2005). Chaves ópticas regulares (não rápidas) disponíveis no mercado..... 114

Figura 48: Tempos de resposta típicos dependendo da aplicação e da tecnologia (BUCHTA; GAUGER, 2008). 115

Figura 49: Chave 1x1: Liga-Desliga (Arquitetura 1) 118

Figura 50: Chave 1x2: Bifurcação (Arquitetura 2) 119

Figura 51: Chave 1x2 com dois SOAs e quatro acopladores (Arquitetura 3) 120

Figura 52: Chave 2x2 com quatro SOAs e seis acopladores (Arquitetura 4)..... 121

Figura 53: Chave 2x2 com seis SOAs e seis acopladores (Arquitetura 5) 122

Figura 54: Chave 2x2 com 4 SOAs e 8 acopladores (Arquitetura 6). 123

Figura 55: Arquitetura auxiliar para arrumar a distribuição de pacotes na rede 124

Figura 56: Chave 2x2 com processo interferométrico 126

SUMÁRIO

1 Introdução 1

1.1 Motivação 2

1.1.1 Granularidade fina 3

1.1.2 Transparência 4

1.1.3 Funcionamento autônomo e auto-organização 5

1.2 Objetivo e Escopo 6

1.3 Organização da Tese 7

2 Visão Geral da Área de Redes Ópticas 8

2.1 Enlaces WDM 9

2.2 Chaveamento de Comprimento de Onda 10

2.3 Redes Ópticas Passivas 13

2.4 Chaveamento de Pacotes Ópticos 15

2.4.1 Projeto KEOPS 16

2.4.2 Projeto DAVID 19

2.4.3 Projeto HORNET 20

2.4.4 Projeto CPqD/Ericsson 21

2.4.5 Chaveamento de Pacotes em Rajadas (OBS) 21

2.4.6 Novos Componentes para Chaveamento de Pacotes Ópticos 22

2.5 O Estado da Arte e Algumas Considerações 25

2.5.1 Desafios da Área 26

2.5.2 Proposta de Trabalho 27

3 Os problemas de Complexidade da Rede e das Chaves Ópticas 28

3.1 Banda passante, Granularidade e Agilidade de Comutação..... 28

3.2 Escalabilidade e Complexidade Computacional..... 29

3.3 Complexidade das Chaves de Pacotes Ópticos..... 32

3.4 Considerações Finais sobre o Problema..... 35

4 Eliminação da Complexidade da Chave e Tratamento da Rede Como Um Sistema Complexo 38

4.1 Chaves Ópticas Simplificadas 39

4.2 Rede Auto-Organizada (Rede BUONA) 42

4.2.1 Funções Emergentes..... 44

4.2.2 Redes Complexas 47

4.2.2.1 Endereçamento Hierárquico 48

4.2.2.2 Auto-Organização 48

4.2.2.3 Robustez. 49

4.3 Proteção e Restauração de Enlace 50

4.3.1 Sinalização Localizada 51

4.3.2 Sistema de Organização por Ruas e Avenidas..... 52

4.3.3 Sistema de Organização por Quarteirão 55

4.4 Considerações sobre a Proposta de Solução 57

5 Modelagem e Validação da Proposta 58

5.1 Modelo Analítico..... 59

5.1.1 Cálculo da Matriz de Topologia (Matriz de Conexão) 60

5.1.2 Cálculo do Caminho Mais Curto (Árvore Adaptativa)..... 61

5.1.3 Cálculo do Número Médio de Saltos 64

5.1.3.1 Fundamentação 65

5.1.3.2 Probabilidade das Portas Preferenciais (Ppp) 66

5.1.3.3 Probabilidade de Ocupação (Poc) 68

5.1.3.4 Probabilidade de Pacote Local (Ppl) 69

5.1.3.5 Probabilidade de Outra Porta (Pop) 70

5.1.3.6 Montagem do Operador de Probabilidades Condicionais 70

5.1.3.7 Algoritmo NUDESA 71

5.2 Simulação 75

5.3 Resultados e Considerações Sobre a Modelagem 78

5.4 Robustez da Rede 82

5.4.1 Proteção para Redes de Muitos Nós 83

5.4.2 Sinalização de Falha para os Vizinhos mais Próximos 85

5.4.3 Segregação dos Efeitos da Falha 87

5.5 Vazão e Atraso 88

5.6 Generalização 90

5.6.1 Generalização para Nós Simétricos 3x3 e 4x4 93

5.6.2 Resultados e Considerações sobre a Generalização 95

5.7 Considerações sobre a Validação 97

6 Viabilidade e Construção Experimental 98

6.1 Chaves Utilizando SOA 98

6.2 Protótipo de Chave Óptica Rápida 102

6.2.1 Módulo Fonte 104

6.2.2 Módulo de Controle 104

6.2.3 Módulo SOA 105

6.2.4 Módulo Acoplador 108

6.2.5 Módulo Conversor de Mídia (Gigabit Ethernet) 108

6.2.6 Módulo *Transceiver* 109

6.2.7 Caracterização do Protótipo 110

6.2.8 Considerações sobre o Protótipo 115

6.3 Possíveis Arquiteturas e Suas Características 116

6.3.1 Arquitetura 1: Liga-Desliga 117

6.3.2 Arquitetura 2: Bifurcação 118

6.3.3 Arquitetura 3: Bifurcação Melhorada 119

6.3.4 Arquitetura 4: Chave 2x2 120

6.3.5 Arquitetura 5: Chave 2x2 com 6 SOAs 121

6.3.6 Arquitetura 6: Chave 2x2 com 8 SOAs 122

6.3.6.1 Saturação da Carga 123

6.3.7 Chaves Utilizando Processos Interferométricos 125

6.3.8 Regeneradores e Apagadores de Pacotes. 127

6.4 Considerações Finais sobre A Viabilidade 128

7 Considerações Finais 129

7.1 Análise Crítica dos Resultados 129

7.2 Principais Contribuições e Inovações. 132

7.3 Trabalhos Futuros 133

7.3.1 Sincronismo 133

7.3.2 Capacidade de Armazenamento da Rede 134

7.3.3 Valor Médio e Desvio Padrão 135

7.3.4 Chaveamento de Lotes de Pacotes 136

7.3.5 Aproveitamento de Situações do Tipo “tanto-faz” 137

7.3.6 Necessidade da Transparência 138

REFERÊNCIAS 140

ANEXO 155

1 Introdução

O tráfego de informação tem aumentado extraordinariamente nos últimos anos e para atender esta crescente demanda é necessário um contínuo desenvolvimento tecnológico com uma contínua criação de novos serviços. A Internet apresenta-se como uma rede que propicia um fluxo de informação sem precedentes, gerando a quebra de paradigmas e substituição de modelos de negócio. Para acompanhar, e ao mesmo tempo para viabilizar o aumento de tráfego de informação, a evolução tecnológica, além de propiciar maior desempenho e criar novos serviços, precisa também considerar a redução de custo.

Os sistemas de comunicações ópticas destacam-se pela grande oferta de banda permitindo transmissão digital com taxas de bit que superam 50 Tbps[1] em uma única fibra óptica (SANO, 2010). Roteadores ópticos (OXC - *Optical Cross Connect*) conferem, a entroncamentos de rede, capacidade de roteamento (CANNONS, 2006) aparentemente sem limites. Entretanto, o custo destes sistemas sempre foi considerado elevado (ZUE, 2003), e sua implantação somente se justifica quando o valor do serviço é rateado por um número muito grande de usuários. Novas tecnologias podem permanecer muito tempo aguardando demandas de serviços que possam alavancar o seu desenvolvimento. Muitas vezes, tecnologias inovadoras são adotadas apenas em redes de longa distância, que carregam tráfego agregado, conseguindo baixar o custo final pago pelos usuários individualmente.

O chaveamento de pacotes ópticos (OPS) é um processo considerado muito caro. Utiliza componentes específicos, de alto custo, ainda não disponíveis no mercado. Nestas condições, é necessário considerar que o produto final possa tratar grande

---

[1]Tbps é abreviação para um Terabit por segundo, sendo que um Terabit corresponde a um trilhão de bits (1 Tbps = 1 x 10^{12} bits por segundo).

quantidade de tráfego agregado para justificar os custos de sua pesquisa e implantação. Contrariamente, este trabalho propõe uma versão bastante simplificada de OPS, que diminui os custos e se torna adequada para aplicações em escala metropolitana, ou escala de rede de acesso. Redes nestas escalas, devido às suas características de proximidade aos usuários finais, operam em condição de tráfego pouco agregado.

Redes como estas, com muitos recursos e baixo custo de implantação e operação, podem estimular novos serviços mesmo antes do aparecimento da demanda.

1.1 Motivação

Podem ser utilizadas para motivar trabalhos sobre pacotes ópticos vantagens do tipo: drástica redução da latência (caso das redes de acesso); baixo consumo de energia (sustentabilidade); baixo custo de instalação e manutenção (economia). Entretanto, a principal motivação para este trabalho foram a granularidade fina e transparência que caracterizam todo tipo de rede de pacotes ópticos.

Outro aspecto motivador, muito importante neste trabalho, é a possibilidade de estudar redes com nós autônomos com perspectiva de se obter uma rede auto-organizada.

A granularidade fina, a transparência e a rede auto-organizada estão apresentadas nas subseções a seguir.

1.1.1 Granularidade fina

O termo “granularidade” (GHOBRIL, 2003) é utilizado como uma característica atribuída às redes de comunicação. Redes de granularidade fina são redes que permitem entregar um fluxo com taxa de bit adequadamente baixa para o usuário final. Por outro lado, rede de granularidade grossa, indica que a menor taxa de bit da rede é muito grande para ser entregue diretamente ao usuário final. No caso de granularidade grossa é necessário utilizar tecnologia auxiliar para baixar a taxa de bit até o nível do usuário final. O que se considera alta taxa ou baixa taxa depende do usuário final e também do momento de evolução tecnológica da rede como um todo. Se um determinado usuário, nas condições de desenvolvimento tecnológico que se encontra, aceita taxas de até 1 Gbps (Ex: Gigabit Ethernet), então, redes que entregam serviços com taxa muito acima deste valor têm granularidade grosseira. Toda rede com chaveamento de pacotes, incluindo o chaveamento de pacotes ópticos, pode utilizar alta taxa de bit no processo de transmissão e, ao mesmo tempo, carregar pacotes de diferentes usuários. A taxa de bit de cada usuário é controlada pela freqüência com que o pacote deste usuário aparece no fluxo total transmitido. Por exemplo, uma transmissão na taxa de 40 Gbps pode transportar dados de 40 usuários que operam na taxa de 1 Gbps, sendo que o pacote de cada usuário aparece em média uma vez em cada lote de 40 pacotes do fluxo total transmitido. É necessário ressalvar que no caso de granularidade fina cada pacote de usuário trafega na rede com alta taxa de bit (p. ex: 40 Gbps; 100 Gbps) e para a entrega final existe a necessidade de redução da taxa de transmissão para compatibilidade com o meio físico do usuário (p. ex: 1 Gbps). A granularidade fina das redes de pacotes não existe nas redes WDM (*Wavelength Division Multiplexing*), em que cada comprimento de onda tem capacidade tão alta quanto 10 Gbps, 40 Gbps, ou até 100Gbps. Um sistema WDM requer tecnologia auxiliar para separar tributários menores contidos dentro de um único comprimento de onda.

Cada comprimento de onda de um sistema WDM pode ser composto por pacotes ópticos de vários usuários, melhorando a granularidade oferecida pela tecnologia.

Por causa desta flexibilidade de transporte de pacotes de vários usuários em diferentes intervalos de tempo, toda rede baseada em chaveamento de pacote tem granularidade fina. Pode-se dizer que as redes multiplexadas, que utilizam o meio elétrico no processo de multiplexação, também têm granularidade fina, mas não sendo transparente, como descrito na próxima seção, pode introduzir atrasos devido ao processo de conversão do sinal do meio óptico para o meio elétrico.

1.1.2 Transparência

Os pacotes são denominados de “pacotes ópticos” quando não são convertidos do meio óptico para o meio elétrico durante o processo de chaveamento. Esta definição exclui os pacote IP que trafegam em um meio óptico mas precisam ser convertidos para o meio elétrico em um *switch* ou em um roteador. Distingue-se também a expressão "rede de pacotes ópticos", que trata pacotes ópticos chaveados sem conversão eletroóptica, da expressão "rede óptica de pacotes", que pode ser utilizada, por exemplo, para se referir a uma rede IP sobre WDM. Com a não conversão de meio físico de transmissão o pacote pode conter diferentes taxas de transmissão ou diferentes pilhas de protocolos que podem passar pelo processo de chaveamento de maneira transparente. Existe transparência (FISHMAN, 2008) quando o sistema deixa passar informações em um ou mais formatos. Por exemplo, dizemos que uma rede óptica é transparente à taxa de bit, dentro de um determinado intervalo de valores, quando permite o uso de qualquer taxa de bit pertencente ao intervalo especificado. O sistema é transparente a protocolos, quando pode ser utilizado para qualquer dos protocolos especificados.

Para as chaves ópticas, não importa quais protocolos estão sendo transportados no interior dos pacotes. Qualquer protocolo ou taxa de bit passa pela chave de maneira transparente. Na condição de transparência, as pilhas de protocolos não precisam ser abertas, tornando mais rápidos os processos de chaveamento. A transparência também é responsável pela redução do espaço físico e do consumo de energia necessários no processo de chaveamento.

1.1.3 Funcionamento autônomo e auto-organização

Esta motivação decorre da possibilidade de se obter uma rede auto-organizada formada por chaves simples e autônomas. Esta característica pode ser usada para resolver problemas ligados à operação de grandes redes, incluindo não somente redes que abrangem grandes áreas, mas principalmente redes com um número muito grande de entroncamentos. O número de roteadores de um domínio, para que não haja problema de convergência nos algoritmos de roteamento, bem como o número máximo de entroncamentos nas redes G-PON (*Gigabit Passive Optical Network*), são limites que podem ser ampliados com adoção de redes auto-organizadas. Em redes com muitos nós, o processo de roteamento é complexo. Exige não apenas sofisticados algoritmos, como também, exige mais banda para suportar o tráfego dos pacotes de sinalização e de controle. As redes auto-organizadas permitem aumentar o número de nós, sem alterar os processos de roteamento e o dimensionamento dos roteadores.

É possível montar um ambiente composto por muitos nós, e projetar o seu funcionamento sem que haja um controle externo. A organização do sistema acontece de baixo para cima. São as chamadas organizações *bottom-up* (Seção 4.2), compostas por funções elementares realizadas localmente. Do conjunto de funções elementares emergem funções atribuídas ao sistema. Liberado destas

funções de controle de tráfego, o gerenciamento pode ser simplificado e os custos de operação e manutenção da rede (OPEX – *OPerational EXpenditures*) podem ser reduzidos.

A perspectiva de que os pacotes ópticos sejam utilizados em grande escala, em um futuro próximo, cria a necessidade de novos projetos de pesquisa. Também, ao se adotar uma rede auto-organizada, opção ainda pouco amadurecida, inicia-se uma aplicação que requer estudos em áreas específicas como inteligência artificial, interação homem-máquina ou robótica.

1.2 Objetivo e Escopo

O objetivo do trabalho é demonstrar a viabilidade do desenvolvimento de redes de comunicação com chaveamento de pacotes ópticos, caracterizada pela escalabilidade (Seção 3.2) do número de nós. A rede proposta para atender estas características possui nós de rede bastante simplificados e autônomos. Esta autonomia faz com que a rede seja auto-organizada e o número de nós escalável. A validação da proposta passa pela montagem de um modelo analítico e por simulação. Para demonstrar a viabilidade de implementação de uma chave óptica rápida, com custo relativamente baixo, o escopo inclui a montagem de um protótipo de chave óptica rápida 2x2, com tempo de chaveamento da ordem de poucos nanossegundos.

Fazem parte do escopo a análise de diferentes topologias e diferentes funções emergentes (Seção 4.2.1) como, por exemplo, a distribuição de tráfego ou a sistemática de proteção de enlace (Seção 4.3).

Para que o escopo seja bem definido é importante listar alguns temas que não fazem parte desta tese. Assim, não faz parte do escopo trabalhos considerados complementares como: investigar técnicas de recuperação de relógio; investigar componentes ópticos para chaveamento rápido; investigar a resposta da rede para outros modelos e outros tipos de tráfego; investigar adaptação da rede para que possa operar em conjunto com redes TCP/IP; investigar a inserção da rede nos protocolos de sistemas GMPLS; investigar novas funções emergentes que possam ampliar as características funcionais ou de desempenho da rede; avaliar a inserção de armazenamento óptico e a inserção de conversão de comprimento de onda em alguns pontos da rede.

1.3 Organização da Tese

A Introdução (Capítulo 1) inclui a apresentação da motivação, dos objetivos e do escopo desta tese. O Capítulo 2 apresenta uma visão geral e o estado da arte da área de redes ópticas. O Capítulo 3 apresenta a descrição do problema, ou de carências tecnológicas para as quais esta tese propõe uma solução ou contribuições inovadoras. No Capítulo 4, a simplificação das chaves ópticas e o tratamento da rede como um sistema complexo são apresentados como proposta de solução. O Capítulo 5 descreve o processo utilizado para validar a proposta, incluindo modelo analítico, simulação, sistema de proteção e generalização para outras topologias. O Capítulo 6 descreve a montagem de um protótipo de chave óptica rápida e uma série de arquiteturas de chave que se pode montar utilizando o protótipo modular. O Capítulo 7 apresenta uma análise crítica e considerações finais.

Seguem, no final, as referências bibliográficas utilizadas e os anexos contendo alguns códigos.

2 Visão Geral da Área de Redes Ópticas

A fibra óptica é um elemento fundamental para promover o aumento de capacidade de transmissão de informação. Sua importância foi corroborada pela atribuição do prêmio Nobel de Física de 2009 a Charles K. Kao, por seu trabalho precursor na obtenção das fibras de baixa atenuação utilizadas nos sistemas de comunicações. O texto em referência (ROYAL SWEDISH ACADEMY OF SCIENCE, 2009) que descreve os fundamentos científicos relativos ao Prêmio Nobel de Física de 2009 na sua primeira parte apresenta um bom resumo dos conceitos envolvidos na tecnologia de fabricação das fibras ópticas.

Desde suas primeiras instalações na década de 70, as tecnologias de comunicações ópticas evoluíram muito. Hoje, não se pode imaginar o mundo sem as redes de longa distância interligando continentes por meio de cabos ópticos submarinos. Entretanto, depois de 40 anos, ainda existe muito desenvolvimento por realizar. A capacidade de transmissão em uma única fibra óptica ainda não está esgotada, e a sua utilização aumenta continuamente para atender a uma crescente demanda por banda passante.

A maior parte das tecnologias disponíveis no mercado segue recomendações do ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*)[2]. As recomendações sobre comunicações ópticas podem ser encontradas principalmente na série G, sendo importante acompanhar também as recomendações da série Y que trata, especificamente, de tecnologias ligadas ao

---

[2] Quase todas as recomendações ITU-T estão disponíveis gratuitamente na internet; http://www.itu.int/pub/T-REC

protocolo IP (*Internet Protocol*). Muitas destas recomendações seguem estudos realizados pelo IETF (*Internet Engineering Task Force*)[3].

Há muita tecnologia, em fase de desenvolvimento, que ainda não consta das recomendações ou dos rascunhos do IETF. É nesta área, ainda em desenvolvimento, que se enquadra o presente trabalho.

2.1 Enlaces WDM

As redes ópticas são compostas por enlaces ópticos. Trabalhar ou aperfeiçoar os enlaces não faz parte desta tese, mas é importante apresentar um exemplo de enlace WDM (*Wavelength Division Multiplexing*) para ilustrar o estado da arte e a capacidade de transmissão que uma rede óptica pode atingir.

Uma única fibra óptica tem potencial para altas taxas de transmissão. Considerando a região de comprimentos de onda entre 1270 nm e 1670 nm, região esta onde a fibra tem atenuação menor do que 0,5 dB/km, existem disponíveis 57 THz de banda passante. Considerando os comprimentos de onda da janela de 800 nm, a banda passante disponível supera 60 THz. Com eficiência espectral de 1 bit/s/Hz e 60 THz de banda passante se consegue transmitir na taxa de 60 Tbps. Com o dobro da eficiência espectral (2 bit/s/Hz) pode-se chegar a 120 Tbps em uma única fibra óptica. Pode-se modular um único comprimento de onda, mas seria muito difícil aproveitar toda banda desta maneira. Com mais facilidade, podem-se modular vários comprimentos de onda com tráfegos de dados independentes em cada um desses

---

[3] O principal endereço do IETF na internet é: http://www.ietf.org. Buscas por documentos podem ser realizadas em: https://datatracker.ietf.org/doc/search/

comprimentos de onda. Tal tecnologia, que utiliza vários comprimentos de onda, é conhecida como WDM. Utilizando-se o WDM, em conjunto com diferentes técnicas de modulação, os experimentos laboratoriais tentam se aproximar do limite teórico de banda disponível pela fibra. Por exemplo, na OFC/NFOEC[4] em fevereiro de 2008, foi apresentado um novo recorde com a transmissão de 164 canais à taxa de 100 Gb/s por uma distância de 2550 km (CHARLET, 2008). A distância é tão importante que os autores apresentam o recorde para o produto taxa [terabit/s] x distância [km] no valor de 41800 terabit.km/s; ou 41,8 petabit.km/s como foi apresentado no trabalho. Mesmo sem considerar o mérito da distância percorrida, este trabalho demonstrou a possibilidade de realizar uma transmissão de até 16,4 Tbps em uma única fibra óptica. Em março de 2010, na mesma conferência, destaca-se o trabalho (SANO, 2010) que relata experimento demonstrando 69,1 Tbps por 240 km. Este trabalho conseguiu demonstrar uma eficiência espectral de 6,4 bit/s/Hz. Descontando-se o fato de ter utilizado menor distância, a taxa de bit aumentou de 16,4 Tbps em 2008 para 69,1 Tbps em 2010.

2.2 Chaveamento de Comprimento de Onda

O sistema WDM permite aumentar a banda efetiva dos enlaces, pela inclusão de vários comprimentos de onda trafegando em uma única fibra óptica. O chaveamento de comprimento de onda é uma operação que permite remover um único comprimento de onda, ou um conjunto deles, utilizando-se filtros de freqüência

---

[4] Optical Fiber Communication Conference (OFC) e National Fiber Optic Engineers Conference (NFOEC) são conferências anuais que reúnem perto de 10.000 pesquisadores de todo o mundo. Realizada alternadamente na costa Leste e costa Oeste dos EUA há 36 anos, desde o início das comunicações ópticas, em 2011 foi em Los Angeles de 8 a 10 de março (http://www.ofcnfoec.org).

óptica. Estes filtros podem ser fixos, ajustáveis, ou gerenciados remotamente. Um esquema típico de chaveamento consiste em fazer a demultiplexação de todos os comprimentos de onda e direcionar cada um deles para chaves ópticas espaciais[5]. Cada chave óptica trata um único comprimento de onda e pode inserir o sinal deste comprimento de onda em diferentes portas de saída. O equipamento que realiza todas estas funções é conhecido por OXC (*Optical Cross Connect*). Além de tratar os diferentes canais que se cruzam em um entroncamento de enlaces, um OXC também desempenha a função de derivação ou inserção do sinal para uso local. Esta função é conhecida pela sua expressão, em inglês, "*ADD-DROP*".

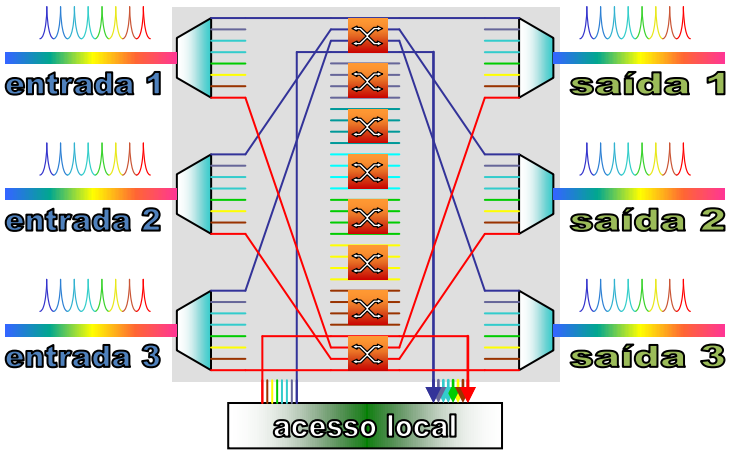


Figura 1: Esquema de chaveamento de comprimento de onda (ROCHA, 2003)

A Figura 1 ilustra este esquema de chaveamento de comprimentos de onda, bastante utilizado na literatura (ROCHA, 2003). Neste exemplo, existem oito comprimentos de onda em cada fibra óptica indicando a necessidade de oito chaves espaciais 4x4. As chaves espaciais precisam ter quatro entradas e quatro saídas para atender três entradas e três saídas de fibra óptica, mais uma entrada e uma saída para acesso local. As chaves espaciais podem ser feitas utilizando dispositivos

[5] Chaves ópticas espaciais são chaves que permitem ligar um sinal óptico de entrada, seja qual for o comprimento de onda, para duas ou mais posições alternativas separadas fisicamente no espaço. As MEMS (*Micro ElectroMechamical Systems*) são exemplos deste tipo de chave.

do tipo MEMS (*Micro Eletro-Mechanical System*). Estas chaves são um milhão de vezes mais lentas do que se propõe no caso do chaveamento de pacotes ópticos, mas são suficientemente rápidas para chavear comprimentos de onda de um sistema SDH (*Synchronous Digital Hierarchy*) sem disparar alarmes de falta de sinal e sem que haja percepção dos usuários finais.

Um consórcio internacional que resume e agrega atividades ligadas ao chaveamento de comprimento de onda é conhecido como GLIF (*Global Lambda Integrated Facility*). As Figuras 2 e 3 ilustram, respectivamente, as participações da parte leste da América do Norte e da América do Sul no consórcio GLIF.

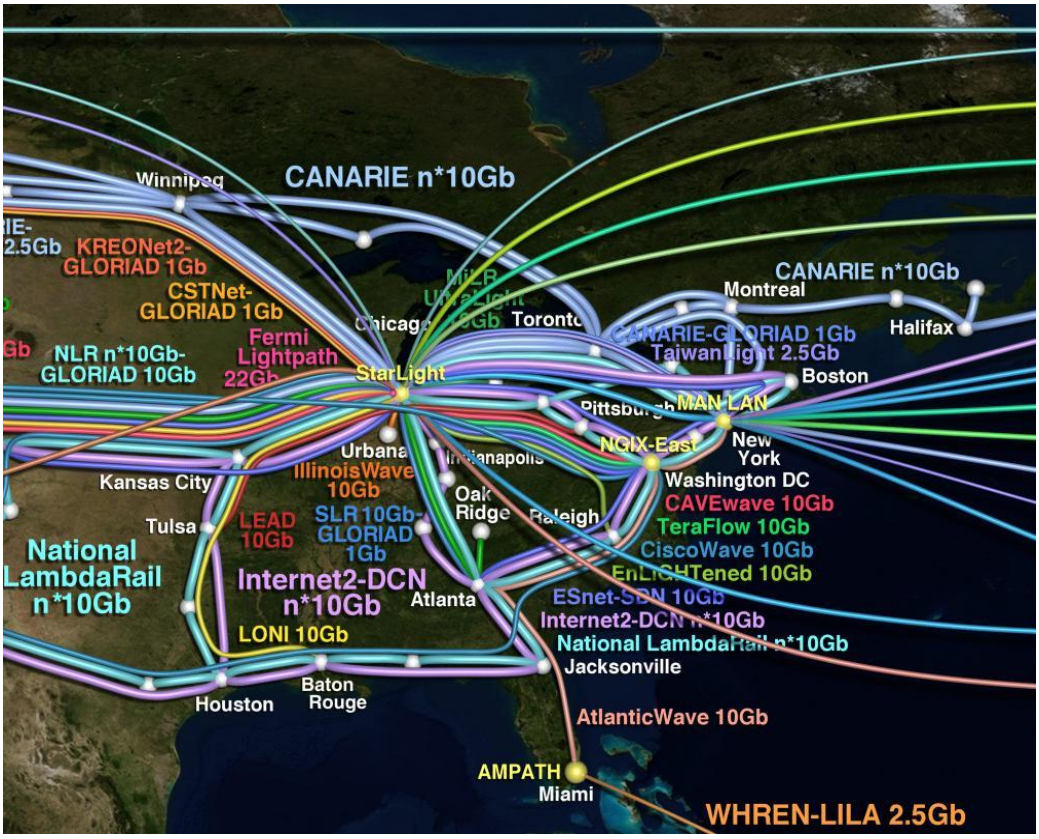


Figura 2: GLIF_Leste da América do Norte. Fonte: (GLIF, 2008)

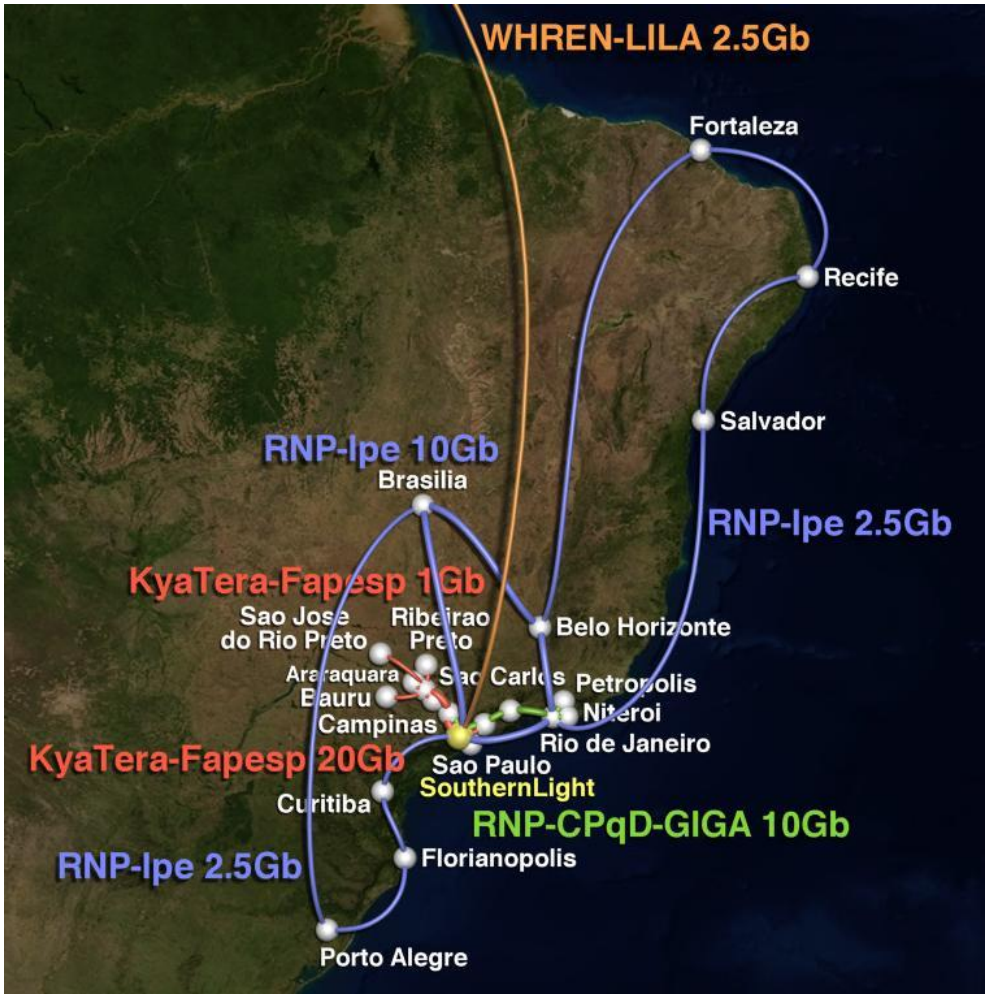


Figura 3: GLIF_América do Sul. Fonte: (GLIF, 2008)

2.3 Redes Ópticas Passivas

A maneira mais simples de dividir um sinal óptico entre vários usuários é pela utilização de acopladores ópticos passivos. Estes dispositivos separam parte da potência óptica sem utilizar alimentação elétrica. Uma rede de acesso em árvore, utilizando acopladores passivos, permite enviar o sinal óptico de um servidor central até o final de cada ramificação, atendendo vários clientes. Esta tecnologia,

conhecida como PON (*Passive Optical Network*), viabiliza o que se convencionou chamar de tecnologia FTTH (*Fiber To The Home*), que permite chegar com a fibra óptica até bem próximo do cliente final. Com baixo custo de instalação e manutenção de dispositivos passivos, uma única rede PON é utilizada para atender um grande número de usuários. O número total de clientes depende da potência óptica transmitida, da sensibilidade do receptor do cliente mais afastado, da sensibilidade do receptor do cliente posicionado depois de muitas ramificações e depende, também, de um protocolo de agendamento que permite o retorno dos pacotes sem colisão. Normalmente, a taxa de retorno é mais baixa, facilitando o agendamento do retorno de muitos usuários sem que haja colisão.

As primeiras versões de rede PON que utilizam o protocolo ATM (*Asynchronous Transfer Mode*) são conhecidas por redes ATM-PON. As versões que utilizam sistemas WDM são denominadas WDM-PON. Estas e diversas configurações de rede PON estão descritas nas recomendações ITU-T da série G.983.X (ITU-T G.983.1, 2005; ITU-T G.983.2, 2005; ITU-T G.983.3, 2001; ITU-T G.983.4, 2001; ITU-T G.983.5, 2002). As redes G-PON, com capacidade para Gigabit Ethernet estão na série G.984.X (ITU-T G.984.1, 2008; ITU-T G.984.2, 2003; ITU-T G.984.3, 2008; ITU-T G.984.4, 2008); (ITU-T G.984.5, 2007; ITU-T G.984.6, 2008; ITU-T G.984.7, 2010).

As redes XG-PON com capacidade para 10 Gigabit Ethernet estão na série G.987.X. (ITU-T G.987, 2010; ITU-T G.987.1, 2010; ITU-T G.987.2, 2010; ITU-T G.987.3, 2010). As redes EPON (Ethernet PON) padronizadas para várias taxas de bit também atingem a taxa de 10 Gbps e são bastante utilizadas no Japão e na Coréia. As recomendações e padronizações das redes EPON para 10 Gbps estão no documento IEEE Std 802.3av™ (2009).

As redes PON são as principais tecnologias de rede óptica de acesso para viabilizar o FTTH. Uma novidade que facilita a instalação destas redes é a fibra dobrável. Esta fibra pode ser dobrada com raio de curvatura de 5 mm, resultando em uma perda de potência inferior a 0,1 dB/volta. O processo, utilizado por alguns fabricantes, para conseguir esta melhoria, envolve nanoestruturas colocadas ao redor do núcleo. Um exemplo, destas novas fibras, é mostrado no artigo de divulgação da Corning citado

como referência (CORNING, 2008). As características mínimas para estas fibras com perdas não sensíveis a dobras podem ser encontradas nas recomendações (ITU-T G.657, 2009)

2.4 Chaveamento de Pacotes Ópticos

No meio do caminho entre as redes de longa distância com tráfego altamente agregado (enlaces de alta capacidade) e as redes de acesso com componentes de baixo custo (enlaces ramificados de baixa capacidade) existem as redes metropolitanas. Estas redes funcionam por um lado junto das redes de acesso, com muitas ramificações e por outro lado ligadas às redes de longa distância, com enlaces de alta capacidade. Uma característica importante para as redes metropolitanas é a agilidade de comutação. Esta característica é necessária, para que possa atender um grande número de usuários e uma grande variedade de serviços. A tecnologia de chaveamento de pacotes ópticos é uma boa candidata que atende aos requisitos necessários para redes metropolitanas.

O projeto, sempre utilizado como referência, para identificar as principais funções de uma rede com chaveamento de pacotes ópticos é o projeto ACTS[6] KEOPS – *KEys to Optical Packet Switching* (GUILLEMOT, 2000), que se encerrou no ano de 1999. Outros projetos como o projeto IST[7] DAVID - *Data And Voice Integration over*

---

[6] ACTS (*Advanced Communications Technologies and Services*) é um programa financiado pela Comissão Européia.

[7] IST (*Information SocietyTechnologies*) é um quadro (*framework*) que apresenta consecutivos programas de planejamento europeus para atividades de pesquisa. O Programa atual (FP7 –

DWDM (DITTMANN, 2003) ou o projeto HORNET - *Hybrid Opto-electronic Ring Network* (WHITE, 2000) seguiram as idéias originais e necessidades fundamentais apresentadas na conclusão do projeto KEOPS. Estes grandes projetos não tiveram continuidade e não resultaram em produtos comerciais, mas lançaram as bases de necessidades tecnológicas para chaveamento de pacotes ópticos. Hoje, há muitos experimentos desenvolvendo novos dispositivos, que tornam o chaveamento de pacotes ópticos ainda mais transparente e mais eficiente.

Nas sub-seções em seqüência, estão apresentadas algumas características e conclusões dos projetos que deram início aos estudos sobre chaveamento de pacotes ópticos; o projeto CPqD/Ericsson (CPqD: Fundação Centro de Pesquisa e Desenvolvimento em Telecomunicações) que inicia as atividades de pesquisa na área de pacotes ópticos no Brasil; os esforços atualmente concentrados em chaveamento de pacotes agregados em lotes e em novos dispositivos para chaveamento e tratamento de cabeçalho de pacotes ópticos de maneira totalmente transparente.

2.4.1 Projeto KEOPS

Participaram do projeto KEOPS empresas e universidades de vários países (GUILLEMOT, 1998): *Alcatel Alsthom Recherche* (França); *France Telecom-CNET* (França); *CSELT* (Itália); *Technical University of Denmark* (Dinamarca); *Alcatel CIT* (França); *Alcatel SEL* (Alemanha); *University of Bologna* (Itália); *ETH-Zürich* (Suíça); *University of Strathclyde* (Inglaterra).

Seventh Framework Program) apresenta planejamento para o período de 2002 a 2013 (http://cordis.europa.eu/fp7/ict/).

A principal conclusão do projeto KEOPS é que o chaveamento de pacotes ópticos confere granularidade fina aos sistemas de comunicação, tendo capacidade para tratamento de altas taxas de bit com grande flexibilidade. Foram desenvolvidos componentes e realizados experimentos de demonstração que permitiram chegar a outras conclusões. Dentre estas conclusões encontra-se a necessidade de criar um cabeçalho óptico adicionado na frente de cada pacote. Este cabeçalho pode ser escrito numa taxa de bit inferior à taxa utilizada na transmissão do conteúdo principal, para permitir que nós ópticos intermediários possam analisar o cabeçalho sem que tenham capacidade para tratamento de altas taxas presentes no conteúdo dos pacotes.

Outras conclusões importantes do projeto KEOPS (GAMBINI, 1998) foram: a necessidade de chaves ópticas rápidas, a necessidade de um tempo de guarda entre os pacotes, a necessidade de um conjunto de bits de sincronização e a necessidade de uma linha de retardo (*DLF – Delay Line Fiber*).

O tempo de guarda é um intervalo de tempo obrigatório deixado entre os pacotes para permitir o processo de chaveamento sem dano aos dados ou ao cabeçalho. O processo de chaveamento ocorre dentro deste intervalo de tempo de guarda.

Os pacotes ópticos do projeto KEOPS eram mantidos dentro de intervalos de tempo sincronizados e fixos. Foi utilizado o valor de 1,646 μs, correspondente ao intervalo de tempo de 1024 bits na hierarquia STM4 do sistema SDH que opera na taxa de 622,08 Mbps.

As chaves ópticas rápidas no projeto KEOPS fizeram uso de conversão de comprimento de onda, linhas de retardo e dispositivos SOA (*Semiconductor Optical Amplifier*) conforme arquitetura esquematizada na Figura 4.

Todos os pacotes têm o seu comprimento de onda alterado por conversores de comprimento de onda totalmente ópticos, de forma que cada pacote passa a ter um comprimento de onda que identifica sua porta de chegada. Todos os pacotes são acoplados em uma única fibra através de um acoplador WDM (*Wavelength Division Multiplexing*). Seguindo a Figura 4, depois dos conversores de comprimento de onda e do acoplador WDM, o sinal é dividido em k braços de fibra óptica em um processo

passivo. Cada braço, contendo réplicas do mesmo sinal óptico, se liga a k linhas de retardo. Todas as linhas contendo pacotes de todas as portas caracterizam a estratégia BS (*Broadcast-and-Select*) adotada nesta arquitetura. Uma bateria de dispositivos SOA (*Semiconductor Optical Amplifier*), controlada por circuitos lógicos eletrônicos, encaminha cada pacote para sua porta de saída depois de selecionado o intervalo de tempo que será ocupado pelo pacote. Os comprimentos de onda são separados e uma nova bateria de dispositivos SOA seleciona, em tempo real, o comprimento de onda encaminhado para cada porta de saída.

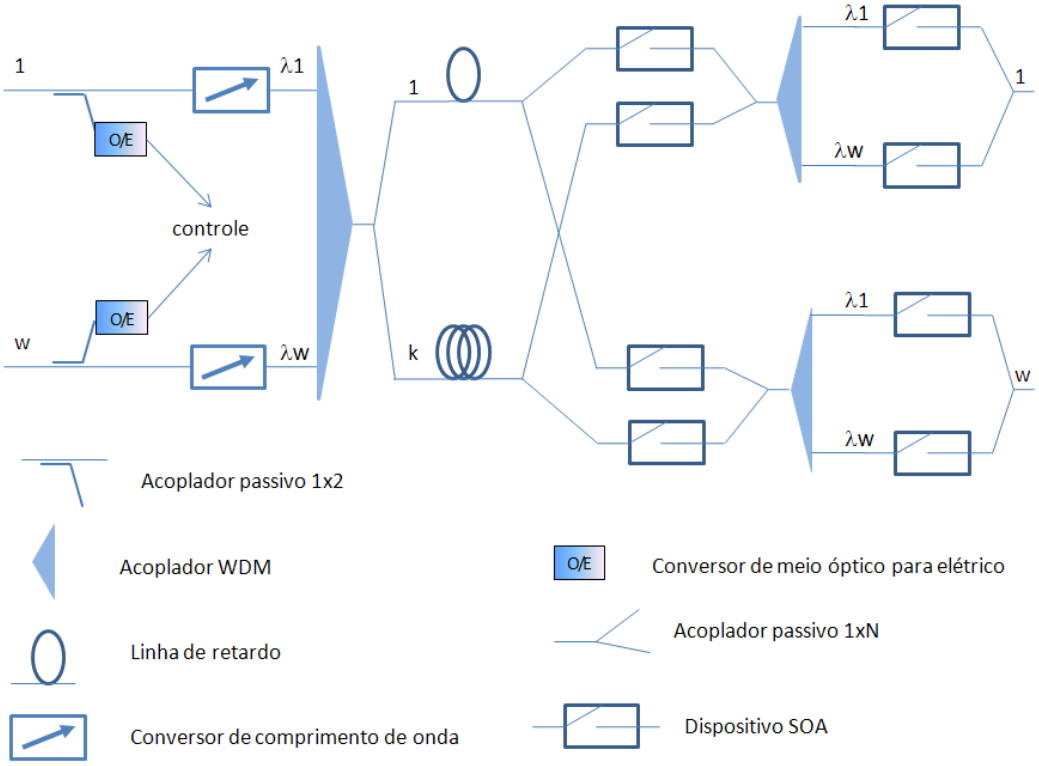


Figura 4: Arquitetura de chave óptica rápida do projeto KEOPS que utiliza conceito de BS (*Broadcast-and-Select*).

2.4.2 Projeto DAVID

O projeto DAVID, a exemplo do projeto KEOPS, também foi executado por empresas e universidades de vários países da Europa: Alcatel SEL (Alemanha); Alcatel CIT (França); Research Center COM (Dinamarca); National Technical University of Athens (Grécia); Ghent University (Bélgica); University of Bologna (Itália); University of Essex (Inglaterra); Laboratoire de Recherche Informatique d'Orsay (França); Politecnico di Torino (Itália); Institut National des Telécommunication (França); BTexact Technologies (Inglaterra); Universitat Politecnica de Catalunya (Espanha); Telenor (Noruega); Telefonica (Espanha).

A Figura 5 representa o funcionamento do *switch* óptico do projeto DAVID. As idéias básicas são as mesmas utilizadas no projeto KEOPS. As chaves ópticas rápidas também utilizam a estratégia BS, mas agora o número de porta total foi fixado em 16 e cada porta tem capacidade WDM com 16 comprimentos de onda totalizando 256 entradas. Foram acrescentados mais controles para suportar pacotes maiores divididos em vários intervalos de tempo, que continuavam fixos e sincronizados. Nesta arquitetura de chave óptica são necessários 8192 dispositivos SOA, ilustrando a complexidade envolvida para montagem de um único *switch* óptico.

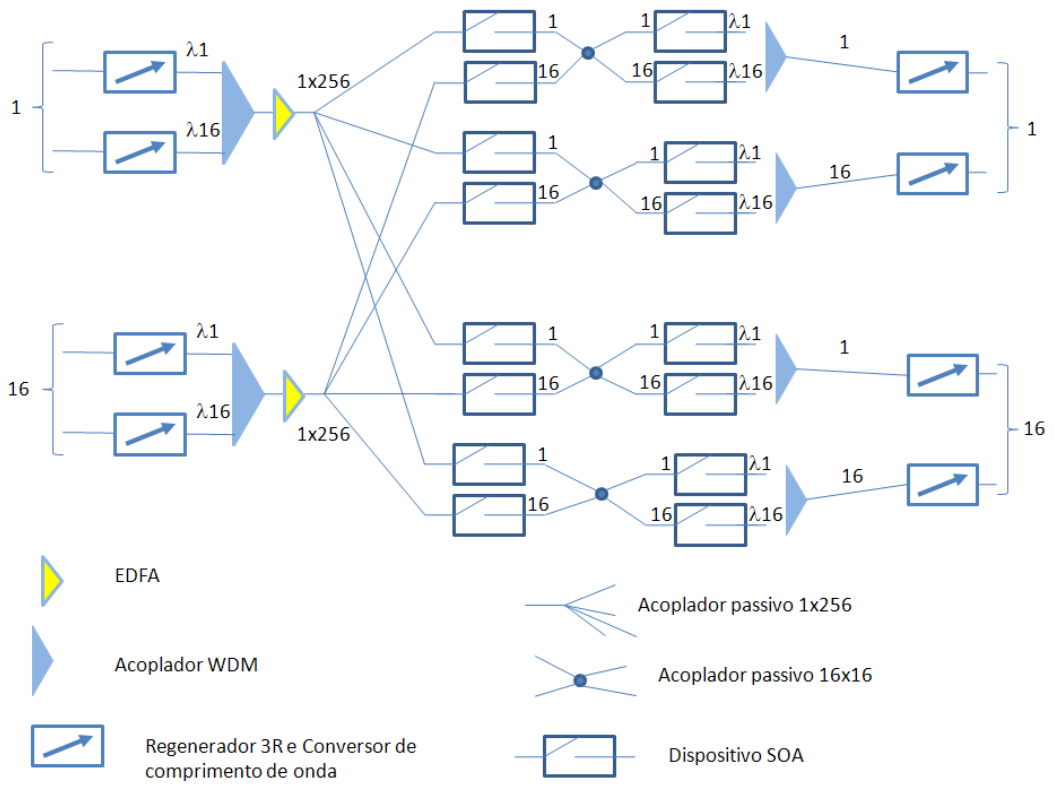


Figura 5: Arquitetura de chave óptica rápida do projeto DAVID

2.4.3 Projeto HORNET

O projeto HORNET (WHITE, 2000) trabalha com topologia em anel. Está orientado a uma rede de acesso com chaveamento de pacotes ópticos. Os pacotes ópticos podem ser inseridos na rede pelo uso de dispositivo laser sintonizável. Tal laser pode alterar o comprimento de onda rapidamente (intervalo de tempo da ordem de picossegundo), permitindo melhor utilização dos comprimentos de onda disponíveis no anel.

2.4.4 Projeto CPqD/Ericsson

No Brasil destaca-se o trabalho de Barbosa (2003) que marca o final do projeto realizado no CPqD (Fundação Centro de Pesquisa e Desenvolvimento em Telecomunicações) com financiamento da Ericsson do Brasil (Ericsson Telecomunicações S/A) e supervisão da Ericsson Research da Suécia. Com este trabalho, seja por escassez de recursos, seja por procura de idéias inovadoras, inicia-se a pesquisa por chaves ópticas 2x2, cujo conceito de simplificação é aplicado nesta tese e tem sido adotado em trabalhos recentes (MACK, 2010) que tratam de chaveamento de pacotes ópticos. O trabalho CPqD/Ericsson gerou uma patente internacional (BARBOSA; SACHS; FURTADO, 2002) e sua correspondente patente nacional (BARBOSA; SACHS; FURTADO, 2002b) que descrevem método de formação de cabeçalho óptico utilizando sobre-modulação do pacote digital com sinais analógicos de baixa freqüência. Em continuidade, com financiamento do FUNTTEL (Fundo para Desenvolvimento Tecnológico das Telecomunicações) o CPqD gerou outra patente nacional (SACHS; BARBOSA; PEZZOLO, 2004) que descreve novo método de formação de cabeçalho separado no tempo em relação ao conteúdo do pacote.

2.4.5 Chaveamento de Pacotes em Rajadas (OBS)

A pesquisa, em todo o mundo, se intensificou em uma tecnologia que simplifica alguns aspectos do chaveamento de pacotes ópticos. Conhecido como OBS (*Optical Burst Switching*), o chaveamento em lotes consiste em agregar pacotes em um grande bloco, que pode ser chaveado como um lote único. As chaves ópticas não

precisam ser tão rápidas, pois os lotes, que passam após cada operação de chaveamento, sendo muito grandes, fazem com que a perda de tempo relativa entre tempo de chaveamento e tempo de passagem de carga útil, seja diminuída. A troca de foco de alguns pesquisadores, ao privilegiar OBS e não OPS deve-se a uma tentativa de aplicação imediata, que pode ser feita utilizando-se as chaves ópticas disponíveis no mercado. Rosberg (2003) resume os aspectos de desempenho da tecnologia OBS. Mobilon (2006) apresenta um protótipo de rede OBS demonstrando o seu funcionamento em laboratório e, mais recentemente, Moraes (2007) apresenta uma proposta de mecanismo de controle de admissão, em função da carga, para garantir qualidade de serviço de redes OBS.

2.4.6 Novos Componentes para Chaveamento de Pacotes Ópticos

Muitas áreas estão se desenvolvendo para viabilizar o chaveamento de pacotes ópticos. Chaves rápidas e esquemas totalmente ópticos para leitura do cabeçalho são reportadas (TEIMOORI, 2008), sendo possível chavear pacotes na taxa de 160Gb/s (CALABRETTA, 2008). Há também estudos sobre a escalabilidade de um comutador óptico limitada pelo acúmulo de dispositivos SOA (BUCHTA, 2008).

A tendência é que sejam desenvolvidos novos dispositivos totalmente ópticos para redes OBS e OPS. Um exemplo de codificação e decodificação óptica está na tecnologia OCDMA (*Optical Code Division Multiple Access)*, que permite chaveamento em tempo real sem retirar nenhuma amostra para análise no meio elétrico. Também estão sendo desenvolvidos dispositivos lógicos totalmente ópticos, que podem ser utilizados em qualquer tomada de decisão que precisa ser feita em tempo real. Sem utilizar conversão para o meio elétrico é possível trabalhar com taxas maiores do que 40 Gb/s nos nós intermediários. Outra área de pesquisa em andamento são os armazenadores totalmente ópticos (*buffer óptico*).

Um dos apelos para o chaveamento de pacotes ópticos é a escalabilidade do número de portas de um entroncamento óptico (BLUMENTAL, 2002). Em um recente trabalho Stavdas (2008) apresenta vários aspectos sobre o chaveamento óptico. O autor faz comparações entre várias técnicas de chaveamento, incluindo a possibilidade não transparente que utiliza tecnologia Ethernet[8]. Faz também comparações entre várias tecnologias utilizadas para construir as chaves ópticas e analisa características como escalabilidade, consumo de energia e desempenho. Mais recentemente ainda (TANEMURA, 2009) pesquisador da Universidade de Tóquio demonstrou chaveamento de 320 Gbps em uma chave 1x5 construída com guias de onda integrados em dispositivo com substrato de fosfeto de índio (InP) formando braços interferométricos de igual comprimento com fase da luz ajustada individualmente pela passagem de corrente elétrica.

A Figura 6 ilustra a nanotecnologia aplicada a dispositivos ópticos (SHINYA, 2008). Furos de 100 nm de diâmetro reduzem o índice de refração de uma camada de InGaAsP[9] de 200 nm de espessura. A omissão de uma faixa de furos cria um guia de onda. Esta tecnologia, baseada em manipulações geométricas de materiais em escala nanométrica, produz dispositivos conhecidos como cristais fotônicos. Com estes dispositivos, que também podem ser feitos utilizando-se cristais de silício, é possível construir uma memória óptica como ilustrado na Figura 7. Neste dispositivo a transmissão de luz apresenta um limiar (começa transmitir depois de 200 mW de potência óptica de entrada) e mantém a transmissão mesmo que a potência de entrada baixe para 50 mW, caracterizando um processo de histerese. Este processo

---

[8] Ethernet é tecnologia de interconexão para rede local.

[9] InGaAsP é uma liga quaternária com átomos de Índio, Gálio, Arsênio e Fósforo. In e Ga são átomos de valência III e As e P são átomos de valência V. Variando-se a proporção entre In e Ga e a proporção entre As e P são obtidos os compostos III-V, cristais semicondutores com diferentes valores de banda proibida, diferentes valores de parâmetro de rede (distância entre átomos) e diferentes valores de índice de refração, entre outras características. São utilizados para fabricação de dispositivos como laser de semicondutor, fotodetector ou guias de onda integrados sobre substratos de fosfeto de índio.

é utilizado para definir o estado “1” (estabelecido depois de a potência ultrapassar o valor limiar de 200 mW) ou estado “0” (conseguido quando a potência incidente fica abaixo de 40 mW). Entre 40 mW e 200 mW o dispositivo pode estar no estado “1” ou “0”, dependendo do histórico do estímulo óptico de entrada. Um dispositivo que apresenta dois estados pode funcionar como um flip-flop óptico, com capacidade de armazenar um bit (memória óptica) ou ser utilizado para circuitos lógicos totalmente ópticos.

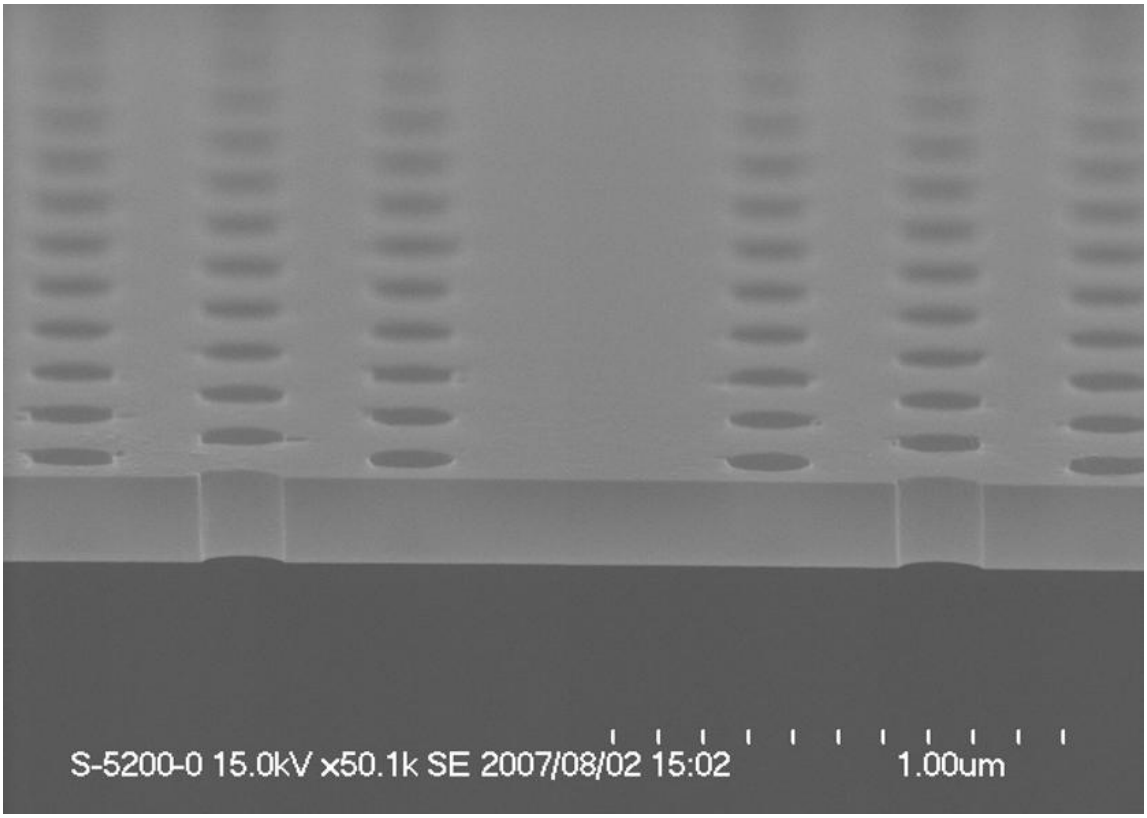


Figura 6: Cristal fotônico (PhC – *Photonic Cristal*) sobre InGaAsP (SHINYA, 2008).

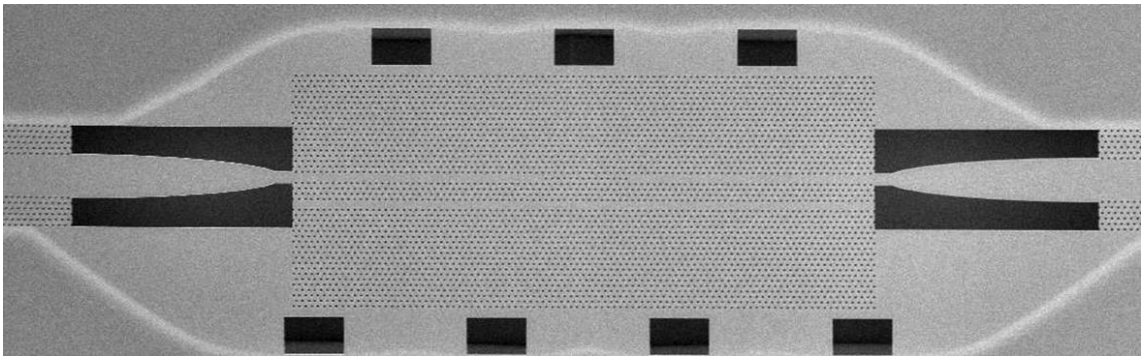


Figura 7: Dispositivo utilizando PhC que pode ser estabilizada no estado “1” ou “0” conforme estímulos ópticos (SHINYA, 2008).

2.5 O Estado da Arte e Algumas Considerações

Cada enlace óptico possui grande banda passante, mas esta não é a única vantagem de uma rede óptica. Existe, também, um grande potencial de chaveamento e de roteamento que, realizados sem conversão do sinal óptico para elétrico, apresentam vantagens de capacidade de tráfego, velocidade de chaveamento, espaço físico e consumo de energia. No entroncamento dos enlaces, espera-se poder utilizar tecnologia óptica para inserir novos canais de usuários, retirar canais de usuários que chegam ao seu destino final e direcionar sinais em trânsito para diferentes portas de saída. Garantir robustez, baixa latência e qualidade de serviço são outras funções da área de redes, que os comutadores ópticos precisam atender, para que possam oferecer vantagens adicionais comparativamente aos comutadores não-ópticos.

Apesar da idéia de queda de desempenho quando os problemas não são resolvidos de forma determinística, privilegiando o chaveamento de circuito em detrimento do chaveamento de pacotes (que sempre carrega certo grau de aleatoriedade), a necessidade de flexibilidade e o aumento da taxa de bits dos enlaces e a economia

de energia fazem ficar cada vez mais importante a necessidade de uma tecnologia de chaveamento totalmente óptica. Em 2010 destacam-se trabalhos voltados à tecnologia de chaveamento de pacotes ópticos que não utilizam conversão do meio óptico para o meio elétrico nem mesmo para o reconhecimento do cabeçalho óptico (STAMATIADIS, 2010).

2.5.1 Desafios da Área

Hoje não há mais projetos como KEOPS ou DAVID que foram estimulados na década de 90 (século XX) pelo grande otimismo com respeito ao aumento da demanda por novos serviços. Entretanto, em função de características como alta capacidade de chaveamento, escalabilidade da capacidade de chaveamento, baixo custo por bit chaveado, economia de espaço físico, economia de energia, os pacotes ópticos continuam sendo pesquisados e considerados como solução para futuras redes muito densas. Os trabalhos estão concentrados em dispositivos capazes de ler e interpretar o cabeçalho óptico, em tempo real, sem convertê-los para o meio elétrico. Há também muito trabalho de desenvolvimento de processos e dispositivos de armazenamento[10] ópticos (TUCKER, 2006), bem como dimensionamento destas memórias ópticas de armazenamento (BEHESHTI, 2006). Tucker (2006) baseia suas análises sobre roteadores de alta capacidade em desempenho esperado e projetado (plausíveis, segundo Tucker) para as memórias ópticas no ano de 2020. Na construção de chaves rápidas, a sincronização dos pacotes em tempo de

---

[10] O dispositivo de armazenamento óptico é, muitas vezes, por falta de uma tradução adequada, tratado como “buffer óptico”. O termo *buffer*, da língua inglesa, significa reserva ou armazenamento, mas inclui também o significado de dispositivo que armazena, ou memória de armazenamento.

propagação, o tratamento do cabeçalho óptico, a conversão de comprimento de onda e a recuperação de relógio continuam sendo desafios tecnológicos não solucionados (STAVDAS, 2008). Problemas como o gerenciamento das operações de chaveamento (plano de controle), o gerenciamento de rede (engenharia de tráfego), escalabilidade da rede e custo de instalação e manutenção também são importantes desafios e demandam novas soluções e novas propostas. Em 2010 os problemas de sincronismo de pacote, armazenamento óptico e conversão de comprimento de onda, que estão ligados a mecanismos de rede, continuam abertos e trabalhos estão sendo realizados para resolvê-los pelo uso de novos componentes com processos totalmente ópticos (MACK, 2010).

2.5.2 Proposta de Trabalho

Esta proposta é um trabalho de desenvolvimento na área de chaveamento de pacotes ópticos, com finalidade de incorporar granularidade fina às redes WDM de alta capacidade. A proposta diferencia-se dos grandes projetos KEOPS e DAVID por ser bastante simplificada, adequada para utilização em redes metropolitanas e redes de acesso. A proposta diferencia-se também por atribuir autonomia aos nós de rede, e por deixar o processo de chaveamento como operação de decisão local. Com chaves autônomas é possível projetar redes auto-organizadas. Tais estudos permitem também estabelecer métodos para tratamento de redes complexas constituindo um caminho importante para resolver o problema de escala.

3 Os problemas de Complexidade da Rede e das Chaves Ópticas

A proposta deste trabalho contribui para solução de três problemas: granularidade grosseira dos caminhos ópticos (Seção 3.1); escalabilidade de número de nós de um domínio (Seção 3.2); e a complexidade dos comutadores nas redes de pacotes ópticos (Seção 3.3).

3.1 Banda passante, Granularidade e Agilidade de Comutação

Um caminho óptico é uma conexão física que liga dois pontos distantes de uma rede utilizando um comprimento de onda de maneira transparente (sem conversão para o meio elétrico). Costuma-se estender o conceito de caminho óptico para o caso onde há conversão do comprimento de onda em alguns enlaces, sem alterar o conteúdo total transmitido. Este conceito pode ser visto, por exemplo, em (STERN, 1999), página 113. A capacidade de um caminho óptico já atinge 100Gbps em enlaces comerciais e valores ainda maiores em propostas experimentais.

Os caminhos ópticos, quando utilizados para transmissão de pouco tráfego, representam desperdício de recursos. Se um caminho óptico utiliza baixa taxa de transmissão, há desperdício de banda, pois potencialmente pode-se utilizar este caminho com taxas maiores. Costuma-se dizer que cada comprimento de onda tem “granularidade grosseira” em contraposição à expressão “granularidade fina”, expressões também utilizadas por Ghobril (2003). A granularidade não constitui

problema nos grandes enlaces intercontinentais ou em qualquer enlace com grande volume de tráfego agregado. Entretanto, nas redes metropolitanas e principalmente nas redes de acesso, mais próximas dos usuários finais, a granularidade pode significar grande desperdício de recursos. Quando se aloca um comprimento de onda com capacidade para 40 Gb/s para atender poucos usuários, há subutilização deste recurso. Os usuários utilizam muito menos do que a banda alocada.

Nas redes metropolitanas, é preciso também atender usuários que necessitam de muita banda, mas durante intervalos de tempo pequenos (tráfego em *burst*). Para atender este tipo de demanda é preciso muita agilidade nos processos de chaveamento e comutação. Os processos de chaveamento de comprimento de onda não são tão rápidos quanto o chaveamento de pacotes.

3.2 Escalabilidade e Complexidade Computacional

A complexidade computacional é caracterizada por problemas que, embora solúveis, requerem muito tempo ou muita memória computacional para serem resolvidos. A matemática que descreve a complexidade computacional tem sido estudada desde o início do século XX. A teoria da complexidade computacional baseia-se na tese de Church-Turing (TURING, 1936) adaptada para casos reais limitados por tempo e capacidade computacional (memória). É possível demonstrar que alguns problemas são insolúveis computacionalmente. Outros problemas, embora possuam solução, podem requerer, para sua solução, tempos ou recursos computacionais (memória) inviáveis no mundo real. Um exemplo típico é o problema do caixeiro viajante, que precisa encontrar o caminho mais curto para visitar um número n de cidades interligadas por estradas. O número de itinerários possíveis é finito e dado pelo fatorial de (n-1). Para n=10, são 9!=362.880 itinerários, e basta verificar qual deles é o mais curto. Esta tarefa é perfeitamente possível para um computador. Mas, para

n=50, são 49! > 10^{62} itinerários, o que demandaria tempo maior que muitos ciclos de vida do universo para qualquer computador real que se possa imaginar. Este exemplo foi adaptado da referência (LEWIS, 1998), incluindo-se a idade do universo e aumentando-se n de 40 para 50, para que se possam imaginar melhores supercomputadores, e mesmo assim, visualizar porque o problema é complexo. Um ano tem 31.556.952 segundos (considerando que o ano tem 365,2425 dias). O universo tem cerca de 13,7 bilhões de anos (KOMATSU, 2009). Portanto, o universo tem apenas um pouco mais do que 4 x 10^{17} segundos de tempo de vida. Para testar 10^{62} itinerários, no tempo de vida do universo, o computador precisa testar mais do que 10^{45} itinerários por segundo. Este desempenho é impossível para os computadores mais rápidos que se consegue imaginar. Encontrar caminhos em redes de comunicação contendo muitos nós, principalmente quando interligados numa topologia em malha, constitui um problema complexo (EVEN, 1975). Estas redes podem ser representadas por grafos contendo “n” vértices, e muitas vezes precisa-se limitar o valor máximo de “n” para não se incorrer em problemas insolúveis ou mesmo para que não haja instabilidade do sistema.

A teoria da complexidade computacional trata problemas solúveis, e classifica a sua complexidade com auxílio da Máquina de Turing[11]. Os problemas complexos podem ser separados em duas classes principais: a classe de complexidade P com tempo de solução, em uma Máquina de Turing qualquer, limitado por um polinômio de grau n; e a classe complementar que contém os demais problemas, não limitados por um polinômio. Presumivelmente, os problemas não limitados por um polinômio são muito mais difíceis de serem resolvidos. Esta parte inclui, por exemplo, os tempos que crescem exponencialmente com n. Existe ainda um tipo de problema intermediário que não é limitado por um polinômio, mas pode ser dividido em problemas paralelos, onde pelo menos um deles é limitado por um polinômio. Isto equivale a dizer que podem ser resolvidos por uma Máquina de Turing não determinística, com vários caminhos alternativos, onde pelo menos um deles é

---

[11] Qualquer forma aceitável de expressão das idéias contidas em um “algoritmo” é equivalente à forma obtida empregando-se uma Máquina de Turing (LEWIS, 1998).

limitado por um polinômio. Tal problema pode não ser resolvido em tempo polinomial, mas existe uma solução que pode ser verificada em tempo polinomial. Estes são chamados de problemas tipo NP (*Non deterministic Polinomial*). Pode-se resumir a definição dos problemas tipo P como problemas solúveis em tempo polinomial e problemas tipo NP como problemas verificáveis em tempo polinomial (SIPSER, 1997). É difícil demonstrar que um problema da classe NP não pertence a P, e portanto não pode ser resolvido em tempo polinomial, mas foi verificado que certos tipos de problema pertencentes à classe NP possuem complexidade individual relacionada à complexidade de toda classe NP. Estes problemas são chamados NP-completos. Qualquer problema de NP pode ser reduzido[12] a um problema NP-completo, e esta redução pode ser feita em tempo polinomial. Se for encontrada uma solução em tempo polinomial para um problema é NP-completo, significa que todos os outros problemas de NP passam a ter solução polinomial e terá sido demonstrado que P=NP. Na hipótese comumente aceita de que P≠NP (demonstração ainda em aberto), demonstrar que um problema é NP-completo é evidência de que não seja possível encontrar um algoritmo para resolver o problema em tempo polinomial, não justificando esforços para encontrar tal algoritmo. O problema de encontrar o caminho mais curto em uma rede com topologia em malha qualquer, assim como o problema do caixeiro viajante descrito no início desta seção são problemas NP-completos (NPC).

Na prática, um problema da classe P, ou classe NP (ou ainda NPC), mesmo que tenha solução em tempo polinomial (esteja na realidade em P) não pode ser resolvido para valores de n arbitrariamente grandes. Nas redes de comunicação, isto limita o crescimento do número de nós que se pode incorporar em um domínio qualquer. Isto significa que há um limite de escalabilidade para o número de entroncamentos de uma rede dentro de um domínio qualquer.

---

[12] Uma redução é uma maneira de converter um problema A em outro problema B de forma que uma solução para B possa ser utilizada para resolver A (SIPSER, 1997).

Os algoritmos de busca pelo caminho mais curto precisam convergir e encontrar a melhor opção de caminho para cada topologia e cada conjunto de métricas adotado pela rede (HERMAN, 2008). A rede altera sua topologia pela incorporação de novos nós ou pela ocorrência de falhas e a complexidade computacional envolvida nos algoritmos de roteamento limita o número de nós que uma rede pode ter em um único domínio (escalabilidade de número de nós da rede).

3.3 Complexidade das Chaves de Pacotes Ópticos

O termo complexidade pode ser utilizado também no sentido comum da palavra para designar sistemas complexos ou sistemas com muitas variáveis. O chaveamento de pacotes ópticos requer muitas funções auxiliares de tratamento do sinal óptico. Nas entradas e saídas, é necessário incluir dispositivos de multiplexação e demultiplexação de comprimento de onda para que se possa aproveitar a grande capacidade das fibras ópticas utilizando transmissão WDM. Os pacotes de cada comprimento de onda devem ser tratados separadamente. Para redes de longa distância, o mesmo esquema de endereçamento por enlace, utilizado na tecnologia ATM (*Asynchronous Transfer Mode*) ou na tecnologia MPLS (*Multi Protocol Label Switching)*, é adotado para diminuir o tamanho do cabeçalho e o tempo de processamento de cada pacote. Após a leitura do cabeçalho dos pacotes na entrada, eles precisam ser removidos e substituídos antes de chegar até a porta de saída. Muitas destas funções podem ser consideradas desnecessárias em casos específicos, mas em outras são essenciais. Os pacotes ópticos, assim como as células ATM, precisam ser sincronizados para que várias entradas possam ter seus pacotes comparados para efeito de prioridade ou simplesmente para se ajustarem a intervalos de tempo previamente estabelecidos, evitando colisões. Além da multiplexação e demultiplexação de comprimento de onda, a Figura 8 ilustra a

necessidade de funções como o sincronismo de pacotes, a conversão de comprimento de onda, a análise de cabeçalho, o armazenamento óptico e a escrita de novos cabeçalhos que podem ser realizadas mais do que uma vez no processo de chaveamento do pacote óptico.

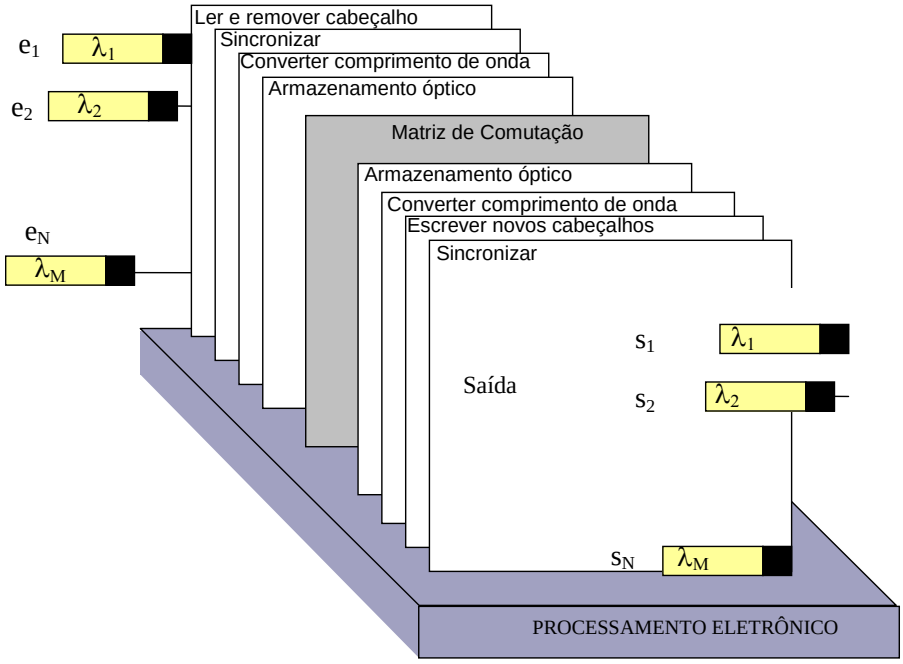


Figura 8: Principais funções presentes em uma chave de pacotes ópticos

A Figura 9 ilustra uma arquitetura de chave óptica com uma entrada e três saídas onde os pacotes podem ter vários comprimentos de onda ($\lambda 1$, $\lambda 2$, ...λn) na entrada e em cada uma das saídas. Pacotes de mesmo comprimento de onda precisam estar separados no tempo dentro de uma mesma fibra, mas pacotes de comprimentos de onda diferentes podem ser sobrepostos. A primeira operação (realizada quando o sinal óptico entra na chave) é a demultiplexação do comprimento de onda. Cada comprimento de onda é tratado isoladamente dos demais, como ilustrado na Figura 9 somente para o comprimento de onda $\lambda 1$. Demais comprimentos de onda ($\lambda 2$, $\lambda 3$, ...λn) são encaminhados para outros setores da chave para que sejam tratados separadamente. Segue-se nesta arquitetura a operação de leitura e remoção do cabeçalho dos pacotes. Depois segue-se a operação de chaveamento espacial onde

o pacote é encaminhado fisicamente para uma das três portas de saída. A etapa seguinte é a inserção de um novo cabeçalho na frente de cada pacote que vai acompanhá-lo para percorrer o próximo enlace. Entretanto, os pacotes não podem seguir diretamente para o enlace de saída, pois pode ser necessário ajustar o seu posicionamento no tempo (sincronismo de pacotes) para não se sobrepor a outros pacotes de mesmo comprimento de onda que estejam ingressando na mesma fibra. Para este ajuste de tempo os pacotes ficam circulando em bobinas de fibra óptica até que chegue o intervalo de tempo correto, a ele reservado. Somente estas bobinas, que funcionam como armazenadores ópticos, carregam uma complexidade muito grande (não ilustrada na figura), pois possuem múltiplos setores com chaves de saída que controlam quanto tempo um pacote precisa ficar armazenado. Depois de devidamente posicionados no tempo para que não haja sobreposição de pacotes de mesmo comprimento de onda em uma mesma fibra, os pacotes são encaminhados para os multiplexadores que recebem os demais comprimentos de onda para juntá-los e encaminhá-los para os três enlaces de saída.

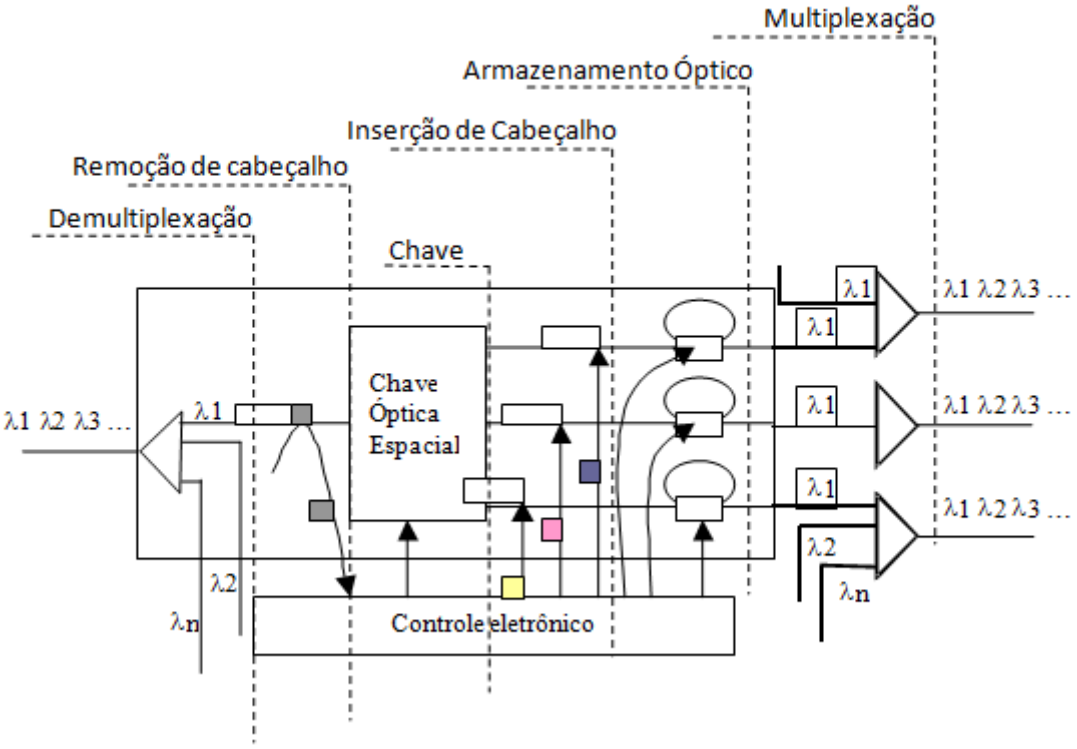


Figura 9: Exemplo de uma arquitetura de chave óptica e de funções usualmente utilizadas para o processo de chaveamento de pacotes ópticos.

O sincronismo de pacotes, a conversão de comprimento de onda, a análise de cabeçalho, o armazenamento óptico e a escrita de cabeçalho são funções presentes na tecnologia OPS. A complexidade de uma chave óptica verificada desde o projeto DAVID (Seção 2.4.1 - Figura 5) que previa um único entroncamento óptico com 8192 dispositivos SOA, constitui um fator complicador para viabilizar a tecnologia de pacotes ópticos. O custo dos roteadores de pacotes ópticos descritos pelos projetos multinacionais do final do século XX, associado à dúvida sobre a demanda por mais banda, fizeram a pesquisa desta tecnologia recuar em muitos países. O volume de trabalhos publicados sobre chaveamento de pacotes ópticos diminuiu dando lugar para trabalhos sobre OBS que possuem perspectiva de menor custo e aplicação mais imediata (O'MAHONY, 2006). Entretanto, a demanda por banda continua aumentando (CISCO, 2008) e pode acontecer que a necessidade do mercado surpreenda e encontre o desenvolvimento tecnológico bastante atrasado, principalmente nos países de baixa tradição em pesquisa e desenvolvimento. O chaveamento de pacotes ópticos sempre foi considerado como tecnologia para o futuro. Sempre são feitas previsões que os pacotes ópticos não serão utilizados pelo menos nos próximos dez anos (TUCKER, 2006).

3.4 Considerações Finais sobre o Problema

A granularidade grosseira dos caminhos ópticos de alta taxa, sem auxílio de técnica auxiliar de multiplexação (p. ex: tributários SDH), não permite a entrega de sinal óptico diretamente aos usuários finais. O chaveamento de pacotes é solução para a granularidade. Muitos estudos estão sendo realizados para comparar as opções tecnológicas que utilizam o pacote convertido para o meio elétrico (IP sobre WDM) ou utilizam tecnologia transparente onde os pacotes não são convertidos para o meio elétrico. Servem de parâmetro para estas pesquisas os custos de instalação e

manutenção, o consumo de energia, o espaço físico necessário para instalação dos equipamentos, o desempenho e a escalabilidade. Não há certeza sobre qual destas tecnologias deve prevalecer no futuro (TUCKER, 2006)

Pacotes ópticos são sempre tratados como tecnologia para o futuro e sua pesquisa caminha devagar, pois depende de novos componentes e muito investimento em novos desenvolvimentos, sem que se tenha certeza sobre qual caminho deve ter melhor aceitação. Por outro lado, as redes têm crescido muito e aproveitam a tecnologia já existente. A capacidade das fibras ópticas nos enlaces de longa distância se estabilizou em 1000 Gbps de 2001 a 2007, enquanto a demanda de tráfego IP em PB (Peta Bytes) por mês tem aumentado conforme ilustra a Figura 10.

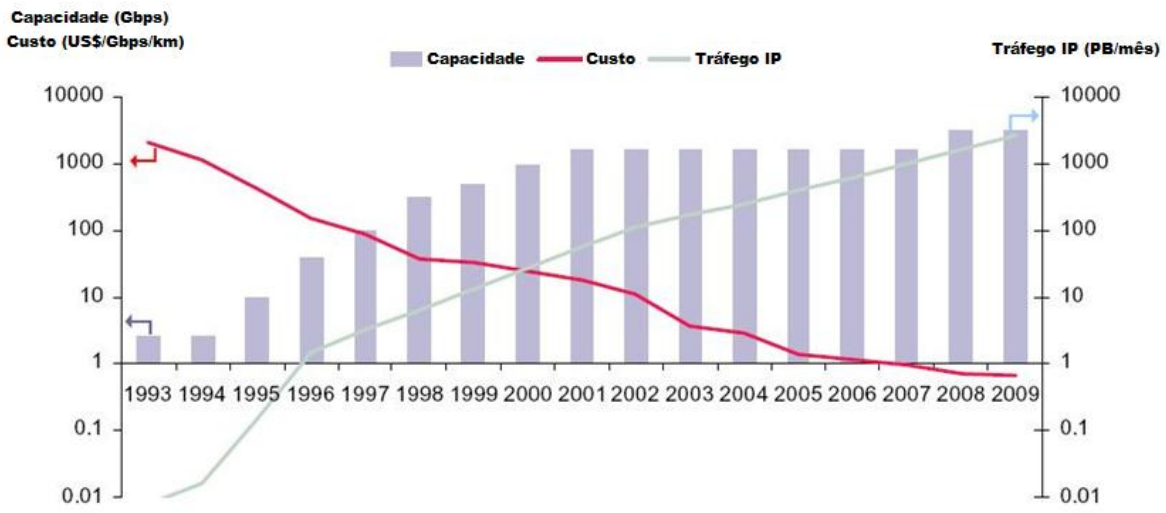


Figura 10: Dados OVUM dos enlaces DWDM: capacidade(Gbps); tráfego IP (PB/mês) e custo (US$/Gbps/km).

Com a demanda aumentando, a capacidade total deve aumentar para atender a demanda, mas é necessário tratar um volume muito grande de tráfego nos entroncamentos. Os pacotes ópticos costumam ser apresentados como solução para entroncamentos de alta capacidade, mas são muito caros. Envolvem tecnologias de componentes ainda não desenvolvidas e disponíveis em pequena escala em laboratórios experimentais. Quanto mais se aproxima do usuário final, nas

redes metropolitanas e redes de acesso, maior é o custo pago por usuário e os pacotes ópticos diminuem ainda mais suas possibilidades de aplicação.

Nas redes de longa distância, a escalabilidade mais importante é do número de portas em um mesmo entroncamento. Nas redes metropolitanas e redes de acesso, há muitos entroncamentos e passa a ser importante a escalabilidade do número de nós de rede. Aumentando-se o número de nós de rede, aparece a complexidade computacional para os cálculos de caminho.

A granularidade grosseira dos caminhos ópticos de alta taxa, a escalabilidade de número de nós de um domínio, e custo de implantação e manutenção das redes de pacotes ópticos são os principais problemas considerados neste trabalho como passíveis de solução pela utilização de chaveamento de pacotes ópticos.

4 Eliminação da Complexidade da Chave e Tratamento da Rede Como Um Sistema Complexo

Uma rede com capacidade de chaveamento de pacotes ópticos, constituída por chaves ópticas rápidas que operam com funções básicas muito simples, que utilizam informações locais e informações contidas no cabeçalho de cada pacote, constitui uma solução para os problemas descritos no Capítulo 3. A operação de cada chave óptica, sendo independente, libera o sistema de gerenciamento para operações que não precisam ser realizadas em tempo real. Com a ausência do sistema de gerenciamento no processo de chaveamento a rede adquire características de rede auto-organizada. Esta rede, também chamada de rede com organização *bottom-up* como descrito no primeiro capítulo (Seção 1.1) está melhor caracterizada a seguir na Seção 4.2.

A simplificação da chave óptica inicia-se pela redução do número de portas para apenas duas portas de entrada e duas portas de saída. A simplificação continua pela eliminação do armazenamento óptico e pela adoção do processo de chaveamento por deflexão (ACAMPORA, 1992). Neste processo de chaveamento cada pacote é enviado para uma porta preferencial de saída e desviado para outra porta disponível se a porta preferencial estiver ocupada. No nó de rede seguinte, há sempre uma nova oportunidade do pacote ser encaminhado para a porta saída preferencial.

Com chaves autônomas, a rede ganha características de auto-organização que são estudadas pela investigação de funções que emergem pela ação em conjunto das pequenas funções básicas executadas pelos nós de rede individualmente. Funções como “redistribuição de tráfego” ou “proteção de enlace” surgem automaticamente, em caso de necessidade.

4.1 Chaves Ópticas Simplificadas

A expressão em inglês *store-and-forward,* que pode ser traduzida por armazena e encaminha, tem sido considerada como um paradigma das redes baseadas em chaveamento de pacotes. Chega a ser considerada como sinônimo de chaveamento de pacotes. Os pacotes, neste paradigma, são armazenados e depois encaminhados para sua porta de saída. Permanecem armazenados enquanto a porta de saída estiver ocupada. Eventualmente, esgota-se a capacidade de armazenamento, e ocorrem perdas de pacotes.

Outra expressão em inglês, *deflection routing* (ACAMPORA, 1992), traduzida por roteamento por deflexão, caracteriza uma maneira de proceder que normalmente se contrapõe ao *store-and-forward*. Neste procedimento, também conhecido como batata quente (*hot potato routing*)[13], não é necessário armazenar os pacotes antes de encaminhá-los para a porta de saída. Não havendo armazenamento, antes que o final do pacote chegue ao nó de rede, a frente do pacote já é encaminhada para o enlace que se segue depois do nó. A chave deve permanecer na mesma posição até que o final do pacote termine de passar. Entretanto existe a possibilidade de utilizar roteamento por deflexão em conjunto com algum tipo de armazenamento fazendo com que *deflection routing* não seja necessariamente contraposto de *store-and-forward.* Pode-se armazenar por algum outro motivo como sincronismo ou verificação de integridade de cada pacote e proceder com o encaminhamento por deflexão realizado para uma porta disponível, mesmo que esta porta não seja a porta preferencial.

A utilização do roteamento por deflexão, sem nenhum auxílio de armazenamento óptico, constitui uma simplificação importante utilizada neste trabalho. A simplificação pode ser ainda maior pela adoção de nós ópticos que possuam apenas

---

[13] O primeiro pesquisador a utilizar o termo “batata quente” foi Baran (1964).

duas portas de entrada e duas portas de saída. Sendo simétrica (mesmo número de portas de entrada e de saída), a chave óptica sempre tem uma porta de saída livre para encaminhar qualquer pacote em trânsito. O encaminhamento é feito pelo ajuste da chave na posição paralela (ligando Entrada 1 com Saída 1 e Entrada 2 com Saída 2) ou na posição cruzada (ligando Entrada 1 com Saída 2 e Entrada 2 com Saída 1). O custo de um destes roteadores simplificados é muito menor do que os roteadores de pacotes ópticos que incluem armazenamento óptico e muitas portas.

A Figura 11 ilustra o processo de deflexão, sem utilizar armazenamento óptico. A principal característica é a presença de situações como na Figura 11, onde o início do pacote passa pela chave, caminha em um novo enlace (Saída 1), enquanto o final do mesmo pacote ainda não chegou e caminha em direção à porta de entrada (Entrada 2). Esta característica, principalmente para pacotes grandes e para casos onde existam muitos nós intermediários, traz um ganho importante no tempo total de propagação. Este ganho pode ser quantificado por simulação.

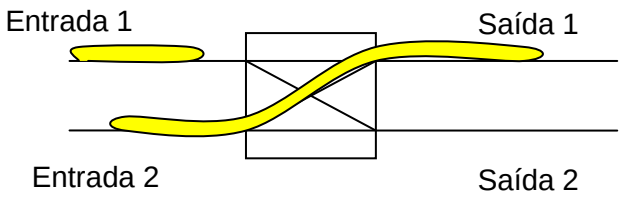


Figura 11: Esquema de deflexão de pacotes sem armazenamento óptico. Quebra do paradigma *"Store-And-Forward"*

No exemplo da Figura 11, o pacote pequeno, na Entrada 1, chega na posição da chave antes que o pacote maior termine de passar. Nesta situação, o pacote pequeno é encaminhado para a Saída 2, independentemente de qual seja a sua saída preferencial. Nas topologias em malha, muitos caminhos são igualmente bons. Caso o caminho tomado pelo pacote pequeno não seja adequado, uma nova oportunidade de retomada do seu caminho preferencial ocorrerá no próximo nó de rede.

Nos processos de disputa entre dois pacotes, nas redes que utilizam o paradigma *store-and-forward*, pode-se dizer que um pacote vence enquanto o outro é contido, em uma memória, aguardando outra oportunidade. Como nesta proposta não se utilizam memórias ópticas, a contenção não é possível, e por isso, foi adotada a expressão "resolução de contenda" em lugar de "resolução de contenção" como tradução do termo em inglês "*contention resolution*".

É necessário que se tenha uma linha de retardo antes de cada entrada para que se possa retirar uma amostra do sinal e fazer a leitura do cabeçalho com tempo hábil para o posicionamento da chave. Esta linha de retardo é constituída por um pedaço de fibra óptica denominada pela sigla DLF (*Delay Line Fiber*). Esta proposta inclui também uma arquitetura de chave óptica que permite a inclusão de novos pacotes sem que haja colisão. Esta arquitetura utiliza uma DLF maior do que seria necessário somente para o posicionamento da chave. Na Figura 12, o tempo de retardo t_0 é a soma de um tempo de retardo necessário para leitura do cabeçalho e posicionamento da chave t_1 com o tempo correspondente ao tamanho do maior pacote que pode ser inserido na rede (t_0–t_1).

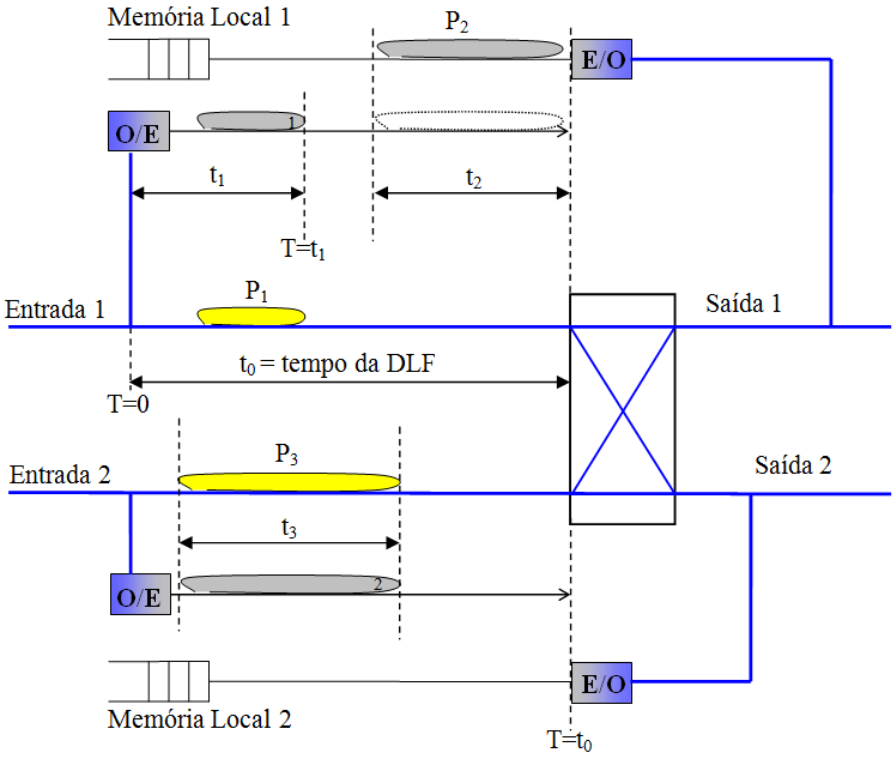


Figura 12: Esquema de inserção sem colisão

O pacote P_1 tem seu endereço e posição identificados depois do tempo $T=t_1$. Na situação da Figura 12, considera-se que o pacote P_3 chega primeiro e escolhe sua porta de saída (porta 2). Assim, a chave já posicionada para atender o pacote P_3, envia o pacote P_1 para a Saída 1 independentemente de sua preferência. Mas existe um pacote P_2 que pode ser inserido antes que o pacote P_1 chegue à posição da chave. Com todos os tempos sob controle, a chave manipula a entrada de novos pacotes sem que haja colisão. Enquanto não houver espaço disponível para inserção de novos pacotes, estes permanecem armazenados no meio eletrônico (Memória Local).

Para que os pacotes maiores (perto do tamanho máximo t_0–t_1) não impeçam a inserção de pacotes menores (com muito maior probabilidade de encontrar intervalo de tempo livre disponível) é proposta uma fila tipo FILO (*First-In-Last-Out*). Assim, mesmo que chegue um pacote grande, que não encontra espaço livre para que possa ser inserido, ele fica aguardando na fila sem que esta fila fique travada. Pacotes menores que chegam depois podem ser inseridos imediatamente, pois na fila tipo FILO a prioridade é do último que chega. Os serviços de maior prioridade devem utilizar pacotes menores para aproveitar esta característica da rede.

4.2 Rede Auto-Organizada (Rede BUONA)

Uma organização *bottom-up*, ou organização de baixo para cima, é uma terminologia associada a sistemas com funções sem gerenciamento, ou sistemas caracterizados por um grande número de elementos com funções específicas agindo conforme informações locais. As formigas de um formigueiro, os neurônios de um cérebro são exemplos de elementos individuais em organizações *bottom-up*. A rede auto-organizada descrita neste trabalho é outro exemplo de organização *bottom-up*. Esta rede é baseada em sistemas complexos compostos por elementos executando

funções localizadas, que geram a organização do sistema como um todo. Uma definição formal da auto-organização pode ser encontrada nas palavras de Debrun (1996):

> "Há auto-organização cada vez que o advento ou a reestruturação de uma forma, ao longo de um processo, se deve principalmente ao próprio processo – a características nele intrínsecas –, e só em grau menor às suas condições de partida, ao intercâmbio com o ambiente ou à presença eventual de uma instância supervisora."

Os sistemas auto-organizados apresentam funções que emergem em caso de necessidade. São compostos por entidades individuais que realizam funções simples utilizando apenas informações locais. Funções do sistema emergem, ou são formadas, pela ação conjunta destas funções elementares (SHEARD, 2008). Um exemplo fantástico de auto-organização é o nosso cérebro, onde os neurônios realizam funções autônomas elementares, sem nenhuma organização supervisora, e a consciência é uma função que emerge de milhares de ações individuais realizadas pelos neurônios (JOHNSON, 2001). Mais detalhes sobre funções emergentes estão apresentados na Seção 4.2.1.

A proposta de chaves autônomas torna possível a rede auto-organizada. Havendo autonomia, as operações de chaveamento podem continuar sendo realizadas, e a rede continuar operando, mesmo enquanto são processados os algoritmos de atualização da topologia. Como a rede continua funcionando, o tempo de processamento de algoritmos de atualização de topologia não precisa ser muito pequeno. Com mais tempo disponível, pode-se aumentar o número de nós de cada sub-rede.

A arquitetura de rede auto-organizada está sendo chamada de rede BUONA, sigla em inglês para *Bottom-Up Organized Network Architecture* (Arquitetura de Rede Organizada de Baixo Para Cima).

4.2.1 Funções Emergentes

O termo “Função Emergente” é utilizado em diferentes áreas como física, química ou biologia. Apesar de não existir uma única definição formal para o termo, duas definições podem ser inferidas:

- Uma função que não existe regularmente em um sistema e aparece ou é ativada automaticamente em uma situação de emergência, pela ação de operações simples realizadas por elementos individuais que constituem o sistema.

- Uma função que está sempre presente em um sistema (ela caracteriza o sistema) e tem origem em operações simples realizadas por elementos individuais que constituem o sistema.

Uma função emergente é associada ao sistema (BRESCIANI, 2000) e não às partes individuais que constituem o sistema, apesar de sua emergência resultar de pequenas alterações nas operações das partes individuais (na primeira definição) ou das operações regulares das partes individuais (na segunda definição).

Os modelos montados para descrever a natureza, desenvolvidos pelos físicos, químicos e biólogos, estão repletos de casos que podem ser considerados como exemplos de sistemas auto-organizados. Todos estes modelos baseiam-se em sistemas complexos compostos por um grande número de elementos, cada um dos quais executando funções muito simples. Milhares de formigas executando funções simples constituem um formigueiro que opera com organização de baixo para cima. Este tipo de organização inclui características desejáveis que emergem da combinação das operações simples executadas individualmente pelas formigas. As características emergentes ou Funções Emergentes não podem ser deduzidas a partir das funções básicas executadas pelos indivíduos se forem utilizados apenas modelos clássicos constituídos por equações reversíveis de movimento. As Funções Emergentes são uma conseqüência de sistemas instáveis e irreversíveis que

precisam ser tratados estatisticamente. Este é o mesmo tratamento utilizado também nos sistemas caóticos (PRIGOGINE, 1993), onde as conseqüências não podem ser derivadas das condições iniciais devido à grande sensibilidade do sistema a pequenas flutuações de tais condições iniciais.

A utilização da terminologia “emergência” na área de engenharia é controversa, porque as características desejáveis resultam da arquitetura do sistema e não são aparições surpreendentes que emergiriam aparentemente do nada. Alguns pesquisadores preferem utilizar a terminologia “Arquitetura Autonômica” (SIFALAKIS, 2006) referindo-se à autonomia que a arquitetura confere às operações da rede. A expressão Função Emergente, entretanto, não indica que algo emerge simplesmente do nada. Mesmo na natureza, as características desejáveis são conseqüências das regras e operações individuais, e nunca são algo que emerge do nada. Nos modelos de evolução analisados pela biologia, os sistemas despenderam longos períodos de tempo para evoluir e definir suas funcionalidades. As correlações entre as funções individuais e as características globais dos sistemas complexos podem não ser conhecidas, mas tais correlações sempre existem e não se pode dizer que as Funções Emergentes aparecem simplesmente do nada.

Há alguns trabalhos (RYAN, 2006; DE WOLF, 2004; JOHNSON, 2001) que discutem a utilização do termo “emergência” na engenharia. Nestes trabalhos, são discutidos os significados e as utilizações do termo, chamando a atenção para abusos de significados como é o caso da utilização de emergência como sinônimo de camada. Este abuso acontece pelo fato das funções emergentes serem, muitas vezes, consideradas funções executadas em camadas ou categorias diferentes das funções básicas executadas pelos elementos individuais.

A expressão Função Emergente é utilizada nesta tese com os dois significados apresentados no início desta seção. O primeiro significado refere-se a funções que somente são executadas em caso de emergência. As funções de proteção são executadas apenas nos casos de falha em algum dos enlaces. A palavra emergência na língua portuguesa tem o significado de urgência ou necessidade urgente, mas também pode significar surgimento. Na língua inglesa se separa o primeiro significado, que é traduzido por “*emergency*”, do segundo significado

traduzido por “*emergence*”. Nesta tese, o termo emergência faz sentido, e é utilizado, com os dois significados.

A função de roteamento nesta tese não é controlada ou executada pela camada de rede (camada 3 do sistema OSI). O roteamento emerge das funções fundamentais executadas pelos nós de rede individualmente. Não é necessário considerar nenhuma entidade superior responsável pela operação das chaves ópticas ou pela rota escolhida pelos pacotes desde a sua origem até o destino. A operação de cada nó de rede é feita exclusivamente com base nas condições locais e nas informações contidas no cabeçalho de cada pacote.

No conjunto de informações locais há também uma tabela de roteamento correlacionando cada endereço final a uma das duas portas de saída. Esta tabela é montada somente na configuração da rede e, diferentemente de outras redes (redes IP, por exemplo), na rede auto-organizada desta proposta não ocorrem atualizações e propagações de tabelas durante a operação da rede. As tabelas se mantém fixas durante os processos de roteamento. Se houver alteração da topologia pelo acréscimo de novos nós ou ocorrência de uma falha, o processo de roteamento continua utilizando as tabelas antigas. Somente as tabelas dos vizinhos mais próximos da região onde a topologia foi modificada precisam de pequenas adaptações. Não havendo urgência para propagação de novas tabelas o problema de convergência dos algoritmos de roteamento pode aceitar maior número de nós da rede. Se as alterações forem definitivas o algoritmo dispõe de bastante tempo para conseguir os novos melhores caminhos. Se as alteração forem de caráter temporário, não é necessário calcular novas tabelas de roteamento. Durante o tempo de cálculo e propagação de novas tabelas o roteamento continua sendo realizado corretamente (embora não otimizado) pelas tabelas antigas e pelos procedimentos locais de tomada de decisão.

Para que este processo funcione cada pacote é enviado para sua porta preferencial de saída ou para a outra porta no caso da porta preferencial estar ocupada. Somente esta regra de operação já torna a rede auto-organizada, ou organizada de baixo para cima. A rede opera de forma autônoma. Sendo assim, o roteamento pode ser considerado uma Função Emergente.

Como o caminho mais curto não é sempre utilizado, a distribuição de tráfego é privilegiada. A carga fica mais distribuída do que no caso em que o pacote é enviado sempre pelo caminho mais curto. A distribuição do tráfego (conjunto de todas as rotas) surge automaticamente pela operação organizada de baixo para cima e constitui também uma Função Emergente.

O acesso de novos pacotes à rede é feito sem colisão. Para isto, cada nó de rede verifica continuamente o conteúdo dentro de uma linha de retardo posicionada antes de cada porta de entrada (Seção 4.1). Desta forma, é possível prever tudo o que deve acontecer em cada porta de entrada com antecedência de alguns micro-segundos. O nó de rede pode prever o futuro com alguns micro-segundos de antecedência. O tamanho da linha de retardo é ajustado para o tamanho do maior pacote que se deseja permitir o acesso à rede. Este procedimento, executado por todos os nós de rede com base nas condições locais, garante o acesso à rede sem colisão. O acesso sem colisão, não necessita de protocolos especiais e é executado localmente pelos nós de rede. Por isso, o controle de acesso é também considerado como uma Função Emergente.

4.2.2 Redes Complexas

Quando se ativa uma rede é preciso executar cálculos de rota, verificação de falha e atuar continuamente para garantir robustez e qualidade de serviço. A tarefa de estabelecer uma rota pode parecer simples, mas, se torna um problema computacional complexo quando o número total de entroncamentos da rede é muito grande. Quando ocorre uma falha, ou quando se acrescenta um entroncamento à rede, as tabelas de roteamento precisam ser refeitas. Quando a rede é muito grande, este procedimento pode demorar mais do que um tempo razoável para que

a rede volte a funcionar adequadamente. Sempre existe a procura por algoritmos mais rápidos para evitar tais atrasos inconvenientes.

4.2.2.1 Endereçamento Hierárquico

Uma opção para tratar grandes redes é limitar o número *N* de entroncamentos dentro de um mesmo domínio. Assim, a grande rede é dividida em domínios com poucos nós de rede. Utiliza-se, por exemplo, domínios contendo, no máximo, 50 nós. Quando um nó de um domínio precisa se comunicar com um nó de outro domínio, não existe uma conexão direta entre eles. Aparece o conceito de hierarquização do sistema de endereçamento. É necessário informar primeiro o endereço da sub-rede e depois o endereço do destino dentro da sub-rede. Este procedimento de hierarquização do endereço permite tratar redes cada vez maiores, mas sempre existem limitações no número de nós de cada domínio (BONANI, 2003).

4.2.2.2 Auto-Organização

Com a adoção da rede proposta nesta tese, o problema de redes complexas fica minimizado porque os cálculos de rota não precisam ser realizados em tempo real. A rede continua funcionando durante o tempo de cálculo e divulgação das tabelas de roteamento. O número de nós de rede pode aumentar em um mesmo domínio resultando em melhor escalabilidade.

Redes complexas auto-organizadas apresentam outras vantagens. É possível incorporar funções emergentes como, por exemplo, a função de proteção que disponibiliza caminhos alternativos em caso de falha, ou a função de restauração da rota quando o enlace danificado recuperar sua operação normal, ou distribuição de tráfego. Estas funções emergentes podem ser estimuladas pela escolha adequada das funções básicas realizadas pelas chaves autônomas individualmente.

4.2.2.3 Robustez.

Outra característica muitas vezes associada a redes complexas é a robustez. Uma rede com topologia em malha é naturalmente robusta por apresentar muitos caminhos alternativos. Em caso de falha de algum enlace, sempre há outro caminho disponível para que a comunicação não seja interrompida. A robustez da rede com topologia em malha, principalmente se possui muitos nós, caracterizando um problema complexo, foi estudada ainda no início da comunicação digital por (BARAN, 1964) que preconizava alta resistência a falha. Na época visualizavam-se redes que podiam suportar grandes destruições, eventualmente causadas por guerra, e permanecer funcionando. Hoje a sobrevivência de uma rede pode ser associada à robustez intrínseca das redes complexas (CARLSON, 2002).

4.3 Proteção e Restauração de Enlace

Para viabilizar o projeto de uma rede que apresente as funções de proteção e de restauração de enlace (consideradas como funções emergentes) foi idealizado um processo com base na manutenção de duas características principais: **roteamento autônomo** e **entroncamento simétrico** (Seção 4.1) em conjunto com um **sistema de sinalização** muito simples descrito a seguir na Seção 4.3.1.

O rompimento de uma fibra óptica pode ser sinalizado em tempo real para o nó de rede imediatamente anterior para que o enlace de saída não seja utilizado enquanto perdurar a falha. Imediatamente depois da falha, o nó de rede notificado do rompimento transmite o aviso para trás para interromper uma das duas entradas garantindo a simetria do nó (**entroncamento simétrico**). Cada nó de rede envolvido no processo de proteção de enlace passa da configuração 2x2 para 1x1.

Com a rede montada convenientemente poucos enlaces são interrompidos, sendo possível preservar a conectividade total. Montar a rede convenientemente significa prepará-la para o acontecimento de falhas. Neste caso, a proposta consiste em dividir a rede em subdomínios pequenos e nomear as portas de entrada e de saída com nomes relativos ao subdomínio que elas pertencem. Nesta tese, são consideradas duas maneiras de realizar esta montagem da rede sistematicamente: sistema de organização por ruas e avenidas (Seção 4.3.2) e sistema de organização por quarteirão (Seção 4.3.3).

4.3.1 Sinalização Localizada

O processo de sinalização é bastante simplificado para não alterar a idéia central de chave simples e rede complexa. Também é muito importante que esta sinalização seja bastante localizada. Não é necessário, nem conveniente, que as informações se propagem por grandes distâncias pela rede. Para identificar a integridade dos enlaces a sinalização é enviada para trás, no sentido contrário ao fluxo de pacotes. Isto é feito enviando-se um sinal óptico inserido em acopladores WDM conforme ilustra a Figura 13. O envio de sinalização no sentido contrário ao da propagação do sinal principal tem sido bastante utilizado. Na rede OMEGA (*Optical Metro network for Emerging Gigabit Applications*) descrita por Rocha (2003) a sinalização é formada por um sinal digital que utiliza comprimento de onda de 1,3 μm para que o acoplador WDM, utilizado para sua inserção, não se constitua em nova fonte de perda para o sinal principal que opera na janela de 1,55 μm. A rede SPINet (*Scalable Photonic Integrated Network*) descrita por Shacham (2005) demonstra a utilização de chaves 2x2 com uma sinalização enviada para trás para funcionar como aviso de recebimento dos pacotes. Nestes dois trabalhos a sinalização consiste em sinais digitais enviados no sentido contrário ao do sinal principal. Nesta tese o mecanismo é ainda mais simples. A sinalização é constituída por um sinal óptico contínuo, sem codificação digital e sem necessidade de processamento. A Ausência do sinal contínuo indica falta de integridade do enlace. Cada chave possui dois lasers inserindo um sinal óptico contínuo nas duas entradas e possui dois fotodetectores recebendo o sinal nas duas saídas (Figura 13). O sinal óptico inicia-se nos dispositivos lasers e termina nos fotodetectores nos nós imediatamente anteriores. Os acopladores WDM, como na rede OMEGA (ROSSI, 2002), evitam aumento de perda de inserção que seria grande no caso de acopladores 3dB e também evitam a propagação da sinalização para outros enlaces da rede, ficando cada sinal restrito a um único enlace cuja integridade está sendo verificada.

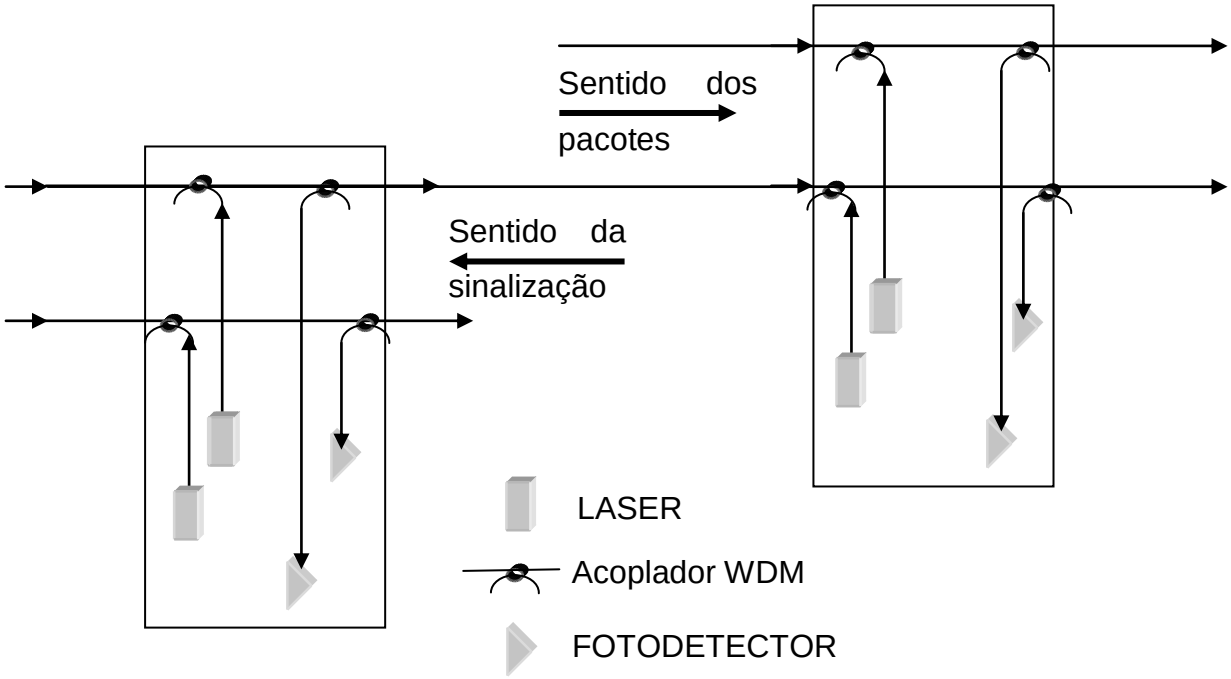


Figura 13: Esquema de sinalização localizada.

4.3.2 Sistema de Organização por Ruas e Avenidas

Várias topologias podem ser utilizadas para o funcionamento deste processo de proteção de enlace. Um exemplo de topologia é mostrado na Figura 14. Esta rede é conhecida como rede *Manhattan Street* por lembrar as ruas e avenidas do bairro de Manhattan em Nova York como ilustra a Figura 16. A rede *Manhattan Street* é uma rede toroidal simétrica, com nós 2x2, como ilustrado para o caso de 16 nós na Figura 14. Neste exemplo, são identificadas as entradas e saídas de forma adequada, diferenciando-se ruas e avenidas. Cada nó de rede, que recebe a sinalização de falha de uma rua de saída, envia a sinalização para trás na rua de

entrada. Este procedimento evita que se escolha uma das duas entradas aleatoriamente para fechamento da porta e divulgação da falha.

Quando ocorre uma falha em uma rua, somente o anel correspondente a esta rua é interrompido. Todos os nós continuam simétricos, todo o processo de roteamento continua sendo executado e todos os nós de rede podem ser alcançados na nova topologia. A Figura 15 ilustra a topologia resultante depois de uma falha em um enlace, do **tipo rua**, localizado no segundo anel horizontal.

Após o fechamento de um anel, as tabelas de roteamento continuam as mesmas, compatíveis com a topologia anterior e podem causar congestionamento e aumento de carga na rede. A única conseqüência do aumento de carga localizado é impedir novos acessos e aumentar a latência, não havendo perda dos pacotes que já estão em trânsito, com exceção dos pacotes presentes nos enlaces interrompidos no exato momento da falha. Todos os pacotes em trânsito, embora com maior latência, chegam a seu destino final.

No momento que a falha é corrigida, os pacotes começam, imediatamente, a utilizar os enlaces recuperados. Este procedimento constitui a função emergente de restauração. Durante o tempo entre a falha e a restauração as tabelas de roteamento ficam inadequadas, mas funcionam e não deixam de encaminhar os pacotes aos seus destinos, mesmo que o destino seja um dos nós que participa da falha. Após a restauração as mesmas tabelas voltam a ser adequadas à topologia fazendo com que a rede recupere suas características iniciais de capacidade e latência.

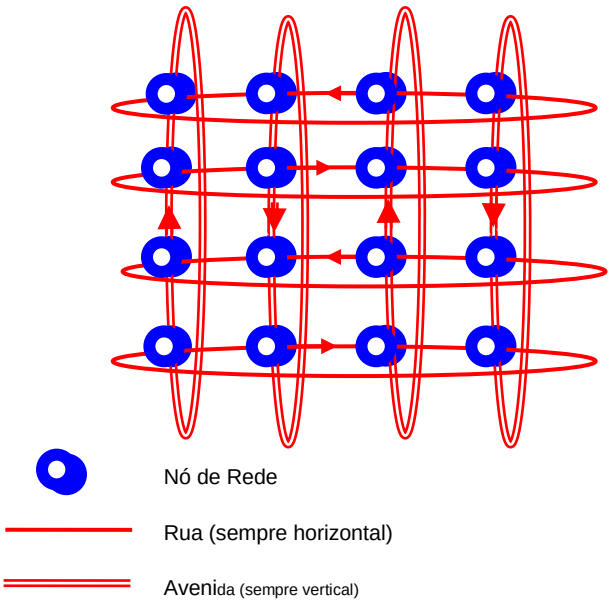


Figura 14: Rede do tipo *Manhattan Street* com 16 nós

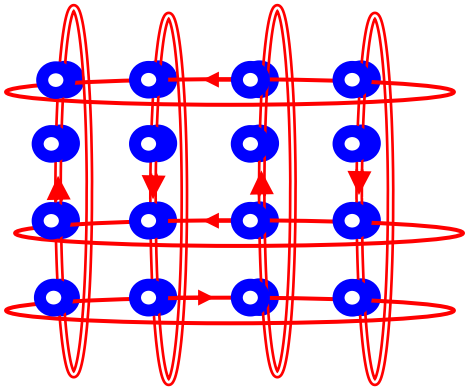


Figura 15: Rede do tipo *Manhattan Street* com 16 nós - Topologia Resultante depois da falha de um enlace horizontal (tipo “rua”)

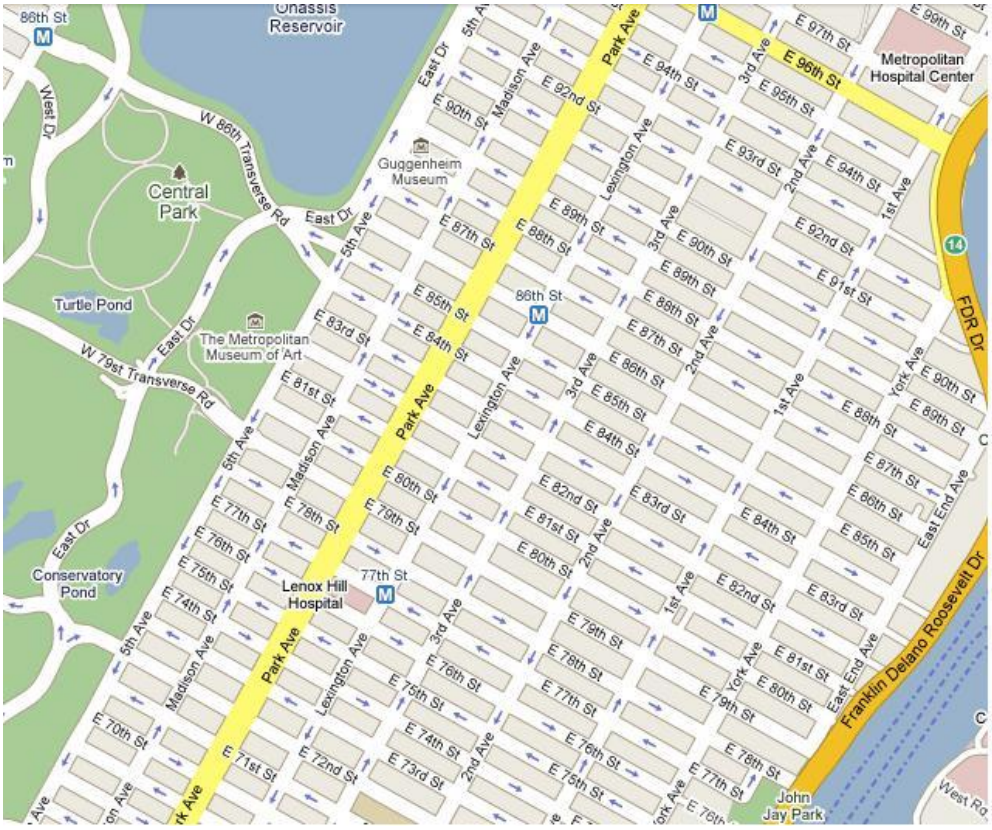


Figura 16: Mapa de Manhattan com ruas horizontais e avenidas verticais. Fonte: GoogleMaps (GOOGLE, 2008)

4.3.3 Sistema de Organização por Quarteirão

Outras convenções para nomear as portas de entrada e portas de saída são possíveis, e podem ser melhores do que a separação entre ruas e avenidas. Se a rede com *N* nós cresce, cada anel **tipo rua**, ou anel **tipo avenida**, também cresce com $\sqrt{N}$, e todos estes nós terão portas desativadas em caso de falha. Quanto maior a rede mais nós são desativados. Uma alternativa para este problema é montar pequenos anéis, com apenas quatro nós, pertencentes a um mesmo subgrupo preparado para desativação em caso de falha de qualquer enlace do anel. Esta nova

maneira de definir os subdomínios permite o funcionamento de um sistema de proteção sem problema de escala, pois são desativados apenas quatro enlaces independentemente do tamanho da rede.

A Figura 17 ilustra este segundo sistema de numeração de portas que consiste em uma organização por quarteirão. Neste sistema, cada nó com duas portas de entrada e duas de saída está ligado a dois subdomínios de enlaces, mas agora, um domínio é caracterizado por anéis de circulação no sentido horário e o outro caracterizado por anéis de circulação no sentido anti-horário. Assim, os subdomínios ligados a cada nó são sempre compostos por 4 nós, independentemente do número de nós da rede. O efeito e benefícios desta nova estratégia de nomeação das portas de entrada e de saída estão apresentados na Seção 5.4 na discussão sobre a robustez da rede.

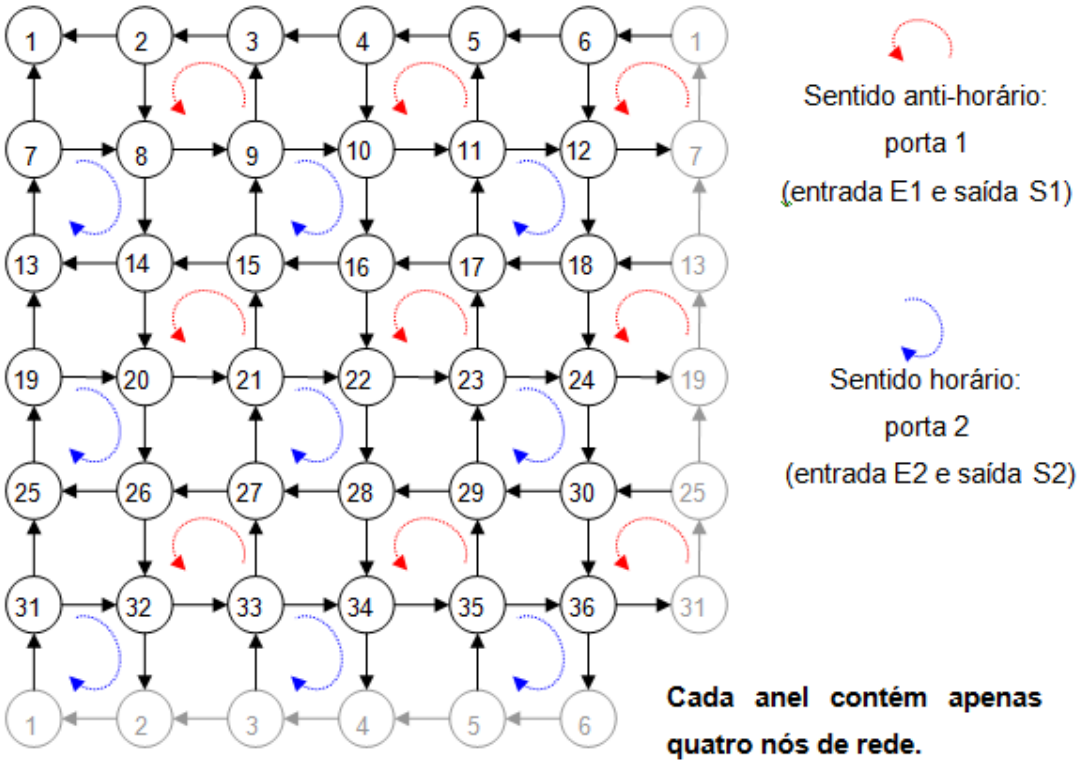


Figura 17: Numeração de portas da rede *Manhattan Street* por quarteirão.

4.4 Considerações sobre a Proposta de Solução

Os pacotes ópticos garantem granularidade fina e a rede auto-organizada permite simplificações do sistema de gerenciamento e permite a escalabilidade do número de nós de um mesmo domínio. Além disso, a rede auto-organizada faz surgir funções emergentes (Seção 4.2.1) como proteção, restauração e distribuição de tráfego, que surgem automaticamente quando estimuladas pela escolha adequada das funções realizadas localmente.

Os problemas de banda, granularidade, agilidade de comutação, escalabilidade, tratamento de redes complexas e custo de implementação são todos resolvidos ou melhorados pela adoção da rede auto-organizada apresentada nesta proposta. A granularidade fina de uma rede de pacotes é intrinsecamente garantida quando não se utilizam pacotes muito grandes como nos chaveamentos em lotes da tecnologia OBS. A rede transparente permite aumentar a taxa de bit até os limites de capacidade das fibras ópticas, reservada a possibilidade de manter um cabeçalho óptico em taxa de bit adequada para as técnicas de chaveamento. A proposta não fixa o método para tratamento dos cabeçalhos. Por isso, se os cabeçalhos forem tratados opticamente, também podem ser escritos em taxas muito altas. Se houver necessidade, como ocorre em muitas redes propostas na literatura, os cabeçalhos podem ser convertidos para o meio elétrico. A rede auto-organizada constitui uma maneira de tratar redes complexas por permitir aumentar o número mínimo de nós de rede sem prejudicar sua operação.

O desempenho da rede, na execução de todos estes processos, pode ser avaliado por simulação. E novos comportamentos podem ser avaliados analiticamente em procedimentos matemáticos que podem tratar redes ainda maiores do que se pode tratar por simulação.

5 Modelagem e Validação da Proposta

A validação da solução através da simplificação, proposta nesta tese, foi obtida por meio de resultados de comportamento da rede verificados com um modelo analítico estatístico que, por sua vez, foi validado por simulação. A proposta foi generalizada para tratar nós de quatro entradas e quatro saídas como na rede NFSNET, comumente utilizada na literatura para análise de novas arquiteturas (BATHULA, 2009). Foram incluídos, também, esquemas de proteção, possibilidades de montagens reais, e a construção de um protótipo de chave óptica rápida. O protótipo, que demonstra a viabilidade técnica e financeira para este tipo de rede, está descrito no Capítulo 6 onde aparece também uma grande variedade de esquemas que podem ser montados utilizando chaves ópticas rápidas de arquitetura simples.

A seguir neste capítulo são apresentados em detalhe os procedimentos e resultados de validação. O modelo analítico está apresentado na Seção 5.1; a validação por simulação aparece na Seção 5.2 e alguns resultados e considerações são apresentados na Seção 5.3. Um resultado importante, decorrente da modelagem, é a robustez da rede destacada na Seção 5.4. A Seção 5.5 apresenta uma discussão sobre vazão e atraso. Na Seção 5.6 é apresentada a generalização para a rede NFSNET. E na Seção 5.7 são tecidas as considerações finais sobre a validação da proposta.

5.1 Modelo Analítico

Um aspecto importante a ser considerado na modelagem é o tempo despendido nos cálculos. Mesmo que o tempo de cálculo aumente polinomialmente com o número de nós de rede (e não exponencialmente), é necessário tomar providências para minimizar este tempo sem, contudo, sobrecarregar os recursos de memória que são utilizados. Com esta finalidade, antes do cálculo do número médio de saltos que um pacote executa entre a origem e o destino (para cada caso com N nós de rede), foi preparada uma matriz de conexão $\boldsymbol{c}$ que informa e identifica todas as conexões diretas existentes na rede. Conseqüentemente, a matriz de conexão traz também toda a informação da topologia de rede. A descrição e cálculo da matriz $\boldsymbol{c}$ são apresentados na Seção 5.1.1. Outra providência importante é calcular o caminho mais curto separadamente para cada caso. Fixados o número de nós e a topologia de rede (representada pela matriz de conexão $\boldsymbol{c}$), calcula-se a matriz de portas preferenciais $\boldsymbol{pp}$. Estas portas preferenciais, por definição, são as portas conectadas ao caminho mais curto. A descrição da matriz $\boldsymbol{pp}$ e a complexidade envolvida no seu cálculo estão apresentadas na Seção 5.1.2. Os resultados destes dois programas (cálculo de $\boldsymbol{c}$ e cálculo de $\boldsymbol{pp}$), gravados em arquivos, podem ser interpretados pelo programa principal que calcula o número médio de saltos. Este último programa (cálculo do número médio de saltos) está descrito na Seção 5.1.3, onde também são apresentadas considerações sobre o tempo de cálculo para esta etapa do modelo.

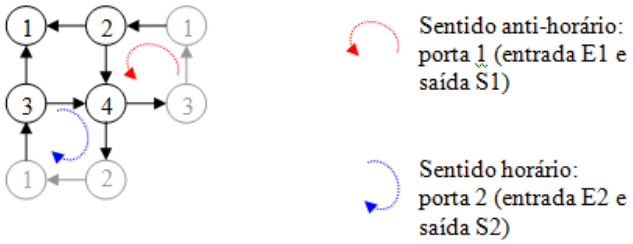
5.1.1 Cálculo da Matriz de Topologia (Matriz de Conexão)

A topologia da rede é representada por uma matriz $\boldsymbol{c}$ que contém informação sobre todas as conexões. Trata-se de uma matriz N x N, onde N é o número de nós da rede. Para esta matriz, valem as seguintes convenções:

- As colunas da matriz representam a posição da origem ou posição atual de um pacote e as linhas os nós de destino que podem ser alcançados com apenas um salto.
- Com exceção dos dois nós conectados diretamente, todos os outros N-2 elementos de matriz são nulos em qualquer coluna de $\boldsymbol{c}$.
- Além de informar quais os nós de rede que estão diretamente ligados, os elementos não nulos de $\boldsymbol{c}$ indicam dois diferentes subdomínios de enlace. Cada nó está ligado a dois outros nós por meio de enlaces pertencentes a dois subdomínios diferentes.
- As posições dos elementos de matriz não nulos indicam os nós que estão diretamente ligados e os valores dos elementos de matriz não nulos indicam o tipo de enlace.
- Dois tipos de enlace são criados para que se possa estabelecer algum critério de escolha no processo de proteção da rede em caso de falha. Esta divisão dos enlaces em dois tipos ou dois subdomínios foi tratada inicialmente na Seção 4.3 onde estão discutidas soluções para proteção de enlace e problemas de escala. Os tipos de enlace podem ser tipos rua e avenida (Seção 4.3.1) ou então tipos quarteirão horário e quarteirão anti-horário (Seção 4.3.2).
- Cada coluna possui dois elementos não nulos que podem ser o número 1 para representar que o enlace de saída pertence ao subdomínio 1 ou o

número 2 para representar que o enlace de saída pertencente ao subdomínio 2.

A Figura 18 ilustra a montagem da matriz $\boldsymbol{c}$ para o caso de uma topologia em anel com quatro nós 2x2, que também corresponde à topologia *Manhattan Street* com $N=4$. Todos os enlaces pertencentes ao quarteirão que circula no sentido anti-horário, ligam entradas e saídas que devem ser denominadas pelo número 1. Todos os enlaces que pertencem ao quarteirão que circula no sentido horário ligam entradas e saídas que devem ser denominadas pelo número 2. Assim é possível reconhecer qual das duas saídas pertence a qual dos dois sub-domínios.



	Origem nó 1	Origem nó 2	Origem nó 3	Origem nó 4
Destino nó 1	0	2	1	0
Destino nó 2	1	0	0	2
Destino nó 3	2	0	0	1
Destino nó 4	0	1	2	0

Figura 18: Montagem da matriz de conexão $\boldsymbol{c}$ para rede de 4 nós.

5.1.2 Cálculo do Caminho Mais Curto (Árvore Adaptativa)

O caminho mais curto para alcançar o destino é calculado uma única vez para o caso da topologia intacta, sem falha. Como cada pacote pode ser defletido para qualquer porta de saída ele pode ser enviado para qualquer parte da rede. Ele

precisa poder retomar seu caminho em direção ao destino partindo de qualquer parte da rede e não apenas partindo da sua origem. Assim, a tabela de informação de caminho mais curto precisa conter dados partindo de todos os nós de rede. Esta tabela de informação é representada por uma matriz ***pp*** (portas preferenciais) com dimensão N x N, onde as colunas representam a posição eventual do pacote na rede e as linhas representam seu destino final. Cada elemento de matriz indica o número da porta preferencial (1 ou 2). Caso não haja preferência, que significa dizer que as duas portas levam ao destino por caminhos igualmente bons, o elemento de matriz indica esta situação com o número 3.

A matriz de portas preferenciais ***pp*** é montada coluna por coluna a partir da matriz de conexões ***c***. Fazer isto coluna por coluna corresponde a um algoritmo que utiliza procedimento inicial não determinístico (PISTORI, 2006). Este procedimento é não determinístico, porque não se sabe a posição do pacote, sendo necessário calcular o caminho mais curto a partir de cada hipótese para sua posição. É necessário montar *N* árvores partindo-se de cada um dos *N* nós da rede e percorrer todas elas e todas as opções válidas até que todos os elementos de ***pp*** tenham sido determinados.

A Figura 19 ilustra uma árvore montada para calcular a coluna 1 de ***pp***. O número 1 no topo da árvore indica a posição eventual do pacote na rede. Considerando como base a rede *Manhattan Street* de 36 nós apresentada na Figura 17 (Seção 4.3.3), o nó número 1 está ligado diretamente ao nó 6 e ao nó 31. Estes números constituem o nível 1 da árvore. Com este procedimento, os demais níveis da árvore são montados, e em cada passo são preenchidos novos elementos da coluna 1 da matriz ***pp***. O elemento de matriz (6,1) é 1, pois a porta que liga o nó 1 ao 6 é a porta 1 (conforme já disponibilizado na matriz ***c***). O elemento de matriz (31,1) é 2 (valor também obtido pela consulta à matriz ***c***). Os números das portas disponibilizados na matriz ***c*** podem ser acompanhados ou verificados na Figura 17 (Seção 4.3.3).

Na seqüência, completando a árvore, todos os nós encontrados do lado esquerdo (a partir do nó 6) podem ser alcançados pela mesma porta número 1 e todos os nós encontrados do lado direito (a partir do nó 31) podem ser alcançados pela porta 2.

Quando um nó é alcançado do lado direito e do lado esquerdo no mesmo nível, o elemento de matriz de ***pp*** é feito igual a 3 para indicar que se trata de um caso **tanto-faz**. O nó pode ser alcançado com o mesmo número de saltos tanto pela porta 1 como pela porta 2.

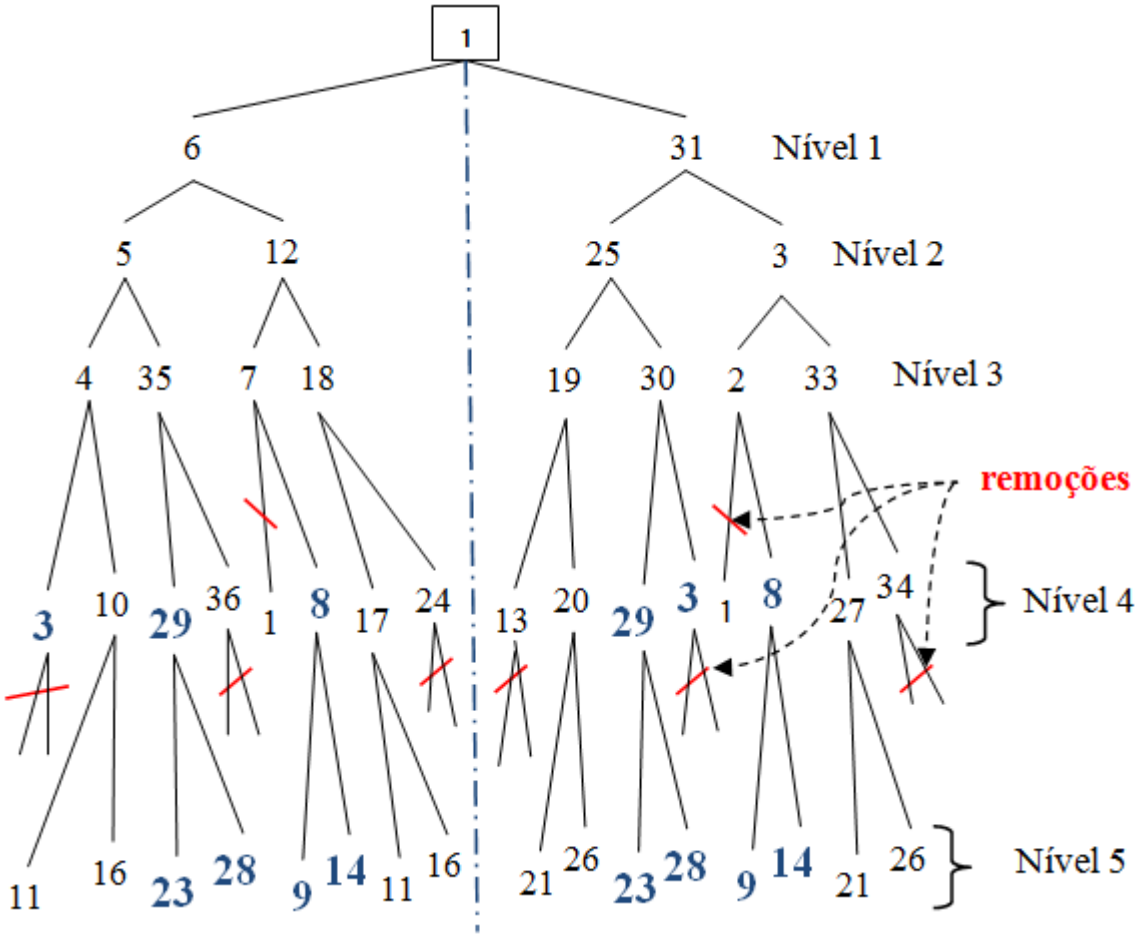


Figura 19: Árvore adaptativa para cálculo da matriz de caminhos preferenciais.

Seguindo este procedimento, o número de elementos em cada nível cresce exponencialmente. Isto constitui uma forte limitação na escalabilidade do número de nós. Para resolver o problema de escalabilidade foi adotado o mecanismo de árvore adaptativa (PISTORI, 2006). Neste mecanismo, a árvore adapta-se em cada nível e todos os nós que já tiverem sido encontrados em níveis anteriores são removidos. Estas remoções estão indicadas na Figura 19. Este procedimento deve ser repetido

N vezes com árvores semelhantes iniciando com cada um dos nós da rede para que se possa montar toda a matriz de portas preferenciais.

A adaptatividade reduz a complexidade computacional fazendo com que o crescimento exponencial do tempo de cálculo seja reduzido para um crescimento polinomial de grau 2 conforme ilustra a Figura 20, onde foram registrados os tempos de cálculo em função do número de nós da rede obtidos em um computador pessoal Pentium 4 com 2GB de memória RAN.

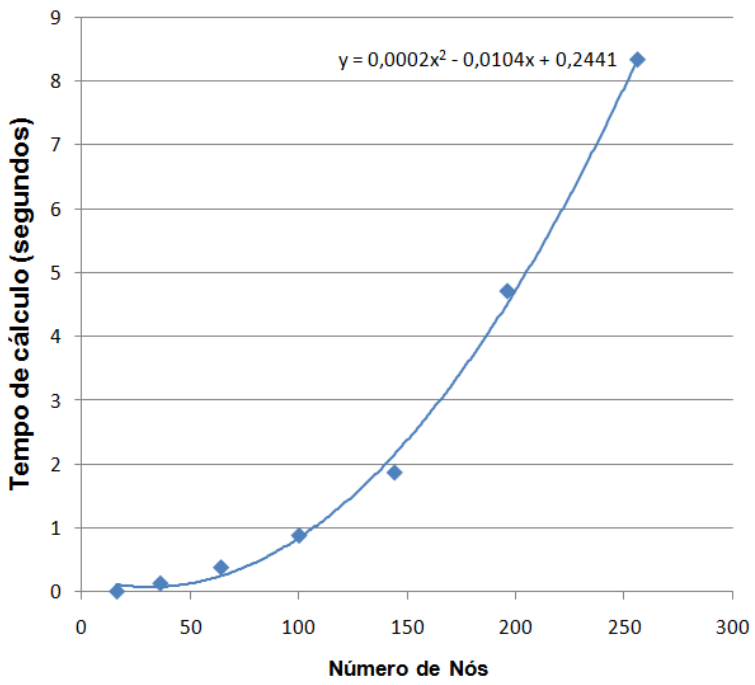


Figura 20: Tempo para calcular o caminho mais curto em função do número de nós de rede

5.1.3 Cálculo do Número Médio de Saltos

O programa principal calcula o número médio de saltos que um pacote executa desde a sua origem até o seu destino. O presente modelo considera a propagação

no tempo de um vetor distribuição de probabilidades definido a seguir na seção 5.1.3.1. As probabilidades envolvidas para que um pacote consiga sair pela porta preferencial, mantendo-se no caminho mais curto, são apresentadas na Seção 5.1.3.2. Outras probabilidades precisam ser modeladas. A probabilidade de ocupação de um enlace (*Poc*) está discutida na Seção 5.1.3.3. A probabilidade de um pacote ser local (Ppl) está na Seção 5.1.3.4. A probabilidade de um pacote concorrente sair por uma porta diferente, probabilidade Pop (Probabilidade de outra porta), está na Seção 5.1.3.5. A descrição e montagem do operador U (Equação 1) de evolução do vetor de probabilidades está na Seção 5.1.3.6. O algoritmo final que permite utilizar este modelo para cálculo do número médio de saltos está descrito na Seção 5.1.3.7.

5.1.3.1 Fundamentação

O modelo tem por base a evolução de um vetor $P(x)$ com N dimensões. O parâmetro x é a posição do pacote ($x = 1, 2, 3, ..., N$) e $P(x)$ representa a probabilidade de que um determinado pacote de teste (um pacote hipotético) seja encontrado na posição x. Este vetor é chamado de vetor de distribuição de probabilidades. Para cada instante de tempo t existe um vetor de distribuição de probabilidades $P_t(x)$. O intervalo de tempo entre t e $t+1$ corresponde a um salto entre dois nós de rede consecutivos, executado por um pacote no seu caminho, de muitos saltos, desde a origem até o destino. O tratamento matemático para calcular a evolução da distribuição de probabilidades com o passar do tempo corresponde a aplicar um operador U ao vetor de distribuição de probabilidades $P_t(x)$ em qualquer instante de tempo t para obter o vetor distribuição de probabilidades $P_{t+1}(x)$ no instante de tempo $t+1$.

$$P_{t+1}(x) = UP_t(x) \qquad \text{(Equação 1)}$$

O operador *U* é análogo ao operador “Perron-Frobenius” utilizado na teoria do caos para cálculo da evolução temporal de uma distribuição de probabilidades (PRIGOGINE, 1993). Pode ser feita uma analogia com a teoria do caos, onde a idéia de trajetória é abandonada e substituída pela evolução de uma distribuição de probabilidades. Nesta tese, a idéia de caminho seguido por um pacote é substituída por um vetor de distribuição de probabilidades que evolui no tempo conforme a Equação (1).

5.1.3.2 Probabilidade das Portas Preferenciais (Ppp)

A porta preferencial de saída sempre é identificada antes do início do programa que calcula o número médio de saltos. Esta identificação está contida na matriz $\boldsymbol{pp}$ calculada previamente conforme procedimento descrito na Seção 5.1.2. A probabilidade de que um pacote utilize a porta preferencial é calculada como se segue.

Se o encaminhamento para uma das duas portas de saída fosse completamente aleatório, a chance para cada porta seria de 50%. Entretanto, a porta correta é ajudada por alguns fatores de desvio (*bias factor*) que a tornam a porta de saída mais provável. O modelo considera que um pacote é encaminhado para sua porta preferencial em três casos:

1) Caso não haja outro pacote no enlace competidor que possa chegar antes;

2) Caso haja outro pacote que pode chegar primeiro, mas tem o endereço local e, portanto é removido antes da competição;

3) Caso haja outro pacote que chega primeiro, que não seja local, mas tem porta preferencial diferente do pacote em teste.

Considerando-se que a probabilidade de ocupação de um enlace é *Poc,* a probabilidade do primeiro caso, ou a probabilidade do enlace concorrente não estar ocupado, é dada por $P_1=1-Poc$. A probabilidade de ocorrer o segundo caso é a probabilidade de não ter ocorrido o primeiro, mas o pacote concorrente tem endereço local e deve ser removido antes que possa atrapalhar ou competir por uma porta de saída. Sendo Ppl a probabilidade de um pacote ter endereço local, o segundo caso tem probabilidade $P_2=Poc.Ppl$. A probabilidade do terceiro caso é a probabilidade de existir pacote concorrente, não ser pacote local, mas desejar outra porta. Se Pop é a probabilidade de um pacote desejar outra porta, o terceiro caso tem probabilidade $P_3 = (Poc)\cdot(1-Ppl)\cdot Pop$. Em resumo, os três casos têm respectivamente as seguintes probabilidades:

$$P_1 = 1 - Poc \qquad \text{(Equação 2)}$$

$$P_2 = Poc \cdot Ppl \qquad \text{(Equação 3)}$$

$$P_3 = (Poc)\cdot(1-Ppl)\cdot Pop \qquad \text{(Equação 4)}$$

A probabilidade de um pacote conseguir sua porta preferencial *Ppp* é dada pela soma destas três probabilidades.

$$Ppp = 1 - Poc + Poc \cdot Ppl + (Poc)\cdot(1-Ppl)\cdot Pop \qquad \text{(Equação 5)}$$

A probabilidade complementar, de não ocorrerem nenhum dos três casos, é a probabilidade de deflexão *Pd* apresentada na Equação 6.

$$Pd = 1 - Ppp \qquad \text{(Equação 6)}$$

Falta incorporar ao modelo uma maneira de avaliar as probabilidades Poc, Ppl e Pop que aparecem na Equação 5.

5.1.3.3 Probabilidade de Ocupação (Poc)

A probabilidade de ocupação de um enlace Poc depende da carga. A Figura 21 ilustra dois enlaces concorrentes na entrada de um nó de rede, colocados paralelamente para que os instantes de chegada de cada pacote possam ser comparados. O pacote P_1 chega à porta de entrada E_2 depois do seu concorrente. Enquanto P_2 chega à frente de seu concorrente. A probabilidade Poc de P_1 ou P_2 encontrarem um concorrente chegando à sua frente corresponde à somatória de todos os espaços ocupados L_j dividida pelo tamanho total do enlace L_T. Somar todos os espaços ocupados em um enlace corresponde a determinar os espaços ocupados pela carga da rede. Assim, a probabilidade Poc é numericamente igual à carga da rede. Carga de 100% corresponde a pacotes preenchendo todos os enlaces, ou seja, a somatória de L_j é igual ao comprimento do enlace L_T. É necessário ressalvar, entretanto, que com o acréscimo de uma linha de retardo os pacotes se distribuem pelos enlaces e pelas linhas de retardo. Em todos os cálculos e simulações foi considerado que a linha de retardo tem o mesmo comprimento que os enlaces, fazendo com que Poc seja sempre numericamente igual à metade da carga.

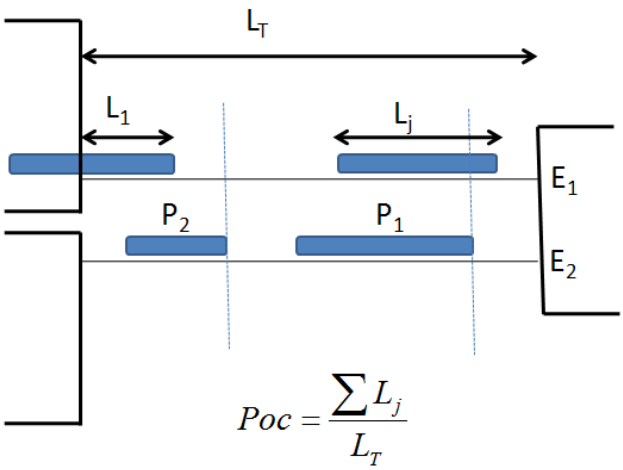


Figura 21: Cálculo da probabilidade de ocupação *Poc*

5.1.3.4 Probabilidade de Pacote Local (Ppl)

A probabilidade de um pacote ter seu endereço final no próprio nó de rede onde se passa a contenda, probabilidade Ppl de um pacote ser local, foi avaliada em um primeiro modelo como sendo $1/(N-1)$. Esta hipótese baseia-se no fato de que um pacote escolhido ao acaso pode ter qualquer endereço, excluindo-se apenas o nó imediatamente anterior ao nó onde se passa a contenda, pois neste caso o pacote nunca teria sido enviado.

Em um segundo modelo, foi considerado que os pacotes em trânsito não podem ter um endereço qualquer. Um pacote em trânsito pode ser encontrado somente no seu caminho entre sua origem e seu destino. E este caminho é constituído por um número de saltos que é muito menor que o número total de enlaces da rede. Considerando que pacotes somente percorrem enlaces que pertençam ao seu caminho, cada pacote está sempre em um destes enlaces. Os caminhos têm um comprimento médio $<H>$ que é o número médio de saltos que se deseja calcular. Um pacote tem endereço local somente no último enlace do seu caminho e a probabilidade de um pacote ser local foi avaliada neste segundo modelo como sendo $Ppl=1/<H>$, que corresponde à probabilidade de um pacote se encontrar no último enlace do seu caminho. Neste segundo modelo é necessário calcular o número médio de saltos, numa primeira aproximação, utilizando o primeiro modelo e depois, de posse de uma boa avaliação de $<H>$, é possível calcular o número médio de saltos definitivo. A Figura 23, com os resultados de simulação apresenta também resultados dos dois modelos de cálculo de Ppl para comparação.

5.1.3.5 Probabilidade de Outra Porta (Pop)

A probabilidade de um pacote concorrente ter outra porta, ou porta diferente, como porta preferencial foi considerada como sendo 50% conforme também foi utilizado em outros trabalhos na literatura (ACAMPORA, 1992; GUEDES, 2005). Não foi encontrado um argumento para polarizar este valor para privilegiar um ou outro lado. Com tráfego uniforme e todos os nós se comunicando com todos os demais, o valor de 50% parece ser mesmo o melhor valor, independentemente da carga ou do tamanho da rede. Fato corroborado também pela concordância entre resultados do modelo analítico e os resultados de simulação.

5.1.3.6 Montagem do Operador de Probabilidades Condicionais

O operador U da Equação 1 é montado a partir da matriz pp de portas preferenciais calculada na Seção 5.1.2. Quando em pp o elemento de matriz é igual a *1*, que representa a saída preferencial, este elemento de matriz é substituído por Ppp que é a probabilidade do pacote sair pela porta preferencial. O elemento de matriz igual a *2* (que representa a porta não preferencial) é substituído por Pd que é a probabilidade complementar a Ppp. O elemento de matriz *3*, que representa uma situação do **tipo tanto-faz**, é substituído por *0,5* para representar probabilidades iguais para os pacotes que não possuem uma porta preferencial. A matriz U montada desta maneira constitui uma matriz de probabilidades condicionais. Dado que o pacote está em uma dada coluna, as linhas representam as probabilidades de passar para cada um dos demais nós da rede.

5.1.3.7 Algoritmo NUDESA

O algoritmo utilizado para o cálculo do número de saltos está sendo chamado nesta tese de NUDESA (sigla para NÚmero DE SAltos). É um algoritmo muito simples que pode ser utilizado para qualquer topologia. Está descrito a seguir para a topologia *Manhattan Street*.

A rede *Manhattan Street* pertence a um grupo de simetria conhecido como automorfismo (GREENBERG, 1986). Isto significa que é impossível diferenciar qualquer nó da rede no que diz respeito à sua posição. Como todas as posições são equivalentes, o número médio de saltos é o mesmo independentemente da posição do destino. Assim, basta calcular o número médio de saltos para uma posição qualquer escolhida como destino. Entretanto, depois de introduzida uma falha qualquer, a rede deixa de ser simétrica e o número médio de saltos passa a depender do destino final. Neste caso é necessário calcular o número médio de saltos para cada um dos possíveis destinos e depois calcular a média aritmética entre eles para conseguir uma média geral.

O número médio de saltos é obtido recursivamente pela Equação 1 começando com $P_0(x)$ (vetor de distribuição de probabilidades inicial) para calcular $P_1(x)$, que representa a probabilidade de chegar ao destino x em um único salto. Depois calcular $P_2(x)$, que representa a probabilidade de chegar ao destino x com dois saltos. A rigor, este procedimento deve ser repetido infinitas vezes, pois não existe um número máximo de saltos. Entretanto, com algumas centenas de vezes as probabilidades se aproximam de zero indicando que todos os pacotes já chegaram nos respectivos destinos. Também acontece que o número de vezes que se repete o procedimento para que se possa parar o cálculo com segurança cresce com o número de nós da rede. Para estabelecer o número de vezes que este procedimento deve ser repetido é necessário estabelecer um critério. A soma das probabilidades de um pacote chegar com 1 salto, com 2 saltos, e assim sucessivamente até a probabilidade de chegar com K saltos, deve se aproximar da unidade para um valor

de K suficientemente alto. O procedimento é repetido K vezes enquanto a probabilidade total for menor que $1-\Delta P$. Este valor é verificado com um critério arbitrário$\Delta P=10^{-6}$. Este critério é considerado suficiente tendo em vista que não há diferença nos resultados obtidos com $\Delta P=10^{-5}$.

O número médio de saltos $<H>$ para cada destino x é calculado pela Equação 7.

$$\langle H \rangle = \sum_{t=1}^{K} t P_t(x) \qquad \text{Equação 7}$$

Onde

$$1-\Delta P < \sum_{t=1}^{K} P_t(x) \leq 1 \qquad \text{Equação 8}$$

Para completar o algoritmo, falta avaliar o vetor inicial de distribuição de probabilidades $P_0(x)$. Em um dado instante qualquer, o **pacote teste**, com destino ao nó y, está em um local desconhecido. Ou seja, o **pacote teste** está em qualquer um dos $(N-1)$ nós diferentes do nó de destino (qualquer nó diferente de y). Assim, a probabilidade de encontrar o **pacote teste** em qualquer destes nós é $1/(N-1)$. Estas probabilidades são colocadas para montar o vetor de distribuição de probabilidades $P_0(x)$. Todos os elementos de $P_0(x)$ são iguais a $1/(N-1)$ exceto $P_0(y)$, que é nulo indicando que o pacote não está no destino. Aplicando-se o operador U resulta o vetor $P_1(x)$, com as probabilidades de se encontrar o **pacote teste** em qualquer um dos nós de rede no instante seguinte (após um salto). Aplicando-se novamente o operador U resulta o vetor das probabilidades de encontrar o pacote depois de dois saltos. Procedendo-se desta forma, depois de repetir esta operação K vezes, resulta o vetor $P_k(x)$ contendo as probabilidades de encontrar o pacote em cada um dos nós da rede depois de k saltos. A probabilidade de o **pacote teste** ter chegado ao seu destino final $y=1$ depois de k saltos é $P_k(1)$, primeiro elemento deste vetor.

Fazendo-se $k= 1, 2, 3, \ldots K$ pode-se calcular o valor médio de k pela relação**:**

$$\langle k \rangle = \sum_{k=1}^{K} k P_k(x) \qquad \text{Equação 9}$$

O valor médio $<k>$ da Equação 9 é o valor médio do número de saltos $<H>$ da Equação 7.

Um exemplo numérico do operador U e do vetor inicial de distribuição de probabilidades $P_0(x)$ é apresentado a seguir, para uma rede com nove nós, conforme esquematizada na Figura 22.

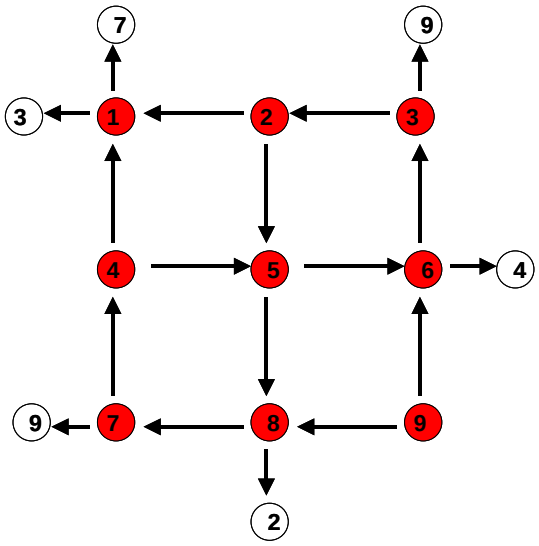


Figura 22: Topologia *Manhattan Street* com 9 nós.

Considera-se que cada nó da rede envia pacotes para todos os outros de forma que a distribuição de tráfego se aproxime de uma distribuição uniforme. Quando a rede apresenta automorfismo, como é o caso da rede *Manhattan Street*, pode-se escolher um nó qualquer como destino de um **pacote teste**. Considera-se, então, que o destino do **pacote teste** é o nó número 1. Se Ppp é a probabilidade do pacote conseguir sair pela porta preferencial e Pd é a probabilidade de ele ser defletido, resulta *U* como a matriz 9x9 da Equação 10. A partir do nó 5 ou do nó 9 não existe porta preferencial para se chagar ao nó 1. Nestes casos, foi adotada a mesma probabilidade de 50% para qualquer uma das duas portas de saída.

$$U = \begin{bmatrix} 0 & Ppp & 0 & Ppp & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & Ppp & 0 & 0 & 0 & 0 & Ppp & 0 \\ 0 & 0 & 0 & 0 & 0 & Pd & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & Ppp & Ppp & 0 & 0 \\ 0 & Pd & 0 & Pd & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & Pd & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & Pd & 0 & 0 & 0 & Pd & 0 & 0 \end{bmatrix}$$

Equação 10

O vetor distribuição de probabilidades inicial $P_0(x)$ é dado pela Equação 11.

$$P_0(x) = \begin{bmatrix} 0 \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \\ 1/(N-1) \end{bmatrix} = \begin{bmatrix} 0 \\ 1/8 \\ 1/8 \\ 1/8 \\ 1/8 \\ 1/8 \\ 1/8 \\ 1/8 \\ 1/8 \end{bmatrix}$$

Equação 11

Quando a rede não tem a propriedade de automorfismo, como ocorre quando falta um enlace depois de uma falha, ou então para outras redes como a rede NFSNET tratada na Seção 5.6, os números médios de saltos para um destino qualquer não serão iguais e é necessário calcular o número médio conforme descrito acima e repetir a operação para cada um dos destinos finais possíveis e depois fazer a média dos N valores obtidos. A Equação 10 deve ser refeita, pois a porta de saída preferencial depende do nó de destino, e a Equação 11 passa a ter zero somente na posição do nó de destino, como já tinha um zero na posição 1 quando o nó 1 foi escolhido como destino.

5.2 Simulação

Foi realizada uma simulação da rede BUONA utilizando o simulador OMNET++, *software* livre disponível na Internet[14]. Foram simuladas redes do tipo *Manhattan-Street* com quatro e com dezesseis nós. A simulação foi montada com as seguintes características:

- Para simular a carga da rede são utilizados pacotes de tamanhos iguais, de forma que cada um deles ocupa uma fração do enlace que corresponde ao valor da carga.
- Todos os nós enviam pacotes para todos os demais, sendo que qualquer pacote gerado tem sempre o destino sorteado entre os destinos possíveis. Esta providência é tomada para simular grande aleatoriedade e distribuição uniforme de carga.
- Cada enlace recebe esta carga logo no início da simulação, respeitado um sorteio do instante exato em que é enviado cada pacote. Este sorteio simula a aleatoriedade na chegada da carga e evita coincidências nos instantes de chegada dos pacotes em cada uma das portas de entrada de cada nó de rede. Esta coincidência é evento muito raro também na rede real, considerada totalmente não sincronizada[15].

---

[14] Códigos com extenção ".zip" para WINDOWS ou ".tgz" para LINUX disponíveis sem custo em http://www.omnetpp.org/

[15] A rede foi idealizada como totalmente não sincronizada. Assim, mesmo que um pacote chegue com poucos nanossegundos de antecedência, chega na frente e tem direito de sair pela porta preferencial. A probabilidade de dois pacotes chegarem juntos será da ordem de nanossegundos divididos por milissegundos (5 milissegundos corresponde a 1 quilômetro de fibra óptica). A

- Para que a carga se mantenha constante durante o tempo de simulação, todo pacote que chega ao seu destino faz gerar um novo pacote com um destino qualquer também sorteado, com cuidado para que não haja colisão.

- Foram considerados enlaces de fibra óptica com um quilômetro de comprimento e pacotes de tamanhos iguais transmitidos na taxa de 40 Gbps.

- A linha de retardo também é considerada com comprimento de um quilômetro, mesmo comprimento do enlace, sendo responsável pelo tempo de 5 μs entre a retirada de uma amostra e a chegada do pacote até a chave.

- Na taxa de 40 Gbps, um único bit demora 1/40 ns para passar por um determinado ponto de referência dentro da fibra óptica, ocupando espaço físico de 5 mm.

- Para simular uma carga de 25%, os pacotes foram montados com o tamanho de 50.000 bits (6,25 kbytes), porque este tamanho ocupa 250 metros de espaço físico, correspondente a 25% do enlace de um quilômetro.

- Pacotes maiores, com o dobro, o triplo e o quádruplo deste tamanho foram utilizados para simular respectivamente os casos de carga de 50%, 75% e 100%.

- Foram realizadas simulações com cinco milhões de pacotes para cada valor de carga e registrados os números de saltos realizados por cada um dos pacotes. A média destes valores para cada condição de carga foi confrontada com a média obtida pelos modelos analíticos (Figura 23).

A Figura 23 mostra o resultado da simulação (linha pontilhada) em comparação com dois modelos analíticos (curvas contínuas). As barras de erro verticais correspondem

---

quantidade de nanossegundos depende apenas da velocidade do circuito eletrônico de detecção para diferenciar o instante de chegada dos dois pacotes.

ao desvio padrão obtido por cinco simulações realizadas independentemente. A curva de valores simulados apresenta uma oscilação que é comum para os casos de 4 nós ou de 16 nós, cuja origem não foi investigada. Independentemente desta oscilação, a simulação segue o Modelo 1 para a rede de 4 nós e segue o Modelo 2 para a rede de 16 nós. O Modelo 2 utiliza $Pop=1/<H>$ (ver Seção 5.1.3.4). Esta concordância valida este segundo modelo analítico (Modelo 2) confirmado como melhor do que o primeiro modelo (Modelo 1) que considera $Pop=1/(N-1)$. Com redes ainda maiores, o primeiro modelo (Modelo 1) produz resultados ainda piores, pois faz com que o número médio de saltos cresça muito mais do que o valor simulado. Isto ocorre porque a probabilidade de um pacote ser local não diminui com $1/(N-1)$, mas diminui mais lentamente com $1/<H>$, como preconiza o segundo modelo (Modelo 2), considerado como modelo mais correto.

Com redes de quatros nós, o primeiro modelo (Modelo 1) mostra melhor concordância com a simulação, mas o número médio de saltos para quatro nós é muito pequeno ($<H> \sim 1{,}5$) e da mesma ordem de grandeza que o valor de $N-1$ utilizado no primeiro modelo (Modelo 1), não produzindo grande divergência entre os dois modelos. Também é possível verificar na Figura 23 que há maior influência dos pacotes locais para situações de maior carga, em que aumenta a probabilidade de que haja um pacote concorrente.

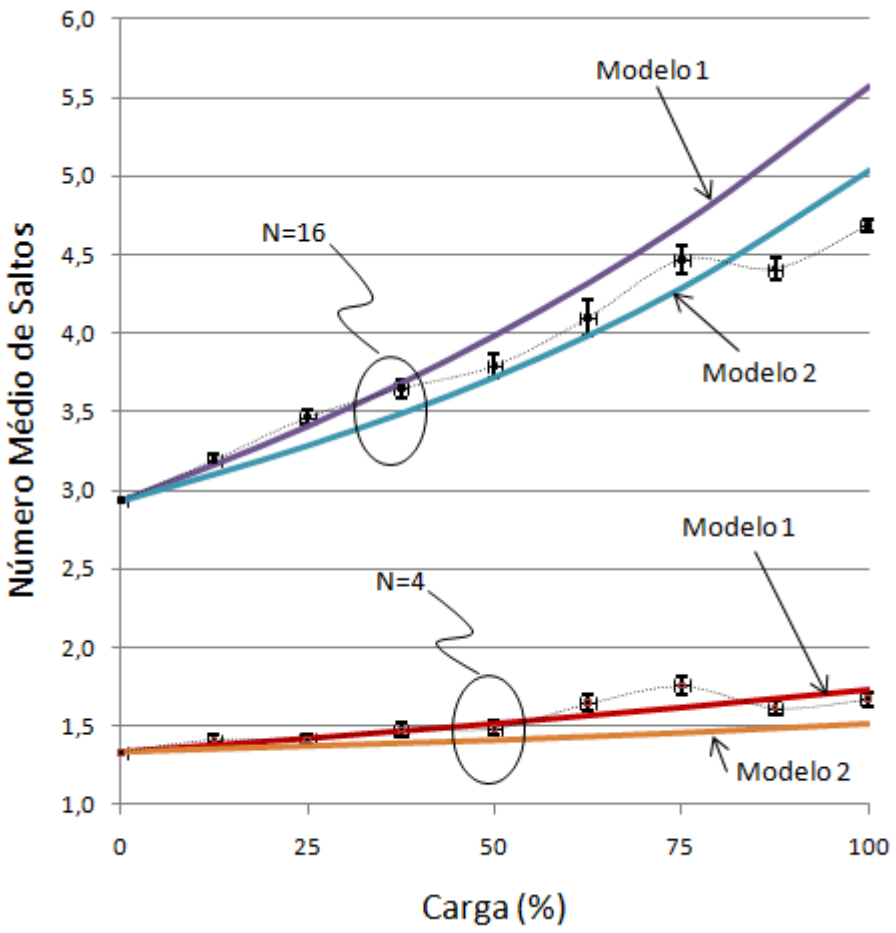


Figura 23: Número médio de saltos em função da carga no enlace. Comparação entre modelos analíticos (curvas contínuas) e simulação (pontos com barras de erro)

5.3 Resultados e Considerações Sobre a Modelagem

A Figura 24 ilustra uma caracterização de redes com até 256 nós. Os pontos da curva para 256 nós foram obtidos em um computador pessoal Pentium 4 com 2 GB de memória RAM em um pouco mais do que um segundo.

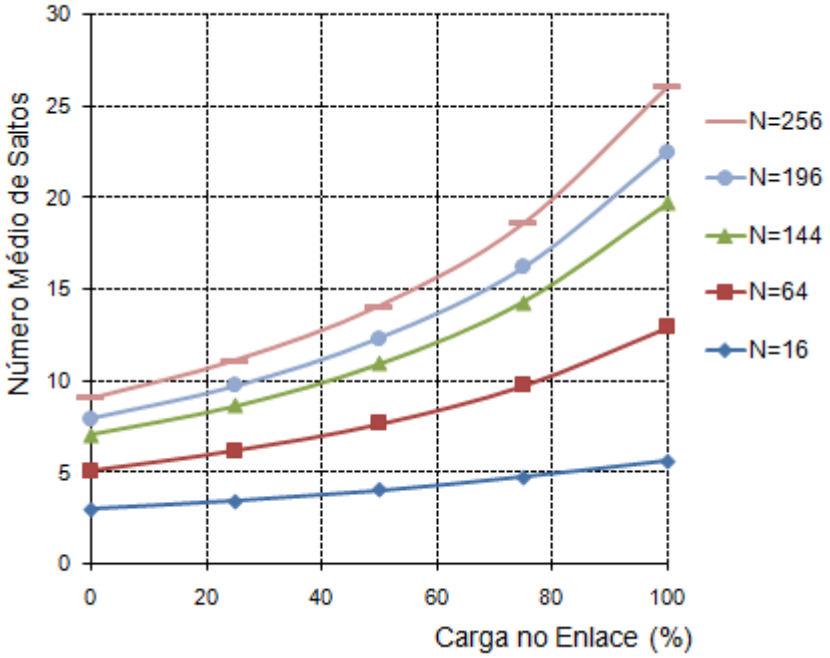


Figura 24: Número médio de saltos em função da carga para rede *Manhattan Street* com N nós.

Para carga igual a zero, os valores obtidos pelo modelo analítico estatístico e também pelo modelo de simulação, correspondem aos valores teóricos exatos para número médio de saltos já conhecidos na literatura (CHUNG, 1990). Estes valores são válidos para os casos de encaminhamento pelo menor caminho. Para redes do tipo *Manhattan Street* com N nós, sendo $n^2=N$ e sendo n um número par[16], valem as relações da Equação 12.

$$\begin{cases} < H > = \dfrac{(N/2)(n+2)-4}{N-1} & \rightarrow (n/2)\ sendo\ \ par \\ < H > = \dfrac{(N/2)(n+2)-2n-2}{N-1} & \rightarrow (n/2)\ sendo\ ímpar \end{cases}$$

Equação 12

[16] Para investigar a escalabilidade da rede foram escolhidos valores crescentes de n, todos pares, por conveniência, pela facilidade de cálculo. As fórmulas para n ímpar e mais detalhes sobre a rede *Manhattan Street* podem ser encontrados na referência (CHUNG, 1990).

Os números de saltos calculados pela Equação 12 para N=256 (n=16, n/2 par); N=196 (n=14, n/2 ímpar); N=144 (n=12, n/2 par); N=64 (n=8, n/2 par) e N=16 (n=4, n/2 par) são, respectivamente, os valores 9,019607843; 7,887179487; 7,020979021; 5,015873016 e 2,93333..., que são os mesmos valores, com todas as suas casas decimais, obtidos pelo modelo analítico estatístico para carga igual a zero, ilustrado na Figura 24.

Quando se introduz uma falha, a rede perde o automorfismo (Seção 5.1.3.7) e é necessário calcular o número médio de saltos para todos os destinos finais possíveis. Neste caso o tempo de cálculo sobe para ordem de 150 segundos (caso de 256 nós utilizando o mesmo computador pessoal Pentium 4 com 2 GB de memória).

A Figura 25 mostra um mapa do número médio de saltos calculado para cada destino final. A primeira linha representa os nós de número 1 a 16. A segunda linha representa os nós de 17 a 32. Na terceira linha (33 a 48) acontece uma falha no enlace entre os nós 45 e 46. O número médio de saltos aumenta quando o destino final é bem próximo da falha. Longe da falha o número médio de saltos não se altera em relação ao número válido para o caso sem falha. A maior parte do mapa se comporta como se a falha não existisse, mantendo o número médio de saltos entre 25 e 27. Próximo da falha o número médio de saltos fica na faixa entre 41 e 42.

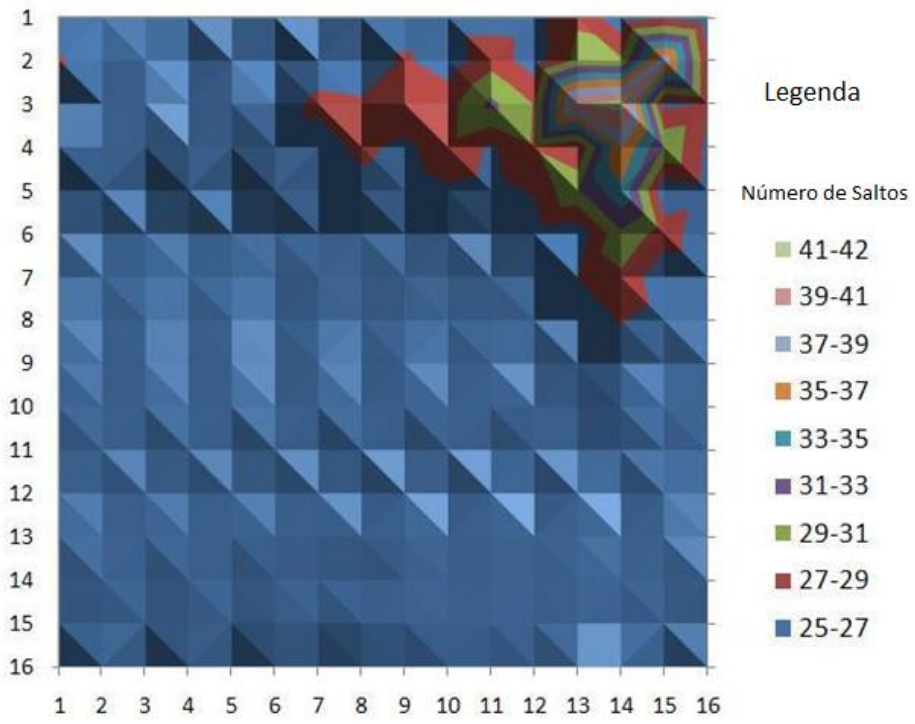


Figura 25: Mapa do número médio de saltos para 256 destinos dispostos em 16 linhas e 16 colunas.

No caso de falha, conforme descrito na Seção 5.4, são desligados quatro enlaces. Os enlaces desligados formam um quadrado de nós adjacentes e mesmo sem automorfismo, uma simetria quadrangular deve permanecer. A falta desta simetria quadrangular na Figura 25 alerta para eventual erro do modelo. Esta falta de simetria decorre do tratamento dado aos nós do **tipo tanto-faz** adotado nas primeiras versões do modelo. Na montagem da Figura 25, foi utilizada uma destas versões antigas. Nestas versões foi considerada como prioritária uma das duas portas de saída dos casos **tipo tanto-faz**. Foi dada prioridade ao nó de menor endereço que corresponde ao primeiro a ser encontrado no algoritmo. Com a correção do modelo que passou a considerar a probabilidade de 50% para cada porta no caso **tanto-faz** (descrito na Seção 5.1.3.6), o mapa mostrou a simetria quadrangular esperada (Figura 29, Seção 5.4.3).

Todos os casos do **tipo tanto-faz** foram identificados e o tráfego supostamente uniforme no início do cálculo deixa de ser uniforme quando a porta 1 (ou 2) é

escolhida de maneira sistemática pelos pacotes do **tipo tanto-faz**. Isto fazia quebrar a simetria quadrangular do mapa de efeitos da falha (Figura 25). Isto foi corrigido, a simetria foi restaurada pela retirada do poder de escolha dos pacotes **tipo tanto-faz** (Figura 29). Para isto foram substituídas as probabilidades Ppp e Pd de todos os pacote do **tipo tanto faz** para 50%. Indiretamente, além de restaurar a simetria quadrangular do tráfego, este procedimento equivale ao procedimento complexo adotado por Acampora (1992), pois a chance de um pacote atrasado ter preferência por uma porta qualquer é de 50% e considerar 50% equivale a ceder a vez para o eventual pacote atrasado. É possível imaginar um mecanismo real que identifique o destino do pacote como não apresentando preferência e aguarde um determinado tempo para encaminhá-lo. Se depois deste tempo chegar algum pacote com porta preferencial bem definida, este conseguirá sair pela sua porta de preferência e o pacote do **tipo tanto faz** será encaminhado para a outra porta, mesmo tendo chegado um pouco antes. A Modelagem pressupõe que este procedimento esteja sendo executado e que caso não haja outro pacote presente, o pacote **tipo tanto faz** deve sortear a porta de saída para manter a simetria do tráfego pela rede

5.4 Robustez da Rede

Como no caso do roteamento, a **proteção** é uma **Função Emergente** que pode ser conseguida pela adoção de procedimentos individuais localizados. A proteção é obtida pela introdução de uma sinalização na direção contrária ao movimento dos pacotes ópticos (Seção 4.3.1) para indicar ao nó de rede que envia os pacotes que a porta de saída está operacional. Com esta simples verificação de continuidade do enlace, adota-se o procedimento de fechar uma das portas de entrada caso uma das portas de saída não esteja operacional. Esta operação é organizada de forma que não seja qualquer porta de entrada a ser desativada, mas sim a porta de entrada

que pertença ao mesmo subdomínio de enlace da porta de saída que deixou de funcionar. Conforme já discutido na Seção 4.3, os subdomínios de enlaces podem ser definidos pela numeração das portas de entrada e de saídas a que estão conectados. A desativação de poucos enlaces torna a falha imperceptível para a maior parte dos nós localizados longe dela.

5.4.1 Proteção para Redes de Muitos Nós

Quanto maior a rede, menor é o efeito da falha no seu desempenho geral. Isto pode ser verificado nas Figuras 26 e 27, que resumem o resultado mostrando que o número médio de saltos, depois da falha, aumenta muito pouco para as redes grandes em comparação com a mesma rede sem falha. O aumento do número médio de saltos para cada rede com o máximo de carga (100%) é tanto menor quanto maior for a rede. A Figura 27 mostra que este aumento tende a zero para redes muito grandes. Esta é mais uma característica de muitos sistemas complexos, que mostram suas funções emergentes tão mais claramente ou mais eficientemente quando é maior a quantidade de indivíduos que formam o sistema.

Outra conclusão que se infere da Figura 26 é que o aumento do número de saltos devido à falha é pior para rede com pouca carga. Isto acontece porque com pouca carga os pacotes são enviados regularmente pelos melhores caminhos, sendo encaminhados para a região com falha e obrigados a aumentar o número de saltos por causa da falha. Com muita carga, o número de saltos é naturalmente alto devido aos freqüentes desvios e a falha tem menor efeito.

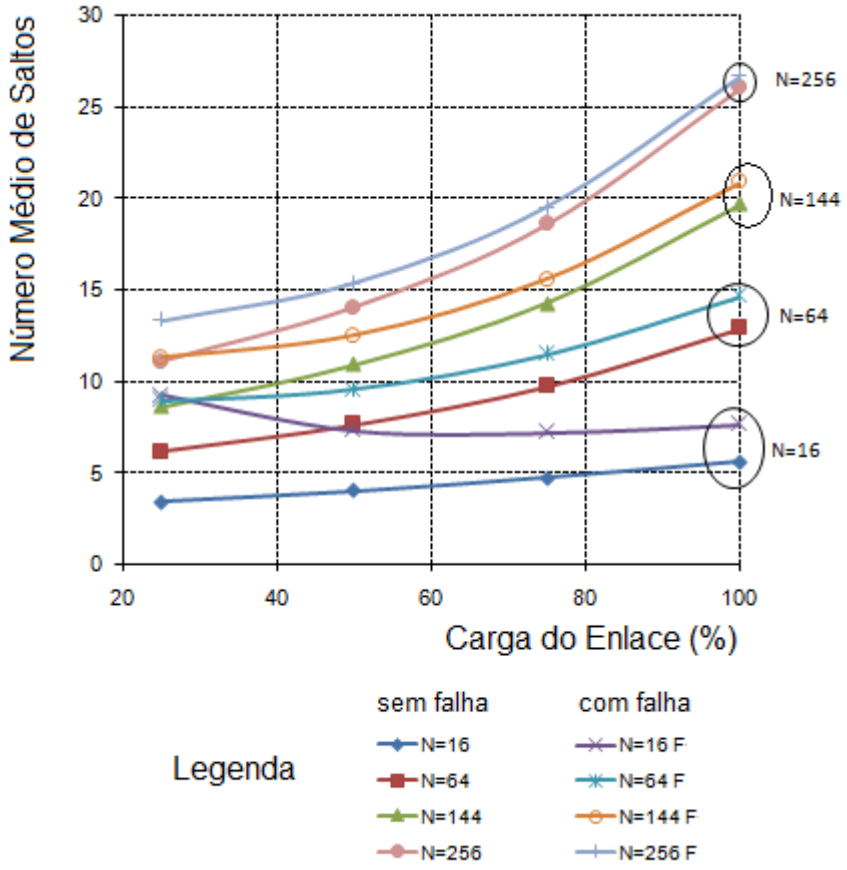


Figura 26: Número médio de saltos com ou sem falha.

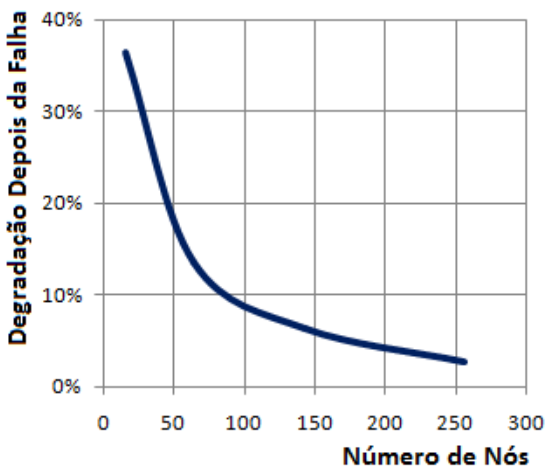


Figura 27: Aumento relativo do número de saltos depois da falha em função do número de nós.

5.4.2 Sinalização de Falha para os Vizinhos mais Próximos

É possível melhorar o processo de proteção pela inserção de uma segunda sinalização. A primeira sinalização descrita na Seção 4.3.1 é a ausência do sinal óptico contínuo que caracteriza a integridade dos enlaces. O sinal de integridade é removido dos enlaces que pertencem ao subdomínio que contém a falha. É possível criar uma segunda sinalização, gerada apenas no caso de falha, que consiste em substituir o sinal contínuo por uma onda quadrada com finalidade de avisar os dois visinhos não envolvidos na falha, que a região está operando de forma restrita.

Além de propagar a falta de continuidade pela porta de mesmo subdomínio, cada nó em falha troca a sinalização enviada para a porta de entrada boa por um sinal do tipo onda quadrada. Este novo sinal indica que a rota que se segue apresenta uma falha, fazendo com que estes vizinhos evitem aquela rota. Quando um nó recebe um sinal do tipo onda quadrada, somente envia pacotes que estejam no seu último enlace. Isto é: não são enviados pacotes para usar a região de falha como passagem, mas somente pacotes cujo destino final é o nó que está enviando a onda quadrada. Com este procedimento os pacotes destinados a um nó com falha conseguem passar e chegar ao seu destino, mas outros pacotes são forçados a evitar a região da falha.

Incluindo esta segunda sinalização no modelo analítico, a rede melhora a sua capacidade de tratar a falha. Este novo procedimento de proteção com dois níveis de sinalização mostra menor aumento do número médio de saltos devido à falha. O resultado está mostrado na Figura 28 para os casos de 16 nós e 256 nós. As curvas indicadas com “F” foram calculadas com um só nível de sinalização. As curvas indicadas com “F2” foram obtidas com dois níveis de sinalização.

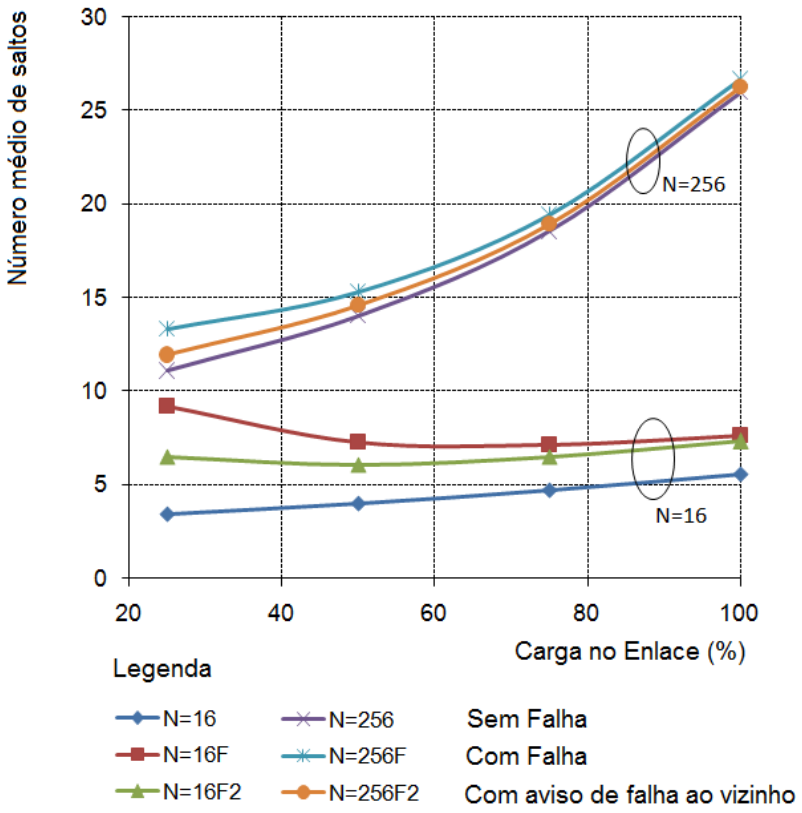


Figura 28: Número médio de saltos com falha, sem falha e com aviso de falha ao vizinho mais próximo.

Este novo sistema de proteção ajuda a entender o mecanismo, já presente na Figura 26 e realçado na Figura 28, descrito a seguir. A rede com 16 nós, na condição de pouca carga (menor que 50%), na condição de falha, tem um comportamento muito afetado pela falha. Tanto que com o aumento da carga o número médio de saltos diminui em lugar de aumentar. Com a inserção do segundo tipo de sinalização, este efeito é minimizado. Avisados com antecedência os pacotes se desviam da falha com mais eficiência. Para o caso de redes maiores este efeito é menos percebido, mas mesmo assim, o aviso aos vizinhos adjacentes à falha faz diminuir a degradação da rede causada pela presença da falha.

5.4.3 Segregação dos Efeitos da Falha

A Figura 29 mostra uma imagem de uma rede com 256 nós (16x16), marcada por curvas de nível contornando a falha. Em todos os nós de rede fora da região demarcada o número médio de saltos é 25, mesmo valor de antes da falha. Cada curva de nível corresponde a um aumento do número médio de saltos de uma unidade, de forma que depois de ultrapassar 8 curvas de nível para chegar na região da falha o número médio de saltos passa a ser 33 (8 unidades a mais). Conforme já discutido na Seção 5.3 a rede com falha não apresenta o automorfismo da rede Manhattan Street, sendo necessário calcular o número médio de saltos para todos os destinos. Nas Figuras 26 e 28, nas curvas com falha, os valores são obtidos pela média aritmética entre os valores calculados para cada destino final. Em lugar de fazer esta média final, a Figura 29 mostra estes valores na forma de mapa para que se possa visualizar o efeito da falha e sua distribuição. O efeito fica confinado na região da falha, sendo que os pacotes com destino longe da falha não têm nenhuma interferência no seu caminho. O número médio de saltos permanece inalterado para a grande maioria dos pacotes caracterizando-se uma segregação dos efeitos da falha no entorno do enlace rompido.

O mapa da Figura 29 tem simetria quadrangular por ter sido adotado o procedimento de sortear a porta de saída nos casos onde não existe uma porta preferencial (**caso tanto faz**) definido na Seção 5.1.3.6 e discutido novamente na Seção 5.3.

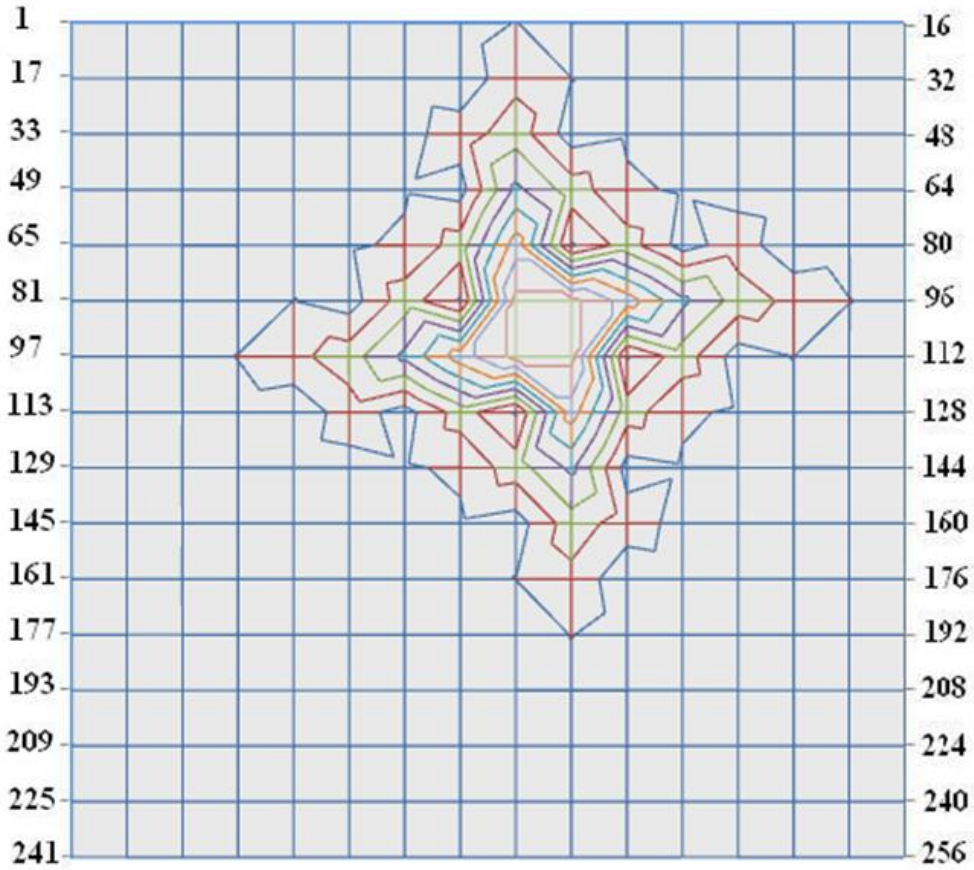


Figura 29: Segregação dos efeitos da falha

5.5 Vazão e Atraso

A vazão da rede e o atraso que cada pacote experimenta ao atravessar a rede podem ser calculados a partir do número médio de saltos.

Define-se vazão como a taxa de bits que a rede consegue transmitir. Isto corresponde à soma de todas as taxas que estão entrando na rede e, em uma situação de equilíbrio, corresponde também à soma das taxas de todos os pacotes

que estão saindo da rede nos seus destinos finais. De posse do valor médio de saltos necessários para chegar ao destino, pode-se calcular a vazão da rede e o atraso que a rede impõe, em média, para cada pacote transmitido.

Se cada cliente transmite com taxa *S* (Gbps), e a taxa de cada enlace da rede é *B* (Gbps), é possível conceber a situação de cada cliente transmitir uma taxa igual à do enlace ($S = B$) somente quando cada cliente transmitir diretamente para os nós de rede vizinhos. No caso de necessidade de mais do que um salto, uma única transmissão ocupa mais do que um enlace e o nó de rede intermediário não consegue dar entrada para seu cliente na mesma taxa. Isto ocorre porque seu enlace de saída está ocupado transmitindo o pacote que está de passagem. Se todos os pacotes enviados precisam passar por dois enlaces cada cliente pode transmitir somente na metade da taxa. Considerando-se que em média o número de enlaces utilizados por um pacote é $\langle H \rangle$, a taxa que cada cliente consegue transmitir é $S=B/\langle H \rangle$. Nesta situação, com todos os clientes inserindo *S* Gbps, a rede fica com 100% de carga (todos os seus enlaces ficam cheios). Para ter algum espaço livre onde as chaves ópticas possam atuar sem risco para os pacotes, é desejável trabalhar com carga menor que a máxima. Para isto, define-se um fator F para limitar taxa de cada cliente, que passa a ser $S=F.B/\langle H \rangle$. Como cada nó pode atender dois clientes, o valor médio de vazão é dado por:

$$\langle \text{vazão (Gbps)} \rangle = 2NFB / \langle H \rangle \qquad \text{Equação 13}$$

Calcular o atraso é mais simples, pois como não há armazenamento óptico, o atraso é função somente do percurso que o pacote tem que atravessar. Como a velocidade da luz dentro da fibra óptica é aproximadamente 200×10^3 km/s o atraso médio em segundos será dado por:

$$\langle \text{atraso (s)} \rangle = L \,.\, \langle H \rangle / (200 \times 10^3) \qquad \text{Equação 14}$$

Onde L é o tamanho do enlace em quilômetros somado com o comprimento das linhas de retardo (DLF). Medindo-se o atraso em milissegundos resulta:

$$\langle \text{atraso (ms)} \rangle = L \,.\, \langle H \rangle / 200. \qquad \text{Equação 15}$$

No caso particular de um rede metropolitana, com enlaces de 5 km e número médio de saltos igual a 15, a Equação 15 fornece um valor médio de atraso de 250 μs, valor muito menor do que em uma rede TCP/IP onde, alem do tempo de propagação, existe também o tempo de processamento dos pacotes em cada roteador. Se em lugar de 5 km fossem 5000 km como acontece na rede NFSNET, o atraso seria de 250 ms, comparável com os valores da rede TCP/IP, pois para longas distâncias quem dita o atraso é o tempo de propagação e não mais o tempo de processamento.

Esta Seção ilustra a importância do parâmetro "número médio de saltos" utilizado nesta tese, a partir do qual pode-se calcular outros parâmetros, como vazão e atraso, comumente utilizados para caracterizar uma rede.

5.6 Generalização

O desempenho da rede pode ser avaliado por comparação com outras redes divulgadas na literatura. Uma rede bastante utilizada como referência é a *National Science Foundation Network* (NSFNet) com 14 nós (NSFNET, 2008).

A NSFNet (Figura 30) considera enlaces bidirecionais. Sendo assim, somente os nós contendo dois enlaces podem ser considerados como chaves com duas entradas e duas saídas como as chaves simplificadas utilizadas neste trabalho. Para comparar o resultado de redes compostas por chaves 2x2 com a rede NFSNET, os nós contendo mais do que dois enlaces bidirecionais podem ser considerados compostos por um anel contendo tantos nós quanto são os enlaces, conforme ilustrado na Figura 31, para um nó de rede contendo quatro enlaces bidirecionais. Este é o caso de Huston e também de Pittsburgh na NFSNet.

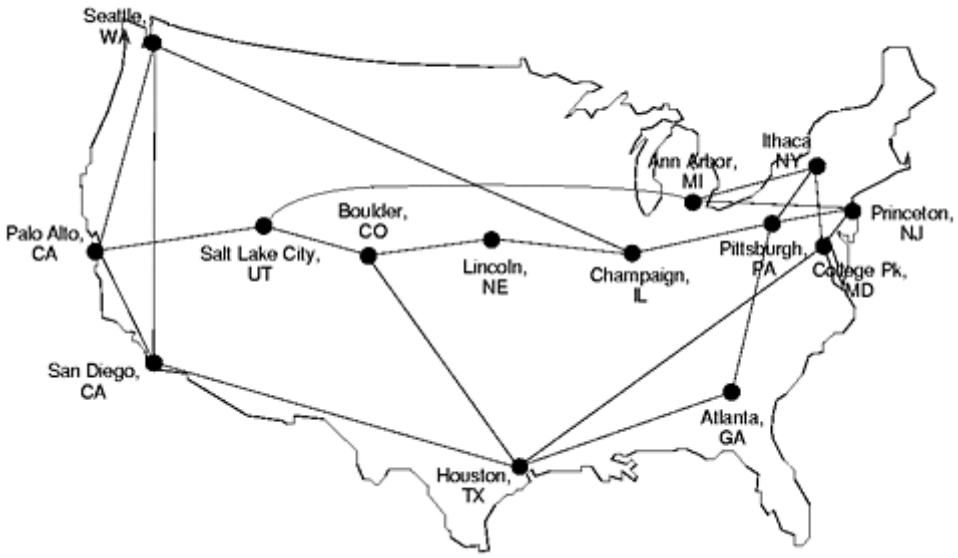


Figura 30: Rede NFSNET utilizada como referência para protocolos de roteamento. Fonte: (NFSNET, 2008)

Dos quatorze entroncamentos da rede NFSNET, dois deles possuem quatro entradas e podem ser representados por 8 chaves 2x2. Dez deles possuem três entradas e podem ser representados por 30 chaves 2x2. Dois deles podem ser representados diretamente por 2 chaves 2x2. No total, é necessário utilizar 40 chaves 2x2. Com este artifício pode ser montada uma matriz de conectividade "*c*", da mesma maneira descrita no item 5.1.1, contando com 40 chaves 2x2 e atendendo a conectividade da topologia NFSNET.

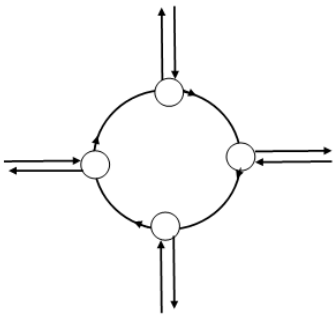


Figura 31: Adaptação em Huston e Pittsburgh da rede NFSNET. Um único nó, com 4 enlaces bidirecionais, pode ser representado por 4 chaves 2x2.

Para incluir um recurso de proteção que diferencia os enlaces de longa distância dos enlaces de curta distância, e também para que o procedimento possa ser utilizado com qualquer rede, foram acrescentados mais dois nós (um em Lincoln e outro em Atlanta) para que todos os nós, mesmo os que podem ser representados por uma única chave 2x2, possam ser representados por uma chave para cada enlace de longa distância. Os subdomínios de enlaces escolhidos para o sistema de proteção são separados em enlaces de longa distância e enlaces de curta distância. Os subdomínios de longa distância têm sempre somente dois enlaces. Os subdomínios de curta distância podem ter até quatro enlaces, mas sendo enlaces internos aos equipamentos, dificilmente são suscetíveis a falhas. Como resultado a topologia NFSNET fica com 42 nós mostrados e numerados na Figura 32, para representar os mesmos 14 nós originais da Figura 30.

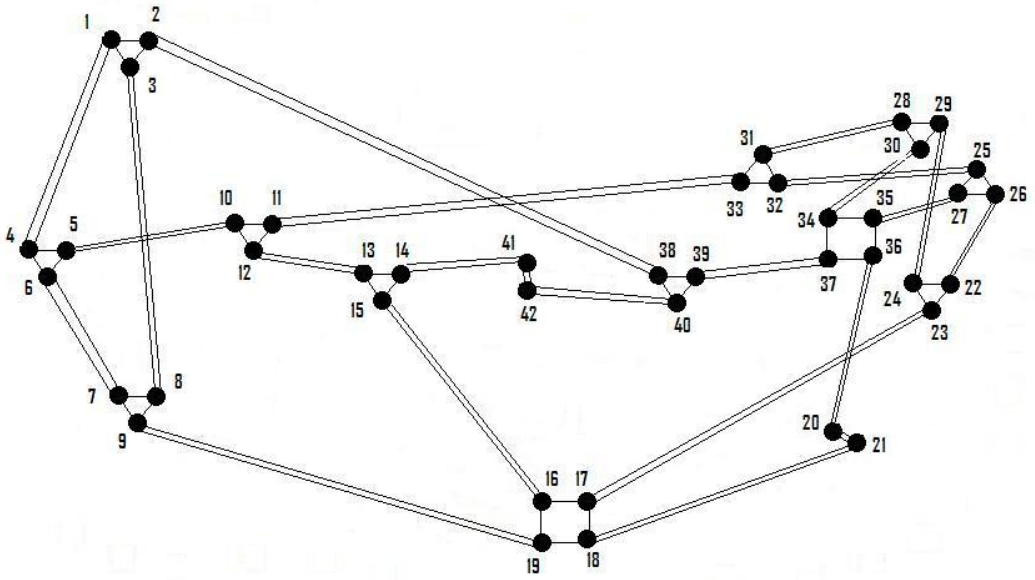


Figura 32: Rede NFSNET com 42 nós que utilizam apenas chaves 2x2.

5.6.1 Generalização para Nós Simétricos 3x3 e 4x4

A Figura 32 ilustra uma possível maneira de montar a rede NFSNET utilizando apenas chaves 2x2. O número de nós aumenta, mas não representa dificuldade para tratamento conforme modelo da rede BUONA. Entretanto, pode-se utilizar o mesmo modelo, mas incluindo-se na análise da evolução estatística os nós 3x3 e 4x4. Estas novas chaves podem ser montadas fisicamente pela composição de chaves 2x2, com um único controle lógico montado em placa com circuitos FPGA (*Field-Programmable Gate Array*) e SERDES (*Serializer/Deserializer)*. Estas chaves também são simétricas e não promovem colisões ou perdas de pacote. Montadas fisicamente em um único equipamento é possível fazer uma única verificação em uma única fibra de retardo para cada uma das portas de entrada (2, 3 ou4 portas de entrada). Desta maneira o sistema tem toda informação para posicionar todas as chaves 2x2 para que cada pacote possa ser atendido sem interrupção durante sua passagem. Esta chave generalizada, simétrica, mas com mais portas de entrada e de saída, consegue tratar melhor o tráfego do uma chave composta por um conjunto de chaves 2x2 completamente independentes. Na Figura 32 há muitos enlaces de tamanho nulo, já com as chaves 3x3 e 4x4 como na Figura 33, a presença de enlaces de tamanho nulo fica descartada.

Para encontrar o caminho mais curto é necessário fazer a árvore adaptativa onde cada ramo pode ser dividido em dois, três ou quatro em cada caso. Também é necessário determinar o segundo e o terceiro caminhos mais curtos se a origem estiver em um nó do tipo 4x4. Basta encontrar o primeiro e o segundo mais curtos nas árvores iniciadas com nós 3x3. Estes segundos e terceiros caminhos mais curtos podem ser caminhos do tipo tanto-faz, que são encontrados no mesmo nível da árvore. A Figura 33 mostra a numeração dos nós utilizada para o cálculo da evolução de probabilidades incluindo os números das portas de saída utilizados nos cálculos.

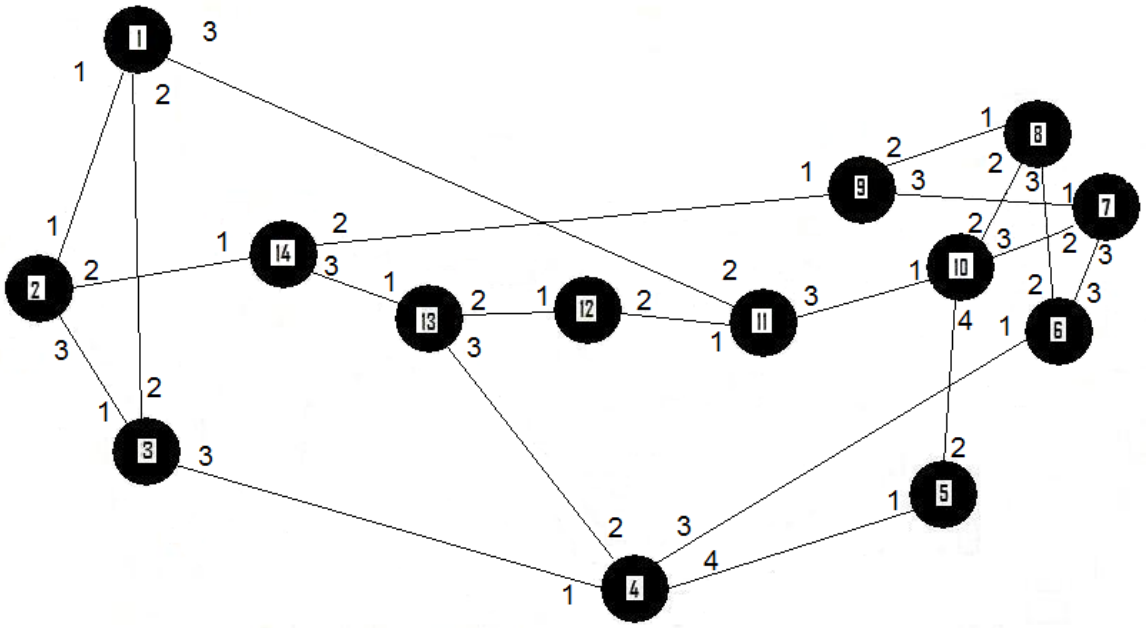


Figura 33: Rede NFSNET com indicação dos números das portas de cada nó de rede.

Ocorre nesta topologia uma peculiaridade decorrente do fato de todos os enlaces serem bidirecionais: nunca uma porta de saída corresponde a um caminho que pode ser mais do que dois enlaces mais longo que o caminho mais curto. Isto porque sempre é possível sair por qualquer porta e voltar para tentar a obtenção do caminho mais curto em uma segunda tentativa. A peculiaridade e também o fato de existirem somente dois nós (nó 4 e nó 11) com possibilidade de escolha de uma terceira melhor opção, optou-se por calcular apenas as duas primeiras opções de porta preferencial. A Figura 34 mostra duas tabelas: a tabela de portas preferências (tabela (a) primeira opção) e a tabela de segunda melhor opção (tabela (b) segunda opção).

0	1	2	1	1	1	2	2	1	1	2	2	3	1
1	0	1	1	1	1	1	1	1	1	2	2	1	1
2	3	0	1	1	1	3	3	1	4	2	2	3	1
2	3	3	0	1	1	3	3	3	4	2	1	3	3
2	3	3	4	0	1	2	2	3	4	3	2	3	3
2	3	3	3	1	0	3	3	3	3	3	1	3	2
3	2	3	3	2	3	0	3	3	3	3	2	3	2
3	2	3	3	2	2	3	0	2	2	3	2	3	2
1	2	1	3	2	3	1	1	0	3	3	1	1	2
3	1	2	4	2	3	2	2	3	0	3	2	3	2
3	1	2	1	2	3	2	2	3	1	0	2	2	1
3	1	2	2	1	1	2	2	1	1	1	0	2	3
1	2	3	2	1	1	3	3	1	4	1	1	0	3
1	2	1	2	1	1	1	1	1	3	2	1	1	0

(a) primeira opção

0	3	1	2	2	3	3	3	3	4	1	1	2	3
2	0	2	2	2	3	3	3	2	4	1	1	3	3
1	1	0	2	2	3	1	1	3	1	3	1	1	3
1	2	1	0	2	3	2	2	1	3	3	2	2	1
3	1	2	2	0	3	3	3	2	3	2	1	2	2
3	2	1	2	2	0	1	2	2	2	2	2	2	3
1	1	2	4	1	2	0	1	2	2	1	1	1	3
1	1	2	4	1	3	1	0	3	3	1	1	1	3
3	1	3	2	1	2	3	3	0	2	2	2	3	3
2	3	3	3	1	2	3	3	2	0	1	1	2	1
1	3	2	4	1	1	3	1	1	2	0	1	3	3
1	2	3	1	2	3	3	3	3	4	3	0	1	1
2	3	1	4	2	3	1	1	3	1	2	2	0	1
0	0	3	1	2	3	3	3	2	4	1	2	2	0

(b) segunda opção

Figura 34: Tabelas de portas preferenciais em primeira opção (a) e segunda opção (b).

Na Figura 34 a matriz representada em (a) apresenta em cada coluna a posição eventual de um pacote na rede NFSNet de 14 nós. Os números representam a porta preferencial pela qual o pacote deve sair para chegar ao destino correspondente a cada linha. Caso a porta preferencial esteja ocupada o pacote é defletido, mas não para uma porta qualquer, pois nas portas restantes pode existir uma segunda porta preferencial. Esta segunda porta preferencial está na tabela (b) da Figura 34.

5.6.2 Resultados e Considerações sobre a Generalização

Com base nas duas matrizes preferenciais da Figura 34 e utilizando-se o algoritmo NUDESA descrito na Seção 5.1.3.7 foi calculado o número médio de saltos da rede

NFSNET com 14 nós e 52 enlaces. A Figura 35 ilustra o resultado comparado com o número médio de saltos de uma rede *Manhattan Street* com 16 nós e 32 enlaces. Com mais enlaces, embora com número de nós muito próximos, a rede NFSNET tem mais opções e produz um número menor de saltos para se chegar ao destino.

A generalização do modelo para chaves 3x3 e 4x4 mostra que a rede pode ser qualquer e que o modelo não se restringe ao caso particular da rede *Manhattan Street*. O modelo pode ser aplicado mesmo para redes de longa distância como é o caso da Rede NFSNET. Entretanto, nestas redes, não havendo necessidade de flexibilidade e agilidade para troca de taxa de bit ou troca de protocolos, pode ser mais adequado trabalhar com tráfego agregado formando grandes canais WDM de alta taxa. Chaves 2x2, 3x3 ou 4x4, utilizadas em redes menores para uso metropolitano, constituem uso mais adequadas para a rede de pacotes ópticos proposta nesta tese.

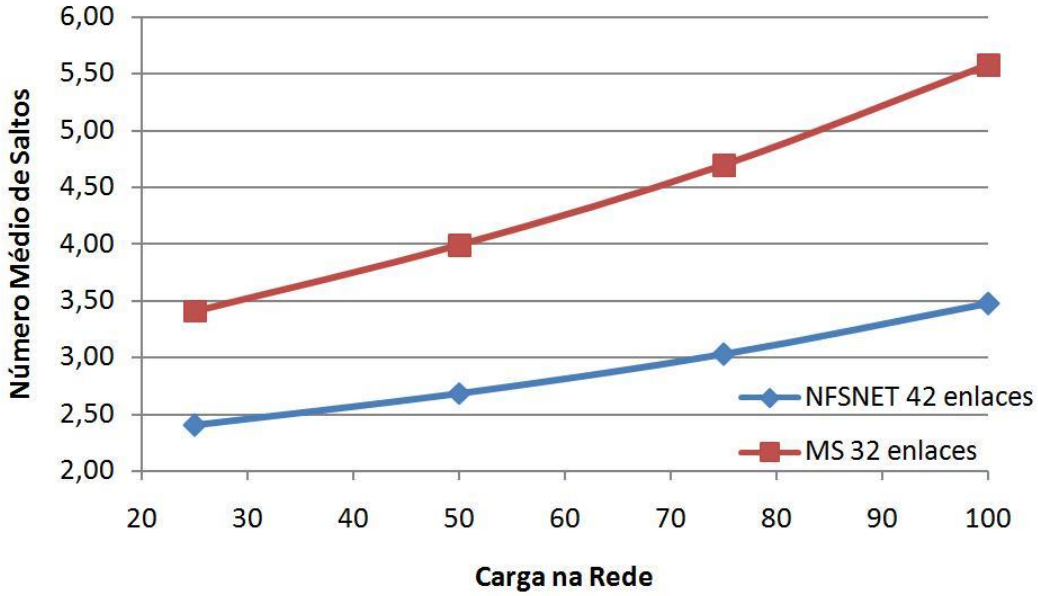


Figura 35: Rede NFSNET com 14 nós 2x2, 3x3 e 4x4 comparada com rede MS com 16 nós 2x2.

5.7 Considerações sobre a Validação

Neste capítulo foram apresentadas cinco etapas utilizadas para validação da proposta de rede auto-organizada utilizando chaveamento de pacotes ópticos:

- montagem de um modelo analítico
- montagem de um modelo de simulação
- verificação da Robustez
- tratamento para vazão e atraso
- generalização

Os modelos analítico e de simulação, utilizam princípios completamente diferentes, e se complementam validando um ao outro. A possibilidade de aplicação para outras redes encontradas na literatura fornece indícios de desempenho e amplia as possibilidades de aplicação da rede proposta. As aplicações mais importantes do chaveamento de pacotes ópticos são em escala metropolitana e de acesso, pela flexibilidade com que diferentes tipos de tráfego e diferentes tecnologias podem ser utilizados e também pela facilidade de instalação, operação e manutenção. Há necessidade de se considerar também as características de granularidade, escalabilidade e robustez das redes de pacotes ópticos desta tese.

A investigação do chaveamento em lotes é uma vantagem adicional que se espera da rede, pois possibilita algum grau de agregação de tráfego, que passa a ser importante nas redes metropolitanas, embora menos importantes nas redes de acesso.

6 Viabilidade e Construção Experimental

Uma grande vantagem da simplificação da chave óptica é a viabilidade que ela confere à tecnologia de chaveamento de pacotes ópticos. Esta técnica pode ser aplicada imediatamente, sem necessidade de aguardar desenvolvimento de novos componentes. Para demonstrar essa viabilidade um protótipo foi construído utilizando-se apenas componentes já existentes no mercado. A função de chaveamento tem por base a operação de dispositivos SOA (*Semiconductor Optical Amplifier*) descrito na Seção 6.1. O protótipo descrito da Seção 6.2 tem característica modular e permite que seja configurado para operar como chave óptica rápida em uma série de arquiteturas possíveis descritas na seção 6.3.

6.1 Chaves Utilizando SOA

Um dispositivo SOA (*Semiconductor Optical Amplifier*) é um amplificador óptico construído a partir de material semicondutor emissor de luz. Possui estrutura muito semelhante à de um laser de semicondutor. Esta semelhança inclui a utilização de compostos como o InP (fosfeto de índio) e ligas quaternárias como $In_xGa_{1-x}As_{1-y}P_y$ (liga de índio, gálio, arsênio e fósforo) na sua construção. Variando-se os valores de x e y da liga quaternária obtém-se materiais semicondutores com diferentes valores de banda proibida e diferentes valores de índice de refração. Ainda de maneira muito semelhante ao laser de semicondutor o SOA é construído pelo crescimento de camadas destas ligas quaternárias sobre substrato de InP para formar uma estrutura que, entre outras características, consegue guiar a luz na camada central, de maior

índice de refração, conhecida como camada ativa. A luz é gerada pela corrente elétrica que injeta portadores na camada ativa. Os fótons de luz gerados caminham pela camada ativa estimulando a geração de novos fótons com mesmo comprimento de onda e mesma direção de propagação. Estes fótons, por sua vez, continuam estimulando a formação de novos fótons idênticos em um processo de amplificação. Nos lasers este processo de amplificação estimulada continua depois da reflexão dos fótons em espelhos formados no final do material (interface do material com o ar ou camada dielétrica protetora) fazendo com que o ganho supere as perdas. A fração de luz que sai do dispositivo possui a coerência da luz de um laser. Nos dispositivos SOA os espelhos são destruídos pelo depósito de camadas anti-refletoras ou pela escolha adequada da geometria do dispositivo para que a luz não encontre os espelhos perpendicularmente. Sem os espelhos, com a luz sendo ampliada em uma única passagem, o ganho não consegue superar as perdas e o estado de funcionamento do laser não é atingido. A grande potência de luz que sai do dispositivo por ter os espelhos pouco refletores constitui a principal fonte de perda que evita o funcionamento como laser, mas o dispositivo funciona muito bem como um amplificador. Mesmo depois de uma única passagem, a luz inserida em uma das extremidades é amplificada enquanto caminha pela camada ativa e estimula os portadores a se recombinarem gerando novos fótons de mesma freqüência, fase e direção. A injeção de novos portadores é garantida pela corrente elétrica que se faz passar pelo dispositivo. O ganho destes dispositivos chega a 20 dB enquanto nos seus concorrentes EDFAs (*Erbium Doped Fiber Aplifiers*) amplificadores a fibra dopada com érbio, pode chegar a 40 dB.

Enquanto nos dispositivos laser, se acopla uma única fibra para que funcione como fonte de luz, nos dispositivos SOA normalmente são acopladas duas fibras ópticas, uma em cada lado do dispositivo, para que se possa inserir luz por um lado e recolher a luz amplificada pelo outro lado.

A Figura 36 ilustra um dispositivo SOA do fabricante Inphenix, com duas fibras acopladas, montado em uma placa de teste do próprio fabricante. O valor mostrado no *display* é a corrente elétrica dada em miliamperes que está passando pelo SOA. A cápsula de 14 pinos permite acesso ao TEC (*Thermo Electric Cooler*) resfriador

termo-elétrico (pinos 1 e 14), ao termistor que mede a temperatura do SOA (pinos 2 e 5), e ao SOA propriamente dito (pinos 10 e 11).

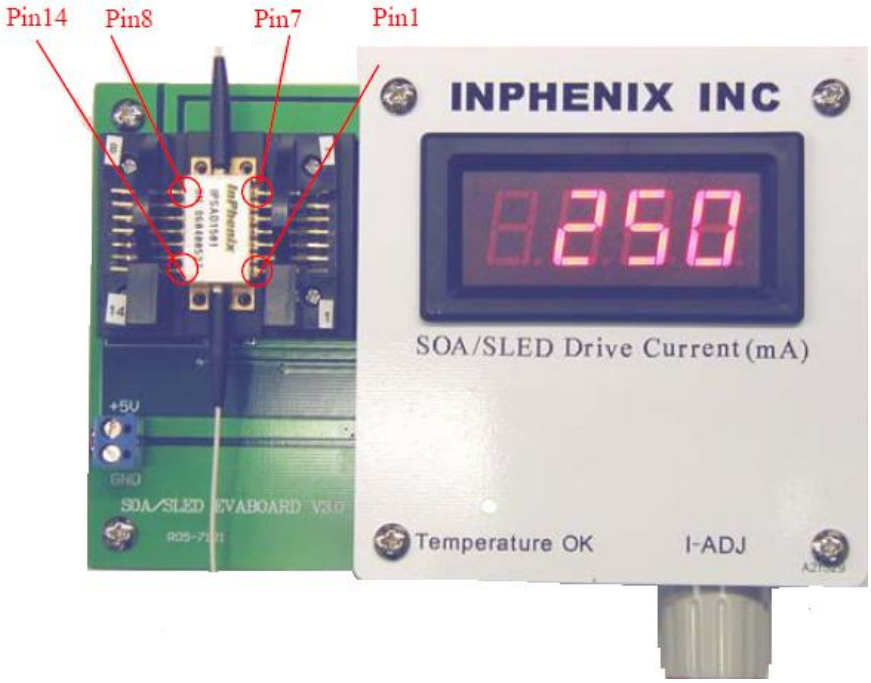


Figura 36: Dispositivo SOA montado na placa de teste do fabricante. Figura retirada do manual de operação (INPHENIX).

O SOA pode ser construído para operar em vários comprimentos de onda. Pode ser utilizado como amplificador óptico na janela de 1,3 μm, onde não funcionam os EDFAs. Estes operam somente na janela de 1,5 μm. Na faixa de comprimento de onda dos amplificadores EDFAs, o SOA perde a concorrência por apresentar menor ganho e também por causa da dependência do ganho com a polarização da luz. Já na janela de 1,3 μm o SOA encontra aplicações como as propostas por (SPIEKMAN, 2007) para ampliar o alcance e aumentar a escalabilidade do número de ramificações das redes ópticas passivas.

Tendo sido idealizado para operar como amplificador óptico, a utilização dos dispositivos SOA para construir chaves ópticas é conseqüência natural pelas suas características. Quando não há corrente elétrica injetando portadores a luz inserida em uma extremidade é toda absorvida pelo material da camada ativa e não chega

quase nada do outro lado. Com isto o SOA funciona como uma chave óptica, deixando passar luz quando ligado e absorvendo a luz quando desligado. A relação entre a potência de luz que sai e a potência da luz inserida na entrada em um dispositivo SOA desligado (sem corrente elétrica) é chamada de razão de extinção.

Para funcionar como chave, a arquitetura do SOA é modificada para melhorar o seu tempo de resposta, mesmo que perdendo um pouco da sua característica de ganho. Mais compridos os dispositivos apresentam mais ganho, mas pioram o tempo de resposta, por aumentar a área da região ativa e sua capacitância residual. Os dispositivos adquiridos para a montagem do protótipo de chave óptica rápida desta tese foram otimizados para funcionar como chave. São mais curtos e apresentam ganho de apenas 10 dB. Com intervalo de tempo subida da ordem de um nanosegundo o protótipo de chave óptica com base nos dispositivos SOA é um milhão de vezes mais rápido do que as chaves MEMS (*Micro Electro-Mechanical System*) utilizadas nas redes de chaveamento de comprimento de onda. Outra característica importante do SOA utilizado como chave óptica é a sua razão de extinção da ordem de 40 dB, que faz com que não passem resíduos de um pacote quando a chave estiver fechada.

Estes dispositivos são muito versáteis. Devido às suas características e potencialidades o SOA pode ser utilizado também para construir conversores de comprimento de onda e dispositivos para codificação e decodificação totalmente ópticos (SCHUBERT, 2004). Todos estes dispositivos podem ser utilizados em uma rede de pacotes ópticos. Em trabalhos futuros, com pouca modificação, estes e outros dispositivos poderão ser emulados no protótipo montado nesta tese.

6.2 Protótipo de Chave Óptica Rápida

Para validação da proposta, no que diz respeito à viabilidade tecnológica e facilidade de implantação da tecnologia, foi montado um protótipo experimental de um nó de rede com chaves ópticas rápidas. A montagem possui quatro dispositivos SOA (*Semiconductor Optical Amplifier*) e oito acopladores passivos 2x2 montados em arranjo modular que permite várias configurações. É possível montar chaves simples, tipo liga-desliga, que interrompe a passagem de luz quando é zerada a corrente elétrica do dispositivo SOA (**chave 1x1**). É possível montar chaves mais completas como **chaves 1x2** para direcionar o tráfego alternativamente entre duas saídas ou ainda montar chaves **2x1** ou **2x2**. Estas duas últimas arquiteturas de chave necessitam esquema de resolução de contenda para evitar colisão entre os pacotes.

Para operações que incluam lógica de chaveamento é necessário acrescentar um módulo de controle rápido que utiliza circuitos lógicos programáveis tipo FPGA[17]. A viabilidade de circuitos lógicos de controle utilizando FPGA já foi demonstrada tanto para OPS (GUEDES, 2005) como para OBS (MOBILON, 2006). Sem um sistema eletrônico de controle a resolução de contenda deve ser realizada por um esquema de agendamento prévio de intervalos de tempo reservados para cada pacote, funcionando como comutação de circuito virtual.

Além do SOA e dos acopladores o protótipo possui outros módulos auxiliares. Os módulos são os seguintes**: Módulo Fonte**; **Módulo de Controle**; **Módulo SOA**; **Módulo Acoplador**; **Módulo Conversor de Mídia** e **Módulo *Transceiver***. Estes módulos podem ser identificados na Figura 37, mostrados da esquerda para a direita

---

[17] FPGA (*Field Programmable Gate Array)* é um *chip* (pastilha semicondutora), com milhares de portas lógicas, que pode ser programado pelo usuário. Normalmente, utiliza-se FPGA em lugar de ASIC (*Application-Specific Integrated Circuit*) no início do desenvolvimento de uma tecnologia.

nesta mesma ordem. O protótipo modular foi todo concebido e projetado no LARC (Laboratório de Arquitetura e Redes de Computadores), financiado pelo Projeto KyaTera da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo). A montagem mecânica e o projeto da fonte e das placas de circuito impresso do Módulo de Controle e do Módulo SOA, bem como a montagem final destas placas foram serviços realizados por contrato pela Empresa Optolink que deixou sua marca na face de cada módulo. Os conversores de mídia e os transceivers comerciais, bem como os componentes SOA foram especificados e adquiridos pelo LARC que também indicou os transistores de chaveamento rápido BFG35 para fornecer corrente elétrica chaveada para os dispositivos SOA. Com relação à placa de circuito impresso que separa os acessos ao laser e ao fotodetector do Transceiver agradeço a participação de Eduardo Mobilon. Nas seções que se seguem são apresentadas as características e funções de cada um destes módulos.

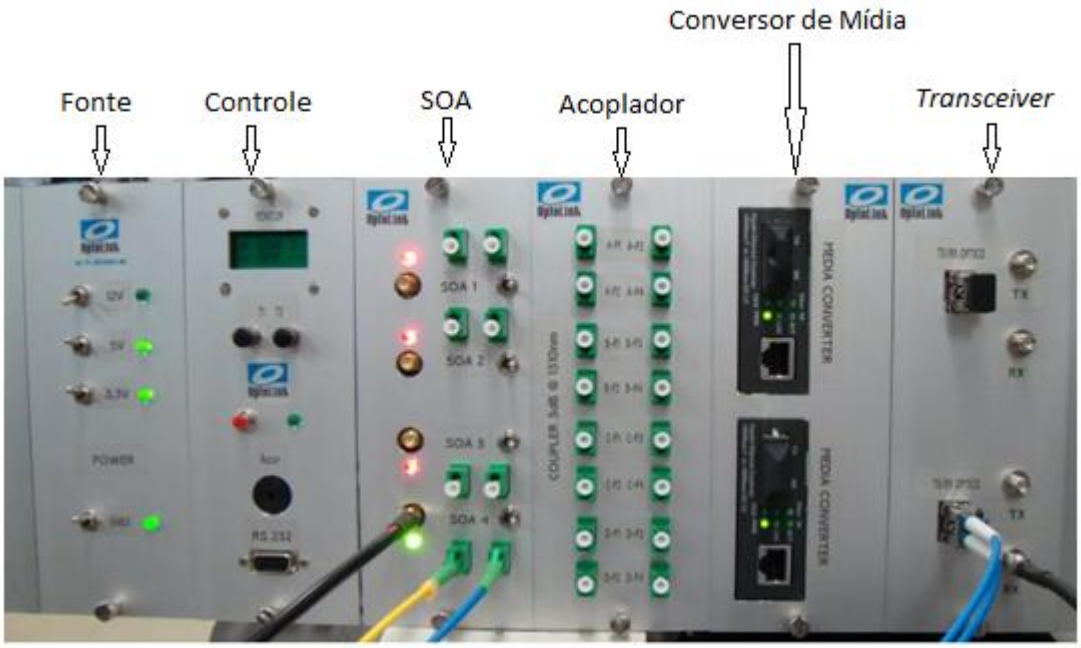


Figura 37: Protótipo montado com os módulos Fonte, Controle, SOA, Acoplador, Conversor de Mídia e Transceiver, mostrados respectivamente da esquerda para a direita.

6.2.1 Módulo Fonte

Mostrado à esquerda na Figura 37 o Módulo Fonte possui saídas de 12 volts, 5 volts, e 3,3 volts para alimentação de diferentes componentes utilizados no protótipo. O módulo possui uma chave geral e uma chave para cada valor de tensão de saída. Todas as chaves são sinalizadas por LED verde quando ligadas.

6.2.2 Módulo de Controle

O segundo módulo mostrado na Figura 37, contando-se da esquerda para direita, é o Módulo de Controle. Este módulo foi projetado e programado pela Optolink. Consiste de um microprocessador (PIC16F874A/877A) que permite ler os valores de corrente e de temperatura de cada dispositivo SOA. Ajustes de corrente ou de temperatura de operação podem ser feitos no Módulo SOA através de potenciômetros multi-voltas (trimpot de precisão) e os valores exibidos no visor digital frontal (LCD 8x2) no Módulo de Controle. O visor também mostra o valor da corrente de cada um dos dispositivos SOA de maneira cíclica durante a operação do protótipo.

6.2.3 Módulo SOA

Dispositivos amplificadores ópticos a semicondutor - SOA (*Semiconductor Optical Amplifier*) - estão montados no terceiro módulo da Figura 37 (contando da esquerda para a direita). Foram utilizados dispositivos SOA com características apropriadas para chaveamento rápido. Conforme descrito na Seção 6.1, estes dispositivos são mais curtos e não apresentam muito ganho, mas propiciam o chaveamento bastante rápido com baixa corrente de operação.

Para aproveitar este potencial de rapidez dos dispositivos SOA foram utilizados transistores de chaveamento que respondem a freqüências de até 4 GHz. Foram utilizados os transistores de chaveamento modelo BFG35 que conseguem ser rápidos e robustos, ligar e desligar corrente elétrica de até 100 mA. A placa deste módulo, ainda aguardando a instalação do SOA e de seus dissipadores de calor, aparece na Figura 38 mostrando a posição dos transistores de chaveamento BFG35. Além da corrente do SOA esta placa controla a corrente do peltier[18] responsável pela temperatura de operação do dispositivo SOA. A informação da temperatura é fornecida pelo termistor[19]. Tanto o peltier como o termistor são componentes que já se encontram encapsulados junto de cada um dos dispositivos SOA (Seção 6.1).

---

[18] Peltier é um dispositivo termoelétrico utilizado para transferir calor pela passagem de corrente elétrica. Tem esse nome por utilizar um efeito descoberto por Jean Charles Athanase Peltier.

[19] Termistor é um dispositivo utilizado para medir a temperatura (sensor de temperatura) cujo funcionamento é baseado em materiais com resistência elétrica que variam com a temperatura.

Figura 38: Montagem mecânica em caixa de 19 polegadas e placa do SOA com transistores de chaveamento BFG35.

A Figura 39 mostra as características do SOA modelo IPSAD1302 de fabricação INPHENIX adquirido para montar o protótipo desta tese. As principais características para funcionamento como chave óptica rápida são o tempo de subida e o tempo de descida de 500 ps, a razão de extinção de 40 dB e o baixo valor de corrente elétrica de funcionamento (100 mA). Alguns dispositivos SOA que operam com 500 mA não são adequados por ser difícil encontrar transistores de chaveamento rápido para corrente muito maior do que 100mA.

Parâmetro		Símbolo	Especificações			Unidade
			Min.	Típico	Máx.	
Corrente de Operação		I_F		100	150	mA
Pico do Comprimento de Onda de Operação		λ_p	1280		1340	nm
Largura de Banda Óptica a 3dB		$\Delta\lambda_{3dB}$	50			nm
Ganho de Pequenos Sinais (-25 dBm) em λ_p		G_{max}		10		dB
Flutuação de Ganho com λ		ΔG		0,2	0,5	dB
Potência de Saída de Saturação		P_{sat}	4			dBm
Figura de Ruído		NF		8		dB
Dependência do Ganho com a Polarização		PDG		0,2	0,5	dB
Razão de Extinção		ER	40			dB
Propriedades de Chaveamento	Tempo de Subida	τ_r		500		ps
	Tempo de Descida	τ_f		500		ps

Figura 39: Parâmetros do dispositivo SOA, modelo IPSAD1302 de fabricação INPHENIX, utilizado no protótipo (Tradução do manual de operação).

Na parte frontal do módulo há 8 conectores ópticos tipo LC/APC[20], uma entrada e uma saída óptica para cada um dos 4 dispositivos SOA. Cada SOA pode ser ligado manualmente ou controlado por sinal rápido do tipo DLV (*Digital Low Voltage*) de 3,3 volts, inserido através de conectores SMA que também podem ser acessados no painel frontal do módulo. Abaixo de cada conector SMA foram instalados LEDs sinalizadores que acendem na cor vermelho quando o dispositivo está ajustado para operar manualmente e na cor verde para indicar que o conector SMA está habilitado para receber o sinal de controle DLV externo.

[20] LC/APC é um tipo de conector óptico de tamanho bastante reduzido. Um par de conectores ocupa o mesmo espaço em painel que um conector RJ45 da tecnologia Ethernet. APC é sigla para *Angle Physical Contact.* LC é sigla para *Lucent Connector* ou *Local Connector*.

6.2.4 Módulo Acoplador

O módulo acoplador foi montado com acopladores ópticos comerciais de 3dB (calibrado para λ=1310 nm) que dividem a potência óptica em partes iguais direcionadas para cada uma das duas portas de saída. Cada acoplador possui duas portas de entrada e duas portas de saída. O acesso é feito através de conectores tipo LC/APC por serem pequenos, permitindo grande quantidade de conectores no mesmo painel e por terem perda de retorno inferior a 60 dB habilitando o protótipo para experimentos que utilizam alta potência óptica ou equipamentos sensíveis à potência de retorno. Foram feitos dois módulos com 4 acopladores cada um, possibilitando a montagem de arquiteturas de chaves com até oito acopladores. Como cada acoplador precisa de quatro conectores, foi necessário acomodar 16 conectores LC em cada módulo. Na Figura 37 o Módulo Acoplador é o quarto módulo contando-se da esquerda para direita.

6.2.5 Módulo Conversor de Mídia (Gigabit Ethernet)

Neste módulo foram montados dois conversores de mídia Gigabit Ethernet, disponíveis no mercado. Estes conversores geram sinais ópticos (conectores ópticos tipo SC) no padrão Gigabit Ethernet 1000Base-LX a partir de sinais elétricos de entrada (conector RJ45) padrão 1000Base-TX. O sinal óptico resultante pode ser enviado por distância de até 10 km e ser convertido para sinal elétrico em dispositivo semelhante colocado do outro lado do enlace. A função deste conversor de mídia no protótipo é possibilitar experimentos com sinais GEth (Gigabit Ethernet) reais,

gerados entre dois computadores que podem se comunicar entre dois protótipos, ou vários computadores que se comunicam numa rede de protótipos iguais ao montado nesta tese. O módulo conversor de mídia é o penúltimo mostrado na Figura 37 (Página 103).

6.2.6 Módulo *Transceiver*

A palavra *transceiver* é a junção da inicial da palavra em inglês *transmitter* (transmissor) com o final de outra palavra inglesa *receiver* (receptor). O componente que possui um transmissor e um receptor é comumente chamado de *transceiver*. Neste módulo homônimo foram inseridos dois *transceivers* comerciais com formato compacto SFP (*Small Form-factor Pluggable*) que operam na taxa de Gigabit por segundo. O componente ilustrado na Figura 40, é um componente comercial típico, não é necessariamente da mesma marca utilizada no protótipo. Estes *transceivers* comerciais possuem um transmissor e um receptor independentes entre si. São utilizados em equipamentos como *Switches* ou Roteadores com entrada óptica. No protótipo foi instalado um soquete no padrão SFP e acessos elétricos independentes ao transmissor e ao receptor. Estes acessos ficam disponibilizados na parte frontal do módulo através de conectores de RF tipo SMA. Este módulo pode ser utilizado como receptor relativamente rápido (até um Gbps) e como fonte transmissora de luz. Pode-se inserir um sinal elétrico gerado por um gerador de pulso para gerar um sinal óptico do mesmo formato. Também se pode utilizar o receptor como fotodetector rápido, que recebe um sinal óptico e fornece um sinal elétrico que pode ser analisado em um osciloscópio. Na Figura 37 (Página 103) o módulo *transceiver* é o último à direita.

Figura 40: *Transceiver* 1000Base-LX 10G comercializado pela ZyXEL. Figura disponibilizada em: http://www.zyxelguard.com/SFP-LX-10.asp Obtida em: 31 de agosto de 2010.

6.2.7 Caracterização do Protótipo

Foram caracterizados dois módulos. No módulo *transceiver* foi caracterizado o tempo de resposta do fotodetector e no módulo SOA o tempo de subida e de descida dos dispositivos SOA na função de chave óptica. A bancada de caracterização está mostrada na Figura 41.

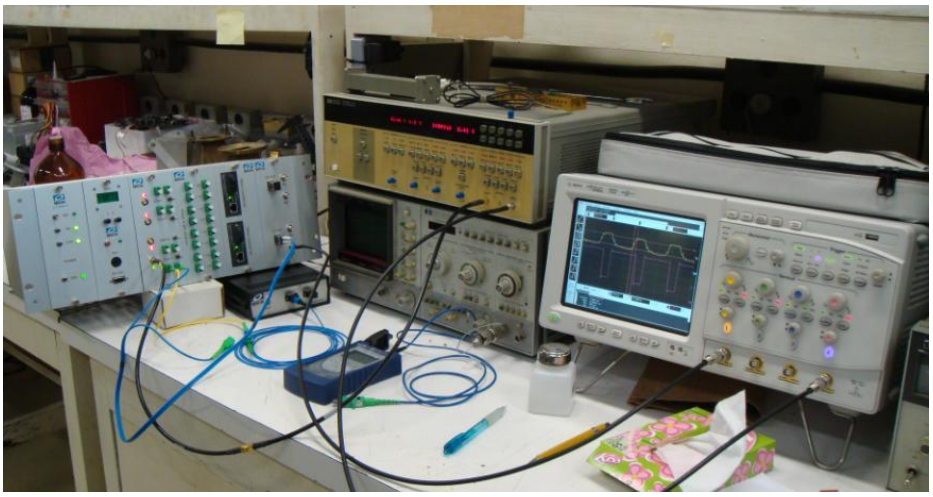


Figura 41: Bancada para caracterização do protótipo

O diagrama da Figura 42 mostra o esquema utilizado para caracterizar o tempo de resposta do fotodetector. Foram utilizados um gerador de pulso HP8133A de 3 GHz e um osciloscópio modelo Agilent Infinium DSO8064A de 600 MHz com amostragem na taxa de 4 GSa/s (Giga Samples per second).

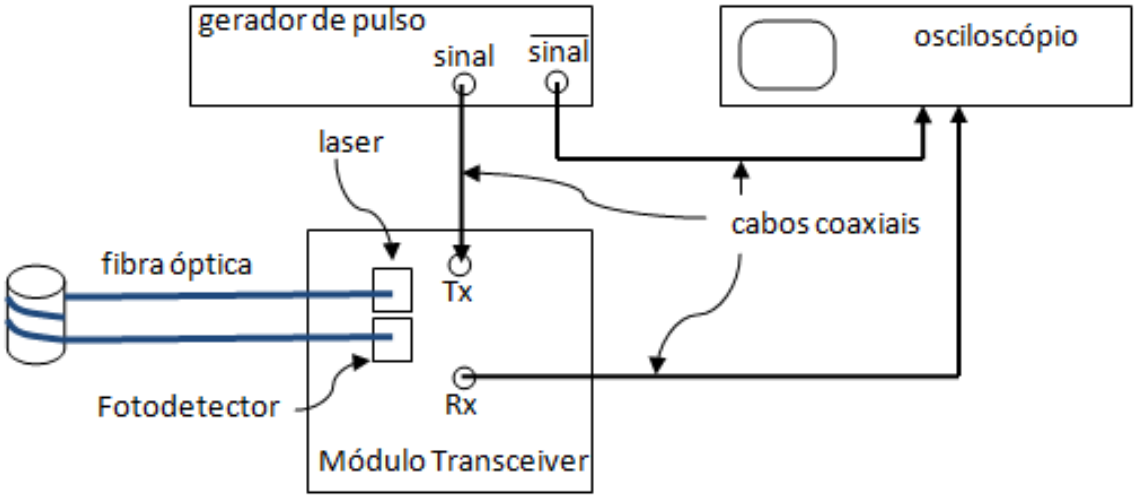


Figura 42: Caracterização do tempo de resposta do transceiver

O gerador de pulso fornece um sinal elétrico e o seu valor complementar $\overline{sinal}$ conforme mostrado na Figura 43. O sinal elétrico é ligado ao conector SMA (conector de RF tipo Sub-miniatura versão A) do transmissor do transceiver. A saída óptica do transmissor é ligada diretamente na entrada óptica do receptor conforme ilustra Figura 42. O conector SMA de saída do receptor é ligado ao osciloscópio. O sinal negativo do gerador de pulso é ligado diretamente a outro canal do osciloscópio.

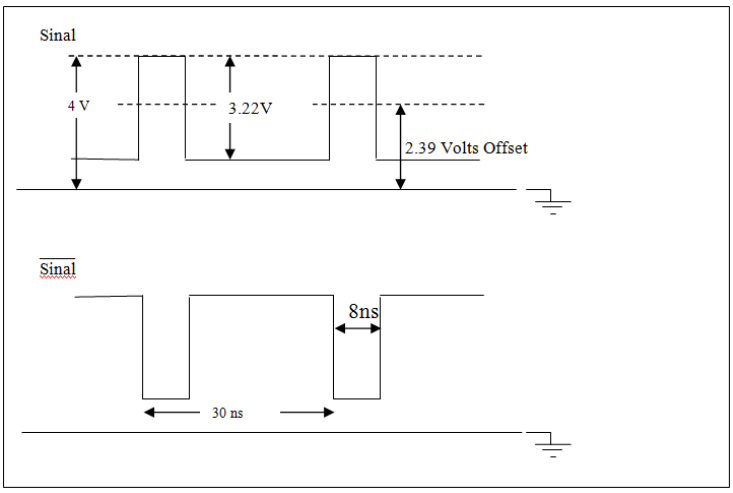


Figura 43: Sinais elétricos utilizados na caracterização.

O tempo de subida e de descida do pulso óptico, após ter passado pelo fotodetector, resultou ser da mesma ordem de grandeza da resolução do osciloscópio (0,4 ns), indicando que o fotodetector não tem tempo de subida ou de descida pior do que este valor. A Figura 44 mostra uma das telas do osciloscópio com resultados desta medida.

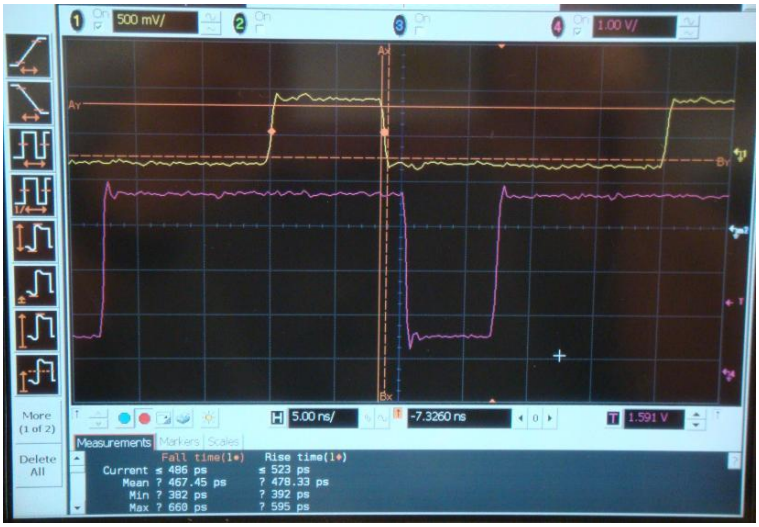


Figura 44: Avaliação do tempo de resposta do fotodetector.

Foi utilizado este fotodetector, com tempo de resposta de 0,4 ns, para caracterizar o tempo de subida e de descida dos dispositivos SOA. Para esta caracterização, esquematizada na Figura 45, além do gerador de pulso (HP8133A) e do osciloscópio (Agilent Infinium DSO8064A) foi utilizado um gerador laser DC (*Direct Current*) do fabricante Optolink que fornece um sinal óptico contínuo com comprimento de onda de 1310 nm. O sinal de laser DC foi inserido diretamente na entrada do SOA. Quando o dispositivo SOA está ligado, sua saída repete o sinal de entrada amplificado. O SOA foi utilizado no modo automático controlado pela entrada elétrica BNC. Como sinal de controle foi utilizado o sinal elétrico do gerador de pulsos, mesmo sinal mostrado na Figura 43, já utilizado na caracterização do fotodetector. Como o sinal tem 4 Volts de pico e período de 30 ns, o SOA permanece ligado durante 8 ns do pulso e desligado durante 22 ns complementares. Os tempos de subida e de descida resultantes foram de $(2{,}3 \pm 0{,}5)ns$ e $(1{,}4 \pm 0{,}3)ns$ respectivamente, em uma média automática realizada pelo osciloscópio depois de 200 mil medidas. Foi utilizada definição de tempo de subida que corresponde ao tempo decorrido entre 10% e 90% da amplitude total do pulso. Equivalentemente o tempo de descida é o tempo para o sinal baixar de 90% para 10% da amplitude total. Um exemplo da tela do osciloscópio com o resultado aparece na Figura 46.

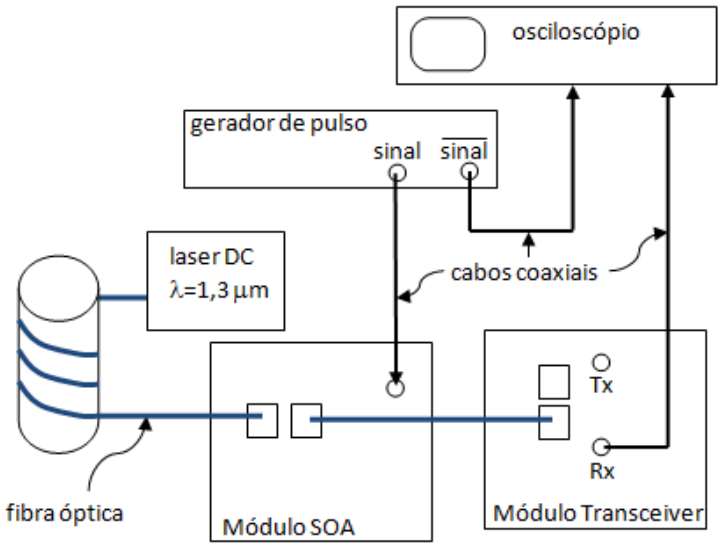


Figura 45: Caracterização do tempo de resposta da chave óptica rápida.

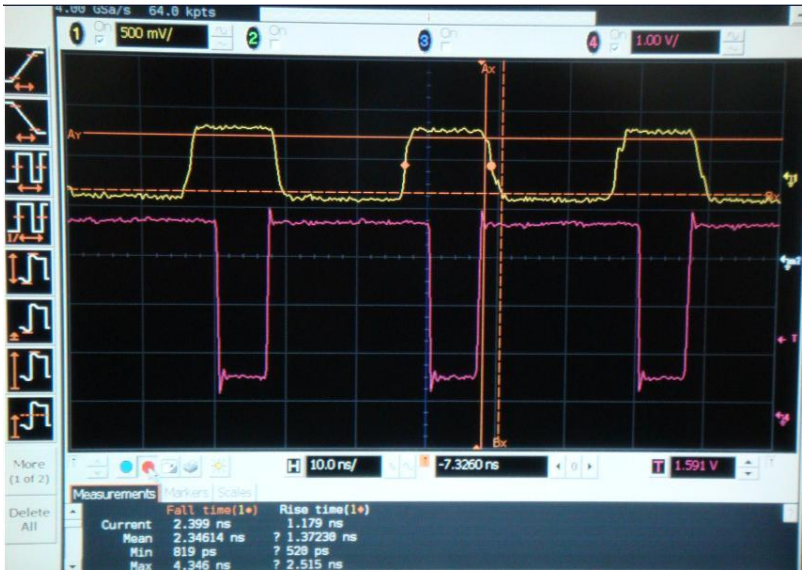


Figura 46: Avaliação do tempo de resposta da chave óptica rápida

Com tempo de resposta da ordem de 2 ns, a chave óptica é suficientemente rápida para ser utilizada em redes de chaveamento de pacotes ópticos. Somente para efeito de comparação, as chaves ópticas do tipo MEMS (*Micro Electro-Mechanical Systems*) utilizadas para chaveamento de comprimentos de onda nos sistemas WDM, têm tempo de resposta várias ordens de grandeza maiores do que o tempo de resposta de uma chave rápida. No exemplo da Figura 47 (MURAKAMI, 2005) uma chave tipo MEMS demora 15 ms para se estabilizar na nova posição a partir do instante que é acionada. A Figura 48 ilustra as regiões de tempo de resposta confrontadas com tipos de chaves ópticas e suas aplicações.

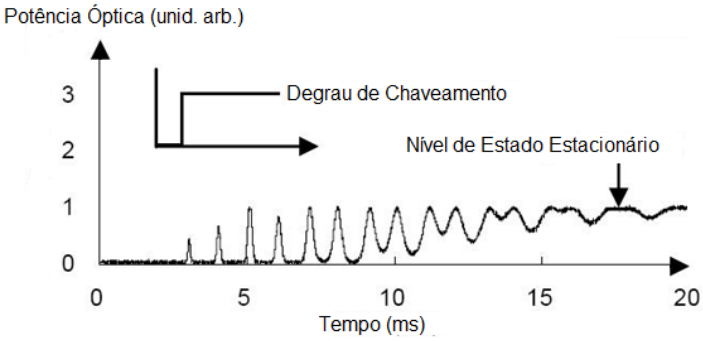


Figura 47: Tempo de resposta de Chaves ópticas MEMS (MURAKAMI, 2005). Chaves ópticas regulares (não rápidas) disponíveis no mercado.

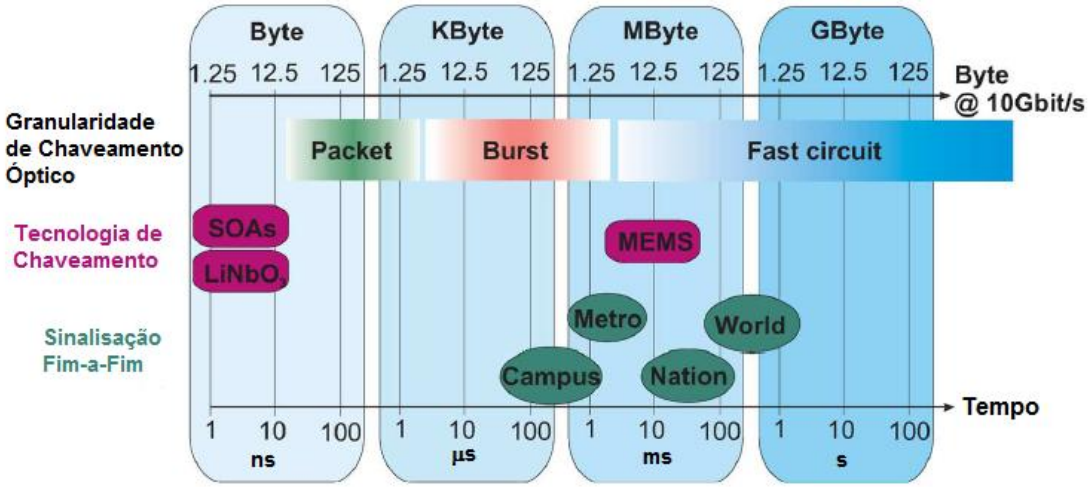


Figura 48: Tempos de resposta típicos dependendo da aplicação e da tecnologia (BUCHTA; GAUGER, 2008).

6.2.8 Considerações sobre o Protótipo

Em uma chave montada com acopladores 3 dB e dispositivos ativos tipo SOA é importante minimizar o número destes dois componentes para baixar a perda de inserção (caso dos acopladores) e baixar o custo (caso dos elementos SOA). O número de dispositivos SOA encarece a chave, e também torna a eletrônica mais complexa, com circuitos lógicos de maior capacidade para operar maior número de dispositivos. Por outro lado, uma chave muito simples (tipo liga-desliga) não permite a conexão de chaves em uma topologia em malha. è necessário pelo menos uma chave 2x2 para montar uma rede em malha sem colisão.

O protótipo montado nesta tese, sendo modular, permite que se faça experimentos com diversos tipos de chaves (1x1, 1x2, 2x2). Carretéis de fibra óptica, ou mesmo

enlaces pequenos existentes entre dois DIO (armário Distribuidor Interno Óptico) podem ser inseridos nos experimentos para formar uma linha de retardo. O módulo *Transceiver* permite realizar experimentos de óptica em geral, pois contem um laser com acesso via conector SMA, que pode ser modulado por um sinal elétrico inserido neste conector, e contem um fotodetector que também conta com acesso via conector SMA que permite ligar o sinal elétrico a um osciloscópio. O módulo Conversor de Mídia permite analisar um sinal real (Gigabit Ethernet) cuja amostra, retirada pelo auxílio do Módulo Acoplador, pode ser analisada em um osciloscópio pelo auxílio do Módulo *Transceiver*.

O protótipo versátil, pode ser utilizado para redes de pacotes ópticos (mostrou tempo de resposta de 2 ns, compatível com este tipo de experimento), e para outros experimentos de óptica até a taxa de 1 Gbps.

6.3 Possíveis Arquiteturas e Suas Características

As chaves ópticas rápidas e simplificadas podem ter muitas arquiteturas e atender diferentes necessidades. Todas estas arquiteturas podem ser montadas com o protótipo apresentado nesta tese, sendo que eventualmente pode ser necessário acrescentar algum elemento de controle. Todas as arquiteturas podem ser utilizadas para que a rede possua auto-organização e apresente funções emergentes ou características desejáveis apresentadas no contexto desta tese. Algumas destas arquiteturas podem ter vantagens como menor perda de potência, maior controle de acesso. Outras podem ter diferentes funções como inserção e derivação de pacotes ou ajuste de espaços disponíveis na rede. Segue uma seqüência de exemplos de arquiteturas de chaves, suas características, possíveis aplicações e funcionalidades. Em todas as arquiteturas a seguir um pacote óptico caminha da esquerda para a

direita e passa por três tipos de componente: **acoplador 3dB**; **DLF** - *Delay Line Fiber (*fibra de retardo); e **SOA** - Semiconductor Óptical Amplifier (amplificador óptico a semicondutor).

6.3.1 Arquitetura 1: Liga-Desliga

A chave mostrada na Figura 49 contem somente um dispositivo SOA e dois acopladores. Trata-se de um AD (*Add-Drop*) que pode deixar passar um pacote ou fazer a derivação ou inserção de um pacote local. Esta chave não permite montar redes ópticas transparentes na topologia em malha ou árvore, mas permite montar topologias em anel unidirecional. Esta arquitetura é muito simples mas necessita de uma DLF (*Delay Line Fiber*) para que o sistema eletrônico tenha tempo para desligar o SOA caso o pacote seja local ou deixá-lo ligado e com ganho caso o pacote esteja apenas de passagem (em trânsito). O componente DLF também tem por função verificar espaçoes livres para que possam ser inseridos novos pacotes. Neste caso, o tamanho da DLF pode ser ajustado para permitir inserção de pacotes grandes (1500 bytes) ou até lotes de pacotes com milhares de bytes.

Nesta estrutura um pacote em trânsito passa por dois acopladores e por isso a potência óptica tem 6 dB de perda. Ao passar pelo SOA a potência tem 10 dB de ganho e o resultado é de um ganho total de 4 dB.

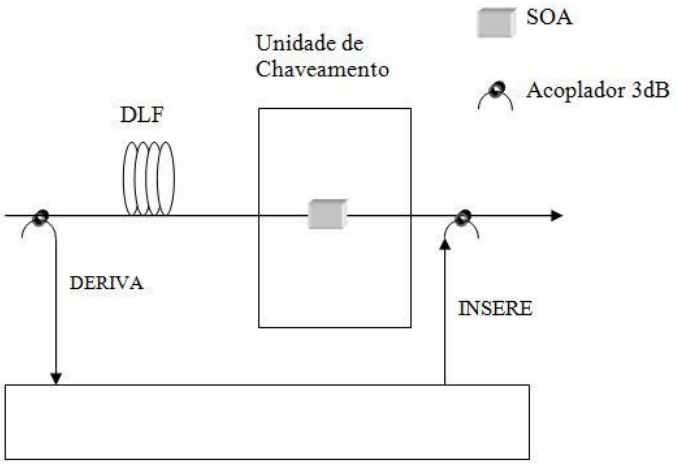


Figura 49: Chave 1x1: Liga-Desliga (Arquitetura 1)

6.3.2 Arquitetura 2: Bifurcação

Acrescentando-se somente mais um dispositivo SOA pode-se criar a possibilidade de dois caminhos de saída. O sinal que chega (à esquerda da figura) pode seguir por dois caminhos distintos e com outras chaves iguais a esta pode ter novas bifurcações possibilitando a formação de uma topologia de rede em árvore. Um pacote que chega pode ter três direcionamentos: destino local, destino porta de saída 1, e destino porta de saída 2. A arquitetura 2, ilustrada na Figura 50, também faz um sinal óptico perder 6 bB de potência nos dois acopladores, mas ganhar 10 dB pela passagem pelo SOA resultando um ganho total de 4 dB como na Arquitetura 1. Um pacote pode ser inserido pelo mesmo acoplador utilizado para criar dois caminhos de saída. No processo de inserção apenas um dos dois dispositivos SOA fica ligado para direcionar o pacote a apenas uma das duas portas de saída.

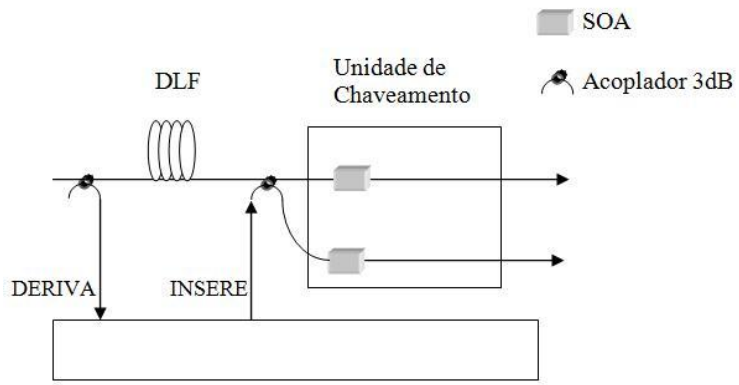


Figura 50: Chave 1x2: Bifurcação (Arquitetura 2)

6.3.3 Arquitetura 3: Bifurcação Melhorada

A Arquitetura 2 utiliza dois dispositivos SOA e dois acopladores. Apresenta a mesma perda de inserção da Arquitetura 1, mas não permite inserir novos pacotes enquanto se faz a derivação de um pacote local, como é possível fazer na arquitetura 1 pelo posicionamento do acoplador de inserção. É possível garantir também esta funcionalidade pelo acréscimo de dois acopladores. Esta terceira arquitetura está ilustrada na Figura 51. Na Arquitetura 3 é possível inserir até dois pacotes simultaneamente enquanto se faz a derivação de um pacote com destino local, ou inserir um pacote ao mesmo tempo que um outro, em trânsito, passa pela chave.

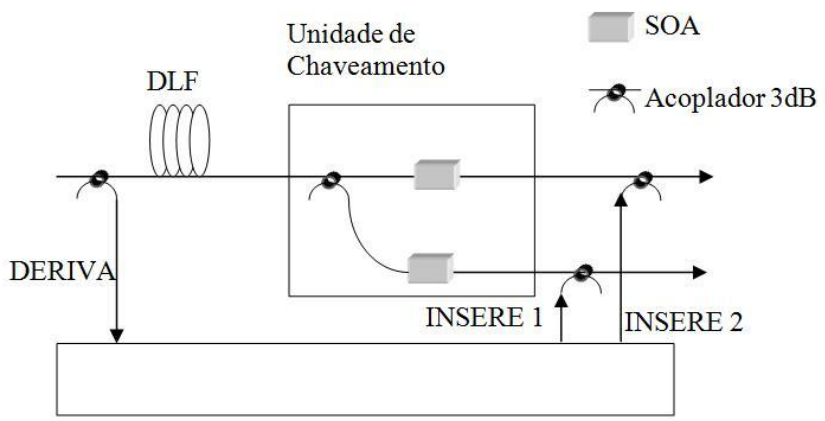


Figura 51: Chave 1x2 com dois SOAs e quatro acopladores (Arquitetura 3)

Nesta configuração o sinal óptico passa por três acopladores e perde 9 dB. Mesmo assim, o ganho de 10 dB do SOA compensa a perda de inserção da chave, mas não deixa margem para perda de potência ao longo dos enlaces.

6.3.4 Arquitetura 4: Chave 2x2

Com chaves 2x2, podem ser montadas redes com topologias em malha. Muitas configurações são possíveis. Todas as configurações apresentadas como exemplo trabalham sem *buffer* óptico, e sem conversão de comprimento de onda, objetivando-se a minimização do número de dispositivos SOA e acopladores 3 dB. Na Arquitetura 4 (Figura 52) o sinal óptico passa por quatro acopladores de 3 dB (perda de 12 dB) e um amplificador (ganho de 10 dB), resultando em 2 dB de perda de inserção.

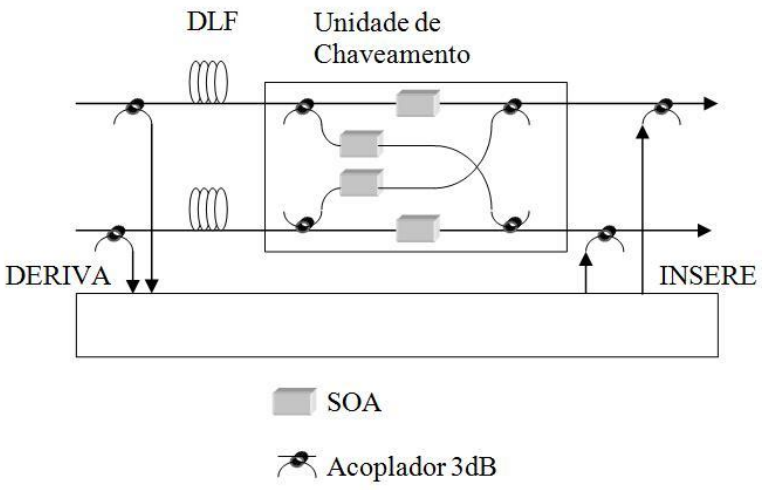


Figura 52: Chave 2x2 com quatro SOAs e seis acopladores (Arquitetura 4)

6.3.5 Arquitetura 5: Chave 2x2 com 6 SOAs

Se forem incluídos mais dois dispositivos SOA, pode-se inserir o sinal óptico aproveitando-se os acopladores de entrada da unidade de chaveamento. Como resultado um pacote em trânsito que passa por dois amplificadores (20 dB de ganho) e apenas 3 acopladores 3 dB (9 dB de perda) experimenta ganho total de 11 dB. Esta configuração, apresentada na Figura 53, é bem melhor que a Arquitetura 4, pois tem um bom ganho (baixa perda de inserção) e permite inserir até dois pacotes simultaneamente enquanto dois outros estão sendo derivados para uso local. O custo da chave é relativamente alto, pois o SOA é o dispositivo mais caro.

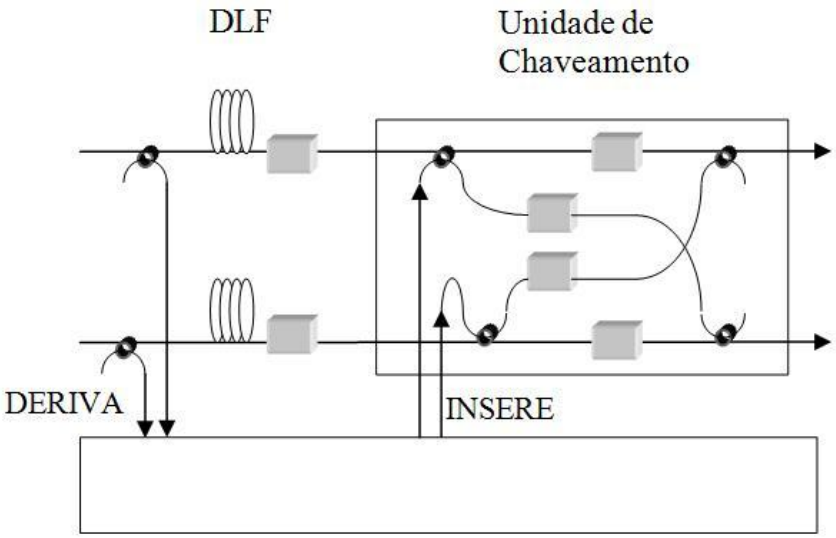


Figura 53: Chave 2x2 com seis SOAs e seis acopladores (Arquitetura 5)

6.3.6 Arquitetura 6: Chave 2x2 com 8 SOAs

A Arquitetura 6 é uma chave ainda mais dispendiosa e complexa do que a Arquitetura 5, mas pode ser necessária para resolver o seguinte problema: uma rede que trabalha com pacotes de tamanho fixo, pode chegar em uma situação de carga, correspondente a 60% dos enlaces ocupados, de tal forma que a separação entre os pacotes fica menor do que o tamanho fixo do pacote a ser inserido. Isto pode acontecer quando os pacotes estiverem distribuídos uniformemente pela rede. Nesta situação não é possível inserir nenhum outro pacote mesmo que estejam sobrando 40% de espaço livre nos enlaces. Não é possível obter carga superior a 60%. Na Arquitetura 6 (Figura 54), o pacote em trânsito passa por 5 acopladores 3 dB (perda de 15 dB) e passa por 2 amplificadores (ganho de 20 dB). Ainda sobra um ganho líquido de 5 dB. O sistema funciona de forma que todos os pacotes passam por duas DLF´s. Para avançar algum pacote, e fazê-lo chegar mais perto do pacote da frente,

basta fazê-lo passar por fora da segunda DLF. É necessário cuidado para deixar o pacote que eventualmente caminha à frente sair da segunda DLF antes de chavear o pacote de trás para passar diretamente. Com este procedimento as chaves conseguem aproximar os pacotes entre si e aumentar os espaços livres contíguos para que se possam inserir novos pacotes.

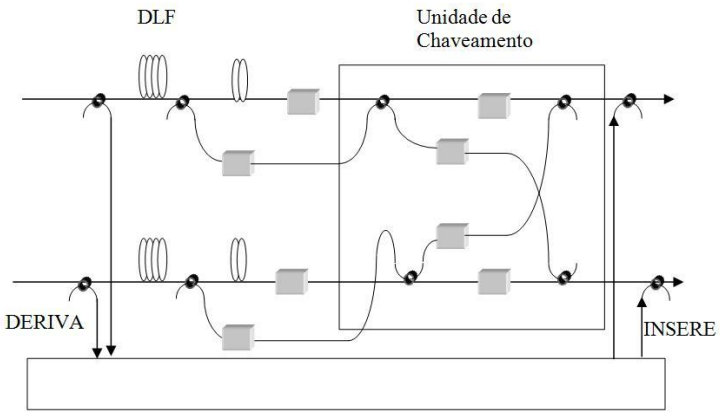


Figura 54: Chave 2x2 com 4 SOAs e 8 acopladores (Arquitetura 6).

6.3.6.1 Saturação da Carga

Estas considerações sobre o preenchimento total da rede ou saturação da carga são importantes e a função de ajuste de posição dos pacotes na rede pode ser útil, mas é preciso analisar também o custo dos dispositivos e verificar que cerca de metade dos pacotes da Internet são pequenos pacotes (40 bytes) carregando, por exemplo, controles TCP (CASTRO, 2011). Estes pacotes podem ocupar estes espaços pequenos e a sofisticação do ajuste, na prática, pode não ser necessária. Entretanto, se a cargas é grande não sobra espaço físico para inserção de pacotes grandes (1500 bytes) e seria muito útil criar uma política de ajuste da carga para garantir recursos para estes grandes pacotes. Em um tráfego com pacotes gigantes, tipo *burst* de pacotes juntados em um único pacote muito longo (operações com OBS), as DLF auxiliares são absolutamente necessárias. A Figura 55 ilustra uma

arquitetura simples, cuja única função é arrumar a distância entre pacotes. Esta estrutura pode ser inserida em alguns pontos distribuídos pela rede separadamente das chaves ópticas. Esta mesma estrutura aparece embutida na arquitetura 6 apresentada na Figura 54. Nesta estrutura de ajuste de posição de pacotes, mesmo que utilizada separadamente do chave óptica, precisa de uma amostra do sinal óptico para identificar o tamanho do pacote e o tamanho dos espaços vazios. Enquanto o pacote passa pela DLF de tamanho "t" o sistema decide se deve passar também pela DLF de "t/2" para retardá-lo ou pelo caminho alternativo sem retardo. A perda total é de 9 dB e o ganho é de 10 dB resultando um pequeno ganho líquido de 1 dB. Com esta estrutura é possível fazer ajustes na distribuição dos pacotes pela rede e com isto abrir espaço físico para novos pacotes evitando a saturação da carga.

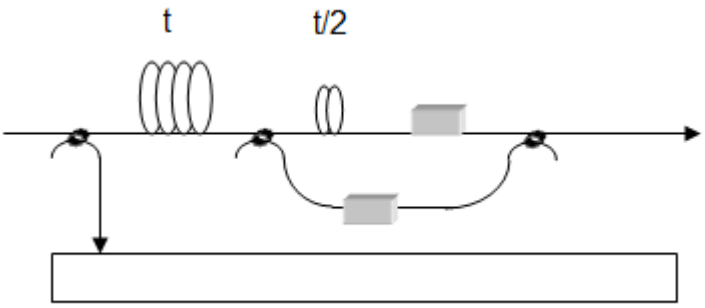


Figura 55: Arquitetura auxiliar para arrumar a distribuição de pacotes na rede

Uma proposta alternativa para tratar evitar a saturação da carga é montar uma rede com pacotes variados onde os pacotes menores têm preferência sem necessidade de algoritmos especiais para controle. *Buffers* diferentes para pacotes de tamanhos diferentes operando numa política de acesso tipo *round-robin*[21], seria suficiente para

[21] Round-Robin é uma expressão utilizada em computação para descrever a política de escolha de um recurso a partir de uma lista. Caracteriza-se por um apontador que percorre a lista, indicando o recurso da vez, e retorna ao primeiro recurso depois de passar pelo último.

barrar os pacotes maiores quando a carga da rede estiver muito elevada. Isto estimularia a inserção de pacotes pequenos de maneira natural possibilitando melhor enchimento da rede. Esta é mais uma função que emerge da rede *bottom-up*. É necessário, entretanto, criar filas separadas para faixas de tamanho de pacotes para que um pacote grande não trave a fila.

6.3.7 Chaves Utilizando Processos Interferométricos

No processo de chaveamento utilizado neste trabalho, o sinal óptico é dividido em duas partes iguais pela passagem por um acoplador passivo 3dB. Em cada braço de saída do acoplador é colocado um dispositivo SOA que quando ligado fornece um ganho de 10 dB e quando desligado não deixa passar a luz. Quando o objetivo é enviar o sinal para as duas portas, basta deixar os dois dispositivos SOA ligados, mas quando se deseja bloquear uma das saídas, somente metade do sinal segue seu percurso. Com a perda de 3 dB no acoplador passivo e ganho de 10 dB no SOA o sinal segue aumentado de 7 dB. Em princípio, este ganho é suficiente para compensar perdas de propagação e outras perdas de inserção que aconteçam pelo caminho. Entretanto o ganho não é limpo, mas envolve geração e amplificação de ruídos. A relação sinal/ruído se degrada em cada passagem pela chave. É necessário avaliar esta degradação para verificar o número máximo de chaves que o sinal pode atravessar até que chegue ao destino (BUCHTA, 2008).

Uma alternativa aos esquemas de chaveamento anteriores é a utilização de processos interferométricos como ilustra a Arquitetura 7 (Figura 55). Neste processo, que também pode ser montado com o protótipo construído neste trabalho, logo depois da DLF o sinal óptico é dividido em dois braços que se juntam novamente na saída pela utilização de um segundo acoplador passivo. Adiciona-se um dispositivo SOA em cada braço. O sinal óptico, neste caso, sai integralmente por uma das

portas de saída, deixando nulo o sinal que sai pela outra porta, dependendo da diferença de fase entre os sinais ópticos de cada braço. O processo de chaveamento, neste caso, não ocorre pelo fato de desligar um dos dois dispositivos SOA, mas por um processo de mudança de fase da luz de maneira diferenciada em cada braço. Esta mudança de fase é conseguida pelo ajuste de corrente em cada um dos dispositivos SOA. Para que o protótipo possa ser utilizado em experimentos interferométricos é necessário complementá-lo com um módulo de controle de fase dotado de circuito de realimentação. Esta realimentação é necessária para compensar flutuações de fase que ocorrem por razões diversas como, por exemplo, pequenas flutuações de temperatura.

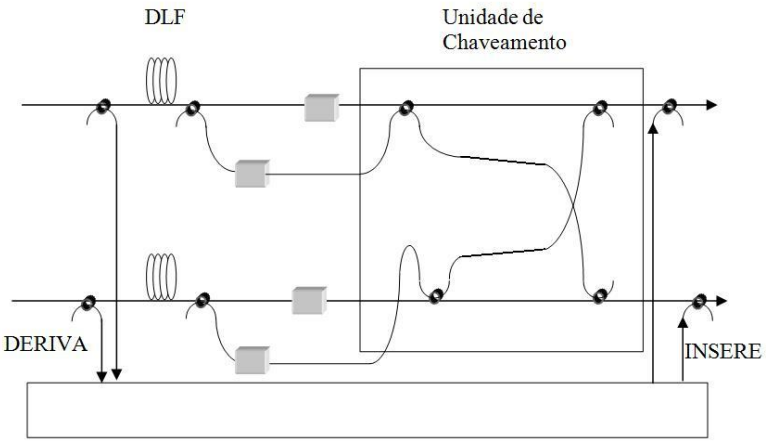


Figura 56: Chave 2x2 com processo interferométrico

Para que a chave tenha duas entradas e duas saídas (chave 2x2) é preciso montar dois interferômetros e depois juntar as saídas dos interferômetros utilizando mais um acoplador. Nesta arquitetura interferométrica (Figura 55) o sinal perde 3 dB no acoplador inicial que retira amostras e também deriva os pacotes com endereço local, não perde nada nos dois acopladores que delimitam os braços interferométricos, mas ganham perto de 10 dB pela passagem pelo dispositivo SOA. Com 7 dB de ganho o sinal passa ainda por mais dois acopladores perdendo 6 dB. No final resulta um ganho pequeno de 1 dB. Este ganho é muito pequeno e requer amplificação complementar, mas nestas redes totalmente ópticas é necessário

incluir não somente amplificadores, mas também regeneradores 3R totalmente ópticos.

No futuro, a tendência é que dispositivos como o SOA e guias de onda, sejam integrados em uma mesma pastilha semicondutora para realizar funções de chaves ópticas rápidas, regeneradores 3R e conversores de comprimento de onda. Um exemplo desta integração pode ser visto no trabalho (KEHAYAS, 2005). Pode-se utilizar o protótipo, montado nesta tese para ensaiar o funcionamento de um circuito óptico integrado.

6.3.8 Regeneradores e Apagadores de Pacotes.

Um apagador de pacotes serve para eliminar pacotes que ficam muito tempo na rede. Um apagador é muito simples de ser desenvolvido a partir dos conceitos desta tese. Todos os nós de rede podem ter um analisador de qualidade de sinal, e um critério de decisão que apaga eventuais pacotes degradados. Como os pacotes se degradam pelo tempo que permanecem na rede estes apagadores de pacote têm a função de eliminar pacotes velhos, o mesmo objetivo do campo TTL (*Time-To-Live*) dos pacotes IP. Para apagar um pacote nas chaves apresentadas nesta tese basta fechar ou desligar o dispositivo SOA que daria passagem para tal pacote degradado. A verificação do tempo do pacote na rede não precisa de um campo contador de enlaces como no pacote IP, pois pode verificar a relação sinal/ruído e remover os pacotes que não estiverem dentro do critério. Outra opção ao *TTL* é a inclusão de regeneradores 3R que fazem o pacote passar por regeneração de amplitude, de formato do bit e recuperação do relógio em lugar de serem eliminados.

6.4 Considerações Finais sobre A Viabilidade

A montagem de um protótipo de chave óptica modular permite validar a possibilidade de baixar o custo das redes de pacotes ópticos. Também constitui um instrumento de laboratório para investigar novas idéias e arquiteturas de chaves ópticas rápidas. Os exemplos de arquiteturas de chaves ópticas demonstram a grande variedade de aplicações para a rede real ou para experimentos preliminares que podem contribuir para o desempenho da nova rede. Neste aspecto destacam-se os tratamentos dados à saturação da carga (Seção 6.3.6.1) e à possibilidades inovadoras como a construção de apagadores de pacote utilizando o protótipo simplificado apresentado nesta tese (Seção 6.2.8).

Foi solicitada uma patente de invenção do protótipo como instrumento de investigação. A concessão da patente constitui outro elemento de validação do trabalho.

7 Considerações Finais

Segue uma análise crítica dos resultados, principais contribuições e inovações e uma série de tratamentos complementares que constituem propostas para futuros trabalhos.

7.1 Análise Crítica dos Resultados

O objetivo da tese (Seção 1.2) de demonstrar a viabilidade do desenvolvimento de redes de comunicação com chaveamento de pacotes ópticos, com escalabilidade do número de nós foi alcançado através da proposta de rede auto-organizada. Durante o desenvolvimento do trabalho muitos detalhes foram tratados de maneira conclusiva e outros foram deixados por concluir. Alguns detalhes caracterizam-se como contribuições originais, outros são melhorias de resultados já obtidos em trabalhos anteriores. A seguir estão destacadas as principais contribuições deste trabalho.

A principal contribuição desta tese é a proposta de simplificação de chaves ópticas rápidas para construção de redes auto-organizadas escaláveis. Esta construção caracteriza- se pelo funcionamento autônomo de cada nó de rede. As funções de rede aparecem como conseqüência das operações descentralizadas e bastante simplificadas executadas em cada um dos nós de rede. Não existe sinalização ou troca de informação entre nós de rede que não sejam seus vizinhos mais próximos e isto permite o aumento do número de nós de rede (escalabilidade do número de nós) limitado apenas pela degradação física do sinal óptico. Esta degradação,

embora não tenha sido tratada nesta tese, pode ser corrigida por regeneradores 3R (Regeneração da amplitude, do formato do bit e do relógio), inclusive executados de forma totalmente transparente, sem conversão do meio óptico para o meio elétrico (ROCHETTE, 2006).

Os resultados foram obtidos principalmente pelo modelo analítico estatístico aperfeiçoado nesta tese. Estimulado por problemas propostos sobre tecnologia 3G (*Terceira Geração de Telefonia Móvel*), solicitados pelos laboratórios de pesquisa da Ericsson em 1999, um modelo analítico foi idealizado no CPqD, Fundação Centro de Pesquisa e Desenvolvimento em Telecomunicações (BARBOSA, 2003; BARBOSA, 2004) e continuou sendo aprimorado, em trabalhos posteriores, que, entretanto, focalizaram mais resultados obtidos por simulação do que resultados obtidos pelo modelo analítico (GUEDES, 2005; BONANI, 2006a; BONANI, 2006b; MARTINS, 2007; MARTINS, 2009). Em novembro de 2009, foram mostrados alguns dos resultados desta tese no IMOC (*Internacional Microwave and Optoelectronics Conference*) em Belém do Pará (SACHS; LOPES; CARVALHO, 2009).

O modelo tem por base trabalho mais antigo (ACAMPORA, 1992) que também trabalhou com o método recursivo já utilizado por Viterbi (1971) para calcular códigos corretores de erro. Diferentemente do trabalho de Acampora (1992), foi eliminada a figura de competição entre pacotes. Na rede proposta nesta tese não há competição da forma usual (pacotes sincronizados e armazenados para que se possa aplicar um critério de prioridade). O pacote que chega à frente, é sempre encaminhado para a melhor porta. Um pacote pode chegar poucos nano segundos à frente (dependendo apenas da velocidade dos componentes responsáveis pela identificação do cabeçalho óptico) e terá o direito de escolher a porta de saída. Se dois pacotes chegam com diferença de tempo inferior ao intervalo de tempo que os componentes conseguem distinguir, então serão considerados como tendo chegado simultaneamente e a porta de entrada vencedora fica previamente estabelecida para estes casos. Chegada simultânea é evento muito raro em redes com pacotes não sincronizados, conforme foi discutido na Seção 5.2 onde foram estabelecidas as condições da simulação. As contribuições desta tese para o modelo analítico incluem:

- Ajuste do cálculo de probabilidade de um pacote ter endereço local (*Ppl*). Esta probabilidade foi subestimada em trabalhos anteriores, sendo uma das causas da falta de concordância entre o modelo e as simulações. Nesta tese propomos utilizar *Plp=1/<H>* (Modelo 2) conforme discutido na Seção 5.1.3.4, fazendo com que o modelo se ajuste aos valores obtidos por simulação (Figura 23).

- Tempo e memória de computador, utilizados pelos algoritmos, se mostraram adequados para calcular redes com até 256 nós, com topologias que apresentam ou não automorfismo (Seção 5.1.3.7). Estes ganhos são atribuídos ao procedimento de preparação da matriz de topologia e da matriz de caminhos preferenciais separadamente do programa principal. Para o cálculo da matriz de caminhos preferenciais foi utilizada técnica de árvore adaptativa (PISTORI, 2006), tratado na Seção 5.1.2.

- Inclusão de técnica de tratamento de falha pela troca da topologia sem falha pela topologia que exclui o enlace da falha e passa a ser tratada como rede sem automorfismo. Como tal, é necessário calcular o caminho médio para todos os destinos, pois já não são iguais entre si como nas redes com automorfismo. Esta inclusão permitiu avaliar esquemas de proteção de enlace e montar mapas de distribuição dos efeitos da falha. A mesma técnica permite tratar outras topologias como realizado para a rede NFSNET.

- Alteração do modelo para garantir simetria de tráfego após a inclusão de uma falha. A alteração baseia-se na identificação de todos os casos do **tipo tanto faz** e atribuição de probabilidade de 50% para porta de saída de todos eles (Seção 5.1.3.6).

7.2 Principais Contribuições e Inovações.

Além da proposta de simplificação que permite montar uma rede auto organizada, além do modelo analítico e de suas características resumidos na Seção 7.1, esta tese apresenta também um **esquema de proteção de enlace** inovador que juntamente com o aparato desenvolvido para demonstrar a viabilidade de fabricação de chaves ópticas rápidas, constitui reivindicação de invenção conforme patente solicitada junto ao INPI (*Instituto Nacional de Propriedade Industrial*). A patente de invenção tem por título: "APARATO MODULAR PARA ACOPLAR DISPOSITIVOS AMPLIFICADORES ÓTICOS DE SEMICONDUTOR PARA FORMAR CHAVE ÓTICA RÁPIDA, MÉTODO DE COMUTAR PACOTES ÓTICOS, REDE ÓTICA AUTO-ORGANIZADA, MÉTODO DE SEGREGAÇÃO DE ENLACES EM SUBDOMÍNIOS, MÉTODO DE VERIFICAÇÃO DE INTEGRIDADE DE ENLACES DE REDE ÓTICA AUTO-ORGANIZADA E MÉTODO DE PROTEÇÃO". Foi encaminhada para o INPI no dia 27.10.10 sob protocolo de nº. 018100040337.

Outra contribuição da tese está na montagem física de um protótipo de chave óptica rápida conforme descrito no Capítulo 6. O protótipo é modular e permite montar muitas configurações de chaves ópticas conforme exemplificadas na Seção 6.2. O módulo *transceiver* (Seção 6.2.6) pode ser utilizado como um fotodetector rápido (1Gbps) ou como um laser rápido que pode ser modulado na taxa de 1Gbps. Um único dispositivo SOA (Seção 6.1 e Seção 6.2.3) também pode ser utilizado como modulador e, conforme especificação do fabricante, permite modulação de sinais ópticos com taxa de até 622 Mbps. Assim, um único protótipo constitui um laboratório bastante completo para estudo de diversos processos utilizados em comunicações ópticas.

7.3 Trabalhos Futuros

Para montar uma plataforma experimental de rede que contemple a auto-organização conforme a proposta desta tese muitos detalhes precisam ser abordados. Além das chaves autônomas é preciso abordar temas como interface entre domínios autônomos. É preciso avaliar qualidade de serviço, segurança, custo de manutenção, interface com redes que trabalham com outras tecnologias e muitos outros detalhes que escapam do escopo deste trabalho. Mesmo na chave óptica autônoma, a montagem física e tratamento de tráfego real dependem de projetos de execução complementares. A seguir estão discutidos alguns destes temas complementares.

7.3.1 Sincronismo

Existem pelo menos dois tipos de sincronismo utilizados em redes de pacotes ópticos. O primeiro envolve o sincronismo de pacotes, semelhante ao sincronismo de células utilizado nas redes ATM, que tem por função ler dois pacotes concorrentes e aplicar critérios de prioridade para verificar quem segue e quem aguarda. Um segundo tipo de sincronismo, não tratado nesta tese, é necessário para identificar o primeiro bit válido de um pacote tanto para leitura do cabeçalho como para a leitura final do conteúdo, provavelmente com taxa muito mais alta do que a taxa do cabeçalho. Com a possibilidade dos pacotes ópticos transportarem informação codificada com taxa da ordem de 40 Gbps, fica muito difícil fazer a recuperação do relógio no destino. Para a leitura do cabeçalho, que pode ser escrito na taxa de 1 Gbps, já existe tecnologia disponível comercialmente para recuperação

de relógio, como por exemplo, a tecnologia utilizada nas redes GPON. É necessário incluir alguns bits de sincronismo na frente de cada pacote, caracterizando um quadro óptico específico que precisa ser desenvolvido para cada tecnologia.

7.3.2 Capacidade de Armazenamento da Rede

A rede tem capacidade de armazenamento, pois os enlaces podem ficar repletos de carga durante o tempo de operação. Esta carga pode ser muito grande já que os enlaces podem ter muitos quilômetros de extensão. Quando a rede entra em operação está vazia e pode aceitar muita carga. Pouco tempo depois, correspondente ao tempo de propagação em um enlace, a rede inicia sua adaptação para a situação de máxima carga que ela suporta.

Na situação de carga máxima, o total de 2*N* enlaces armazenam temporariamente o total de 2.*N.P* pacotes, onde *P* é o número de pacotes que cabe em cada enlace. Para taxa *B* Gb/s cada bit tem 1/*B* ns. Na taxa de 40 Gb/s cada bit demora 25 ps e ocupa 5 mm de fibra trafegando na velocidade *c/n*, onde $c \approx$ 300.000 km/s e $n \approx$ 1,5. Se cada bit ocupa 5 mm, um enlace de 30 km acomoda 6 milhões de bits. Para pacotes de 1500 bytes ou, equivalentemente, 12000 bits, cabem 500 pacotes acomodados instantaneamente no enlace. De maneira geral o número de pacotes de 1500 bytes acomodados instantaneamente em um enlace é calculado por:

$$P = \frac{B(Gb/s) \cdot L(km) \cdot n}{12000 \cdot c(km/s)} = \frac{5}{12} BL \qquad \text{Equação 16}$$

Em uma rede com 16 nós, com enlaces de 30 km, trabalhando na taxa de 40Gb/s ficam armazenados instantaneamente 2 x 16 x 500 = 16.000 pacotes de 1500 bytes. Esta capacidade de armazenamento depende do comprimento dos enlaces e merece ser melhor estudada em futuros trabalhos.

7.3.3 Valor Médio e Desvio Padrão

A Equação 9 na Seção 5.1.3.7 permite calcular o valor médio do número de saltos que um pacote executa da origem até o destino. Representando o valor médio por μ, o desvio padrão σ pode ser calculado numericamente da mesma maneira, considerando uma soma executada um número finito K de vezes, com K suficientemente grande para que os erros fiquem confinados a valores aceitáveis.

$$\mu = \sum_{t=1}^{K} tP_t(x) \qquad \text{Equação 17}$$

$$\sigma^2 = \sum_{k=1}^{K} t^2 P_t(x) - \mu^2 \qquad \text{Equação 18}$$

O valor médio tem um significado importante que permite calcular vazão e atraso médios que caracterizam a rede. Entretanto, o desvio calculado desta maneira, principalmente em redes muito grandes, o simples fato de existirem números de salto pequenos e grandes, a Equação 18 produz um desvio muito grande por estar considerando todos os possíveis números de salto da rede. É importante saber o desvio que existe para um único pacote, ou para um dado par origem-destino. O número mínimo de saltos pode ser obtido pelo mesmo algoritmo da Seção 5.1.3.7 com a condição de carga nula. A maneira correta de avaliar desvios, neste caso, é considerar um único par origem-destino onde existe um valor mínimo de saltos para o caso em que o pacote utiliza o menor caminho e desvios deste valor para cima para os casos onde há deflexão.

Em redes pequenas (redes de acesso) o chaveamento de pacotes por deflexão reduz o tempo de propagação em ordens de grandeza, passando de milissegundos para microssegundos. Isto porque no chaveamento por deflexão fica eliminado o tempo de processamento dos pacotes nos roteadores. Nas redes maiores (redes nacionais ou internacionais de longa distância) o tempo de propagação pela fibra aumenta muito e supera os tempos de processamento dos pacotes, fazendo com

que o chaveamento de pacote não tenha tanta vantagem no quesito de atraso. O atraso e a variação do atraso são parâmetros muito importantes que merecem tratamento especial em futuros trabalhos.

7.3.4 Chaveamento de Lotes de Pacotes

Chaveamento em Lotes equivale ao termo em inglês: *Burst Switching*. Este termo pode ser traduzido também como comutação em rajadas. Na área de redes ópticas esta tecnologia é conhecida como OBS (*Optical Burst Switching*). A tecnologia utiliza conceitos do chaveamento de pacotes ópticos, mas monta vários pacotes em um único lote com endereço comum e envia todos ao mesmo tempo após alguma negociação ou reserva de banda. Ao chavear um grande número de pacotes simultaneamente, o tempo de chaveamento e a tecnologia empregada nas chaves ópticas influenciam menos do que no caso do chaveamento pacote a pacote. O processo de chaveamento de pacotes necessita de chaves muito rápidas. Um exemplo desta necessidade pode ser verificado com pequeno pacote de controle TCP de 40 bytes na taxa de transmissão de 40 Gbps. Este pacote demora apenas 8 ns para passar pela chave e, portanto, as chaves ópticas devem ser muito rápidas para conseguir completar o processo de chaveamento em intervalo de tempo de pelo menos 1 ns.

O presente trabalho diferencia-se do chaveamento em lotes, por não precisar montar grandes lotes. Os pacotes, por menores que sejam, podem ser enviados individualmente. Mesmo assim, a montagem de grandes lotes é possível e de simples adaptação. Para montar um lote, basta juntar pacotes sem tempo de guarda entre eles. Cada lote, precedido por um único cabeçalho, passa pelas chaves como se fosse um único pacote, mantendo a chave travada durante todo o tempo de sua passagem. Isto é possível porque a chave é liberada para movimentar-se somente

quando não há pacote em nenhuma de suas entradas e saídas. Também é necessário adaptar a linha de retardo óptico para o tamanho do lote que se deseja inserir na rede. Para não haver colisão, o pacote, ou o lote a ser inserido, precisa ter espaço livre garantido. Sem armazenamento óptico, este espaço precisa ser verificado na linha de retardo. O espaço livre, dentro da linha de retardo, precisa ser maior do que o lote a ser inserido. Portanto, a própria linha de retardo deve ser maior do que os lotes que se deseja inserir. Além da linha de retardo as chaves não têm nenhuma visibilidade. A única informação sobre o conteúdo da linha de retardo é obtida pela amostra que é retirada na entrada de tal linha de retardo. Todo o lote, uma vez inserido, é enviado integralmente até o destino final. O tamanho máximo, destes pacotes agregados em lotes (*burst)*, pode ser determinado em função de parâmetros como taxa de bloqueio e tempo médio de espera, que interferem no comportamento geral da rede.

Nas redes de grandes enlaces como a NFSNET utilizar pacotes com a metade do tamanho dos enlaces já caracteriza chaveamento em lotes. O modelo analítico apresentado nesta tese não impõe tamanho máximo de pacotes e todas as conclusões podem ser estendidas para redes OBS.

7.3.5 Aproveitamento de Situações do Tipo “tanto-faz”

Quando um pacote chega ao nó e a chave se posiciona para atendê-lo, é possível que chegue outro pacote pela outra porta, ainda com tempo para uma troca de decisão. Isto pode acontecer porque a linha de retardo é maior do que o necessário para o chaveamento. A linha de retardo é aumentada para possibilitar a inserção de pacotes grandes (maiores do que o tempo necessário para o chaveamento). Neste caso, é possível verificar se existe um dos dois pacotes em situação tipo tanto-faz e em caso positivo proceder à operação onde o pacote tipo tanto-faz possa ceder a

vez para o outro pacote mesmo que tenha chegado à frente dele. Este procedimento aumenta a probabilidade de usar o menor caminho sem aumentar recursos físicos ou computacionais. A lógica de chaveamento deve considerar que a chave permaneça na posição que se encontra quando chega um pacote tipo tanto faz. E, além disso, deve-se criar um tempo crítico configurável, a partir do qual, não se troca mais a posição da chave. Antes do referido tempo, a chave permanece em posição de espera para atender o próximo pacote. Estes casos foram tratados adequadamente no trabalho de Acampora (1992), pois o autor considera a possibilidade de um pacote aumentar a sua probabilidade de escolher a saída quando encontra um pacote, à sua frente, do **tipo tanto-faz**. Este pacote, embora com direito de escolha, pode ceder a sua vez para o pacote que chega depois, desde que isto aconteça dentro de um intervalo de tempo previamente estabelecido. Este tipo de ganho de probabilidade foi considerado nesta tese apenas em parte quando todos os casos **tipo tanto-faz** foram identificados e quando foi estabelecida a probabilidade de 50% para cada porta de saída de todos eles. Seção (Seção 5.1.3.6).

Um trabalho complementar importante, proposto para futuros trabalhos é a inclusão do aproveitamento dos casos **tipo tanto-faz** na simulação e também no modelo analítico.

7.3.6 Necessidade da Transparência

Em todas as configurações discutidas nesta tese, o sinal é removido no primeiro momento juntamente com a amostra utilizada para identificar o cabeçalho óptico. Sendo assim, todos os nós que funcionam como destino final devem ter capacidade para altas taxas. O sinal óptico que trafega pela rede deve poder ser interpretado em todos os nós da rede. Existindo este recurso, o cabeçalho óptico pode ser escrito na

mesma taxa do conteúdo do pacote, não sendo necessário um cabeçalho de menor taxa, como tradicionalmente acontece nas redes de pacotes ópticos. Na verdade, estas estruturas permitem trabalhar diretamente com o endereço IP sem necessidade do quadro Ethernet. Entretanto é preciso incluir um quadro com alguns bits de sincronismo, na frente do pacote óptico, para garantir o sincronismo necessário para identificar o relógio e o instante do primeiro bit válido. Estes bits de sincronismo são necessários mesmo que seja incluído o quadro Ethernet, pois os tradicionais sete bytes do preâmbulo do quadro Ethernet não são suficientes para o sincronismo de bits na taxa de 1Gbps.

Alguns nós podem utilizar taxas maiores transmitindo, por exemplo, na taxa de 10Gb/s. Neste caso terá que acrescentar um cabeçalho na taxa de 1Gb/s na frente de seus pacotes para que possa ser roteado pela rede durante o percurso. Somente o destino deve ter capacidade para 10Gb/s. A rede permanece transparente à taxa.

A constatação de que não é necessário utilizar cabeçalho com taxa mais baixa levanta uma questão importante: Porque não utilizar conversão eletro-óptica em todos os nós? A resposta não é simples e precisa ser investigada. Pode ser feito um trabalho de confrontação dos custos de implantação e manutenção das duas tecnologias ou, em termos de atraso e variação de atraso, ou consumo de energia e de espaço físico ou ainda todas estas considerações conjuntamente.

REFERÊNCIAS

ACAMPORA, A. S.; SHAH, I. A. Multihop lightwave network: a comparison of store-and forward and hot potato routing. **IEEE Transactions on Communications**, v.40, n.6, p. 1082-1090, 1992.

BARABÁSI, A. L. The Architecture of Complexity; **IEEE Control Systems Magazine**, p33-42, August, 2007.

BARABÁSI, A.; ALBERT, R. Emergence of Scaling in Random Networks**,** ***Science*** 15 October 1999. v. 286, n. 5439, p. 509 – 512, 1999. Disponível em: <http://www.sciencemag.org/cgi/content/full/286/5439/509>, acessado em 28/nov/2007.

BARAN, P. On Distributed Communications Networks; **IEEE Transactions on Commnications Systems**, vol l2, 1964

BARÁN, B.; SOSA, R. A new aproach for AntNet routing. In: **Proc. of Ninth International Conference on Computer Communications and Networks,** p. 303-308; 2000.

BARBOSA, F. R.; MAIA, D.; PEZZOLO, L.; SACHS, A. C.; SALVADOR, M. R.; Optical Packet Switching Node for Metro-Access Networks. In: **European Conference on Optical Communications**, ECOC'2003, Rimini, Italy, Sep. 2003.

BARBOSA, F. R.; SACHS; A. C. Transparent Optical Packet Switching Node based on Bottom-up Organization Network. In: Simpósio Brasileiro de Telecom. SBT 2004, Belem - PA. In: **Anais XXI Simp. Brasileiro de Telecom SBT 2004**. Belém - PA : Unama, v. 01; p. 45-51; 2004.

BARBOSA, F. R.; SACHS; A. C.; FERREIRA, R. S.; FURTADO, M. T. New Photonic System for Optical Packet Switching. In: **Proc. 6th World Conference on Systemics, Cybernetics, and Informatics** – SCI'2002, Orlando, FLA, USA, July 2002.

BARBOSA, F. R.; SACHS, A. C.; FURTADO, M. T. **Apparatus, system and method for optical packet switching using frequency header**. US Pat. 7577358. Jan 30, 2002.

BARBOSA, F. R.; SACHS, A. C.; FURTADO, M. T. **Método para gerar um pacote óptico, método para comutar um pacote óptico, dispositivo de comutação óptica, rede óptica, gerador de pacote óptico, e, sinal de pacote óptico**. BR PI 0215569-9. 30 jan 2002.

BARBOSA, F. R.; SACHS, A. C.; FURTADO, M. T.; ROSOLEM, J. B. Optical Packet Switching: a transmission and recovery demonstration using a SCM header. In: **Proc. XIX Simpósio Brasileiro de Telecomunicações** – SBT'2001, Fortaleza – CE – Brasil, Setembro 2001.

BATHULA, B.G.; ELMIRGHANI, J.M.H. Constraint-Based Anycasting Over Optical Burst Switched Networks, **J. OPT. COMMUN. NETW**, v. 1, n. 2, p. A35-A43, 2009.

BEHESHTI, N.; GANJALI, Y.; RAJADURAY, R.; BLUMENTHAL, D.; McKEOWN, N. Buffer sizing in all-optical packet switches, Optics Classification and Indexing Scheme –OCIS codes: (060.4250) Networks, (060.1810) Couplers, switches, and multiplexers. In: **Optical Fiber Communication Conference**, OFC 2006.

BLUMENTHAL, D. J.; BOWERS, J.; CHIU, Y.; CHOU, H.; OLSSON, B.; RANGARAJAN, S.; RAU, L.; WANG, W. Optical Packet Switching and Associated Optical Signal. In: **Proc. IEEE/LEOS Summer Topical Meeting**, Jul. 2002, Mont-Tremblant, Canada (invited talk), 2002.

BONANI, L. H. **Contribuição ao estudo de redes fotônicas de pacotes**. Dissertação (Mestrado), Faculdade de Engenharia Elétrica e de Computação da UNICAMP, Campinas, 2003.

BONANI, L. H. **Proposta de Arquitetura Inovadora Para Redes de Pacotes Baseada em Chaveamento Fotônico**. Tese (Doutorado). Faculdade de Engenharia Elétrica da UNICAMP, Campinas, ago. 2006.

BONANI, L. H.; RUDGE BARBOSA, F.; MOSCHIM, E. Fully Optimized Mesh Topologies for Optical Packet Switching Network Architectures. In: **Proc. Of the 13th International Conference on Telecommunications**, ICT 2006, paper ON1-03, Funchal, Madeira Island, Portugal, maio, 2006.

BRESCIANI, F. E.; D´OTTAVIANO, I. M. L. Conceitos Básicos de Sistêmica, em: **Auto Organização – Estudos Interdisciplinares**, org. por I. M. L. D´Ottaviano & M. E. Q. Gonzales, Campinas: Coleção CLE, vol. 30, 2000. p. 283-306.

BUCHTA, H.; GAUGER C. M. Maximum Size and Throughput of SOA-Based Optical Burst Switching Nodes With Limited Tuning-Range Wavelength Converters and FDL Buffers; **Journal of Lightwave Technology**, vol. 26, no. 16, p 2919- 2927, August 2008.

CALABRETTA, N.; JUNG, H.; HERRERA, J.; TANGDIONGGA, E.; KOONEN, T.; DORREN, H. 1 x 4 All-Optical Packet Switch at 160 Gb/s Employing Optical Processing of Scalable In-Band Address Labels. In: **Proc. Optical Fiber Communication Conference.** Post Deadline paper PDP33 in OFC 2008

CANNONS, J.; DOUGHERTY, R.; FREILING, C. Network Routing Capacity; **IEEE Transactions on Information Theory**, v. 52, n. 3, March 2006.

CARLSON, J. M., DOYLE, J. Complexity and Robustness; **Proceedings of the National Academy of Sciences** - PNAS, February 19, v. 99, suppl. 1, p. 2538–

2545, 2002.

CASTRO, E. R. S. **Modelo para a Distribuição de Probabilidade do Comprimento dos Pacotes em Redes de Computadores**. Tese (doutorado), Departamento de Engenharia Elétrica da Universidade Federal de Campina Grande, Campina Grande - PB, março de 2011.

CHARLET, G; RENAUDIER, J; MARDOYAN, H; TRAN, P; PARDO, O. B.; VERLUISE, F; ACHOUCHE, M.; BOUTIN, A; BLACHE, F; DUPUY, J. Y.; BIGO. S. Transmission of 16.4Tbit/s Capacity over 2,550km Using PDM QPSK Modulation Format and Coherent Receiver; **Proc. Optical Fiber Communication Conference**; postdeadline paper PDP3; San Diego, 2008

CHUNG, T.,Y.; D.P.AGRAWAL, D.,P. On the Network Characterization of and Optimal Broadcasting in the Manhattan Street Network. In: **INFO-COM´90**, p.465-472, 1990.

CISCO. Cisco Visual Networking Index – Forecast and Methodology, 2007–2012. White Paper. Disponível em http://newsroom.cisco.com/dlls/2008/ekits/Cisco_Visual_Networking_Index_061608.pdf Acessado em janeiro de 2008.

CORNING. ClearCurve Optical Fiber brochure; Disponível em: http://www.corning.com/WorkArea/showcontent.aspx?id=8831. Acessado em: setembro de 2008.

DE WOLF, T.; HOLVOET, T.; BERBERS, Y. Emergence as a Paradigm to Engineer Distributed Autonomic Software, Katholieke Universiteit Leuven, Department of Computer Science, Celestijnenlaan 200A 3000 Heverlee (Belgium). **Report CW380**, Mar. 2004.

DEBRUN, M. A Idéia de Auto-Organização, em: Auto-Organização, org. por M. Debrun, M.E.Q. Gonzales & O. Pessoa Jr., Coleção CLE 18, Campinas, p. 3-23,

1996. Disponível em: http://www.homeopathicum.com/arquivos/aotexto2.doc Acessado em: agosto de 2010.

DIJKSTRA, E.W. A Note on Two Problems in Connexion with Graphs, **Numerische Mathematik**, v. 1, p. 269-271, 1959.

DITTMANN, et al. The European IST Project DAVID: a Viable Approach towards Optical Packet Switching; JSAC Special Issue on High-Performance Optical/Electronic Switches/routers for High-Speed Internet II. **IEEE Journal on Selected Areas in Communications**. v. 21, n. 7, p. 1026 – 1040, Sept. 2003.

EIDO, T.; DUNG T. N.; ATMACA, T. Packet Filling Optimization in Multiservice Slotted Optical Packet Switching MAN N. In: **Proc. Fourth Advanced International Conference on Telecommunications**, 2008. AICT apos;08. Issue 8-13, p. 221 – 226, June 2008.

EVEN, S.; ITAI, A.; SHAMIR, A. On the complexity of time table and multi-commodity flow problems. In: **Proc. 16th Annual Symposium on Foundations of Computer Science**, p. 184-193, 1975.

FERREIRA, A. B. de H. **Novo Dicionário da Língua Portuguesa**, JEMM Editores Ltda., 1986.

FISHMAN, D. A.; KAO, Y.; LIU, X.; CHANDRASEKHAR, S. Transmission in optically transparent core networks. **Journal of Optical Networking**, v. 7, Issue 4, p. 310-320, 2008.

GAMBINI, P.; et al. Transparent Optical Packet Switching: Network Architecture and Demonstrators in the KEOPS Project, **IEEE Journal on Selected Areas in Communications**, v. 16, n. 7, p. 1245-1259, September 1998.

GOOGLE. **GoogleMaps**. Disponível em: www.googlemaps.com. Acessado em: dezembro de 2008.

GUEDES, B. C. L.; MOSSO, M. M.; SILVA, H. J. P. P.; LIMA, R. A. A.;

PODCAMENI, A.; SACHS, A. C.; BARBOSA, F. R. Performance Analysis of an Optical Switched Manhattan Street Network, **Photonic Network Communications**, v.10, n.3, p. 361–370, 2005.

GUILLEMOT, C.; et al. Transparent Optical Packet Switching: The European ACTS KEOPS Project Approach, **Journal of Lightwave Technology**, v. 16, n. 12, p 2117-2134, December 1998.

GUILLEMOT, C.; HENRY, M.; CLEROT, F.; LE CORRE, A.; KERVAREE, J.; DUPAS, A.; GRAVEY, P. KEOPS optical packet switch demonstrator: architecture and testbed performance. In: **Proc. Optical Fiber Communication Conference**; p. 204-206 v.3; Baltimore, 2000

GHOBRIL, P.; TOHME, S. In: **Proceedings of 2003 5th International Conference on Transparent Optical Networks.** Issue 29 June-3, p. 51 – 54, v.1, July 2003.

GLIF – Global Lambda Integrated Facility Home Page; Disponível em: http://www.glif.is/ ; acesso em outubro de 2008.

GREENBERG, A.G.; GOODMAN, J. Sharp approximate models of adaptative routing in mesh networks. **Telegraffic Analysis Computer Performance Evaluation**. Elsevier Science - North Holland, p 255-269, 1986.

HERMAN, W. P. **Formulação Algébrica para a Modelagem de Algoritmos de Roteamento Multi-restritivo Hop-By-hop**, tese (Doutorado), Escola Politécnica da USP, São Paulo, abril de 2008.

IEEE **Std 802.3av^{TM} - 2009**: Amendment 1: Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks. Disponível em: http://standards.ieee.org/getieee802/download/802.3av-2009.pdf. Acessado em: 06 de maio de 2011.

ITU-T (Telecommunication Standardization Sector of ITU). **G.657**: Characteristics of a bending loss insensitive single mode optical fibre and cable for the access network (11/2009). Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: 25 jan. 2011.

_____. **G.983.1**: Broadband optical access systems based on Passive Optical Networks (PON) (01/2005). Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: 25 jan. 2011.

_____. **G.983.2**: ONT management and control interface specification for B-PON, 07/2005. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011

_____. **G.983.3**: A broadband optical access system with increased service capability by wavelength allocation, 03/2001. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.983.4**: A broadband optical access system with increased service capability using dynamic bandwidth assignment, 11/2001. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.983.5**: A broadband optical access system with enhanced survivability, 01/2002. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.984.1**: Gigabit-capable passive optical networks (GPON): General characteristics, 03/2008. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.984.2**: Gigabit-capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) layer specification, 03/2003. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro

de 2011.

_____. **G.984.3**: Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification, 03/2008. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.984.4**: Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification, 02/2008. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.984.5**: Gigabit-capable Passive Optical Networks (G-PON): Enhancement band, 09/2007. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

ITU-T (Telecommunication Standardization Sector of ITU). **G.984.6**: Gigabit-capable passive optical networks (GPON): Reach extension, 03/2008. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.984.7**: Gigabit-capable passive optical networks (GPON): Long reach, 07/2010. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.987**: 10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations, and acronyms, 10/2010. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.987.1**: 10-Gigabit-capable passive optical networks (XG-PON): General requirements, 01/2010. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.987.2**: 10-Gigabit-capable passive optical networks (XG-PON): Physical media dependent (PMD) layer specification, 10/2010. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

_____. **G.987.3**: 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) specifications, 10/2010. Disponível em: http://www.itu.int/itu-t/recommendations/index.aspx?ser=G. Acessado em: janeiro de 2011.

JOHNSON, S. **Emergence (The Connected Lives of Ants, Brains Cities and Software)**. Scribner, New York, 2001.

KEHAYAS, E.; TSIOKOS, D; BAKOPOULOS, P.; APOSTOLOPOULOS, D.; PETRANTONAKIS, D.; L. STAMPOULIDIS,L.; A. POUSTIE, A.; McDOUGALL, R.; MAXWELL, G.; LIU, Y.; ZHANG, S.; DORREN, H. J. S.; SEOANE, J.; HOLM-NIELSEN, P. V.; JEPPESEN, P.; AVRAMOPOULOS, H. 40-Gb/s all-optical processing systems using hybrid photonic integration technology. **Opt. Expr**., v. 13, n. 2, p. 475–480, Jan. 2005.

KNOX, L; CHRISTENSEN, N; SKORDIS, C. The Age of the Universe and the Cosmological Constant Determined From Cosmic Microwave Background Anisotropy Measurements; **The Astrophysical Journal**, 563:L95–L98, 2001 December 20

KOMATSU, E.;et al. Five-Year Wilkinson Microwave Anisotropy Probe Observations: Cosmological Interpretation. **The Astrophysical Journal Supplement**, v. 180, Issue 2, p. 330-376, 2009.

LEWIS, H.R.; PAPADIMITRIOU, C.H. **Elements of the Theory of Computation**. Printice-Hall, 1998.

MACK, J.P.; NGUYEN, K.N.; GARCIA, J.M.; BURMEISTER, E.F.; DUMMER,

M.M.; POULSEN, H.N.; STAMENIC, B.; KURCZVEIL, G.; HOLLAR, K.; COLDREN, L.A.; BOWERS, J.E.; BLUMENTHAL, D.J. Asynchronous 2x2 Optical Packet Synchronization, Buffering, and Forwarding. OThN1. OSA / OFC/NFOEC 2010.

MARTINS, I.B. **Análise de Tráfego, Capacidade e Proteção em Redes de Pacotes Ópticos com Chaveamento Fotônico**. 2007. 109p. Dissertação (Mestrado) – Faculdade de Engenharia Elétrica e de Computação, UNICAMP, Campinas, 2007.

MARTINS, I.B.; BARBOSA, F.R.; SACHS, A.C.; MOSCHIN, E. Innovative Architectures for Future OPS/OBS Advanced Photonic Networks; **SBMO/IEEE MTT-S International Microwave &Optoelectronics Conference** (IMOC 2009), 2009

MOBILON, E.; et al. Hardware Architecture for Optical Packet and Burst Switching Applications, 8th International Conference. In: **Proceedings of ITS 2006**, Jhongli, Taiwan, June 26-30, p278, 733; 2006

MORAES, I. M.; DUARTE, O. C. M. B. Uma Avaliação Multienlace do Mecanismo de Controle de Admissão Baseado no Grau de Ocupação em Redes Ópticas. In: **Anais do 25° Simpósio Brasileiro de Redes de Computares e Sistemas Distribuídos**, 2007

MOTTER, A. E.; TOROCZKAI, Z. Introduction: Optimization in networks**,** Chaos 17, 026101 (2007). Copyright © 2007 American Institute of Physics. Disponível em: <http://www.nd.edu/~networks/Publication%20Categories/03%20Journal%20Articles/Computer/OptimzationNetworks_Chaos-28Jun07.pdf>; acesso em 28/Nov/2007.

MURAKAMI, M.; SEKI, T.; ODA, K.; YAMAGUCHY, J.; Impact of MEMS-based optical cross connect switching on optical amplifier transient response for

automatically switched optical network applications. In: **Proceedings of Optical Amplifiers and Their Applications (OAA)**, WC5, Budapest, Hungary. August 7, 2005.

NETO, J. J. Adaptative Rule-Driven Devices – General Formulation and Case Study. Lecture Notes in Computer Science. Watson, B. W. and Wood, D. (Eds.): **Implementation and Application of Automata 6th International Conference**, CIAA 2001, v. 2494, Pretoria, South Africa, July 23-25, Springer-Verlag, 2001. p. 234-250. Disponível em:< http://www.pcs.usp.br/~lta/artigos/neto_ciaa2001.pdf>; acesso em 28/Nov/2007.

NSFNET: **A Partnership for High-Speed Networking Final Report** 1987-1995; Disponível em: http://www.merit.edu/networkresearch/projecthistory/nsfnet/pdf/nsfnet_report.pdf ; Acessado em: set. 2008.

O'MAHONY, M.J.; POLITI, C.; KLONIDIS, D.; NEJABATI, R.; SIMEONIDOU, D. Future Optical Networks. **Journal of Lightwave Technology**, v. 24, n. 12, p. 4684- 4696, December 2006

PAVLOSOGLOU, I.; LEESON, M. S.; GREEN, R. J. Towards bottom-up network architectures, ISBN: 1-9025-6009-4 © 2003 PGNet, 2003

PISTORI, H.; NETO, J. J.; PEREIRA, M. C. Adaptive Non-Deterministic Decision Trees: General Formulation and Case Study. **INFOCOMP Journal of Computer Science**, Lavras, MG, 2006.

PRIGOGINE, I. **As leis do caos**. São Paulo: Fundação Editora da UNESP, 2000. Traduzido de Le leggi del caos. Laterza: Roma-Bari, 1993.

ROCHA, M.L.; ROSSI, S.M.; BARROS, M.R.X.; PEZZOLO, L.; ROSOLEM, J. B.;OLIVEIRA, M.F.; PARADISI, A. Experimental performance evaluation of five-node IP over WDM laboratory test-bed, **Electronics Letters**, v. 38, n. 23, p.

1460-1462, November 2002.

ROCHA, M. L.; et al. Effects of External Modulation Transmission at 10 Gb/s Without Dispersion Compensation Through an All-Optical Node Concatenation. In: **Proceedings SBMO/IEEE MTT-S IMOC 2003**, PD18 v.3 Print ISBN: 0-7803-7824-5, Foz do Iguaçu-PR, 2003.

ROCHETTE, M.; BLOWS, J.L.; EGGLETON, B.J. 3R optical regeneration: an all-optical solution with BER improvement. **Optics Express**, v. 14, Issue 14, p. 6414-6427, 2006.

ROSSI, S.M., et al., Optical WDM networks with distributed IP-centric control plane. SBM0'2002, Recife, Brazil, Paper 170. In: **Proc. 10th Brazilian Microwave and Optoelectronics Symp.**, 2002.

ROYAL SWEDISH ACADEMY OF SCIENCE, Two Revolutionary Optical Technologies, compiled by the Class for Physics of the Royal Swedish Academy of Sciences, (2009). Disponível em: http://nobelprize.org/nobel_prizes/physics/laureates/2009/sciback_phy_09.pdf. Acessado em: 10 jan. 2011.

ROSBERG, Z.; HAI, L. V.; ZUKERMAN, M. W. Performance analyses of optical burst-switching networks. **IEEE Journal on Selected Areas in Communications**, v. 21, Issue 7, p. 1187 – 1197, Sept. 2003.

RYAN, A. Emergence is coupled to scope, note level. **Adaptation and Self-Organizing Systems (nlin.AO)**, available at http://arxiv.org/abs/nlin/0609011v1 , submited in Sept., 2006.

SACHS, A.C.; BARBOSA, F.R.; PEZZOLO, L. **Estrutura de pacote óptico com cabeçalho de endereçamento por freqüência; arquitetura de nó, método e dispositivo para roteamento de pacotes ópticos com cabeçalho de endereçamento por freqüência em redes fotônicas.** BR PI 0405093-2, 02 set

2004.

SACHS, A.C., LOPES, C.M.B., CARVALHO, T. C. M. B. Protection Schema for Optical Packet Switching Network with Large Number of Nodes. In: **SBMO/IEEE MTT-S International Microwave &Optoelectronics Conference** (IMOC 2009), 2009.

SANO, A.; et al. 69.1-Tb/s (432 x 171-Gb/s) C- and Extended L-Band Transmission over 240 Km Using PDM-16-QAM Modulation and Digital Coherent Detection. In: **Optical Fiber Communication Conference**; postdeadline paper PDPB7; San Diego, 2010.

SCHUBERT, C.; LUDWIG, R.; WEBER, H-G. **J. Opt. Fiber Commun.** Rep. 2, p. 171–208, 2004.

SHEARD, S. A.; MOSTASHSRI, A. Principles of complex systems for systems engineering. **Systems Engineering**, v. 12, Issue 4, p. 295 – 311, 2008

SHINYA, A. et al. All-optical on-chip bit memory based on ultra high Q InGaAsP photonic crystal. **Optics Express**, v. 16, n. 23, p. 19384, Nov. 2008.

SIFALAKIS, M.; LOUCA, A.; MAUTHE, A.; PELUSO, L.; ZSEBY, T. A Functional Composition Framework for Autonomic Network Architectures, Autonomic Network Architecture (ANA) Project, which is sponsored by the EU-IST initiative on Future and Emerging Technologies, 2006.

SIPSER, M.; **Introduction to the Theory of Computation**. Boston: PWS, 1997.

SMALL, B. A.; SHACHAM, A.; BERGMAN, K. A Modular, Scalable, Extensible, and Transparent Optical Packet Buffer. **Journal of Lightwave Technology**, v. 25, n. 4, p. 78-985, Apr. 2007.

SPIEKMAN, L.; PIEHLER, D.; IANNONE, P.; REICHMANN, K.; LEE, H.

Semiconductor Optical Amplifiers for FTTx. In: **Proc. of 9th International Conference on Transparent Optical Network**, 1-5 July 2007, v. 2, p. 48, Jul. 2007.

STAMATIADIS, C.; BOUGIOUKOS, M.; MAZIOTIS, A.; BAKOPOULOS, P.; STAMPOULIDIS, L.; AVRAMOPOULOS, H. All-Optical Contention Resolution using a single optical flipflop and two stage all-optical wavelength conversion. OThN5. OSA / OFC/NFOEC 2010.

STAVDAS, A.; POLITI, C.; ORPHANOUDAKIS, T.; DRAKOS, A. Optical packet routers: how they can efficiently and cost-effectively scale to petabits per second [Invited]**. Journal of Optical Networking**, v. 7, n. 10, p. 876-894, Oct. 2008.

STERN, T. E.; BALA, K. **Multiwavelength Optical Networks**. Massachusetts: Addison Wesley, 1999

TANEMURA, T.; NAKANO, Y. Design and scalability analysis of optical phased-array 1×N switch on planar lightwave circuit. **IEICE Electron Express** n. 5, p. 603-609, 2008.

TANEMURA, T.; TAKEDA, K.; NAKANO, Y. Wavelength-multiplexed optical packet switching using InP phased-array switch. **Optics Express**; v. 17, n. 11, May 2009.

TEIMOORI, H.; APOSTOLOPOULOS, D.; VLACHOS, K.G.;WARE, C.; PETRANTONAKIS, D.; STAMPOULIDIS, L.; AVRAMOPOULOS, H.; ERASME, D. Optical-Logic-Gate Aided Packet-Switching in Transparent Optical Networks. **Journal of Lightwave Technology**, v. 26, n. 16, p. 2848- 2856, Aug. 2008.

TUCKER, R. S. The Role of Optics and Electronics in High-Capacity Routers. **Journal of Lightwave Technology**, v. 24, n. 12, p. 4655-4673, Dec. 2006.

TURCOTTE, D. L. RUNDLE, J. B. Self-organized complexity in the physical,

biological, and social sciences. In: **Proceedings of the National Academy of Sciences – PNAS**, February 19, vol. 99, suppl. 1, p. 2463–2465, Feb. 2002.

TURING, A. On computable numbers with an application to the entscheidungsproblem. **Proc. London Math. Soc.**, Ser. 2, v. 42, p. 230-265, 1936.

_____. On computable numbers, with an application to the entscheidungsproblem. A Correction; **Proc. London Math. Soc.**, Ser. 2, v. 43, N. 2198, p 544-546 (1936).

VITERBI, A. J. Convolutional Codes and Their Performance in Communication Systems. **IEEE Transactions on Communications Technology**, p 751-772, Oct. 1971

WAI, P.K.A.;XU, L.; LUI, K.L.F.; LI, C.; CHAN, L.; TAM, H. A Minimalist Approach to All-Optical Packet Switching. disponível em: http://www.osa-opn.org/Content/ViewFile.aspx?id=6693 acessado em janeiro de 2009. **Optics & Photonis News**, Mar. 2005.

WHITE, I. M.; WONGLUMSOM, D.; SHRIKHANDE, K.; GEMELOS, S. M.; ROGGE, M. S.; KAZOVSKY, L. The architecture of HORNET: A packet-over-WDM multiple-access optical metropolitan area ring network. **ELSEVIER Computer Networks**, v. 32, n. 5, p. 587-598, 2000.

ZUE, H.; ZUE K.; MUKHERJEE, B. Cost-Effective WDM Backbone Network Design with OXCs of Different Bandwidth Granularities. In: **Proc. of OFC 2003**, v. 2, p. 784, 2003.

ANEXO

Códigos utilizados na modelagem analítica

Foram utilizados três códigos para a modelagem analítica da proteção e escalabilidade. Um código para gerar as matrizes de conectividade de até 256 nós de rede na topologia *Manhattan Street*, com ou sem falha em um dos enlaces. Um segundo código que parte da matriz de conectividade e calcula o caminho mais curto montando uma matriz de comutação. Um terceiro código para calcular o número médio de saltos com ou sem falha.

O terceiro código tem duas versões complementares: um para calcular mapeamento com tráfego mais simétrico e outro para considerar com *Ppl=1/H* (Modelo 2)

<u>Primeiro código</u>

```
//Módulo: gera conectividade para rede tipo "Manhattan Street" para simulação adaptativa.

//Opção adaptativa 2: proteção que desliga apenas 4 enlaces em caso de falha (BUONA).

//autor: Antonio de Campos Sachs

//data: testado em 10 de novembro de 2008

//data: testado com falha em 12 de março de 2009

//23 de agosto de 2009 - incluido diretorio para arquivos de saida
```

```
clear;
falha=0; n=16; N=n^2; c=zeros(N,N);
//linhas ímpares
  for i=1:2:n-1;
    for j=2:2:n-1;
    c((i-1)*n+j,(i-1)*n+j+1)=1; c(i*n+j,(i-1)*n+j)=1;
    c(i*n+j+1,i*n+j)=1; c((i-1)*n+j+1,i*n+j+1)=1;
    end;
  c(i*n,i*n-n+1)=1; c(i*n+n,i*n)=1;
  c(i*n+1,i*n+n)=1; c(i*n-n+1,i*n+1)=1;
  end;
//linhas pares
  for i=2:2:n-1;
    for j=1:2:n-1;
    c((i-1)*n+j+1,(i-1)*n+j)=2; c(i*n+j+1,(i-1)*n+j+1)=2;
    c(i*n+j,i*n+j+1)=2; c((i-1)*n+j,i*n+j)=2;
    end;
  end;
  for j=1:2:n-1;
    c(j,j+1)=2; c(N-n+j,j)=2;
    c(N-n+j+1,N-n+j)=2; c(j+1,N-n+j+1)=2;
```

```
  end;
//falha no enlace n >> n-1
if falha==1; porta=c(n-1,n);c(n-1,n)=0;
  [w]=find(c(n,:));if c(n,w(1))==porta;c(n,w(1))=0; prox=w(1); end;
  if c(n,w(2))==porta;c(n,w(2))=0; prox=w(2); end;
  [w]=find(c(prox,:));if c(prox,w(1))==porta;c(prox,w(1))=0; prox=w(1);end;
  if c(prox,w(2))==porta;c(prox,w(2))=0; prox=w(2); end;
  [w]=find(c(prox,:));if c(prox,w(1))==porta;c(prox,w(1))=0; end;
  if c(prox,w(2))==porta;c(prox,w(2))=0; end;
end;
//arquivar
if falha==1; arq="./topoF/AMS"+code2str(n)+"F"+".txt";
  else arq="./topo/AMS"+code2str(n)+".txt"; end;
u=file('open',arq); write(u,c,'(100(I))'); file('close',u);
// ARQUIVO DE SAÍDA
// if falha==0; result="./result/AMS"+code2str(n)+"v"+code2str(v)+".txt";
//  else result="./resultF/AMS"+code2str(n)+"v"+code2str(v)+".txt";end;
// for i=1:contmax;
//  saida(i,1)=(i-1)*intervalo; //inclui zero
//  saida(i,1)=(i)*intervalo;     //exclui zero
//  saida(i,2)=esaltos(i); end
```

```
// u=file('open',result); write(u,saida,'(2(g))'); file('close',u);
```

Segundo código

```
// PORTA PREFERENCIAL

// Autor: Antonio deCampos Sachs

// Julho de 2008 - calcula cada origem separadamente -

// Este programa parte de arquivos com matriz de conectividade adaptativa que diferencia as portas de saída.

// Calcula matriz pp de portas preferenciais e portas "tanto faz"

// Calcula matriz pniv contendo número de saltos

// As transições são marcadas com 1 ou com 2 conforme matriz de conectividade adaptativa

// As transições "tanto faz" são marcadas com 3

//    São necessárias as matrizes:

//    c contendo a conectividade

//    pp matriz de saída com as portas preferenciais e tanto faz

//     ppp matriz de uns NxN para controlar origens que já completaram todos os caminhos
```

// per vetor dos permanecentes que devem ser utilizados no passo ou nível seguinte na árvore

// perpro vetor dos permanecentes no próximo passo. Inicia vazio em cada passo.

// pniv matriz indicando os níveis dos pares destino-origem

// 4 nós - 0 segundos

// 16 nós - 0.0468003 segundos 0.015625 segundos

// 36 nós - 0.1872012 segundos 0.140625 segundos

// 64 nós - 0.5928038 segundos 0.390625 segundos

// 100 nós - 1.4352092 segundos 0.890625 segundos

// 144 nós - segundos 1.875 segundos

// 196 nós - segundos 4.7112302 segundos

// 256 nós - segundos 8.3304534 segundos

// anel com falha: 35 36 06 e 05; sinalizar também respectivamente:34 30 01 e 11

// N-1 N n n-1 N-2 N-n 1 2n-1

// pp(:,N-2)=1; pp(:,N-n)=1; pp(:,1)=1; pp(:,2*n-1)=1; //derruba o programa;

// pp(N-1,N-2)=2; pp(N,N-n)=2; pp(n,1)=2; pp(n-1,2*n-1)=2; //erro de consistencia de variáveis;

//if falha==1 then destinos=N; else destinos=1; end;

//if falha==1 then mc=read(arqf,N,N); else mc=read(arq,N,N); end;

//Em P, a terceira dimensão é carga === P(:,:,1) => carga=zero

//Ppl é a PROBABILIDADE DE PACOTE SER LOCAL

```
//Pop é a Probabilidade do competidor desejar outra porta (no pior caso Pop=1)
mprintf('inicio'); timer();
clear;
n=16; N=n^2; falha=1; arq="AMS"+code2str(n)+".txt";
arquivo="./topo/AMS"+code2str(n)+".txt";
//nao precisa considerar topoF pois não estou calculando nada com isso ainda
c=read(arquivo,N,N); pp=c; ppp=ones(N,N);pniv=zeros(N,N);
for i=1:N; ppp(i,i)=0;end;
for j=1:N; fff=find(c(:,j)); ppp(fff(1),j)=0; ppp(fff(2),j)=0; end;
  for ii=1:N;
[w]=find(c(:,ii),2);
per=[w(1) w(2)]; nivel=1;
while sum(ppp(:,ii))>0; nivel=nivel+1;//inicia no nível 2
  perpro=[];
  k1=sum(size(per))-1;//k1 é o número de permanecentes no nível atual
  for i=1:k1;//permanecentes
    [w]=find(c(:,per(i)),2);
    for j=1:2;//duas saídas
        ori=ii; des=w(j); pai=per(i);
        if ppp(des,ori)==1;//novo par ori-des
          if pp(pai,ori)<>0;//pai já é acessado pela mesma origem
```

```
            pp(des,ori)=pp(pai,ori);

            ppp(des,ori)=0;

            pniv(des,ori)=nivel;

            perpro=[perpro w(j)];

          end;

        elseif pp(des,ori)<>pp(pai,ori)&pniv(des,ori)==nivel&pp(pai,ori)<>0;

          pp(des,ori)=3; end;

    end;//j=duas saídas

  end;//i=todos os permanecentes

  per=perpro;

end;

end;

if falha==1;

  pp(:,N-2)=2; pp(:,N-n)=2; pp(:,1)=2; pp(:,2*n-1)=2; //derruba o programa;

  pp(N-1,N-2)=1; pp(N,N-n)=1; pp(n,1)=1; pp(n-1,2*n-1)=1; //erro de consistencia de variáveis;

end;

if falha==0; arq="./pp/pp"+arq; else arq="./ppF/ppF"+arq; end;

nn=string(int(N));

u=file('open',arq,w);

write(u,pp,'('+nn+'(I))');
```

```
file('close',u);

mprintf(' fim'); timer()
```

Terceiro código

```
clear; stacksize(50000000);

//Baseado no arquivo: AMS-v5.sci - Adaptive Manhattan Street

//Autor: Antonio de Campos Sachs - junho de 2009

//COM FALHA: N=64 => 17 segundos; N=144 => 120 s conforme AMS-v4.sci; N=256 => 147s NESTA VERSÃO

//SEM FALHA: N=196 => 0.8580055 SEGUNDOS; N=256 => 1.1544074 SEGUNDOS

// anel com falha: 35 36 06 e 05; sinalizar também respectivamente:34  30  01  e 11

//              N-1  N  n  n-1                          N-2  N-n   1   2n-1

// estas falhas foram consideradas na geração do arqivo ppF

// neste programa basta ulizar o arquivo ppF já gerado

mprintf(' Nova simulação'); timer();

mprintf(' - número de nós de rede');

intervalo=25;  falha=1;  v=7;  n=16;  N = n**2;   deltaPk=1.0D-5;
```

```
contmax=int(100/intervalo)+1; maximo=(contmax-1)*intervalo;

arq="./topo/AMS"+code2str(n)+".txt";  mc=read(arq,N,N);

arqpp="./pp/ppAMS"+code2str(n)+".txt"; arqppf="./ppF/ppFAMS"+code2str(n)+".txt";

if falha==1; mprintf(' COM FALHA'); destinos=N; pp=read(arqppf,N,N);

  else mprintf(' SEM FALHA'); destinos=1; pp=read(arqpp,N,N); end;

//NÚMERO MÉDIO DE SALTOS

P=zeros(N,N,contmax); Ppl = 1/(N-1); Pop = 0.5;

contmax=contmax-1; //para excluir um dos casos (caso de carga zero)

for co=1:contmax; esoma(co)=0; //co=caso de carga

    c=(co)*intervalo;         //começa com carga = intervalo

//     c=(co-1)*intervalo;         //c é a carga. Para intervalo=25, c=0, 25%, 50%, 75% e
100%

    Poc=c/100;  Poc=Poc/2;    //Se linha de retardo = comprimento do link

    Ps = 1-Poc+Poc*Ppl+(Poc*Pop)*(1-Ppl); //PROBABILIDADE DE SUCESSO

//    if Ps==1&falha==1; Ps=0.95; end;

    Pd = 1-Ps;                          //PROBABILIDADE DE DEFLEXÃO

    for t=1:destinos; Ehops(co,t)=0;// t é o destino final utilizado em cada caso

        for j=1:N;                // j é a dimensão do nó de origem

            [w]=find(mc(:,j));s=size(w);//mc é a matriz de comutação definida na linha 14

              if s(2)==2;

                if mc(w(1),j)==pp(t,j)| pp(t,j)==3;
```

```
                P(w(1),j,co)=Ps; P(w(2),j,co)=Pd;
              else P(w(1),j,co)=Pd; P(w(2),j,co)=Ps;end;end;
            if s(2)==1; P(w(1),j,co)=1; end;
        end;
        TT=zeros(N,N); TT(:,:)=P(:,:,co); TT(:,t)=0;
        Pk0 = (1/(N-1))*ones(N,1); Pk0(t)=0;
        kint=1; Pk=Pk0;
        while sum(Pk)>deltaPk; Pk = TT*Pk; mat(kint,co,t)=Pk(t); kint=kint+1;end;
        kmax=kint-1;
        for k = 1:kmax; Ehops(co,t) = Ehops(co,t)+k*mat(k,co,t);end;
        esoma(co)=esoma(co)+Ehops(co,t);
    end;
    esaltos(co)=esoma(co)/destinos;
end; //casos de carga
mprintf(' TEMPO TOTAL'); timer()
//ARQUIVO DE SAÍDA
if falha==0; result="./result/AMS"+code2str(n)+"v"+code2str(v)+".txt";
  else result="./resultF/AMS"+code2str(n)+"v"+code2str(v)+".txt";end;
for i=1:contmax;
//  saida(i,1)=(i-1)*intervalo; //inclui zero
  saida(i,1)=(i)*intervalo;     //exclui zero
```

```
  saida(i,2)=esaltos(i); end

u=file('open',result); write(u,saida,'(2(g))'); file('close',u);
```

Terceiro código (tráfego mais simétrico para cálculo do mapa)

```
clear; stacksize(50000000);

//Baseado no arquivo: AMS-v5.sci - Adaptive Manhattan Street

//Autor: Antonio de Campos Sachs - junho de 2009

//COM FALHA: N=64 => 17 segundos; N=144 => 120 s conforme AMS-v4.sci; N=256 => 147s NESTA VERSÃO

//SEM FALHA: N=196 => 0.8580055 SEGUNDOS; N=256 => 1.1544074 SEGUNDOS

// anel com falha: 35 36 06 e 05; sinalizar também respectivamente:34  30  01  e 11

//              N-1  N  n  n-1                          N-2  N-n   1   2n-1

// estas falhas foram consideradas na geração do arqivo ppF

// neste programa basta ulizar o arquivo ppF já gerado

//29 de novembro de 2009: mais simétrico no caso tanto-faz

mprintf(' Nova simulação'); timer();

mprintf(' - número de nós de rede');
```

```
intervalo=25;  falha=0;  v=10;  n=16;  N = n**2;   deltaPk=1.0D-6;

contmax=int(100/intervalo)+1; maximo=(contmax-1)*intervalo;

arq="./topo/AMS"+code2str(n)+".txt";  mc=read(arq,N,N);

arqpp="./pp/ppAMS"+code2str(n)+".txt"; arqppf="./ppF/ppFAMS"+code2str(n)+".txt";

if falha==1; mprintf(' COM FALHA'); destinos=N; pp=read(arqppf,N,N);

  else mprintf(' SEM FALHA'); destinos=1; pp=read(arqpp,N,N); end;

//NÚMERO MÉDIO DE SALTOS

P=zeros(N,N,contmax); Ppl = 1/(N-1); Pop = 0.5;

contmax=contmax-1; //para excluir um dos casos (caso de carga zero)

for co=1:contmax; esoma(co)=0; //co=caso de carga

    c=(co)*intervalo;         //começa com carga = intervalo

//     c=(co-1)*intervalo;         //c é a carga. Para intervalo=25, c=0, 25%, 50%, 75% e
100%

    Poc=c/100;  Poc=Poc/2;    //Se linha de retardo = comprimento do link

    Ps = 1-Poc+Poc*Ppl+(Poc*Pop)*(1-Ppl); //PROBABILIDADE DE SUCESSO

//    if Ps==1&falha==1; Ps=0.95; end;

    Pd = 1-Ps;                          //PROBABILIDADE DE DEFLEXÃO

    for t=1:destinos; Ehops(co,t)=0;// t é o destino final utilizado em cada caso

        for j=1:N;                // j é a dimensão do nó de origem

            [w]=find(mc(:,j));s=size(w);//mc é a matriz de comutação definida na linha 14

              if s(2)==2;
```

```
            if mc(w(1),j)==pp(t,j);
              P(w(1),j,co)=Ps; P(w(2),j,co)=Pd;end;
            if mc(w(2),j)==pp(t,j);
              P(w(1),j,co)=Pd; P(w(2),j,co)=Ps;end;
            if pp(t,j)==3;
             P(w(1),j,co)=0.5; P(w(2),j,co)=0.5;end;end;
          if s(2)==1; P(w(1),j,co)=1; end;
        end;
        TT=zeros(N,N); TT(:,:)=P(:,:,co); TT(:,t)=0;
        Pk0 = (1/(N-1))*ones(N,1); Pk0(t)=0;
        kint=1; Pk=Pk0;
        while sum(Pk)>deltaPk; Pk = TT*Pk; mat(kint,co,t)=Pk(t); kint=kint+1;end;
        kmax=kint-1;
        for k = 1:kmax; Ehops(co,t) = Ehops(co,t)+k*mat(k,co,t);end;
        esoma(co)=esoma(co)+Ehops(co,t);
    end;
    esaltos(co)=esoma(co)/destinos;
end; //casos de carga
mprintf(' TEMPO TOTAL'); timer()
//ARQUIVO DE SAÍDA
if falha==0; result="./result/AMS"+code2str(n)+"v"+code2str(v)+".txt";
```

```
  else result="./resultF/AMS"+code2str(n)+"v"+code2str(v)+".txt";end;

for i=1:contmax;

//  saida(i,1)=(i-1)*intervalo; //inclui zero

  saida(i,1)=(i)*intervalo;     //exclui zero

  saida(i,2)=esaltos(i); end

u=file('open',result); write(u,saida,'(2(g))'); file('close',u);
```

Terceiro código (cálculo do Modelo 2 para *Ppl*) - (*Ppl=1/H*)

```
clear; stacksize(50000000);

//Baseado no arquivo: AMS-v5.sci - Adaptive Manhattan Street

//Autor: Antonio de Campos Sachs - junho de 2010

//COM FALHA: N=64 => 17 segundos; N=144 => 120 s conforme AMS-v4.sci; N=256 => 147s NESTA VERSÃO

//SEM FALHA: N=196 => 0.8580055 SEGUNDOS; N=256 => 1.1544074 SEGUNDOS

// anel com falha: 35 36 06 e 05; sinalizar também respectivamente:34   30   01   e 11

//              N-1  N  n  n-1                          N-2  N-n    1   2n-1

// estas falhas foram consideradas na geração do arqivo ppF
```

```
// neste programa basta ulizar o arquivo ppF já gerado

// para gerar mapa faca mapa=1 e falha=1

// 29 de novembro: considerado tanto-faz 232 segundos para cálculo do mapa de 256 nós

mprintf(' Nova simulação'); timer();

mprintf(' - número de nós de rede');

intervalo=25;  falha=0;  v=4; mapa=0; n=2;  N = n**2;   deltaPk=1.0D-8;

contmax=int(100/intervalo)+1; maximo=(contmax-1)*intervalo;

arq="./topo/AMS"+code2str(n)+".txt";  mc=read(arq,N,N);

arqpp="./pp/ppAMS"+code2str(n)+".txt"; arqppf="./ppF/ppFAMS"+code2str(n)+".txt";

if falha==1; mprintf(' COM FALHA'); destinos=N; pp=read(arqppf,N,N);

  else mprintf(' SEM FALHA'); destinos=1; pp=read(arqpp,N,N); end;

//NÚMERO MÉDIO DE SALTOS

P=zeros(N,N,contmax); Ppl = 1/(N-1); Pop = 0.5;

contmax=contmax-1; //para excluir um dos casos (caso de carga zero)

for co=1:contmax; esoma(co)=0; //co=caso de carga

    c=(co)*intervalo;         //começa com carga = intervalo

//     c=(co-1)*intervalo;         //c é a carga. Para intervalo=25, c=0, 25%, 50%, 75% e 100%

    Poc=c/100;  Poc=Poc/2;    //Se linha de retardo = comprimento do link

    for aval=1:2; if aval==2; esoma(co)=0; Ppl=1/H;end;

        Ps = 1-Poc+Poc*Ppl+(Poc*Pop)*(1-Ppl); //PROBABILIDADE DE SUCESSO
```

```
//    if Ps==1&falha==1; Ps=0.95; end;
    Pd = 1-Ps;                          //PROBABILIDADE DE DEFLEXÃO
    for t=1:destinos; Ehops(co,t)=0;// t é o destino final utilizado em cada caso
        for j=1:N;                  // j é a dimensão do nó de origem
            [w]=find(mc(:,j));s=size(w);//mc é a matriz de comutação definida na linha 14
              if s(2)==2;
                if mc(w(1),j)==pp(t,j);
                  P(w(1),j,co)=Ps; P(w(2),j,co)=Pd;end;
                if mc(w(2),j)==pp(t,j);
                  P(w(1),j,co)=Pd; P(w(2),j,co)=Ps;end;
                if pp(t,j)==3;
                 P(w(1),j,co)=0.5; P(w(2),j,co)=0.5;end;end;
              if s(2)==1; P(w(1),j,co)=1; end;
        end;
        TT=zeros(N,N); TT(:,:)=P(:,:,co); TT(:,t)=0;
        Pk0 = (1/(N-1))*ones(N,1); Pk0(t)=0;
        kint=1; Pk=Pk0;
        while sum(Pk)>deltaPk; Pk = TT*Pk; mat(kint,co,t)=Pk(t); kint=kint+1;end;
        kmax=kint-1;
        for k = 1:kmax; Ehops(co,t) = Ehops(co,t)+k*mat(k,co,t);end;
        esoma(co)=esoma(co)+Ehops(co,t);
```

```
    end;
    esaltos(co)=esoma(co)/destinos;H=esaltos(co);
    end; //avaliacoes 1 e 2
end; //casos de carga
mprintf(' TEMPO TOTAL'); timer()
//ARQUIVO DE SAÍDA
if mapa<>1;
  if falha==0; result="./result/AMS"+code2str(n)+"v"+code2str(v)+".txt";
  else result="./resultF/AMS"+code2str(n)+"v"+code2str(v)+".txt";end;
    for i=1:contmax;
    //  saida(i,1)=(i-1)*intervalo; //inclui zero
    saida(i,1)=(i)*intervalo;     //exclui zero
    saida(i,2)=esaltos(i); end;
  u=file('open',result); write(u,saida,'(2(g))'); file('close',u);
else result="./mapa/mapa"+code2str(n)+"v"+code2str(v)+".txt";
  for i=1:n;
    for j=1:n;
    saida(i,j)=Ehops(contmax,(i-1)*n+j); end; end;
  u=file('open',result); write(u,saida,'(16(g))'); file('close',u);
end;
```