UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ALGORITMO DE RWA COM CONSIDERAÇÕES DE SOBREVIVÊNCIA BASEADO EM HEURÍSTICA-ALGORITMO GENÉTICO PARA REDES IP/WDM

EDUARDO TOMMY LÓPEZ PASTOR

ORIENTADOR: Dr. HUMBERTO ABDALLA JUNIOR

Departamento de Engenharia Elétrica – Universidade de Brasília

CO-ORIENTADOR: Dr. JOSEP PRAT GOMÀ

Departament de Teoria del Senyal i Comunicacions – Universitat Politècnica de Catalunya – Espanha

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.TD - 016 A/07

BRASÍLIA/DF: Março-2007

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ALGORITMO DE RWA COM CONSIDERAÇÕES DE SOBREVIVÊNCIA BASEADO EM HEURÍSTICA-ALGORITMO GENÉTICO PARA REDES IP/WDM

EDUARDO TOMMY LÓPEZ PASTOR

TESE SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR.

APROVADA POR:

Prof. PhD Humberto Abdalla Júnior (Limoges- FR)
(Orientador)

Prof. Dr. William Ferreira Giozza (UNIFACS-BA-BR)
(Examinador Externo)

Dr. Honorio Assis Filho Crispim (UnB-BR)
(Examinador Externo)

Prof. Dr. Antonio José Martins Soares (UNICAMP-SP-BR)
(Examinador Interno)

Prof. Dr. Luis Fernando Ramos Molinaro (USP-BR)
(Examinador Interno)

Prof. Dr. Paulo Henrique Portela de Carvalho (Limoges-FR)
(Examinador Interno)

BRASÍLIA-DF, 9 DE MARÇO DE 2007

FICHA CATALOGRÁFICA

LÓPEZ-PASTOR, EDUARDO TOMMY
Algoritmo de RWA com considerações de Sobrevivência baseado em Heurística-Algoritmo Genético para Redes IP/WDM - [Distrito Federal] 2007.
xix, 217p., 210x297 mm (ENE/FT/UnB, Doutor, Engenharia Elétrica, 2007).
Tese de Doutorado – Universidade de Brasília. Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.
1.RWA 2.Sobrevivência (S-DRWA)
3.Redes IP/WDM 4.Algoritmos Genéticos (GA)
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

LÓPEZ-PASTOR, E.T. (2007). "Algoritmo de RWA com considerações de Sobrevivência baseado em Heurística-Algoritmo Genético para Redes IP/WDM". Tese de Doutorado em Engenharia Elétrica, Publicação PPGENE.TD - 016 A/07, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília: DF, 236p.

CESSÃO DE DIREITOS

AUTOR: Eduardo Tommy López Pastor
TÍTULO: Algoritmo de RWA com considerações de Sobrevivência baseado em Heurística-Algoritmo Genético para Redes IP/WDM
GRAU: Doutor ANO: 2007

Eduardo Tommy López Pastor
Carrer de L'Alcalde Comas 19-2-2, Barberà del Vallès
08210 Barcelona - Espanha

"Respondeu-lhe Jesus: Eu sou o CAMINHO, e a verdade, e a vida; ninguém vem ao Pai senão por mim"
(Jo 14:6)

Dedico esta Tese:

A Jesús, meu SENHOR e Salvador

À minha esposa Rocio e aos meus filhos

Otto Eduardo, Deborah Fabiola e Paulo Eduardo

À minha mãe Mercedes

AGRADECIMENTOS

A realização deste trabalho de Tese só foi possível gracias à ajuda invalorável de pessoas e instituições. Assim, agradeço de tudo coração:

- Em primeiro lugar a DEUS criador de todas as coisas, por sua misericórdia e amor, e ao seu filho, Jesús, o Espírito que dá sentido e direção a minha vida.
- À minha amada esposa Rocio e aos meus amados filhos Otto Eduardo, Deborah Fabiola e Paulo Eduardo, pelo amor, motivação, compreensão e paciência em todo este processo de doutoramento.
- Ao meu orientador Dr. Humberto Abdalla Júnior, pela sua orientação, por acreditar em mim e por ter-me dado toda condição para fazer este curso.
- Ao Dr. Josep Prat Gomà pela implicação neste trabalho, suas sugestões e aportes, e pela ajuda e suporte na minha estada na Universitat Politecnica de Catalunya – Espanha.
- A minha querida mãe Mercedes e a meu pai Juan, meus queridos irmãos Jaime, Carlos, Mario, Mary e Jorge, minha avô Juana, meu Tio César, meu sogro Ramiro e demais familiares, pelo afeto e apoio sem reservas.
- Ao amigo e irmão, Dr. TC. Honório Crispim, pela sua provada amizade, pelo apoio ilimitado e sem reservas, pelas suas relevantes contribuições a esta Tese e nos trabalhos que publicamos em equipe, e a Ariene por sua amizade, seu apoio e suporte.
- Ao Georges Amvame, amigo e irmão, assim como a Flavio Lima, Vladimir, Marçal e Ivan, caros colegas.
- Aos meus amigos e companheiros do Labcom da UnB, e do GCO (Grupo de Comunicações Ópticas) da UPC, pelo apoio moral e a convivência saudável.
- A todos os Irmãos da "Igreja em Brasília" e a "Església a Barcelona" pelo suporte espiritual e suas constantes orações em meu favor e da minha família.
- Aos Professores do Programa da pós-graduação em Engenharia Elétrica da UnB pela sua contribuição a minha formação, tanto cientifica como humana. Meu reconhecimento especial aos professores Martins, Leo, Paulo, Molinaro, Lúcio, Adson, Camargo e Franklin.
- Aos funcionários e pessoal administrativo e de serviço desta casa de estudos. Meu agradecimento especial à Cássia e ao Fernando.
- Ao CNPq pela ajuda neste curso através da bolsa de doutorado. O presente trabalho foi realizado com apoio do CNPq, Conselho Nacional de Desenvolvimento Científico e Tecnológico - Brasil
- A Sandro Rossi e demais funcionários do CPqD, assim como ao Prof. Josep Solé i Pareta da UPC e William Giozza da UNIFACS, pelas valiosas contribuições.

Muito Obrigado!!!!

RESUMO

ALGORITMO DE RWA COM CONSIDERAÇÕES DE SOBREVIVÊNCIA BASEADO EM HEURÍSTICA-ALGORITMO GENÉTICO PARA REDES IP/WDM

Esta Tese descreve a criação, o desenvolvimento e a aplicação de um novo algoritmo híbrido heurístico-GA (HGA) para a otimização dos mecanismos de Alocação de Rota e Comprimento de onda (RWA) dinâmico visando sobrevivência (S-DRWA), orientado à reserva de capacidade baseado em compartilhamento de rotas de proteção e aplicado em redes de transporte IP sobre WDM. Nesta operação conjunta, heurísticas fazem a seleção dos melhores caminhos de trabalho com seus respectivos caminhos backup e o Algoritmo Genético faz o aprovisionamento para o "melhor" par de rotas trabalho/proteção com a alocação do comprimento de onda adequado, estabelecendo assim o caminho requerido.

ABSTRACT

RWA ALGORITHM WITH SURVIVABILITY CONSIDERATIONS IN HEURISTICS- GENETIC ALGORITHM BASED TO IP/WDM NETWORKS

This thesis describes the creation, development and application of a novel hybrid Heuristic-GA algorithm, for the optimization of dynamic routing and wavelength assignment mechanisms with survivability (S-DRWA), guided to the reserve of capacity based on sharing routes protection and applied in IP transport network over WDM. In this joint operation, heuristics make the election of the best routes with their respective backup routes and the Genetic Algorithm makes the "best" provision for pair of routes working/protection with the allocation of the adjusted wavelength, thus establishing the required route.

RESUMEN

ALGORITMO DE RWA CON CONSIDERACIONES DE SOBREVIVENCIA BASADO EN HEURÍSTICA-ALGORITMO GENÉTICO PARA REDES IP/WDM

Esta Tesis describe la creación, desenvolvimiento y aplicación de un nuevo algoritmo híbrido heurístico-GA (HGA) para la optimización de los mecanismos de asignación de ruta y longitud de onda (RWA) dinámico orientado a sobrevivencia (S-DRWA), objetivando la reserva de capacidad basado en el uso compartido de rutas de protección y aplicado en redes de transporte IP sobre WDM. En esta operación conjunta, las heurísticas hacen la selección de los mejores caminos de trabajo con sus respectivos caminos backup y el algoritmo genético se encarga del aprovisionamiento para el "mejor" par de rutas trabajo/protección con la asignación de la longitud de onda adecuada, estableciendo de esta manera el camino requerido.

SUMÁRIO

Capítulo 1 1

1 INTRODUÇÃO 1

1.1 CONSIDERAÇÕES GERAIS 1
1.2 PROPOSTA DA TESE 2
1.3 JUSTIFICATIVA 2
1.4 CONSIDERAÇÕES FEITAS NO PROJETO 4
1.5 CENÁRIO DE DESENVOLVIMENTO DESTE TRABALHO 4
1.6 ORGANIZAÇÃO DESTE TRABALHO 4

Capítulo 2 6

2 ARQUITETURA DE REDES DE TRANSPORTE ÓPTICAS 6

2.1 INTRODUÇÃO 6
2.2 SISTEMA DE COMUNICAÇÕES ÓPTICAS 9
2.2.1 Elementos de um Enlace 9
2.3 EVOLUÇÃO DAS REDES DE TRANSPORTE 14
2.3.1 Redes de Comutação por Circuitos 15
2.3.2 Redes de Comutação a Pacotes 17
2.3.3 Evolução da Demanda de Tráfego 18
2.4 ARQUITETURA DE REDE MULTICAMADA 19
2.4.1 IP sobre ATM sobre SDH 23
2.4.2 IP sobre ATM diretamente sobre fibra 26
2.4.3 IP sobre SDH ou PoS (*Packet over SONET*) 28
2.4.4 GFP (Generic Frame Procedure) 32
2.4.5 IP sobre Gigabit Ethernet 33
2.5 IP SOBRE OTN BASEADO EM WDM 36
2.5.1 Tecnologia WDM (*Wavelength Division Multiplexing*) 37
2.5.2 Evolução da Tecnologia de Transporte sobre WDM 39
2.5.3 Evolução dos mecanismos de Encaminhamento sobre WDM 42
2.5.4 Arquitetura da rede IP sobre WDM 43
2.5.5 Plano de Controle IP/WDM 44
2.5.6 Modelos de Implantação de Rede Óptica 47
2.5.7 Serviços de Transporte Ópticos 48
2.6 REDES ÓPTICAS COMUTADAS AUTOMATICAMENTE (ASON) 49
2.6.1 Arquitectura lógica ASON 50
2.6.2 Plano de Controle ASON 51
2.6.3 Multiprotocol Lambda Switching (MPλS) 51
2.6.4 Generalized Multiprotocol Label Switching (GMPLS) 52
2.7 COMENTÁRIOS E CONCLUSÕES 57

Capítulo 3 59

3 ALOCAÇÃO DE ROTA E COMPRIMENTO DE ONDA (RWA) .. 59

3.1 INTRODUÇÃO 59
3.1.1 Redes roteadas por comprimento de onda 60
3.2 FUNDAMENTOS SOBRE ALGORITMOS DE RWA 61
3.2.1 O Algoritmo de *Dijkstra* 63
3.3 CLASSIFICAÇÃO DOS ALGORITMOS DE RWA 66

3.4 ALGORITMOS DE SELEÇÃO DE ROTA 68
3.4.1 Roteamento Fixo (FR) 69
3.4.2 Roteamento Alternativo (AR) 69
3.4.3 Roteamento à Exaustão (ER) 69
3.4.4 Roteamento Adaptativo (*adaptive routing*) 69
3.5 ALGORITMOS DE ALOCAÇÃO DE COMPRIMENTO DE ONDA 69
3.5.1 Mais Utilizado (MU) 70
3.5.2 Menos Utilizado (LU) 71
3.5.3 Ordem Fixa (FX) 71
3.5.4 Ordem Aleatória (RN) 71
3.6 ALGORITMOS DE RWA 72
3.6.1 Roteamento Fixo (*Fixed Routing* – FR) 72
3.6.2 Roteamento Fixo Alternativo (*Fixed Alternate Routing* – FAR) 73
3.6.3 Roteamento à Exaustão (*Exhaust Routing* – ER) 74
3.6.4 Roteamento pelo Caminho Menos Congestionado (LCR) 75
3.6.5 Seleção Conjunta de Rota e Comprimento de Onda (JWR) 75
3.7 CONSIDERAÇÕES NO PROJETO DE RWA 76
3.7.1 Considerações acerca do Custo das Rotas 76
3.7.2 Justiça / Eqüidade no atendimento de requisições 77
3.7.3 Controle Centralizado e Controle Distribuído 79
3.8 OUTRAS PROPOSTAS PARA RWA 80
3.9 ALGORITMOS DE RWA ESTÁTICOS E DINÂMICOS 81
3.10 RWA COM CONVERSÃO DE COMPRIMENTO DE ONDA 84
3.11 COMENTÁRIOS E CONSIDERAÇÕES FINAIS 86
Capítulo 4 87
4 SOBREVIVÊNCIA 87
4.1 INTRODUÇÃO 87
4.1.1 Ameaças ao Sistema da Rede 89
4.1.2 Controle do Mecanismo de Sobrevivência: Centralizado ou Distribuído 90
4.1.3 Demanda de Tráfego Estática ou Dinâmica 90
4.2 CRITÉRIOS DE SELEÇÃO DE ESQUEMAS DE SOBREVIVÊNCIA 91
4.3 ETAPAS NA SOBREVIVÊNCIA DE UMA REDE 92
4.3.1 Mecanismos de Recuperação 92
4.4 EVOLUÇÃO DA SOBREVIVÊNCIA NA REDE DE TRANSPORTE 96
4.4.1 Sobrevivência baseada em APS (*Automatic Protection Switch*) 96
4.4.2 Sobrevivência em Topologias em Anel 99
4.4.3 Sobrevivência em Redes em Anel com MultiplexaçãoWDM 100
4.4.4 Sobrevivência em Redes Malha com multiplexação WDM 100
4.5 PROTEÇÃO COMPARTILHADA EM REDES EM MALHA WDM 101
4.6 RECUPERAÇÃO DE FALHA EM REDES MULTICAMADAS 104
4.7 SOBREVIVÊNCIA EM REDES GMPLS 104
4.7.1 Mecanismos de proteção GMPLS 106
4.7.2 Mecanismos de restauração em GMPLS 108
4.8 RWA SOBREVIVENTE (S-RWA) 111
4.8.1 Alocação de Reserva de Capacidade 113
4.9 USO DE HEURÍSTICAS BASEADAS EM ALGORITMO GENÉTICO 116
4.10 COMENTÁRIO FINAL 120
Capítulo 5 121

5 ALGORITMOS GENÉTICOS 121

5.1 INTRODUÇÃO 121
5.2 CONCEITOS BÁSICOS 121
5.2.1 Algoritmo 121
5.2.2 Heurística 121
5.2.3 Algoritmos Evolucionários 122
5.2.4 Processos Estocásticos 122
5.3 ALGORITMOS GENÉTICOS 122
5.3.1 Terminologia usada em GA 123
5.3.2 Componentes de um GA 124
5.4 IMPLEMENTAÇÃO DE UM ALGORITMO GENÉTICO 125
5.4.1 Codificação das Soluções Candidatas 126
5.4.2 Função Avaliação 126
5.4.3 Método de Seleção e Procedimento de Amostragem 128
5.4.4 Operadores Genéticos 129
5.4.5 Métodos de Substituição de População 130
5.4.6 Configuração dos Parâmetros 130
5.4.7 Pseudocódigo de um algoritmo genético simples 132
5.5 QUANDO NÃO UTILIZAR GA 132
5.6 JUSTIFICATIVA PARA A ESCOLHA DO GA NESTA TESE 133
5.7 CONSIDERAÇÕES FINAIS 135

Capítulo 6 136

6 PROPOSTA DE MECANISMO S-DRWA PARA REDES IP/WDM BASEADO EM HEURÍSTICA-GA 136

6.1 PROBLEMÁTICA 136
6.1.1 Otimização de Recursos: Problemática de RWA 136
6.1.2 Capacidade de recuperação: Problemática de Sobrevivência 137
6.2 PROPOSTA: ALGORITMO HÍBRIDO HEURÍSTICO-GA (HGA) 137
6.2.1 Premissas 138
6.2.2 Desenvolvimento proposto 138
6.2.3 Cenário de desenvolvimento do trabalho 140
6.3 IMPLEMENTAÇÃO DAS HEURÍSTICAS 141
6.3.1 Algoritmo de Dijkstra modificado - Caminhos Primários 141
6.3.2 Algoritmo de Árvores de busca - Rotas de Proteção ou Backup 142
6.4 IMPLEMENTAÇÃO DO ALGORITMO GENÉTICO 143
6.4.1 Codificação dos indivíduos candidatos 144
6.4.2 Pseudo-código do GA 146
6.4.3 Desenvolvimento passo-a-passo do Algoritmo Genético proposto 147
6.4.4 Tabela de Códigos e *Lightpaths* 152
6.5 ESTRUTURAS DE DADOS UTILIZADAS 155
6.6 ANÁLISE DA COMPLEXIDADE DE UM ALGORITMO 156
6.6.1 Complexidade do Tempo 156

Capítulo 7 157

7 IMPLEMENTAÇÃO E AVALIAÇÃO DA PROPOSTA 157

7.1 ASPECTOS COMPUTACIONAIS DA IMPLEMENTAÇÃO 157
7.1.1 Funcionalidades do Mecanismo 157

7.1.2 Diagrama de Classes ... 158
7.1.3 Análise dos Comandos na UNI ... 161
7.1.4 Arquivo de definição de topologia ... 161
7.1.5 Solicitações para a criação de caminhos ... 164
7.1.6 Lógica para tratamento de uma falha no enlace ... 167
7.2 AVALIAÇÃO DO DESEMPENHO DO ALGORITMO HGA PROPOSTO ... 167
7.2.1 Gerador de Demandas ... 167
7.2.2 Comando de criação de requisições aleatórias ... 168
7.2.3 Parâmetros de avaliação de desempenho ... 170
7.3 COMPLEXIDADE DO ALGORITMO HGA ... 171
7.3.1 Complexidade do Algoritmo Genético proposto ... 171
7.4 PROBABILIDADE MÈDIA DE BLOQUEIO ... 173
7.4.1 Probabilidade Média de Bloqueio ... 173
7.4.2 Probabilidade Média de Bloqueio como função de G e P ... 174
7.4.3 Probabilidade de Bloqueio: HGA vs. algoritmo do SIMOMEGA ... 175
7.4.4 Probabilidade de Bloqueio: HGA vs. PIBWA vs. HÍBRIDO-LE ... 176
7.5 TEMPO MÉDIO DE EXECUÇÃO ... 177
7.5.1 Tempo médio de execução como função de G e P ... 178
7.5.2 Probabilidade de Alocação de Indivíduos por Geração ... 179
7.5.3 Tempo médio de execução: HGA vs. SIMOMEGA ... 179
7.6 TAXA DE REDUNDÂNCIA DA REDE E CAPACIDADE DE COMPARTILHAMENTO ... 180
8 CONCLUSÕES ... 184
8.1 ANÁLISE DOS RESULTADOS ... 184
8.2 CONCLUSÕES DO TRABALHO ... 188
8.3 TRABALHOS FUTUROS ... 189
8.3.1 Reconfiguração da rede para contornar o problema de bloqueio ... 189
8.3.2 Avaliação do algoritmo HGA em outros planos de controle ... 189
8.3.3 Interface de Configuração do Algoritmo ... 189
ANEXOS ... 190
A. A REDE OMEGA ... 190
A.1. PLANO DE TRANSPORTE DA REDE OMEGA ... 190
A.2. PLANO DE CONTROLE DA REDE OMEGA ... 194
A.3. RWA NA REDE OMEGA ... 196
A.3.1. Procedimento para liberação de um caminho óptico ... 198
A.4. MECANISMO DE PROTEÇÃO DA REDE OMEGA ... 199
B. EMULAÇÃO DO PLANO DE CONTROLE DA REDE OMEGA 201
C. TESTBED SIMOMEGA ... 203
C.1. ELEMENTOS DE REDE FÍSICOS ... 203
C.2. ELEMENTOS LÓGICOS ... 203
C.3. ALGUNS TESTES NO SIMOMEGA ... 205
D. REDE NSFNet ... 206
REFERÊNCIAS BIBLIOGRÁFICAS ... 207

LISTA DE TABELAS

TABELA 2.1 – BANDAS ESPECTRAIS (ITU) 13
TABELA 2.2 - TAXAS DE TRANSMISSÃO PARA SONET/SDH 17
TABELA 2.3 – CONTRASTE ENTRE OS SISTEMAS DE COMUNICAÇÕES LEGADOS E OS ATUAIS 17
TABELA 2.4 - DISTRIBUIÇÃO DOS TAMANHOS DE PACOTES PREDOMINANTES NO *BACKBONE* INTERNET. 25
TABELA 2.5 – CALCULO DO *OVERHEAD* PARA IP/ATM/SDH 26
TABELA 2.6 – CÁLCULO DO *OVERHEAD* PARA IP/ATM DIRETAMENTE SOBRE FIBRA 27
TABELA 2.7 - CÁLCULO DE *OVERHEAD* PARA IP/PPP/SDH 31
TABELA 2.8 - PORCENTAGEM DE *OVERHEAD* - DIFERENTES MÉTODOS DE ENCAPSULAMENTO A 2,4 GBPS 31
TABELA 2.9 – COMPARAÇÃO DAS CARACTERÍSTICAS DO GFP-T E GFP-F 33
TABELA 2.10 - *OVERHEAD* INSERIDO PELA PROPOSTA IP/GBETH 35
TABELA 3.1 - ALGORITMO DE *DIJKSTRA* 63
TABELA 4.1 – TAXAS DE FALHAS E TEMPOS DE REPARAÇÃO. 89
TABELA 4.2 – TEMPO DE RECUPERAÇÃO DE VÁRIOS MECANISMOS DE SOBREVIVÊNCIA 104
TABELA 4.3 - ALGUNS ESQUEMAS DE SOBREVIVÊNCIA PARA GMPLS 109
TABELA 4.4 - REQUERIMENTOS DE TRÁFEGO, CAMINHOS DE TRABALHO E CAMINHOS DE PROTEÇÃO. 118
TABELA 5.1 – PARALELO ENTRE UM ALGORITMO PADRÃO E O GA 123
TABELA 5.2 - PSEUDOCÓDIGO DE UM ALGORITMO GENÉTICO SIMPLES 132
TABELA 6.1 - PSEUDO-CÓDIGO DO GA DESTA PROPOSTA 146
TABELA 6.2 - TABELA DE ALOCAÇÃO Λ-LINK 152
TABELA 6.3 - INFORMAÇÃO DE ALOCAÇÃO DE *LIGHTPATHS* PARA AS REQUISIÇÕES DADAS 153
TABELA 6.4 – ESTADO DA TABELA DE ALOCAÇÃO Λ-LINK PARA O EXEMPLO PROPOSTO 153
TABELA 6.5 – AVALIAÇÃO DOS CANDIDATOS A CAMINHO ÓPTICO 154
TABELA 7.1 – MECANISMOS A SEREM COMPARADOS COM A PROPOSTA HGA 171
TABELA 7.2 – COMPARATIVA DA COMPLEXIDADE DO HGA COM PIBWA E HIBRIDO-LE 173
TABELA 7.3 – PROBABILIDADE DE BLOQUEIO MÉDIA PARA O ALGORITMO HGA 173
TABELA 7.4 – PROBABILIDADE DE BLOQUEIO COMO FUNÇÃO DE G E P 174
TABELA 7.5 – PROBABILIDADE DE BLOQUEIO DOS ALGORITMOS PIBWA, HIBRIDO-LE E HGA 176
TABELA 7.6 – TEMPO MÉDIO DE EXECUÇÃO EM FUNÇÃO DE G E P 178
TABELA 7.7 – ALOCAÇÃO DE ENLACES E COMPRIMENTOS DE ONDA PELO ALGORITMO HGA PARA 30 SOLICITUDES DE *LIGHTPATH* 182
TABELA 7.8 – *LAMBDAS* USADOS PELOS ENLACES PARA OS CAMINHOS DE TRABALHO E PROTEÇÃO 182
TABELA A.1 - CARACTERÍSTICAS TÍPICAS DA CHAVE TERMO-ÓPTICA 8 X 8 FABRICADA PELA NEL 192
TABELA A.2 - CARACTERÍSTICAS TÍPICAS DOS DISPOSITIVOS DO NÓ ÓPTICO 193
TABELA A.3 - GRADE ITU-T UTILIZADA PELA REDE OMEGA 194
TABELA **C.1** - RESULTADOS ENTREGADOS PELO SIMOMEGA PARA 30 REQUISIÇÕES 205

LISTA DE FIGURAS

FIGURA 2.1 - CENÁRIO DAS REDES DE TELECOMUNICAÇÕES E COMUNICAÇÃO DE DADOS 7
FIGURA 2.2 - ENLACE BÁSICO DE COMUNICAÇÕES ÓPTICAS. 9
FIGURA **2.3**- ESPECTRO DE SAÍDA DE DIFERENTES TIPOS DE EMISSORES. 10
FIGURA **2.4**- ATENUAÇÃO E DISPERSÃO EM FUNÇÃO DO COMPRIMENTO DE ONDA 10
FIGURA 2.5 -DISPERSÕES INTRAMODAIS 12
FIGURA **2.6** - CURVA DE ATENUAÇÃO EM FUNÇÃO DO COMPRIMENTO DE ONDA E JANELAS DE TRANSMISSÃO (MODIFICADO – [ESQUIVIAS, 2006]) 13
FIGURA **2.7** - JANELAS DE TRANSMISSÃO ÓPTICAS NO ESPECTRO ELETROMAGNÉTICO. 14
FIGURA 2.8 - EVOLUÇÃO DA DEMANDA DE TRÁFEGO 19
FIGURA **2.9** - ARQUITETURA DE REDE MULTICAMADA 20
FIGURA **2.10** - SUB-CAMADAS DA CAMADA OTN 22
FIGURA **2.11**- SUB-CAMADAS DA OTN EM UM ENLACE DE UMA REDE ÓPTICA. 22
FIGURA **2.12** - CÉLULA ATM 23
FIGURA **2.13** - EXEMPLO DE UMA REDE IP/ATM USANDO ENCAPSULAMENTO LLC. 24
FIGURA **2.14** - DISTRIBUIÇÃO DO TAMANHO DE PACOTES NUM ENLACE DOMÉSTICO (MODIFICADO, [THOMPSON, 1997]) 26
FIGURA **2.15** – PROCESSO DE TRANSMISSÃO DE UM QUADRO SDH. 29
FIGURA **2.16** - EXEMPLO DE UMA REDE IP/SDH USANDO ENCAPSULAMENTO PPP-HDLC. 30
FIGURA **2.17** - CONFIGURAÇÕES DE REDES IP SOBRE SDH. 30
FIGURA **2.18** - CONFIGURAÇÃO TÍPICA DE UMA REDE IP/GBETH/WDM 34
FIGURA **2.19** – EVOLUÇÃO DA ARQUITETURA DE TRANSPORTE ÓPTICA 36
FIGURA **2.20** - SISTEMA ÓPTICO COM TECNOLOGIA WDM TÍPICO 38
FIGURA **2.21** - PRIMEIRA GERAÇÃO DAS REDES DE TRANSPORTE FOTÔNICAS. 40
FIGURA **2.22** - SEGUNDA GERAÇÃO DAS REDES DE TRANSPORTE FOTÔNICAS. 41
FIGURA **2.23** - EVOLUÇÃO DOS MECANISMOS DE ENCAMINHAMENTO (MODIFICADO [SATO, 2002]). 43
FIGURA **2.24** – ARQUITETURA IP SOBRE OTN 44
FIGURA **2.25** - PLANO DE CONTROLE CENTRALIZADO. 45
FIGURA **2.26** - PLANO DE CONTROLE DISTRIBUÍDO. 45
FIGURA **2.27** - INTERFACES NA ARQUITETURA IP/OTN-WDM 46
FIGURA **2.28** - ARQUITETURA DO MODELO *OVERLAY* 47
FIGURA **2.29** - ARQUITETURA DO MODELO *PEER*. 48
FIGURA **2.30** - ARQUITETURA ASON 50
FIGURA **2.31** - PLANO DE CONTROLE E PLANO DE TRANSPORTE DE DADOS. 53
FIGURA **2.32** - DOMÍNIOS DAS INTERFACES EM GMPLS (MODIFICADO [BANERJEE1, 2001]). 54
FIGURA **2.33** - HIERARQUIA DE LSPS 55
FIGURA **2.34** – ARQUITETURA DA REDE CARISMA [CARISMA, 2006] 56
FIGURA 3.1 - MODELO DE CAMADAS DA REDE DE TRANSPORTE 59
FIGURA 3.2 - ARQUITETURA DE REDES ROTEADAS POR COMPRIMENTO DE ONDA 60
FIGURA 3.3 - FUNCIONAMENTO DO ALGORITMO DE *DIJKSTRA* 65

FIGURA 3.4. CLASSIFICAÇÃO FUNCIONAL DE ALGORITMOS DE RWA (MODIFICADO [CHOI, 2000]) 83
FIGURA 4.1 - ESQUEMAS DE RECUPERAÇÃO: CAMINHO, SUB-CAMINHO E ENLACE. 95
FIGURA 4.2 - ESQUEMAS DE PROTEÇÃO E RESTAURAÇÃO PARA REDES EM MALHA WDM 95
FIGURA 4.3 - PROTEÇÃO 1+1 APS 98
FIGURA 4.4 - PROTEÇÃO 1:N APS 99
FIGURA 4.5 - COMPARTILHAMENTO BACKUP NÍVEL 1. 102
FIGURA 4.6 - COMPARTILHAMENTO BACKUP NÍVEL 2. 102
FIGURA 4.7 - COMPARTILHAMENTO BACKUP NÍVEL 3 103
FIGURA 4.8 - PROTEÇÃO DE ENLACE 107
FIGURA 4.9 - PROTEÇÃO DE CAMINHO 108
FIGURA 4.10 – COMPOSIÇÃO DO TEMPO DE INTERRUPÇÃO DE SERVIÇO. 110
FIGURA 4.11 - PROTEÇÃO COMPARTILHADA PARA DIVERSAS ROTAS DE TRABALHO. 117
FIGURA 5.1 - ETAPAS DE UM ALGORITMO GENÉTICO 131
FIGURA 6.1 - ALGORITMO DE ÁRVORES DE BUSCA 142
FIGURA 6.2 – DIAGRAMA DE BLOCOS DO ALGORITMO PROPOSTO 144
FIGURA 6.3 – BUSCA DO CAMINHO ÓPTICO PARA A REQUISIÇÃO 2 -5 145
FIGURA 6.4 – CÓDIGO-INDIVÍDUO: REPRESENTAÇÃO IMPLÍCITA DO PAR ROTA PRIMÁRIA-*BACKUP* 145
FIGURA 6.5 – OPERAÇÃO GENÉTICA DE CRUZAMENTO. 150
FIGURA 6.6 – OPERAÇÃO GENÉTICA DE MUTAÇÃO. 151
FIGURA 7.1 – DIAGRAMA DE CLASSES. 159
FIGURA 7.2 - ARQUIVO DE TOPOLOGIA DA REDE OMEGA 162
FIGURA 7.3 - ARQUIVO DE TOPOLOGIA PARA A REDE NSFNET 163
FIGURA 7.4 – CONFIGURAÇÃO DA TOPOLOGIA DA REDE NSFNET PARA OS TESTES 164
FIGURA 7.5 – INÍCIO DE UMA SESSÃO *TELNET* DESDE A *CONSOLE* DO *KDEVELOP* 164
FIGURA 7.6 – USO DO COMANDO ACTION CREATE E ALOCAÇÃO DO CAMINHO SOLICITADO 166
FIGURA 7.7 – USO DO COMANDO ACTION PATH E ALOCAÇÃO DO CAMINHO SOLICITADO 167
FIGURA 7.8 – USO DO COMANDO ACTION RAMDOM E ALOCAÇÃO ALEATÓRIA DE CAMINHOS. 169
FIGURA 7.9 – RESULTADOS MOSTRADOS PELO COMANDO DEBUG REQUEST 170
FIGURA 7.10 – RESULTADOS MOSTRADOS PELO COMANDO DEBUG NODE 170
FIGURA 7.11 – PROBABILIDADE DE BLOQUEIO OBTIDA COM O MECANISMO HGA. 174
FIGURA 7.12 – PROBABILIDADE DE BLOQUEIO COMO FUNÇÃO DE G E P 175
FIGURA 7.13 – COMPARAÇÃO DAS PROBABILIDADES DE BLOQUEIO HGA – SIMOMEGA 175
FIGURA 7.14 –PROBABILIDADES DE BLOQUEIO: PIBWA, HIBRÍDO-LE E HGA 177
FIGURA 7.15 – TEMPO DE CRIAÇÃO DE CADA UM DOS CAMINHOS COM PROTEÇÃO 177
FIGURA 7.16 – TEMPO MÉDIO DE EXECUÇÃO EM FUNÇÃO DE G E P 178
FIGURA 7.17 - PROBABILIDADE DE ALOCAÇÃO DE INDIVÍDUOS POR GERAÇÃO NO HGA 179
FIGURA 7.18 – COMPARAÇÃO DO TEMPO MÉDIO DE EXECUÇÃO HGA – SIMOMEGA 180
FIGURA **A.1** - TOPOLOGIA DA REDE OMEGA. 191
FIGURA **A.2** - ESTRUTURA FÍSICA DE UM NÓ DA REDE OMEGA 191
FIGURA **A.3** - ELEMENTOS DE UM NÓ ÓPTICO DA REDE OMEGA 192

FIGURA A.4 - *OPTICAL CROSS-CONNECT* (OXC) DA REDE OMEGA. 193
FIGURA A.5 - PORTAS ETHERNET DO SISTEMA DE CONTROLE. 195
FIGURA A.6.: MENSAGENS DE CONTROLE UTILIZADAS PARA ESTABELECER UM CAMINHO ÓPTICO 197
FIGURA A.7. MENSAGENS DE CONTROLE PARA ESTABELECER E DESTRUIR UM CAMINHO ÓPTICO. 199
FIGURA A.8 - DIAGRAMA DE ESTADO DO MECANISMO DE SOBREVIVÊNCIA DA REDE OMEGA. 200
FIGURA B.1 – ARQUITETURA FÍSICA DA REDE OMEGA 201
FIGURA B.2 – CONFIGURAÇÃO DO PLANO DE CONTROLE EMULADO NO LABORATÓRIO DA UNB 202
FIGURA C.1 - SIMULAÇÃO DOS ELEMENTOS FÍSICOS 203
FIGURA C.2 - ARQUITETURA DA REDE SIMOMEGA 204
FIGURA D.1 - INTERCONEXÕES E TOPOLOGIA DA REDE *NSFNET*. 206

LISTA DE SÍMBOLOS, NOMECLATURA E ABREVIAÇÕES.

AAL-5	*ATM adaptation layer type 5*
ANSI	*American National Standards Institute*
APD	*Diodo de avalancha*
APS	*Automatic Protection Switching - Comutação automática de proteção*
ARP	*Address Resolution Protocol*
ASON	*Automatic Switched Optical Network*
ASTN	*Automatic Switched Transport Nework*
ATM	*Asynchronous Transfer Mode (Modo de Transferência Assíncrono)*
BER	*Bit Error Rate*
BGP	*Border Gateway Protocol*
BLSR	*Bidirectional Line Switched Rings*
CCABA	*Centre de Comunicacions Avançades de Banda Ampla*
CCAMP	*Common Control and Management Plane*
CPqD	*Centro de Pesquisa e Desenvolvimento em Telecomunicações*
CRC	*Cyclic redundancy check*
CR-LDP	*Constraint-Based Routing Label Distribuition Protocol*
CSMA/CD	*Carrier Sense Multiple Access / Collision Detection (Acesso Múltiplo de Sentido da Portadora com Detecção de Colisão)*
CWDM	*Coarse WDM*
DWDM	*Dense Wavelenght Division Multiplexing (Multiplexação Densa Por Divisão do Comprimento de Onda)*
DXC	*Digital Cross Connect*
EDFA	*Amplificadores de Fibra Dopada a Érbio*
EP	*Programação Evolucionária*
ES	*Estratégias Evolutivas*
FCC	*Federal Communications Commission*
FDDI	*Fiber Distributed Data Interface*
FDL	*Fibra de retardo*
FDM:	*Frequency Division Multiplexing*
FSC	*Fiber-switch capable*
FTTH	*Fiber to the Home*
FWM	*Mistura de Quatro Ondas*
GA	*Genetic Algorithm*
GCO	*Grupo de Comunicaçoes Opticas*
GFP	*Generic Frame Procedure*
GMPLS	*Generalised Multiprotocol Label Switching (Protocolo Generalizado de Comutação por Rótulos)*
GP	*Programação Genética*
GPL	*General Public License*
HGA	*Heurística-Algoritmo Genético*
HDLC	*High Level Data Link Control*
IDE	*Entorno Integrado de Desenvolvimento*
IETF	*Intenernet Engineering Task Force (Força Tarefa para Engenharia da Internet)*
IGRP	*Interior Gateway Routing Protocol*
ILP	*programação linear inteira*
IP	*Internet Protocol (Protocolo de Internet)*
ISDN	*Rede Digital de Serviços Integrados*
ISI	*intersymbol interference*
IS-IS	*Intemediate System-Intermediate System*
ITU-T	*International Telecommunication Union – Telecommunication (União*

	Internacional de Telecomunicações - Telecomunicações)
LCAS	*Link Capacity Adjustment Scheme*
LED	*Diodo emisor de luz*
LLC	*Logical Link Control*
LMP	*Link Management Protocol*
LOF	*Loss-of-Framing*
LOL	*Loss-of-Light*
LSC	*Lambda switch capable*
LSP	*Label Switch Path*
LSR	*Label Switch Roteador*
LSP	*Label Switched Path (Caminho por Comutaçãode Rótulo)*
MAC	*Media Access Control*
MMF	*Multimode Fiber*
MMTR	*Mean Time To Repair*
MPLS	*Multiprotocol Label Switching (Multiprotocolo de Comutação por Rótulo)*
MPλS	*Multiprotocol Lambda Switching (Multiprotocolo de Chaveamento por Lambda)*
MTBF	*Mean Time Bettwen Failure*
NMI	*Network Management Interface*
NNI	*Netwok-Network Interface*
OADM	*Optical Add-Drop Multiplexer (Multiplexador Óptico de Inserção-Derivação)*
OC	*Optical Carrier- n*
OMS	*Seção de Multiplexação Óptica*
OMEGA	*Optical Metro network for Emerging Gigabit Applications*
OSI	*Open Systems Interconnection (Interconexão de Sistemas Abertos)*
OAM	*Operation Administration and Maitenance*
OBS	*Optical Burst Switching*
OCS	*Optical Circuit Switching*
OIF	*Optical Internetworking Forum*
OPS	*Optical Packet Switching*
OTDM	*Optical Time Division Multiplexing (Multiplexação por Divisão Óptica no Tempo)*
OTN	*Optical Transport Network*
OVPN	*Redes privadas virtuais ópticas*
OXC	*Optical Cross-Connect (Comutador Óptico)*
PDH	*Plesiochronous Digital Hierarchy*
PDU	*Unidade de Dados de Protocolo*
PNNI	*Private Network-to-Network Interface*
PoF	*Fibra de plástico*
PON	*Passive Optical Network*
PoS	*Packet over SDH/SONET*
PPP	*Point-to-point protocol*
PSC	*Packet switch capable*
QoS	*Quality of Service*
RIP	*Routing Information Protocol*
RPR	*(Resilient Packet Ring*
RWA	*Routing and Wavelength Assignment (Roteamento e Alocação de Comprimento de Onda)*
SDH	*Synchronous Digital Hierarchy (Hierarquia Digital Síncrona)*
SDL	*Simplified Data Link*
S-DRWA	*Survivability Dynamic Routing and Wavelength Assigment*
SHR	*Self-Healing Rings*
SLE	*Static Lightpath Establishment*
SMF	*Single-mode Fiber*
SNAP	*Sub-Network Access Point*

SNR	*Signal-to-noise ratio (Razão Sinal-Ruído)*
SONET	*Synchronous Optical Network (Rede Óptica Síncrona)*
SPE	*Ssynchronous payload envelope*
SPM	*Self Phase Modulation*
SRLG	*Shared Risk Link Group (Grupo de Enlaces de Risco Compartilhado)*
STL	*Standard Template Library*
STM	*Synchronous Transfer Mode*
STM-1	*Synchronous Transport Module 1*
STS-1	*Synchronous Transport Signal Level 1*
TDM	*Multiplexação por Divisão de Tempo*
UnB	*Universidade de Brasília*
UNI	*User-Network Interface*
UPSR	*Unidirectional Path Switched Ring*
VCAT	*Concatenação Virtual*
WDM	*Wavelength Division Multiplexing (Multiplexação por Divisão do Comprimento de Onda)*
XPM	*Cross Phase Modulation*

Capítulo 1

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES GERAIS

As telecomunicações são uma área importante para o mundo pelos serviços que provêm à sociedade. O surgimento da Internet e de novos serviços levaram a necessárias modificações na arquitetura das comunicações, tanto no aspecto físico como no lógico. As necessidades de banda para o transporte de informação têm aumentado em proporções gigantescas, sendo imperativas novas tecnologias para satisfazer tais demandas. Uma tecnologia que possui todo o potencial para prover a largura de banda necessária para os serviços de hoje é a rede de transporte óptica transparente WDM. Porém, o desenvolvimento desse tipo de rede apresenta uma série de desafios, tanto na fase de projeto como na otimização dos seus recursos.

Existem potencialmente muitas aproximações de solução para a problemática do projeto que incluem programação matemática, heurísticas específicas ao problema, algoritmos evolucionários (EAs) [GOLDBERG, 1989] [CORNE, 1999] [SINCLAIR, 1999] [DEB, 2001] [ZITZLER, 1999], *Tabu Search* (TS) [GLOVER, 1990] e *Simulated Annealing* (SA) [KIRKPATRICK, 1983].

Os problemas de projeto e otimização relacionados com alocação de rota e comprimento de onda (RWA: *routing and wavelength assignment*) e sobrevivência (*Survivability*), como os que serão abordados neste trabalho, freqüentemente requerem algoritmos de tipo não-polinomiais (NP). Instâncias de tais problemas são difíceis de abordar com os métodos exatos da programação matemática devido ao longo tempo de processamento e requerimentos de memória de computador [PROESTAKI, 1999]. Assim, pesquisadores têm optado por técnicas heurísticas específicas relacionadas ao problema em questão.

Por outro lado, algoritmos evolucionários tem chamado grande atenção por sua aplicação na solução de problemas complexos e de otimização em diferentes campos da ciência,

incluindo as Telecomunicações. Aplicações nesta última área incluem projeto de redes, roteamento de chamadas, RWA, gerência de rede etc. Os algoritmos evolucionários se subdividem em subáreas: algoritmos genéticos (GA), programação evolucionária (EP), estratégias evolutivas (ES), programação genética (GP) e classificação de sistemas (CS), entre outros [FOGEL, 1998] [MITCHELL, 1993] [SINCLAIR2, 1999].

Embora os algoritmos evolucionários tenham sucesso nos problemas de procura, de propósito geral e procedimentos de otimização, e sejam também uma boa aproximação para problemas específicos, em algumas aplicações resultam inviáveis pelo tempo de execução que demanda o processo computacional. Uma poderosa alternativa para problemas específicos é a modelagem híbrida baseada em Heurísticas e Algoritmos genéticos, que combina a melhor heurística para a solução do problema dentro da estrutura robusta que oferece o algoritmo genético.

1.2 PROPOSTA DA TESE

Esta Tese propõe a aplicação de um novo algoritmo híbrido heurístico/GA, chamado de HGA, para a otimização dos mecanismos de Alocação dinâmica de Rota e Comprimento de onda (DRWA) no cenário das redes de transporte IP sobre WDM. Em comparação com outros trabalhos relatados, este algoritmo híbrido é orientado à reserva de capacidade com base em compartilhamento de rotas de proteção, visando sobrevivência.

Nesta operação conjunta, dada uma requisição, um mecanismo heurístico procura as melhores rotas de trabalho e suas respectivas rotas de proteção. Esta informação forma o espaço de busca para o Algoritmo Genético, que faz a seleção da “melhor” rota de trabalho e a “melhor” rota de proteção compartilhada, bem como o aprovisionamento do comprimento de onda adequado, estabelecendo assim o caminho óptico solicitado.

1.3 JUSTIFICATIVA

É o principal interesse deste trabalho a otimização de recursos por compartilhamento da reserva de capacidade para o atendimento de requisições de tráfego e sobrevivência da rede, sendo este considerado, junto com a probabilidade de bloqueio e o tempo de

computação, como os parâmetros mais importantes para a avaliação do desempenho do mecanismo e da sua qualidade.

A motivação para abordar esta problemática surgiu com a necessidade de se dotar de um melhor mecanismo de RWA para o *testbed* da rede OMEGA (Rede óptica experimental do *CPqD: Optical MEshed network for Gigabit Applications - Campinas-Brasil*), e que foi emulado na UnB sob o nome de SIMOMEGA [CRISPIM, 2006], otimizando os seus recursos e visando sobrevivência. Embora partindo de uma necessidade "particular", o objetivo desta proposta de algoritmo é ser útil a outras arquiteturas de redes ópticas em geral. Assim, o nicho de trabalho escolhido é uma rede de transporte transparente (toda óptica) típica, usada em algumas implementações assim como em *testbeds*. Ela é baseada em tecnologia IP/WDM, com topologia malha arbitrária e roteamento de comprimento de onda. Cada nó óptico da rede caracteriza um roteador-comutador de comprimento de onda (canal óptico) sem conversão de comprimento de onda. Cada enlace inclui fibras unidirecionais, com pelo menos uma fibra em cada direção, e cada fibra tem capacidade de receber a multiplexação de até "n" comprimentos de onda.

A razão de se usar um Algoritmo híbrido Heurístico/Genético foi motivada pelas limitações na aplicação de um GA simples, nos aspectos de codificação e nos resultados inferiores, em comparação com modelos baseados em Heurística segundo trabalhos relatados [SINCLAIR3, 1993] [TAN, 1995].

Embora a aproximação híbrida Heurístico/Genético seja promissora, esta tem algumas limitações. Dado que esta é uma forma de procura estocástica guiada, não existe garantia de que um valor ótimo global possa ser alcançado. Em compensação, uma aproximada "boa solução" pode ser conseguida. Por outro lado, uma potencial população de soluções e uma codificação específica ao problema serão utilizadas, com os quais quantidades razoáveis de tempo de computação e memória poderiam ser necessárias em comparação com outras técnicas. Porém, isto pode ser aliviado com um bom projeto dos parâmetros do algoritmo, como foi feito neste trabalho.

O GA é um método genérico que precisa ser customizado para a problemática em particular que se deseja abordar. Assim, o projeto para o mecanismo de codificação dos indivíduos, o tamanho da população, o número de gerações (iterações), o critério de parada

(*stopping*) e os diferentes operadores foram adaptados às características do problema em questão para otimizar o tempo de computação.

1.4 CONSIDERAÇÕES FEITAS NO PROJETO

Será assumida a possibilidade de ocorrência de uma única falha durante um dado intervalo de tempo, considerando que a probabilidade de duas falhas acontecer simultaneamente é muito baixa [XIN, 2002]. Também considera-se que falhas de enlace é o cenário dominante em falhas de rede [ZHANG, 2004].

Assume-se que depois de uma falha no caminho de trabalho não é prioritária a mesma QoS no caminho de proteção (em termos de latência de propagação). Também ao acontecer uma falha na rede, um protocolo de sinalização será acionado para re-rotear o tráfego para o caminho backup.

1.5 CENÁRIO DE DESENVOLVIMENTO DESTE TRABALHO

O cenário de desenvolvimento deste trabalho é a rede SIMOMEGA da UnB emulado a partir da rede OMEGA do CPqD, porém com um plano de controle centralizado. Uma referência para comparação e avaliação desta proposta será o algoritmo de RWA deste protótipo, baseado em *Dijkstra* para seleção de rota e do algoritmo *First-Fit* para a alocação de comprimento de onda. Um mecanismo de proteção do tipo 1:N é usado nesta arquitetura. Também foram selecionadas algumas propostas algoritmicas baseadas em S-RWA, e publicadas internacionalmente, para comparação de desempenho e validação do nosso mecanismo. Para tal, a topologia da rede *NSFNet* também será usada para avaliação.

1.6 ORGANIZAÇÃO DESTE TRABALHO

Este trabalho é sub-dividido em 8 Capítulos. Este primeiro Capítulo apresenta a introdução, a qual considera a problemática a ser abordada, algumas considerações do projeto e a proposta de solução do problema.

O Capítulo 2 apresenta uma sólida base de conhecimentos em tecnologias e redes ópticas, partindo da sua evolução até atingir o momento atual de desenvolvimento, com destaque para as redes IP/WDM e as novas propostas para este paradigma.

O Capítulo 3 apresenta os algoritmos de alocação de rota e comprimento de onda (RWA), os princípios de funcionamento, classificação e tipos de algoritmos.

O Capítulo 4 faz uma abordagem sobre os mecanismos de proteção, sua evolução e os esquemas existentes, com destaque aos esquemas baseados em reserva de capacidade e heurísticos.

O Capítulo 5 oferece uma introdução aos algoritmos genéticos, às métricas usadas, aos operadores genéticos e suas aplicações.

O Capítulo 6 apresenta a proposta deste projeto, as características do algoritmo, seu desenvolvimento e aplicação.

O Capítulo 7 mostra os procedimentos de testes de desempenho, os resultados obtidos neste trabalho e a avaliação da proposta. Para a validação da proposta foram feitas simulações de desempenho e posterior implementação sobre o plano de controle do protótipo da Universidade de Brasília, nomeado de SIMOMEGA, e sobre as topologias da rede óptica OMEGA e da rede *NSFNet*.

O Capítulo 8 nos mostra a análise e as conclusões do trabalho, assim como as sugestões para projetos futuros.

A rede OMEGA é apresentada nos Anexos como um caso de implementação de rede óptica transparente. Outras implementações, tais como a rede protótipo SIMOMEGA e a topologia da rede *NSFnet*, cenários de desenvolvimento deste trabalho, são também apresentados.

Capítulo 2

"Lâmpada para os meus pés é a tua palavra,
e LUZ para os meus CAMINHOS".
SI 119:105

2 ARQUITETURA DE REDES DE TRANSPORTE ÓPTICAS

2.1 INTRODUÇÃO

As redes de transporte de telecomunicações e comunicação de dados estão mudando rapidamente com a introdução de novas tecnologias e a necessidade por novos serviços de valor agregado, alta disponibilidade e integração.

Assim, três motores têm conduzido constantemente a evolução da arquitetura das redes de telecomunicações: o crescimento do tráfego, o desenvolvimento de novos serviços e os avanços na tecnologia, sendo que estas forças não são independentes entre si [EL-SAYED, 2002]. Por exemplo, a competição entre fabricantes e os avanços da tecnologia resultam numa redução de custos, o qual estimula o crescimento do tráfego e leva a desenvolvimento de novos serviços.

No sentido mais geral, uma rede de transporte pode ser considerada como um conjunto de meios e equipamentos que transportam informação entre elementos de rede, os quais comutam ou roteiam a informação do cliente dentro da rede de transporte de maneira a levar os dados deste cliente ao destino apropriado, com a rede de transporte sendo responsável pela entrega confiável dos dados. A Figura 2.1 apresenta o cenário das redes de telecomunicações e comunicação de dados desde o ponto de vista geográfico.

Com o desenvolvimento da tecnologia fotônica e da fibra óptica como meio de transmissão de alta capacidade, os sistemas de comunicações começaram a dispor da fibra como meio de transporte em substituição das linhas baseadas em cobre, bem como de novos elementos de rede com capacidades de comutação a alta velocidade.

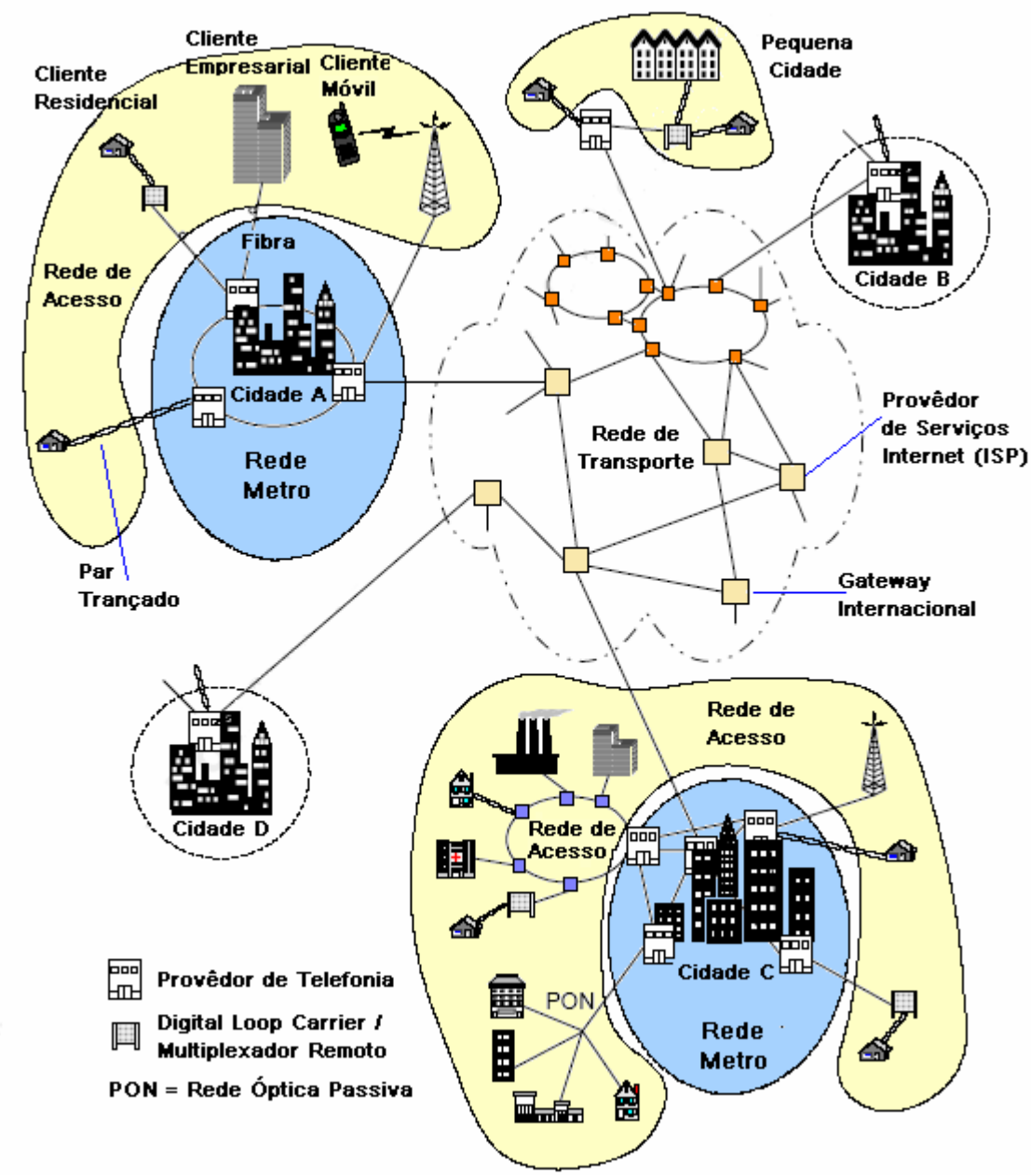


Figura 2.1 - Cenário das Redes de Telecomunicações e Comunicação de Dados

As redes baseadas em fibra começaram a ser implementadas no começo da década dos anos 80 sendo atualmente muito usadas em redes de telecomunicações. No final dessa década e início dos anos 90 começou-se a planejar arquiteturas de redes inovadoras, além da simples transmissão ponto-a-ponto. Assim, surgiram diversos padrões de transmissão, como o *Synchronous Optical Network* (SONET)/*Synchronous Digital Hierarchy* (SDH).

Entretanto, visto que nessas redes, apenas os enlaces de transmissão passaram a pertencer ao domínio óptico, todas as operações de comutação, processamento e roteamento continuavam sendo feitas no domínio elétrico. Estes tipos de redes são nomeadas por alguns autores como Redes Ópticas de Primeira Geração [RAMASWAMI, 2002]. Na

atualidade, estas redes formam parte importante da infra-estrutura pública de telecomunicações.

Com o incremento exponencial da demanda de capacidade para transmissão de dados comutados por pacote, principalmente IP (*Internet Protocol*), por causa do avanço da Internet, surge a necessidade de se incorporar, além do plano de transporte de tecnologia fotônica, um plano de controle baseado em IP que permita à rede de transporte óptica adequar-se ao tráfego das suas redes cliente. Também pesquisadores e fabricantes procuraram por novas tecnologias para estender a largura de banda disponível. Assim, de um simples enlace ponto a ponto com um único comprimento de onda (anos 80), passamos para o desenvolvimento de sistemas totalmente ópticos (final da década de 90), operando com multiplexação WDM (Multiplexação por Divisão de Comprimento de Onda) de 8, 16 e 32 comprimentos de onda por fibra, cada qual transportando informações a 2,5 Gbps e 10 Gbps, e com comprimentos de enlace de centenas de quilômetros, empregando amplificadores ópticos EDFA (Amplificadores de Fibra Dopada a Érbio).

A introdução dos EDFAs e de dispositivos fotônicos como os OADMs (*Optical Add-Drop Multiplexers*) e OXCs (*Optical Cross-Connects*) procuram evitar a conversão optoeletrônica do sinal em pontos intermediários da rede óptica, minimizando atrasos e otimizando a grande largura de banda da fibra. Isto permitirá a substituição das redes ópticas opacas (SONET/SDH), nas quais existem nós intermediários onde ocorrem conversões optoeletrônicas.

O desenvolvimento de sistemas com taxas de 40 Gbps com 100 GHz de espaçamento entre canais [BODUCH, 2006], e também em 50 GHz [XU, 2006] direcionam claramente o rumo das redes de transporte. Atualmente, pesquisas laboratoriais vêm testando taxas acima dos 100 Gbps por canal. Em [SANO, 2006], por exemplo, com taxas de 111 Gbps por canal, com 140 canais WDM por fibra e com espaçamentos de 50 GHz por portadora, testado sobre 160 Km de enlace consegue-se uma capacidade total de 14 Tbps (2bps/Hz).

Tudo isto demonstra que a tecnologia fotônica se apresenta como solução factível aos grandes problemas de largura de banda. Porém, ainda é necessário aprimorar o desempenho nas camadas superiores, em particular a definição de um plano de controle adequado para fazer tangível um transporte otimizado do tráfego IP diretamente sobre WDM.

O propósito deste capítulo é apresentar uma visão geral das redes de transporte de telecomunicações que possa servir como suporte e referência aos seguintes capítulos deste trabalho e a futuros trabalhos na área. Este começa com uma descrição básica dos sistemas de comunicações ópticas. Posteriormente é apresentada a evolução histórica das redes de transporte WDM e as tecnologias, para concluir com o estado da arte da arquitetura.

2.2 SISTEMA DE COMUNICAÇÕES ÓPTICAS

Todo sistema de comunicações é projetado para trafegar informação. Em um sistema de comunicações ópticas a informação é enviada por meio de pulsos de luz ou por sinais modulados de luz.

2.2.1 Elementos de um Enlace

Um enlace básico de comunicações ópticas tem três blocos funcionais [BORELLA, 1997], apresentados na Figura 2.2.

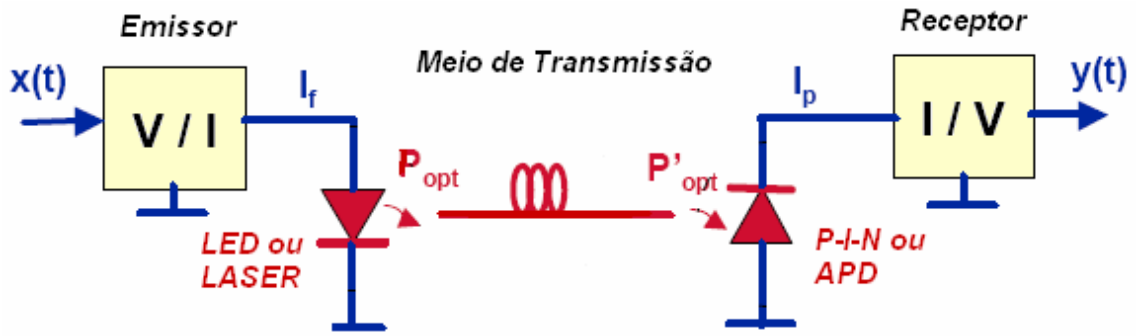


Figura 2.2 - Enlace básico de Comunicações Ópticas.

Emissor. É a fonte produtora de luz, geralmente um diodo laser ou um diodo emissor de luz (LED). O bloco emissor possui também uma série de circuitos eletrônicos destinados a gerar os sinais a serem transmitidos e entregues ao dispositivo opto-eletrônico receptor. São emitidos comprimentos de onda na região do infravermelho próximo. A Figura 2.3 mostra o espectro de saída de diferentes tipos de emissores.

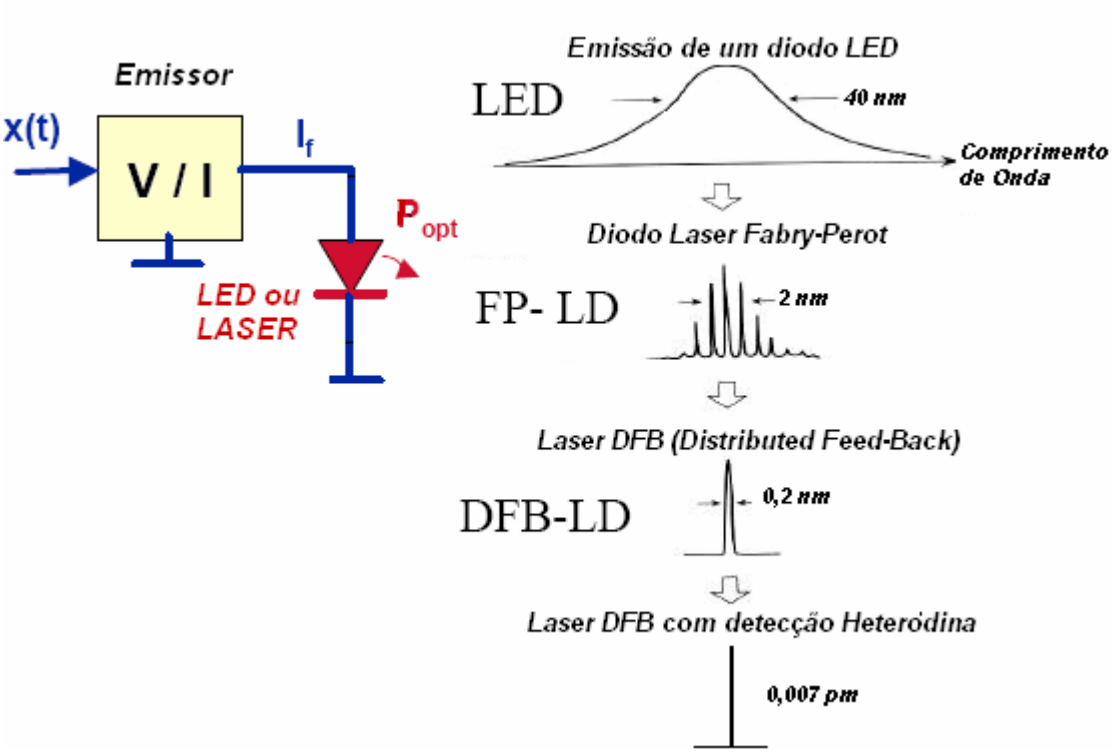


Figura **2.3**- Espectro de saída de diferentes tipos de emissores.

Meio de Transmissão. Embora existam comunicações ópticas atmosféricas, espaciais ou submarinas não guiadas, a grande maioria é realizada através de um meio dielétrico. O meio por excelência é a fibra óptica. O material mais comumente usado é a sílica (SiO2), pela sua extraordinária transparência. Este material básico é dopado com outros componentes para modificar suas propriedades, em especial seu índice de refração[JUNYENT, 2006]. A Figura 2.4 mostra a relação entre atenuação e dispersão em função do comprimento de onda.

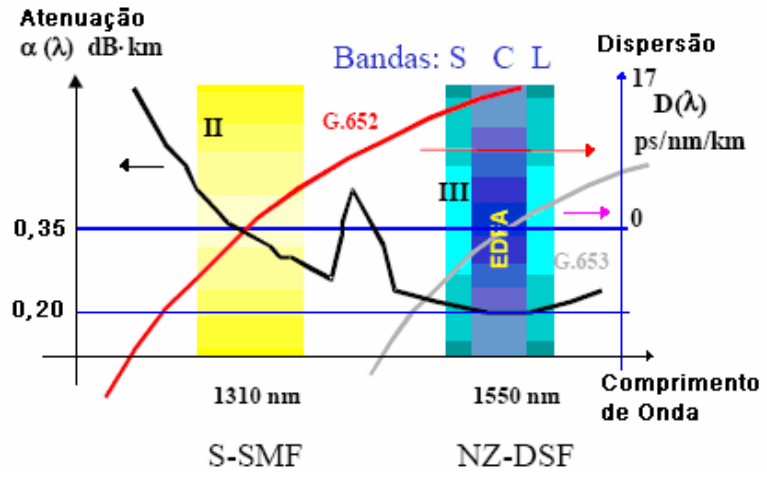


Figura **2.4**- Atenuação e Dispersão em função do Comprimento de Onda

Uma fibra típica tem 125 μm de diâmetro, a luz se guia por um núcleo (*Core*) cujo diâmetro oscila entre 4 e 100 μm dependendo do tipo de fibra (tipicamente entre 4 e 62,5 μm). O resto da fibra óptica é envolvido (Cladding) com o mesmo material, que recobre o núcleo, e que está modificado de maneira a ter um índice de refração ligeiramente inferior ao do núcleo. É precisamente esta mudança de índice que faz com que a luz se guie pelo interior da fibra. Em comunicações ópticas a curta distância (alguns metros) estão sendo usadas também as fibras de plástico (POF).

Receptor. O circuito de recepção consta de um detector – geralmente opto-electrônico, seja um fotodiodo p-I-n (PIN), seja um fotodiodo de avalanche (APD)– e de uma série de circuitos recuperadores dos sinais: amplificadores, filtros, comparadores, etc.

Os sistemas de comunicações ópticas adicionalmente contêm outros elementos, que variam segundo a aplicação. Assim, quando a distância de cobertura de um enlace supera certo limite (algumas dezenas de km, usualmente), o sinal se degrada e se atenua excessivamente, o que torna necessária a instalação de repetidores. Os repetidores podem ser simples amplificadores do sinal, ou incluir também regeneradores do sinal.

Até há pouco tempo todos os repetidores instalados eram eletrônicos: o sinal óptico era detectado e passado para o domínio elétrico, manipulado e logo reconvertido para sinal óptico. Atualmente, estes regeneradores estão sendo substituídos por amplificadores ópticos de fibra dopada (EDFA). Estes dispositivos amplificam diretamente o sinal óptico sem conversões opto-eletrônicas.

A manipulação dos sinais ópticos é mais complexa do que a dos sinais elétricos, dado que para transmitir o sinal, não basta o contato físico, como nos cabos elétricos, mas precisa-se que as propriedades ópticas da junção sejam adequadas para permitir o acoplamento da luz. Com o desenvolvimento das fibras ópticas como meio de transmissão, tem surgido toda uma série de dispositivos de apoio, que se encarregam do encaminhamento do sinal óptico. Os dois tipos mais importantes são os acopladores e os multiplexadores em comprimento de onda.

Fatores que limitam a Transmissão

Os pulsos que se propagam por uma fibra sofrem alargamentos que eventualmente limitam a largura de banda (na realidade, o produto largura de banda x distância) pela sobreposição

de pulsos contíguos (ISI, *intersymbol interference*). Adicionalmente, o sinal se atenua por vários fatores concorrentes, o que incide numa limitação da distância alcançável pelo sinal [ESQUIVIAS, 2006]. Estes dois fenômenos são conhecidos como Dispersão e Atenuação, respectivamente.

Dispersão

A dispersão temporal dos pulsos tem duas origens básicas: intermodal e intramodal. A dispersão intermodal, a mais grave, pode ser reduzida se utilizando fibras multimodo de índice gradual, ou se evitar utilizando fibras monomodo.

As fibras monomodo, por tanto, apresentam só dispersão intramodal. Esta dispersão, por sua vez, é originada de duas causas diferentes, nomeadas de dispersão de guia de onda e dispersão do material, como mostrado na Figura 2.5. Acontece que no espectro de comprimentos de onda, os efeitos destas duas dispersões são contrapostos, podendo existir um λ com dispersão nula. Numa fibra óptica de sílica sem modificação, este ponto está ao redor dos 1310 nm.

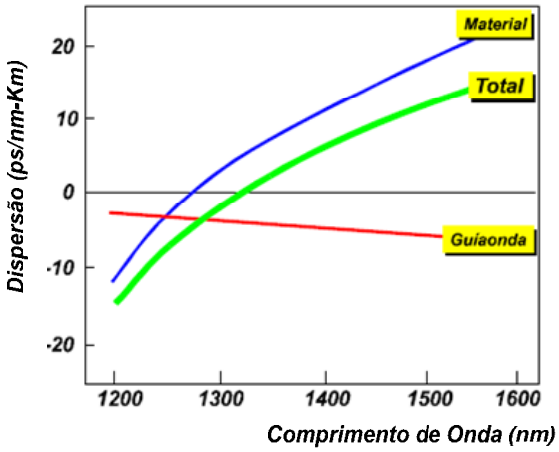


Figura 2.5 -Dispersões Intramodais

Atenuação

Existem também dois fenômenos fundamentais que atenuam o sinal nas fibras: a reflexão difusa ou *scattering*, e a absorção. A primeira tem uma dependência potencial inversa com o comprimento de onda. A outra apresenta máximos na zona ultravioleta e infravermelha do espectro. Entre uma e a outra configuram zonas ou janelas nas quais dão-se as melhores condições para transmissão por fibra óptica.

Os primeiros sistemas ópticos utilizavam a primeira janela (centrada em 850 nm). As duas janelas mais usadas na atualidade são a segunda janela, a 1310 nm, e a terceira janela, a 1550 nm. A segunda janela, também, coincide com a zona de mínima dispersão, enquanto que a terceira janela é a que produz mínima atenuação. A Figura 2.6 apresenta a curva de atenuação em função do comprimento de onda e as janelas de transmissão.

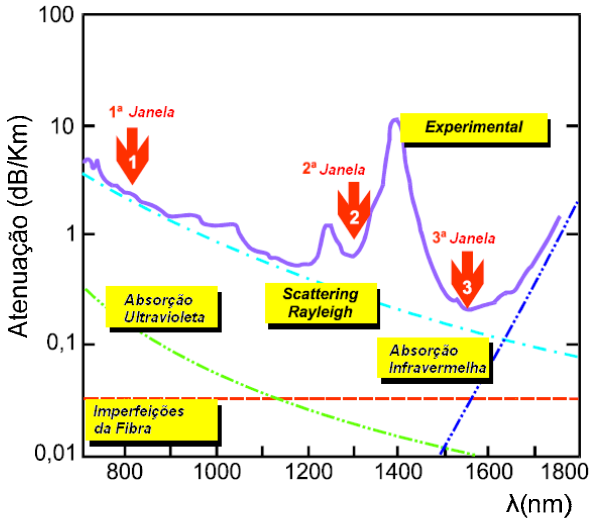


Figura **2.6** - Curva de atenuação em função do comprimento de onda e Janelas de Transmissão (modificado – [ESQUIVIAS, 2006])

A Dispersão pode ser compensada com fibras compensadoras de dispersão (DCF), enquanto que a Atenuação através de amplificadores ópticos. Porém, outras perturbações aparecem para potências relativamente altas (acima de 5dBm), tais como o ruído ASE (*Amplified Spontaneus Emission*), os efeitos não lineares da fibra (SPM, XPM, FWM, SRS, SBS), e o *Crosstalk* linear (em OXCs, filtros).

Bandas Espectrais

A Tabela 2.1 mostra as bandas espectrais, segundo sua nomenclatura ITU.

Tabela 2.1 – Bandas Espectrais (ITU)

Banda	Descritor	Range do Espectro (nm)
O	Original	1260-1360
E	Estendida	1360-1460
S	Curta	1460-1530
C	Convencional	1530-1565
L	Longa	1565-1625
U	Ultra-Longa	1625-1675

A tendência atual é usar preferencialmente a terceira janela (Banda C). Além da sua mínima atenuação, é a região espectral onde podem ser empregados amplificadores de fibra dopada. Para melhorar as características de dispersão, se têm projetado fibras ópticas de dispersão deslocada e de dispersão plana, que apresentam mínimos de dispersão na terceira janela. A Figura 2.7 mostra as janelas de transmissão ópticas e a sua posição dentro do espectro de freqüências eletromagnético.

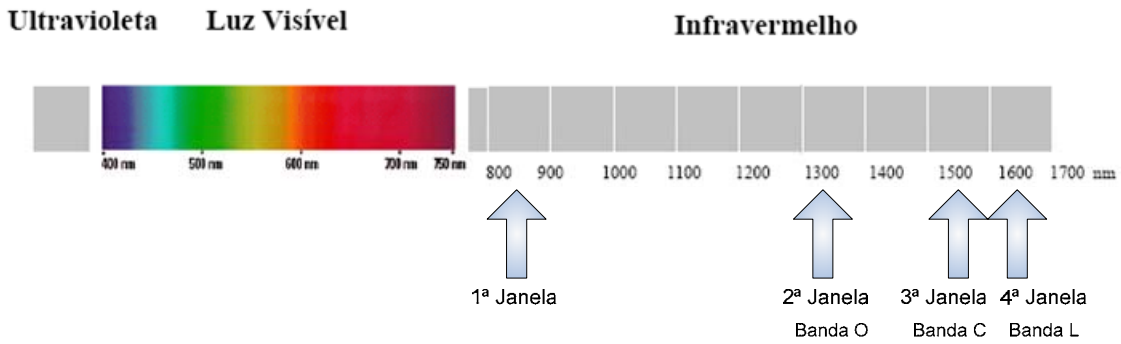


Figura **2.7** - Janelas de Transmissão ópticas no espectro eletromagnético.

Tendo sido a tecnologia de redes ópticas basicamente introduzida, resta analisar como as aplicações do cliente interagirão com esta camada físico-óptica. Tal interação tem provado ser um desafio dentro da atual arquitetura das redes de transporte, na disponibilidade de soluções que habilitem os provedores de serviços a transportar grande tráfego de uma maneira eficiente em termos de custo e desempenho. Antes, é apresentada a evolução das redes de transporte.

2.3 EVOLUÇÃO DAS REDES DE TRANSPORTE

A rede de transporte evolui com os avanços da tecnologia e a necessidade de satisfazer novos serviços. As primeiras redes de transporte foram construídas com cabos de cobre ponto-a-ponto, separados e dedicados para cada canal de voz, e comutados manualmente nos *patch panels* pelos operadores. Esta estratégia, nada escalável, causou a introdução de mecanismos de multiplexação, de maneira que múltiplos canais de voz pudessem ser transportados pelo mesmo conjunto de cabos. Assim, na década de 60 foi apresentada a primeira tecnologia de multiplexação, a Multiplexação por Divisão de Freqüência (FDM: *Frequency Division Multiplexing*), a mais apropriada para o transporte de sinais analógicos.

Contudo, as dificuldades para estender cabos por longas distâncias motivaram o uso de ondas de radiofreqüência. A transmissão por micro-ondas foi uma resposta às necessidades desse momento, e foi um meio bastante utilizado como rede de transporte.

Com o desenvolvimento da tecnologia de transmissão digital, sinais digitais modulam uma portadora analógica e são transmitidas. Este processo permitiu uma regeneração mais fácil reduzindo dramaticamente a degradação do sinal, melhorando assim a relação sinal-ruído (SNR: *signal-to-noise ratio*). Para a tecnologia de transmissão digital, a mais apropriada multiplexação foi a Multiplexação por Divisão de Tempo (TDM).

O desenvolvimento da TDM constituiu um grande aporte para tal evolução. O mecanismo TDM é usado para compartilhar o tempo de transmissão de um enlace de comunicação entre vários canais a fim de se conseguir maior eficiência na transmissão com uma melhor utilização da banda de transmissão. Esse mecanismo pode ser realizado de forma síncrona ou assíncrona.

No TDM síncrono são transmitidos vários canais de informação digital, intercalados no domínio do tempo, com intervalos de tempo fixos. O TDM assíncrono ou estatístico aloca dinamicamente os intervalos de tempo variáveis de acordo com a demanda. Assim, nem todos os canais precisam transmitir ao mesmo tempo.

As hierarquias digitais obtidas com a multiplexação TDM estão presentes nas redes de transmissão das operadoras de telecomunicações, especialmente na borda da rede. São hierarquias padronizadas resultantes de organizações da área de telecomunicações, como o ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*) [ITU-T-G.707, 1995] ou ANSI (*American National Standards Institute*) [ANSI-105, 1995]. A padronização foi direcionada ao perfil básico de tráfego para o transporte de comunicação de voz, ou seja, 64 kbps.

2.3.1 Redes de Comutação por Circuitos

As técnicas digitais tornaram as redes de comunicação mais complexas a partir do início dos anos 80. A demanda das grandes operadoras de telecomunicações e de seus usuários pelas vantagens dessas redes aumentou de tal forma que não poderia ser atendida com os padrões de transmissão existentes. Era o tempo da técnica de multiplexação plesiócrona ou PDH (*Plesiochronous Digital Hierarchy*). Logo, foi aceito que o novo método de

multiplexação deveria ser síncrono e tendo como base a interpolação de bytes e não de bits como no PDH. Surgiram, então, o SDH e o SONET. Esses métodos de multiplexação propiciam o mesmo nível de flexibilidade de comutação de taxas primárias, mais opções de gerenciamento, controle da rede de maneira centralizada e atendimento de novos serviços.

2.3.1.1 Tecnologia SONET/SDH

SONET é um *standart* ANSI que provê multiplexação e transmissão para sinais de alta velocidade dentro da infra-estrutura de telecomunicações com taxas, formatos e especificação de parâmetros de camada física para interfaces elétricas e ópticas com capacidades desde 51 Mbps (OC-1) até 9,8 Gbps (OC-192). O SONET, padrão nos Estados Unidos, é equivalente a SDH, especificado pela ITU-T, que foi adotado na Europa, Japão, Brasil e o resto da região latino-americana, e provê taxas, formatos e especificação de parâmetros de camada física para interfaces elétricas e ópticas com capacidades desde 155 Mbps (STM-1) para 9,8 Gbps (STM-64).

Embora SONET e SDH tenham similaridades como: a mesma taxa de bit e organização do formato do quadro (elemento básico de transmissão); esquemas idênticos de sincronização de quadros; as mesmas regras de multiplexação e demultiplexação; entre outras, trata-se de dois padrões distintos. Contudo, uma vez que o interesse é nas características da multiplexação e da transmissão, que são idênticas, costuma-se tratá-los como um único sistema denominado SONET/SDH.

O tempo de recuperação ante falhas, importante característica dos equipamentos SDH é melhorado pelo protocolo de comutação automática de proteção (APS). O APS fornece proteção contra falhas no enlace por meio do redirecionamento automático do tráfego afetado para rotas alternativas. Este tema será abordado no Capítulo 4.

Sinais SONET são expressos de duas maneiras: Sinais STS-n, de natureza elétrica, usados para a geração do *quadro*; e OC-n (*Optical Carrier-n*), denominação usada para a interface com outros equipamentos ópticos [ELSENPETER, 2002].

Assim, a interface óptica correspondente a STS-3 é o OC-3, para STS-12, STS-48, STS-192, tem-se definidas OC-12, OC-48 e OC-192, respectivamente. As taxas de operação SONET/SDH são mostradas na Tabela 2.2.

A tecnologia SDH, pela sua importância atual na rede de transmissão, ainda continuará presente por um bom tempo, porém a forte emergência do tráfego de pacotes trouxe muitas mudanças no cenário das redes de transporte.

Tabela 2.2 - Taxas de transmissão para SONET/SDH

SONET (ANSI)	SINAL ÓPTICO	SDH (ITU-T)	TAXA DE BITS (Mbps)
STS-1	OC-1	-	51.84
STS-3	OC-3	STM-1	155.52
STS-9	OC-9	STM-3	466.56
STS-12	OC-12	STM-4	622.08
STS-18	OC-18	STM-6	933.12
STS-24	OC-24	STM-8	1244.16
STS-36	OC-36	STM-12	1866.24
STS-48	OC-48	STM-16	2488.83
STS-96	OC-96	STM-32	4976.64
STS-192	OC-192	STM-64	9953.280
STS-n	OC-n		n X 51.84

A Tabela 2.3 apresenta algumas das características mais importantes dos sistemas de comunicações legados, contrastando com os atuais sistemas.

Tabela 2.3 – Contraste entre os Sistemas de Comunicações legados e os atuais

Sistemas de Comunicação: Ontem	**Sistemas de Comunicação: Hoje**
Comutação de Circuitos	Comutação de Pacotes
Voz – Canais fixos de 64 Kbps	Dados – Rajadas de grande largura de banda
Média por sessão: 3 min	Média por sessão: 30 min
Perfil de Tráfego: Previsível	Perfil de Tráfego: Imprevisível
Distribuição geográfica do tráfego	Tráfego geograficamente independente

2.3.2 Redes de Comutação a Pacotes

No caso das redes de dados baseados em pacotes, são usadas técnicas de comutação com base em multiplexação estatística. Esta técnica permite economia da banda passante, quando comparada à técnica de comutação de circuitos, entre outras vantagens. A rede comutada a pacotes foi projetada para transmitir dados. Cada pacote possui carga útil (*payload*) e um cabeçalho (*overhead*) de controle.

2.3.2.1 Roteamento IP

No roteamento IP não há necessidade de cada roteador conhecer a rota completa até o destino, mas apenas o próximo roteador para o qual deve enviar a mensagem. A decisão de roteamento tem como base uma tabela de rotas que relaciona cada rede destino ao roteador para onde o pacote deve ser enviado, e se ajusta automaticamente em decorrência de mudanças nas topologias das redes. É importante ressaltar que o pacote IP a ser roteado é endereçado fisicamente ao roteador (endereço MAC), mas também logicamente (endereçamento IP) à estação destino. Dessa forma, quando o roteador recebe um pacote que não é endereçado a ele, tenta roteá-lo.

Assim, em uma rede de dados IP os pacotes são entregues ao primeiro nó da rede, que verificará as informações do cabeçalho e os enviará para o próximo nó. Esse processo é repetido até cada pacote chegar ao seu destino. Uma conexão entre dois nós pode ser usada por vários pacotes de diferentes destinos e origens. Assim, um caminho não será exclusivo, podendo ser compartilhado por outros usuários.

Existem basicamente duas técnicas para o envio de pacotes: a do *datagrama* e a do circuito virtual. Na técnica do *datagrama*, todos os pacotes são enviados pela rede independentemente um dos outros. Assim, pacotes de uma mesma mensagem podem seguir diferentes caminhos na rede com base em informações de tráfego, compartilhadas entre os nós, usando protocolos de roteamento. No destino, a mensagem é reordenada com o auxílio do protocolo de transporte (TCP).

Na técnica de comutação a pacotes denominada circuito virtual, antes de qualquer pacote ser entregue à rede é feita uma definição da rota, da origem até o destino, por onde todos os pacotes irão passar, percorrendo os mesmos nós da rede. Nenhuma decisão de roteamento será feita no caminho. Esta técnica é parecida com a técnica usada pelas redes comutadas a circuito, porém, aqui não existem canais dedicados e, por tanto, num mesmo enlace da rede podem trafegar vários circuitos virtuais [PASTOR2, 2005].

2.3.3 Evolução da Demanda de Tráfego

A demanda de capacidade para transmissão de dados (principalmente IP) está se incrementando rapidamente. Tráfego de dados cresce a uma taxa de 7-20% por mês, de uma forma geral o crescimento do tráfego de voz ocorre a uma taxa de 13% por ano

[PARETA, 2006]. A Figura 2.8 apresenta como a demanda de serviços de dados de banda larga cresce exponencialmente, com o conseqüente aumento do tráfego na rede.

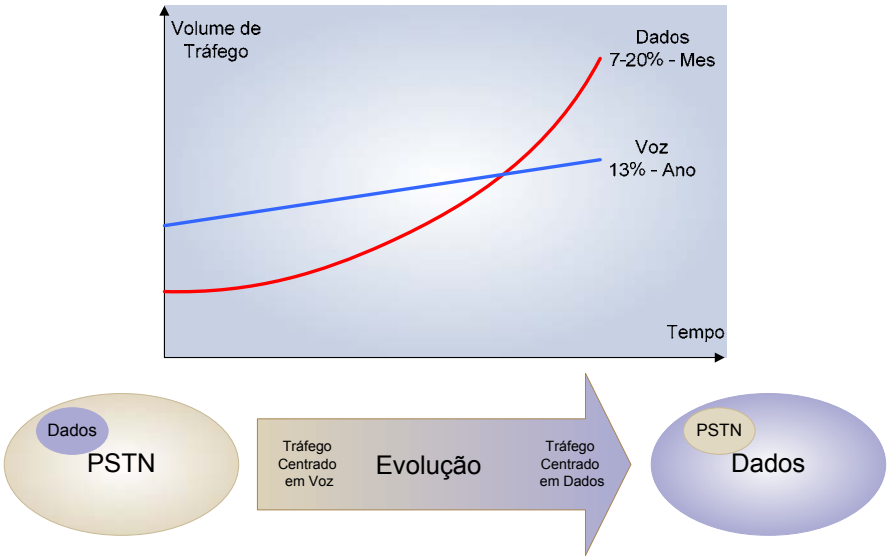


Figura 2.8 - Evolução da demanda de tráfego

Neste panorama difícil para as operadoras de telefonia, há fortes cortes de orçamento que dificultam novos investimentos. Assim, se busca maximizar o uso dos grandes investimentos já realizados, mesmo com o paradoxo dos preços dos serviços que são cada vez mais baixos. O maior problema está no fato que a infra-estrutura das redes existentes não estão habilitadas para suportar as demandas dos novos serviços.

A infra-estrutura de telecomunicações pública tem de ser atualizada para cobrir tal evolução da demanda de tráfego. Uma solução adotada pelas operadoras vem sendo a adaptação das redes legadas aos novos serviços para cobrir tanto a demanda crescente de capacidade como o mercado emergente de serviços puramente ópticos. Assim, se vem desenvolvendo a camada óptica com funcionalidades de comutação, além das funcionalidades de transmissão. Como resultado da evolução das tecnologias ópticas nas redes de transporte se está consolidando a rede óptica comutada por comprimento de onda.

2.4 ARQUITETURA DE REDE MULTICAMADA

Arquitetura de rede multicamada está baseada em múltiplas tecnologias de rede em pilha. A arquitetura para o transporte de dados mais usada atualmente pelas operadoras é formada por tecnologia IP/ATM/SDH/OTN, com IP para o roteamento de aplicações e serviços, ATM (*Asynchronous Transfer Mode*) para a Engenharia de Tráfego e QoS, SONET/SDH

para transporte e proteção de dados, e OTN (*Optical Transport Network*) com DWDM (*Dense Wavelength Division Multiplexing*) para proporcionar altas capacidades de transporte Isto é apresentado na Figura 2.9.

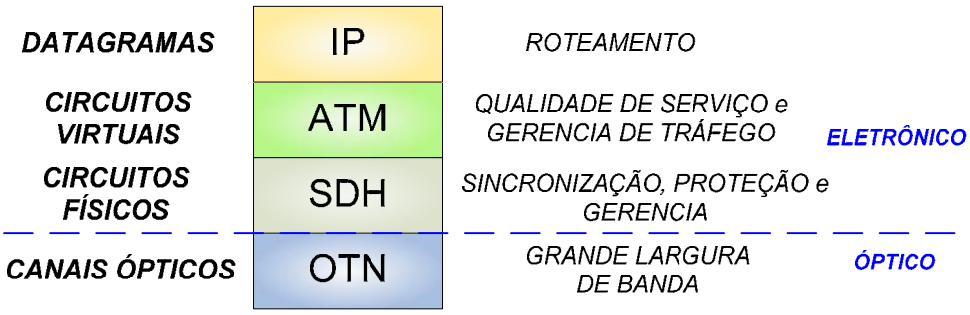


Figura **2.9** - Arquitetura de rede multicamada

Porém, esta arquitetura vem se mostrando redundante e incapaz de proporcionar o transporte de grandes volumes de tráfego com eficiência e custo acessível. De fato, arquiteturas multicamadas tipicamente apresentam efeitos nos quais uma camada pode limitar a escalabilidade de redes inteiras, tanto quanto aumentar os custos das mesmas.

Estas redes multicamadas foram projetadas inicialmente para comutação de circuitos e orientadas à transmissão de voz, que constituía o tráfego dominante, como foi visto, porém não se adeqüa bem a transmissão de dados, principalmente em termos de eficiência e custo. Cada camada não sabe muito bem o que acontece nas outras, sendo necessário o aumento do cabeçalho para um melhor controle, existindo ainda a possibilidade de duplicação de serviços.

No topo desta pilha temos a camada IP, o qual permite a transmissão de *datagramas* pela rede com funções de *internetworking* sem conexão. Uma das razões para sucesso do protocolo IP é o fato de ter sido projetado para operar sobre uma grande variedade de camadas inferiores, as camadas de enlace de dados segundo o modelo OSI (*Open System Interconnection*) da ISO (*International Standardization Organization*). Algumas dessas camadas de enlace estão associadas aos padrões de redes locais mais populares, tais como Ethernet e Token Ring; aos de redes metropolitanas, por exemplo, FDDI (*Fiber Distributed Data Interface*); como também aos protocolos destinados à operação sobre linhas alugadas das operadoras públicas, como é o caso do HDLC (*High Level Data Link Control*).

O protocolo IP fornece às camadas superiores apenas serviços em modo datagrama que, embora mais simples quanto a processamento, não garante a entrega dos pacotes. Por ter sido concebido para a comunicação de dados, os pacotes IP são de tamanhos variáveis. Quando montado sobre a infra-estrutura ATM, seus pacotes de tamanhos variáveis são segmentados em tamanhos fixos correspondentes aos da célula ATM.

Nos primeiros estágios das redes IP, roteadores eram interconectados usando serviços *leased-line* (linhas privadas) para produzir configurações ponto-a-ponto, este serviço é conhecido como IP sobre SDH. Com a contínua expansão do tráfego foi necessário o aumento das capacidades do nó. Assim, foram desenvolvidos roteadores IP eletrônicos para roteamento na ordem de Terabits/s a fim de interconectar estes com enlaces WDM de grande capacidade. Esta técnica é conhecida como IP sobre SDH sobre WDM. O protocolo IP, embora seja o mais utilizado nas redes de longa distância, não possui qualquer garantia de qualidade de serviço (QoS - *Quality of Service*).

Paralelamente, a tecnologia ATM (*Asynchronous Transfer Mode*) é introduzida em redes IP de larga escala para permitir conexões de roteadores usando rotas e canais virtuais sobre redes tipo malha (IP sobre ATM). Isto habilita a capacidade de comutação nos nós e promove as bases para a engenharia de tráfego e qualidade de serviço (QoS) na rede; contudo, ainda sem total integração, pois as camadas IP e ATM são gerenciadas separadamente. Para a sincronização da informação a ser transmitida, para a introdução de capacidades de sobrevivência à rede e para a gerência de circuitos é utilizada a tecnologia SDH (ou SONET).

Por fim, a informação será transmitida em grande largura de banda na camada de transporte óptica (OTN). A OTN é formada por três subcamadas especificadas na recomendação ITU-T G 709: OCh (Seção de Canal Óptico), OMS (Seção de Multiplexação Óptica) e OTS (Seção de Transmissão Óptica). Sinais como SONET/SDH, Ethernet, IP e ATM são mapeados do formato digital para o formato óptico na camada OCh. Isto é apresentado na Figura 2.10.

A Seção de Canal Óptico (OCh) define uma conexão óptica (*lightpath*) fim a fim entre duas entidades cliente para transmitir, de forma transparente, informação com diferentes tipos de formatos. Esta camada gerencia individualmente os canais ópticos. O OCh é equivalente a um *comprimento de onda* na linguagem DWDM.

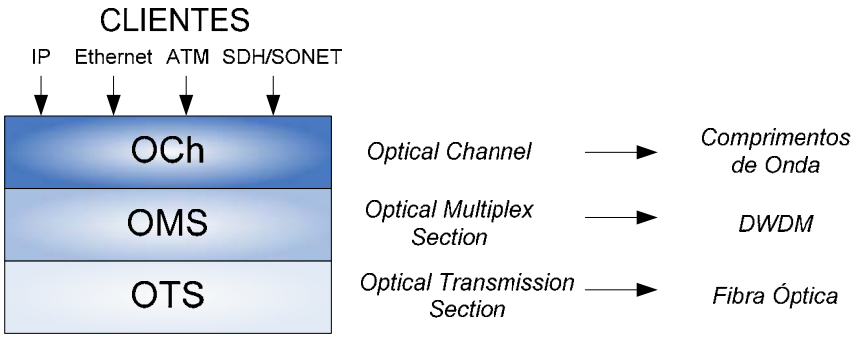


Figura **2.10 -** Sub-camadas da camada OTN

A Seção de Multiplexação Óptica (OMS) define a conectividade e o tratamento para a multiplexação ou agrupamento das conexões do nível OCh, ou seja, multiplexa e gerencia um conjunto de vários comprimentos de onda. Na seção OMS um grupo de *lambdas* vão sobre um cabo de fibra-óptica entre dois multiplexadores DWDM.

A Seção de Transmissão Óptica (OTS) define como os sinais ópticos são transmitidos sobre o meio óptico. Esta camada provê funcionalidades para a transmissão do sinal óptico em meios ópticos de vários tipos (distintos tipos de fibras), executando assim o transporte de um feixe composto de vários comprimentos de onda da camada OMS.

Então, os canais presentes na camada OCh são multiplexados pela camada OMS, e estes canais multiplexados são transportados opticamente em um segmento de fibra pela camada OTS. A Figura 2.11 ilustra como estas subcamadas da OTN apresentam-se em um enlace de uma rede óptica. A estrutura destas camadas é similar às subcamadas de seção, linha e caminho da arquitetura SONET/SDH [BLACK, 2002].

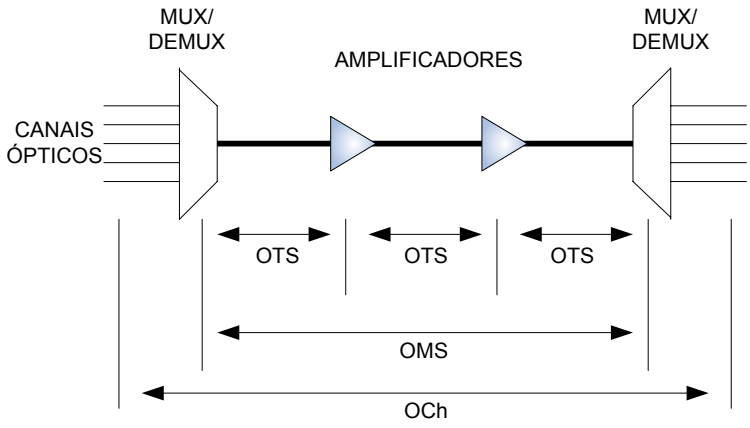


Figura **2.11**- Sub-camadas da OTN em um enlace de uma rede óptica.

2.4.1 IP sobre ATM sobre SDH

A configuração IP sobre ATM sobre SONET/SDH é uma das mais usadas atualmente pelos provedores de transporte, possibilitando taxas de transmissão de 155 Mbps e 622 Mbps, com capacidades de engenharia de tráfego (ATM) e gerenciamento, detecção de falhas e proteção/restauração (SONET/SDH).

ATM é uma tecnologia de comunicação de dados por comutação de circuitos virtuais baseados em *cell-switched* (comutação de células). Uma célula, como mostrado na Figura 2.12, tem um comprimento fixo de 53 bytes (5 de *overhead* e 48 de *payload*) para transmitir informação de usuário e sinalização, diferente de sistemas tais como IP, X.25 ou *Frame Relay* que fazem uso de pacotes de dados de comprimento variável.

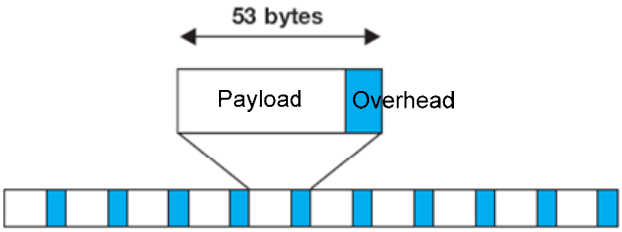


Figura **2.12** - Célula ATM

ATM foi projetado para *operadoras*, principalmente para privilegiar o transporte de voz, porém provê capacidades de integração de Voz + Imagem + Vídeo + Dados, assim como gerência de tráfego, sinalização e comutação com qualidade de serviço.

A camada ATM, posicionada acima da camada SONET/SDH, provê tecnologia orientada a conexão que precisa de uma conexão virtual (VC) entre a fonte e o destino antes da informação ser trocada.

A principal desvantagem de ATM é a pouca eficiência em questões de largura de banda, já que por cada célula de 53 bytes tem-se uma "penalidade" de 5 bytes de cabeçalho de informação de controle. Outro problema é a escalabilidade: os protocolos de roteamento IP não escalam bem com muitos enlaces. Um VC é considerado um enlace e conectando N roteadores IP em uma topologia em malha serão necessários configurar e gerenciar $O(N^2)$ VCs. Além do mais, ATM introduz complexidade a um custo pouco competitivo no sistema final, uma das razões pelo qual não pode alcançar diretamente aos usuários residenciais.

No mapeamento IP sobre ATM sobre SONET/SDH cada datagrama IP é encapsulado dentro de um quadro da subcamada AAL-5 (ATM *adaptation layer type 5*) [GROSSMAN, 1999] usando LLC (*logical link control*), e encapsulamento SNAP (*subnetwork attachment point*). Posteriormente, o quadro AAL-5 é segmentado em células ATM de 48 bytes de *payload*. Finalmente, células ATM são mapeadas dentro do quadro SONET/SDH.

2.4.1.1 Encapsulamento LLC (*Logical Link Control*)

O encapsulamento LLC (RFC2684) é necessário quando diferentes protocolos são transportados sobre o mesmo enlace. A unidade de dados de protocolo (PDU) LLC/SNAP (*Sub-Network Access Point*) é transportada no *payload* do PDU do protocolo AAL5. Por sua vez, o PDU LLC/SNAP encapsula os pacotes IP a serem transportados no circuito virtual ATM.

Na Figura 2.13 se apresenta o modo de encapsulamento para a transmissão de dados entre um usuário final e um servidor remoto.

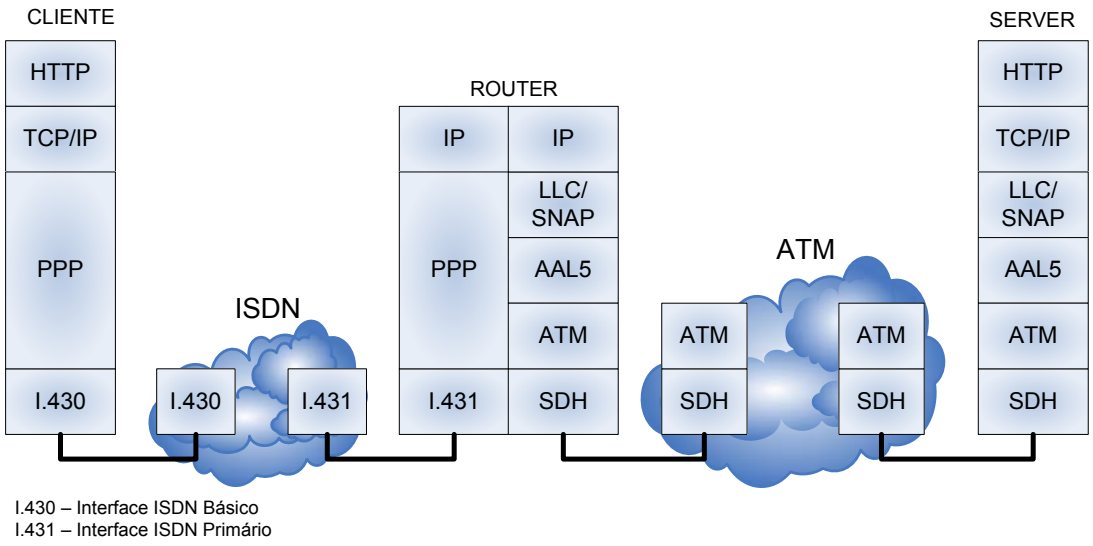


Figura **2.13** - Exemplo de uma rede IP/ATM usando encapsulamento LLC.

O usuário acessa a rede via modem usando uma interface básica ISDN (Rede Digital de Serviços Integrados - I.430). O roteador, implementado também com uma interface ISDN mas usando uma interface primaria (I.431), recebe os pacotes e os roteia para uma rede de transporte baseada em ATM sobre SDH. Para o acesso à dita rede os pacotes IP são encapsulados em LLC/SNAP e logo adaptados via o protocolo AAL5, para usar a

tecnologia ATM. Uma vez estabelecido o circuito virtual, a informação é transmitida usando-se enlaces SDH até o destino.

2.4.1.2 Eliminando a camada ATM

A Tabela 2.4 mostra a distribuição dos cinco predominantes tamanhos de pacotes em um *backbone* Internet, a partir de uma amostra de cinco minutos (mais de 18 milhões de pacotes, totalizando 6,7 GB) tomada pela *National Laboratory of Advanced Network Research*, num enlace OC-3/STM-1 (155,52 Mbps) presente no *backbone* da *MCI Telecommunications Corporation* em junho de 1997 [THOMPSON, 1997].

Tabela 2.4 - Distribuição dos tamanhos de pacotes predominantes no *backbone* Internet.

Tamanho do Pacote (Bytes)	Total de Pacotes (%)	Total de Bytes (%)
40	38,9	4,4
1500	11,5	48,7
552	10,1	15,8
44	6,1	0,8
576	4,9	7,9

As estatísticas apresentadas na Tabela 2.4 mostram que 45% dos pacotes IP são de um comprimento entre 40-44 bytes. Para este tamanho de pacotes serão necessárias duas células ATM, com a segunda célula quase vazia. A Figura 2.14 apresenta a medida da distribuição do tamanho de pacotes num certo enlace, onde aproximadamente 50% dos pacotes são PDUs muito curtos.

Os provedores de serviço Internet procuram por soluções para ir com IP diretamente sobre SDH. A razão principal é o excesso de *overhead* que introduz ATM para o transporte de IP.

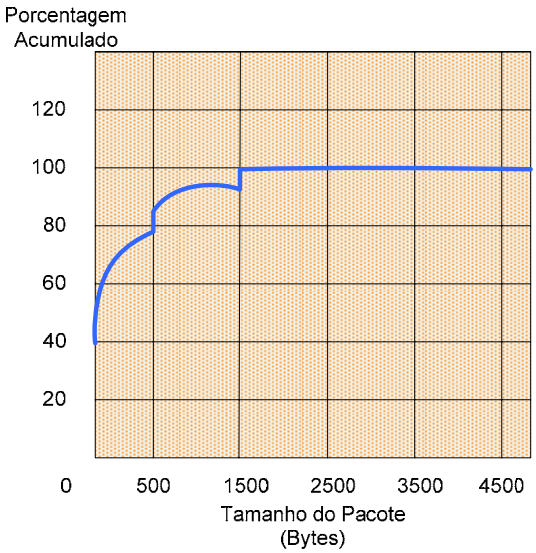


Figura **2.14** - Distribuição do tamanho de pacotes num enlace doméstico (Modificado, [THOMPSON, 1997])

O seguinte exemplo, apresentado na Tabela 2.5, nos mostra o *overhead* que se alcança com uma arquitetura de transporte baseada em IP/ATM/SDH, e quanto de carga útil é desperdiçada (no exemplo, 22%) em relação ao pacote a ser transmitido.

Tabela 2.5 – Calculo do *Overhead* para IP/ATM/SDH

	Tamanho de Pacote (Bytes)	**Overhead (OH) acumulado**	**Comentários**
Pacote IP	350	0%	Tamanho típico de pacote IP
LLC/SNAP	358	2%	8 octetos de OH
AAL5	390	10%	8 octetos de OH + 24 octetos (em média para preencher a ultima célula ATM
ATM	431	19%	5 octetos x cada 48 bytes
SDH	447	22%	Overhead SDH ~3% para 431 bytes
Para 1 STM-1 (155 Mbps) ter-se-ia uma capacidade útil de: 121 Mbps			

Os resultados nos mostram que, a partir de uma perspectiva de *overhead*, o mapeamento IP/ATM é extremamente ineficiente.

2.4.2 IP sobre ATM diretamente sobre fibra

Nesta proposta, as células ATM não precisam ser encapsuladas em *quadros* SDH, elas são enviadas diretamente sobre o meio físico depois do *scrambling*. Aqui é usada uma camada física baseada em células ATM.

2.4.2.1 Benefícios de IP/ATM/fibra com relação a IP/ATM/SDH

- Técnica de transmissão mais simples;
- *Overhead* de camada física menor (~16 vezes menor);
- Não há um rígido mecanismo de temporização a ser colocado na rede.

A Tabela 2.6 apresenta a quantidade de *overhead* introduzida por IP/ATM/fibra e quanto de carga útil é desperdiçada (no exemplo, 19%) com relação ao pacote IP a ser transmitido.

Tabela 2.6 – Cálculo do *Overhead* para IP/ATM diretamente sobre fibra

	Tamanho de Pacote (Bytes)	Overhead (OH) acumulado	Comentários
Pacote IP	350	0%	Tamanho típico de pacote IP
LLC/SNAP	358	2%	8 octetos de OH
AAL5	390	10%	8 octetos de OH + 24 octetos (média para preencher a ultima célula ATM
ATM	431	19%	OH ATM: 5 octetos por cada 48 octetos
OAM	432	19%	Adiciona 1 célula OAM por cada 431/53 células ATM
Para 1 STM-1 (155 Mbps) teria-se uma capacidade útil de: 126 Mbps			

As células OAM (*Operation Administration and Maitenance*) permitem ao administrador da rede ATM monitorar erros que possam acontecer, determinar a qualidade da conexão e medir desempenho [SCHULTZ, 2003]. Nesta proposta a célula OAM é usada como elemento de sincronização e delimitação para a carga que está sendo transportada pelas células ATM. No exemplo, para os 431 bytes que são transportados nas 9 células (431/53) é adicionada 1 célula OAM.

Porém, esta proposta não está sendo adotada pela indústria devido à proposta mais atrativa do MPLS (*Multiprotocol Label Switching*).

Assim, para alcançar maior eficiência e escalabilidade, a rede precisava reduzir o número de camadas. Embora o roteamento de nível 3 (IP) tenha sido bastante utilizado, os nós de comutação operam cada vez mais sobre uma comutação de nível 2, que se mostra mais eficiente. Para eliminar a camada ATM, a função de engenharia de tráfego executada por

ela deveria ficar a cargo da camada IP. Isto pode ser alcançado através da inclusão de funcionalidades proporcionadas pela tecnologia MPLS, proposta da IETF (*Internet Engineering Task Force*) dentro da camada IP [ROSEN, 2001]. A tecnologia MPLS implementa gerência integrada de camada 2 (enlace) e camada 3 (rede) do modelo OSI.

O MPLS é um modelo híbrido que explora as melhores propriedades do roteamento de pacotes e da comutação de circuitos. Essa técnica tem, entre outras possibilidades, a capacidade de criar circuitos virtuais para controlar o roteamento do tráfego, diminuindo o tempo de encaminhamento de pacotes e evitando o processamento de nível 3, bem como atualização das tabelas de roteamento, cálculo de métricas e descoberta de rede [PASTOR2, 2005].

A arquitetura MPLS usa comutação de pacotes no modo circuito virtual. Neste cenário surge a necessidade de sinalização para esses circuitos. Assim, o MPLS define um plano de controle e um plano de encaminhamento. O plano de controle utiliza protocolos de sinalização e roteamento que permitem configurar, de maneira dinâmica, os circuitos virtuais. O plano de encaminhamento é utilizado basicamente para o transporte dos dados.

Para transporte de pacotes, o MPLS é baseado no paradigma de comutação de rótulos. Um rótulo é um identificador de tamanho fixo (20 bits) e tem significado local. Um domínio MPLS é formado por roteadores de núcleo e roteadores de borda, que interligam subdomínios. Quando um pacote entra no domínio MPLS, a ele é atribuído um rótulo, que, na prática, permite o desacoplamento entre o roteamento e o encaminhamento. Desta forma, os roteadores só analisam os rótulos para poder encaminhar o pacote.

Assim, o MPLS permite incorporar as funções de comutação e engenharia de tráfego, suprimindo a necessidade de camadas intermediárias.

2.4.3 IP sobre SDH ou PoS (*Packet over SONET*)

SDH tem melhor escalabilidade que ATM em termos de taxa de transmissão. A tecnologia IP/ATM é limitada a um máximo de 622 Mbps. Já o IP/SDH pode escalar até 10 Gbps.

Porém, um problema que se apresenta quando se deseja implementar IP/SDH são os processos de encapsulamento. IP não provê sincronização de bit nem delimitação de pacote (demarcação de pacote). Em IP/LANs, a sincronização de bit e a delimitação de quadro são providos pela camada MAC. Já na rede de transporte IP/ATM, SDH provê sincronização

de byte, ATM provê sincronização de célula e AAL5 delimitação de *quadro*. Ainda que em IP diretamente sobre SDH se tem sincronização de bit, mas também é necessário prover delimitação de pacotes IP. Assim, IP/SDH requer um encapsulamento adicional para a delimitação de pacotes para o qual é usado encapsulamento PPP/HDLC (RFC 1662).

O PPP (*point-to-point protocol*) [SIMPSON, 1999] [CAVENDISH, 2000] é um método *padrão* para transportar datagramas multi-protocolos multiplexados sobre um enlace ponto-a-ponto, o qual provê:

– Encapsulamento de pacotes IP (valor máximo *default*: 1500 bytes);
– Controle de erros (descarta quadros corrompidos);
– Inicialização de Enlace.

O HDLC (*High-Level Data Link Control*) é um protocolo de comunicação de dados ponto-a-ponto entre dois elementos da rede. Proporciona recuperação de erros em caso de perda de pacotes, falhas de seqüência e outros benefícios. É um protocolo de propósito geral, que opera em nível de enlace de dados, oferecendo uma comunicação confiável entre trasmissor-receptor. Assim, o HDLC provê:

– Reporte de erros;
– Delimitação dos pacotes IP encapsulados em PPP (usando "*byte stuffing*") (ver RFC 1662).

A ordem apropriada de operação durante a transmissão de dados é apresentada na Figura 2.15. A transmissão do *quadro* SDH é precedida do processo de *scrambling padrão* de SDH. Também, a recepção do quadro SDH é seguida do processo de *descrambling padrão* de SDH.

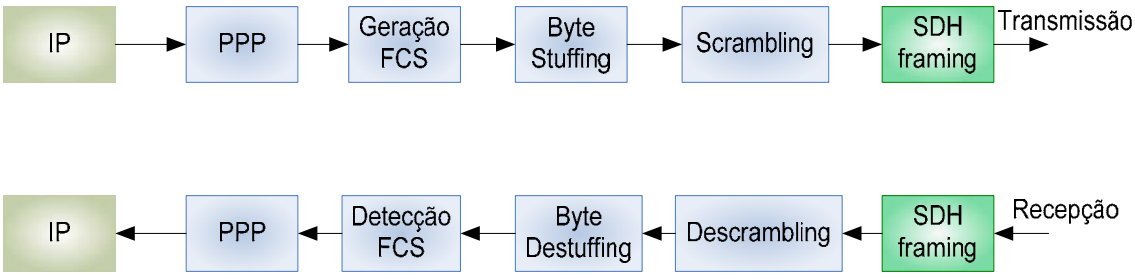


Figura **2.15** – Processo de transmissão de um quadro SDH.

A Figura 2.16 apresenta um exemplo de uma rede IP/SDH fazendo uso de encapsulamento PPP-HDLC.

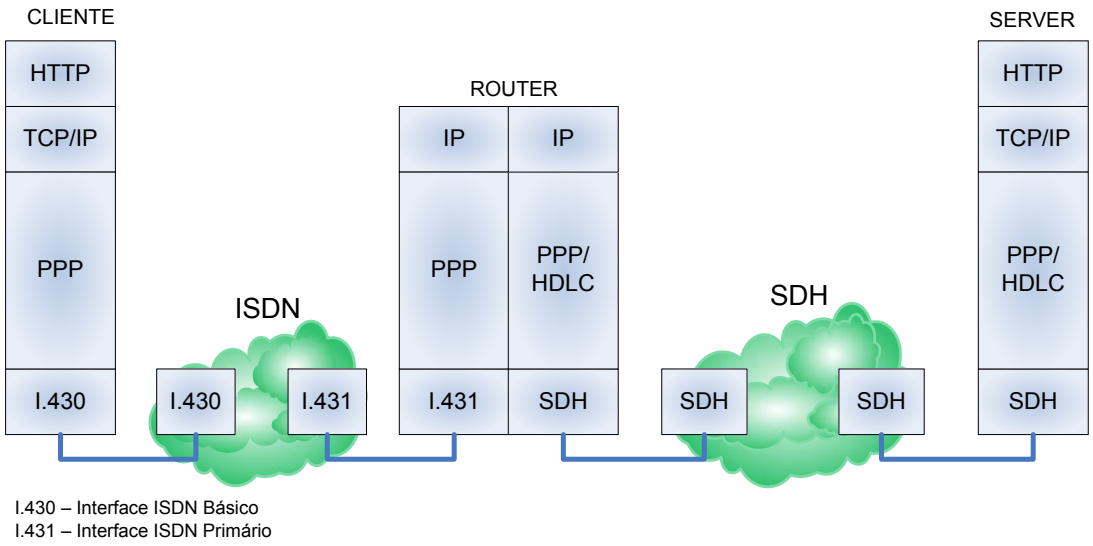


Figura **2.16** - Exemplo de uma rede IP/SDH usando encapsulamento PPP-HDLC.

A Figura 2.17 mostra algumas configurações de redes PoS.

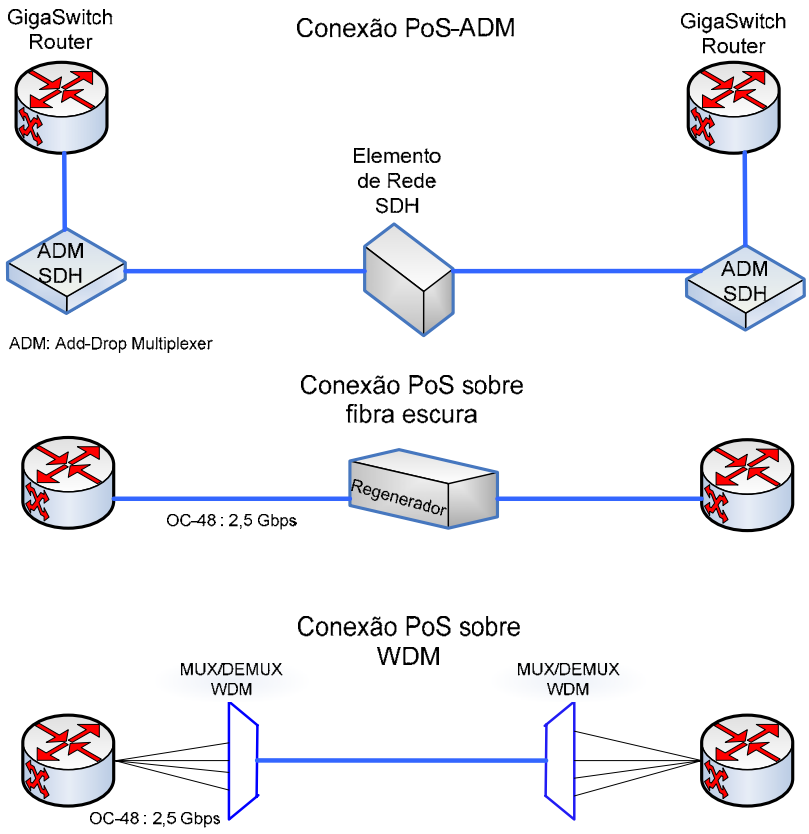


Figura **2.17** - Configurações de Redes IP sobre SDH.

2.4.3.1 Desvantagens de IP sobre SDH

Escalabilidade até 2,4 Gbps (OC-48/STM-16) - O mecanismo de delimitação baseado em HDLC não escala facilmente acima de 2.4 Gbps [PARETA, 2006]. No lado do transmissor, cada saída de pacotes precisa ser monitorada e o *stuffing* chamado. O receptor precisa monitorar cada entrada de dados e fazer o *destuffing*.

Capacidade de crescimento incremental - SDH não provê muita flexibilidade em termos de capacidade de expansão. Esta é uma das motivações para a migração das redes *backbone* IP para transporte baseado em tecnologia WDM.

SDH é uma tecnologia *circuit switching* - Com o desenvolvimento da Internet e o incremento na transmissão de dados, a tecnologia mudou para serviços *packet switching*, o qual cria a necessidade de tecnologias de adaptação para o uso de SDH, o que significa, na prática, a introdução de maior *overhead* na rede. A Tabela 2.7 apresenta o cálculo de o*verhead* para IP/PPP/SDH.

Tabela 2.7 - Cálculo de *Overhead* para IP/PPP/SDH

	Tamanho de Pacote (Bytes)	Overhead (OH) acumulado	Comentários
Pacote IP	350	0%	Tamanho típico de pacote IP
PPP/HDLC	358	2%	8 octetos de OH para pacotes menores que 1500 bytes
SDH	371	6%	Overhead SDH: 10 colunas por cada 270
Para 1 STM-1 (155 Mbps) teria-se uma capacidade útil de: 146 Mbps			

Em resumo, a Tabela 2.8 apresenta uma porcentagem de *overhead* e capacidade de enlace para os diferentes métodos de encapsulamento considerando um enlace a 2,4 Gbps.

Tabela 2.8 - Porcentagem de *overhead* - diferentes métodos de encapsulamento a 2,4 Gbps

Encapsulamento/Framing	Overhead	Capacidade do Enlace (Mbps)
IP/ATM/SDH	22%	1944
IP/ATM/Cell-based	19%	2011
IP/PPP/SDH	6%	2338

Para eliminar a camada SONET/SDH, a capacidade de transporte da tecnologia SONET/SDH (proteção e comutação) deverá ser feita na camada óptica. Esta funcionalidade é alcançada por comutadores ópticos em conjunto com os sistemas DWDM.

2.4.4 GFP (Generic Frame Procedure)

O GFP é um protocolo de adaptação de tráfego padronizado [ITU-T- G.7041, 2001], para aplicações de transporte de banda larga. Provê um mecanismo amigável de QoS e eficiência para mapear, tanto sinais de camada de enlace lógico ou de camada física, para um canal sincronizado por Byte. O mecanismo de adaptação usa ponteiros e cabeçalho CRC para delinear o encapsulado de PDUs de comprimento fixo ou variável. Suporte é provido para o mapeamento direto tanto de sinais de dados cliente ponto-a-ponto como multiponto. Todas estas características fazem de GFP particularmente apropriado para adaptação de dados sobre SONET/SDH bem como transporte de IP sobre OTN/WDM.

A diferença dos mecanismos de delimitação de *quadro* baseados em padrões *codeword*, faz com que o GFP não precise de especial pré-processamento dos *streams* de bytes cliente. Em lugar de confiar em bits de dados/controle embutidos, tais como em codificação 8B/10B e 64B/66B, ou delimitação de *flags* como do *framing* HDLC, o GFP confia no comprimento do atual *payload* e uma verificação de controle de erro (*error control check*) para delimitar os limites do quadro. A validação satisfatória destes dois itens, no cabeçalho do GFP, é usada para determinar a sincronização do enlace de dados adequada e o número de bytes para a próxima entrada do quadro.

O GFP originalmente apareceu para direcionar algumas limitações do ATM e outras tecnologias de PoS. Posteriormente foi adotado pela ITU-T e publicado como *padrão* sob a Recomendação G.7041 [ITU-T- G.7041, 2001].

No GFP se faz a adaptação dos serviços de dados sobre os *payloads* de SDH de forma flexível, robusta e com menor "*overhead*". GFP preserva a informação MAC, permitindo assim suportar múltiplos protocolos de nível 2. Há dois tipos de GFP: o GFP Transparente (GFP-T) e o GFP Baseado em *quadros* "*Framed-Based*" (GFP-F) [HERNANDEZ, 2002].

O GFP-T mapeia todo o sinal (todos os bits) em quadros GFP de tamanho fixo, o que faz com que seja totalmente transparente, com tempos baixos de latência de transmissão de sinal e fácil implantação, porém com maior consumo de largura de banda.

O GFP-F mapeia, em cada um dos *quadros*, só os bytes que serão transmitidos, fazendo assim um melhor uso da largura de banda. Porém, só é capaz de suportar protocolos orientados a quadros com adaptação particular para cada um dos protocolos suportados [IGLESIAS, 2004]. A Tabela 2.9 compara as características particulares dos dois tipos de GFP.

Tabela 2.9 – Comparação das características do GFP-T e GFP-F

Característica Suportada	GFP-T	GFP-F
Transparência a códigos de controle de quadros	Sim	Não
Otimização da largura de banda	Não	Sim
Permite monitorização de cada quadro	Não	Sim
Minimiza a latência para serviços sensíveis ao retardo	Sim	Não
Permite opcionalmente correção de erros	Sim	Não
Permite compartilhar o canal de transmissão entre vários clientes	Sim	Sim

GFP faz uso de tecnologias de concatenação virtual (VCAS) [ITU-T G.707, 2003], [ITU-T G.7043/Y.1343, 2004], e LCAS (*Link Capacity Adjustment Scheme*) [ITU-T G.7042, 2004], para criar canais de transporte de tamanho flexível. Embora GbEthernet apareça como uma alternativa de transmissão de pacotes para WAN, a conversão desde uma rede *backbone* SONET/SDH para uma rede *backbone* GbEthernet teria um custo muito elevado pelos equipamentos necessários para a interoperabilidade entre ambas tecnologias. O GFP, ao contrário, permite eficiente transporte de pacotes dentro do existente *backbone* SONET/SDH se tornando muito atrativo para as *operadoras* [GORSHE_2, 2005] [EHRHARDT, 2006] [ELANTI, 2005].

2.4.5 IP sobre Gigabit Ethernet

A tecnologia Gigabit Ethernet pode ser usada para estender a alta capacidade das LANs para redes MANs e WANs.

Em Gigabit Ethernet para WDM [GILARDI, 2002], a funcionalidade CSMA/CD não é usada. Usa-se simplesmente um método de encapsulamento e *framing*. Os comutadores Ethernet podem ser usados para estender a topologia de rede além do enlace ponto-a-ponto (observar que *Ethernet switching* é baseado no endereço MAC).

No caso de 10-Gigabit Ethernet, este só funciona sobre fibra óptica. Mesmo sendo ao nível MAC idêntico ao GbEthernet, haverá dois tipos de interfaces físicas diferentes:

1) PHY WAN: Para entornos de área ampla SDHs existentes. Nesta interface se adiciona uma camada "leve" de SDH (SDH *framing*). Opera a 9,953 Gbps (OC-192c/STM-64c). É assíncrona como o SDH.
2) PHY LAN: Para entornos de área local. Opera a 10,3 Gbps, e é similar ao existente.

Placas de linha Gigabit Ethernet podem custar 5 vezes menos que placas de linha SDH [PARETA, 2006].

2.4.5.1 10-Gigabit Ethernet (10GbE)

IEEE 802.3ae foi adaptado para incluir transmissão *full-duplex* a 10Gbps sobre cabo de fibra óptica. As similaridades básicas entre 802.3ae e 802.3 são notórias. Esta tecnologia foi desenvolvida não só para LANs, mas também para MANs e WANs [HELD, 2005].

Com o formato de *quadro* e outra especificação Ethernet camada 2, compatível com os padrões prévios, 10GbE pode prover incrementos de largura de banda interoperáveis com a existente infra-estrutura de rede.

A compatibilidade com redes SONET/SDH operando acima de velocidades de OC-192 (9,584640 Gbps) faz de 10GbE uma tecnologia WAN viável [ITU-T G.709, 2001]. A Figura 2.18 apresenta uma configuração típica de rede IP/GbEth/WDM. Interfaces GbE nos ADMs permitem que comutadores GbE possam inserir/receber dados de roteadores IP.

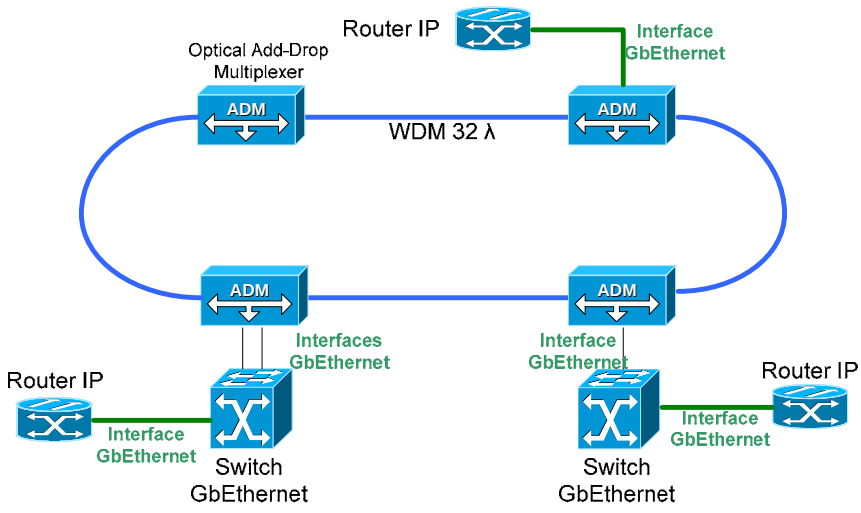


Figura **2.18** - Configuração típica de uma rede IP/GbEth/WDM

O 10GbE compete com ATM em algumas aplicações. De uma forma geral, 10GbE comparado com outras variedades de Ethernet apresenta as seguintes características:

- O formato de quadro é o mesmo, isto permite interoperabilidade entre todos os tipos de Ethernet: legado, *Fast*, Gigabit, 10Gigabit, sem *re-framing* ou conversão de protocolo;
- O tempo de bit (*bit time*) é de 0,1 nanosegundos;
- Dado que são estabelecidos circuitos baseados em fibra, CSMA/CD não é necessária;
- As subcamadas IEEE 802.3 dentro das camadas 1 e 2 do modelo OSI são preservadas, com algumas adições, para acomodar enlaces de fibra a 40 km e interoperabilidade com tecnologia SONET/SDH;
- Redes Ethernet flexíveis, eficientes, confiáveis e de relativo baixo custo fim-a-fim se tornam possíveis; [JAEGER, 2006]
- TCP/IP pode rodar sobre LANs, MANs, e WANs com um método de enlace camada 2.

Vantagens:

- Multiplexação estatística (eficiente e flexível uso da largura de banda);
- Tamanho de quadro = Tamanho de pacote. Comutação de pacotes mais eficiente e fácil de implementar;
- Tecnologia *Broadcast*;
- Formato de dados consistente com formato LAN;
- Gerência *padrão* SNMP/MIBs, mas também accessível por TMN;
- *Padrão* interoperável com muitos fabricantes;
- Não *scrambling*;

A Tabela 2.10 mostra o *overhead* inserido quando se deseja transmitir pacotes usando-se esta proposta.

Tabela 2.10 - *Overhead* inserido pela proposta IP/GbEth

	Tamanho de Pacote	**Overhead cumulativo**	**Comentários**
Pacote IP	350	0%	
GbE	388	10%	GbE *framing*: 38 bytes/pacote
Código de Linha	485	28%	8B/10B da 1,25 Gbps
1 GbE link provistos			902 Mbps de capacidade

Desvantagens:

- Código de Linha 8B/10B (perda de eficiência de 20%). Porém, 10Gigabit Ethernet usa codificação mais eficiente (64/66);
- A gerência ou monitoramento "*out of band*" é não *padrão*, porém WDM supre a carência provendo esta funcionalidade;
- As capacidades de proteção/restauração são ineficientes.

Ethernet geralmente confia no protocolo *Spanning Tree* para eliminar todos os *loops* de uma rede comutada. Ainda que o protocolo *Spanning Tree* possa ser utilizado para alcançar redundância de caminho, este se recupera lentamente desde uma ruptura de fibra, comparado com outros mecanismos de recuperação de falha. *Link aggregation* (802.1ad) pode prover uma solução, mas é comparativamente lento (~500 ms vs. ~50 ms providos por SDH/SONET) e não é apropriado para promover proteção a nível de caminho.

Então, para reduzir o número de camadas e redistribuir as suas funcionalidades nas outras camadas, sempre que possível, se tem propostas de novas arquiteturas baseadas em IP/WDM, com IP/ASON-GMPLS, IP/OBS (*Optical Burst Switching*) e IP/OPS (*Optical Packet Switching*). A Figura 2.19 mostra uma visão da evolução da arquitetura de transporte óptica.

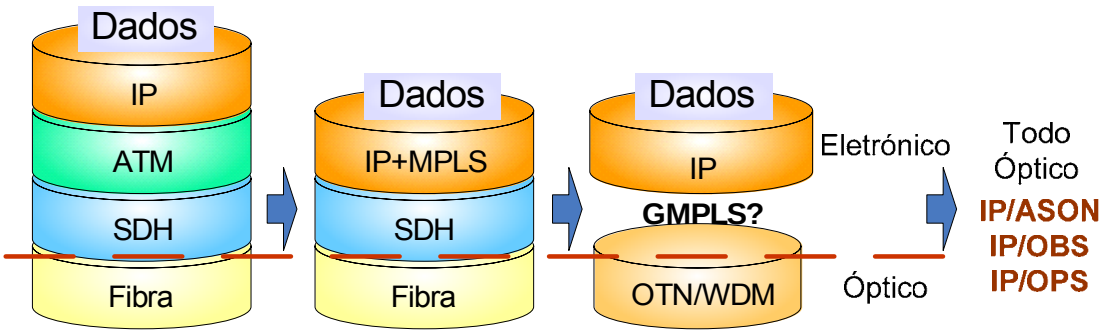


Figura **2.19** – Evolução da Arquitetura de Transporte Óptica

2.5 IP SOBRE OTN BASEADO EM WDM

A multiplexação estatística de pacotes surge como a tecnologia de multiplexação predominante para o cada vez mais crescente fluxo de dados, já que permite um melhor aproveitamento da largura de banda.

Como se tem visto, SDH não provê muita flexibilidade em termos de expansão de capacidade e controle, e ATM se tem mostrado ineficiente em termos de excesso de *overhead*. Estes são alguns dos motivos da migração das redes *backbone* IP para transporte direto sobre OTN com tecnologia WDM.

WDM é uma tecnologia com maturidade para desenvolver também funcionalidades de rede por meio de outros elementos de rede óptica tais como OADM e OXC. Através da tecnologia DWDM, o OTN pode prover uma alta soma de largura de banda suportando a entrega de grandes volumes de tráfego IP.

2.5.1 Tecnologia WDM (*Wavelength Division Multiplexing*)

A instalação de mais fibras para suportar a demanda sem precedentes por maior capacidade originada pela Internet é muito cara. Incrementar a taxa de transmissão do sistema TDM não provê muita flexibilidade. A multiplexação por comprimento de onda se apresenta como o caminho mais adequado.

A tecnologia WDM supera muitas dificuldades de implementação e restrições que limitam o desempenho dos sistemas TDM. Assim, em lugar de incrementar a taxa de dados para manipular mais informação, WDM simplesmente transporta vários sinais ópticos, cada um deles em um comprimento de onda e na sua respectiva taxa de transmissão, todos eles sobre uma mesma fibra.

Esta estratégia é similar aos antigos enlaces de comunicações, os quais utilizavam a multiplexação por divisão de freqüência (FDM), na qual a multiplexação de canais era realizada se alocando faixas de freqüência para cada canal e transmitindo-os em um único meio de transmissão. Na multiplexação por comprimento de onda cada canal é associado a um comprimento de onda específico e transmitido via uma única fibra, se criando múltiplas fibras virtuais. Isso proporciona um grande aumento na largura de banda disponível, mantendo-se a infra-estrutura de fibra existente e maximizando seu uso.

A Figura 2.20 apresenta um sistema óptico típico com tecnologia WDM. Observe que a tecnologia TDM pode ser usada para multiplexar/demultiplexar dados para cada um dos canais WDM, otimizando ainda mais a informação a ser transportada.

Vantagens de WDM

- Permite incrementos flexíveis de capacidade: Por exemplo,

  – Granularidade SONET: 51 Mbps, 155 Mbps, 466 Mbps, 622 Mbps, etc;
  – Granularidade SONET/WDM: 51 Mbps, 2x51 Mbps, 3x 51 Mbps, 4x 51 Mbps, etc;

- Maximiza o re-uso e minimiza o custo do ciclo de vida das instalações de fibra existente. Por exemplo: WDM pode ser usado para prover quatro interfaces OC-12 (622 Mbps) IP/ATM/SDH num único par de fibras. Para alcançar a mesma capacidade, sem WDM, seriam necessários quatro pares de fibra.

- Provê solução de transporte para sinais TDM de alta capacidade. Para roteadores Gigabit emergentes com interfaces de alta velocidade (ex. OC-48), a existente infra-estrutura de transporte pode se transformar num gargalo.

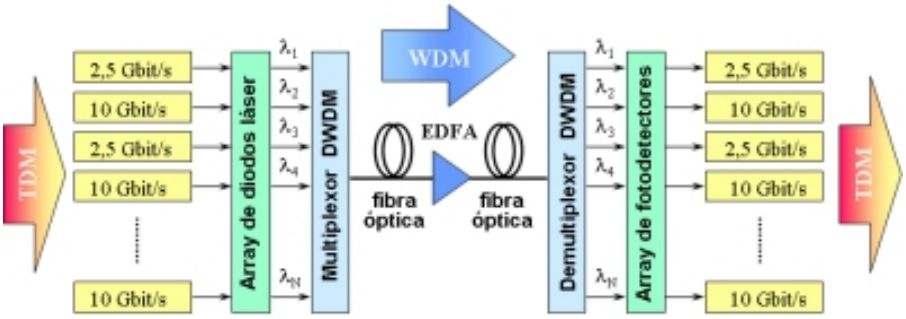


Figura **2.20** - Sistema óptico com tecnologia WDM típico

- WDM é uma solução de excelente custo-benefício que toma vantagem da capacidade comercial da fibra. Uma fibra servindo como meio de transporte para um circuito OC-12 (622 Mbps) está usando só 0,4% da capacidade da fibra para 16 comprimentos de onda e 0,2% para 32 comprimentos de onda.

- Permite a co-existência de múltiplos tipos de interface na mesma fibra:

  – IP/ATM/SDH;
  – IP/PPP/HDLC/SDH;
  – Alguma tecnologia futura.

Estas e outras vantagens têm levado ao dramático incremento do número de comprimentos de onda no mesmo cabo, resultando em um espaçamento entre canais cada vez mais

estreito que caracteriza uma nova classe dentro da tecnologia WDM denominada "WDM densa" (DWDM), apresentando acima de 16 canais com os respectivos comprimentos de onda, ampliados para 32 canais no final da década dos 90 [ALFERNESS, 1999].

Maiores capacidades de transmissão alcançáveis com DWDM vêm sendo experimentadas pela academia e pela indústria. Em [GNAUCK, 2006] é conseguida uma taxa de 12,3 Tbps de capacidade de transmissão, com uma eficiência espectral de 3,2 bps/Hz, sobre 77 canais WDM espaçados de 50 GHz, e só usando a banda C, sobre 240 Km de fibra.

Em [FABREGAS, 2006] tecnologia *Ultra-Dense* WDM, com espaçamento entre canais de 3GHz e 1 Gbps de capacidade por canal, com potencialmente 1280 portadoras por fibra sobre 25Km de enlace é apresentada e experimentalmente demonstrada.

A multiplexação por divisão "grossa" de comprimento de onda (CWDM: *Coarse* WDM) é outra classe dentro da tecnologia WDM. Foi utilizada no início dos anos 80 para aplicações em redes Metro, como no transporte de sinais de vídeo (CATV) sobre fibra multimodo. Foi padronizado pela ITU-T sob a norma ITU-T G.694.2 no ano 2002. Possui um intervalo freqüencial de 2.500 GHz (20nm), o qual permite um máximo de 18 comprimentos de onda, definidos no intervalo de 1270 a 1610 nm. Os CWDM atualmente tem seu limite em 2,5 Gbps, tendo um alcance típico de cerca de 80 Km. Suas aplicações estão nos serviços de curto alcance como: SDH, CATV, ATM, FTTH–PON, 10GibagitEth, entre outros.

2.5.2 Evolução da Tecnologia de Transporte sobre WDM

De maneira similar às redes de transporte sobre cobre, uma das primeiras topologias de Transporte sobre WDM foi a configuração ponto-a-ponto. Esta topologia é caracterizada por velocidades de canal ultra-altas, confiabilidade e proteção. O uso de amplificadores ópticos permite a transmissão de sinais ópticos em enlaces com milhares de quilômetros sem qualquer conversão eletro-óptica.

Posteriormente, topologias de redes ópticas em anel baseadas em tecnologia WDM passaram a fazer parte do cenário das redes de transporte. Configurações em anel podem ser desenvolvidas com um ou mais nós OADMs (multiplexadores *add/drop* ópticos), que fazem a seleção dos comprimentos de onda a serem inseridos ou retirados do anel. A Figura 2.21 ilustra a chamada "primeira geração" das redes de transporte sobre WDM [SATO, 2002].

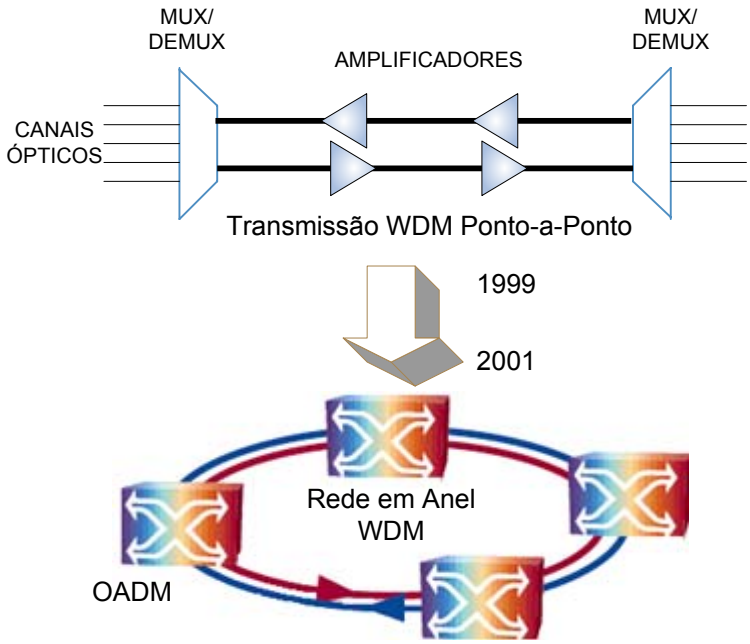


Figura **2.21** - Primeira geração das redes de transporte fotônicas.

Na geração seguinte, Figura 2.22, foram introduzidos os OXCs ou chaves ópticas, fundamentais na arquitetura de uma rede totalmente óptica. O OXC pode comutar um sinal óptico, desde N portas de entrada para N portas de saída, sem fazer qualquer tipo de conversão eletro-óptica.

Um outro sistema orientado a IP, o roteador fotônico é também uma grande opção para a nova geração de redes ópticas. Dois tipos são possíveis: o roteador fotônico MPLS [SATO2, 2002], que usa o comprimento de onda como rótulo para *bit-streams* de camada física; e o roteador fotônico que usa comprimentos de onda para rotular cada rajada (*burst*) ou cada pacote de informação.

Assim, três tecnologias de comutação óptica têm sido propostas para o transporte de tráfego IP sobre WDM: Comutação de Circuitos Ópticos (*Optical Circuit Switching* – OCS), Comutação de rajadas Ópticas (*Optical Burst Switching* – OBS) e Comutação de Pacotes Ópticos (*Optical Packet Switching* – OPS).

A Comutação de Circuitos Ópticos (OCS) é uma tecnologia já madura que usa *lightpaths* como circuitos ópticos estabelecendo um caminho roteado em comprimento de onda. Este caminho permite a transmissão e comutação de capacidades fixas, não fazendo uso de multiplexação estatística e tirando assim pouco proveito das enormes capacidades (2,5Gbps, 10Gbps ou 40Gbps) que oferece a largura de banda dos sistemas ópticos (pouca

granularidade). Se o aprovisionamento de rotas requer intervenção manual do administrador da rede, a rede é dita "estática".

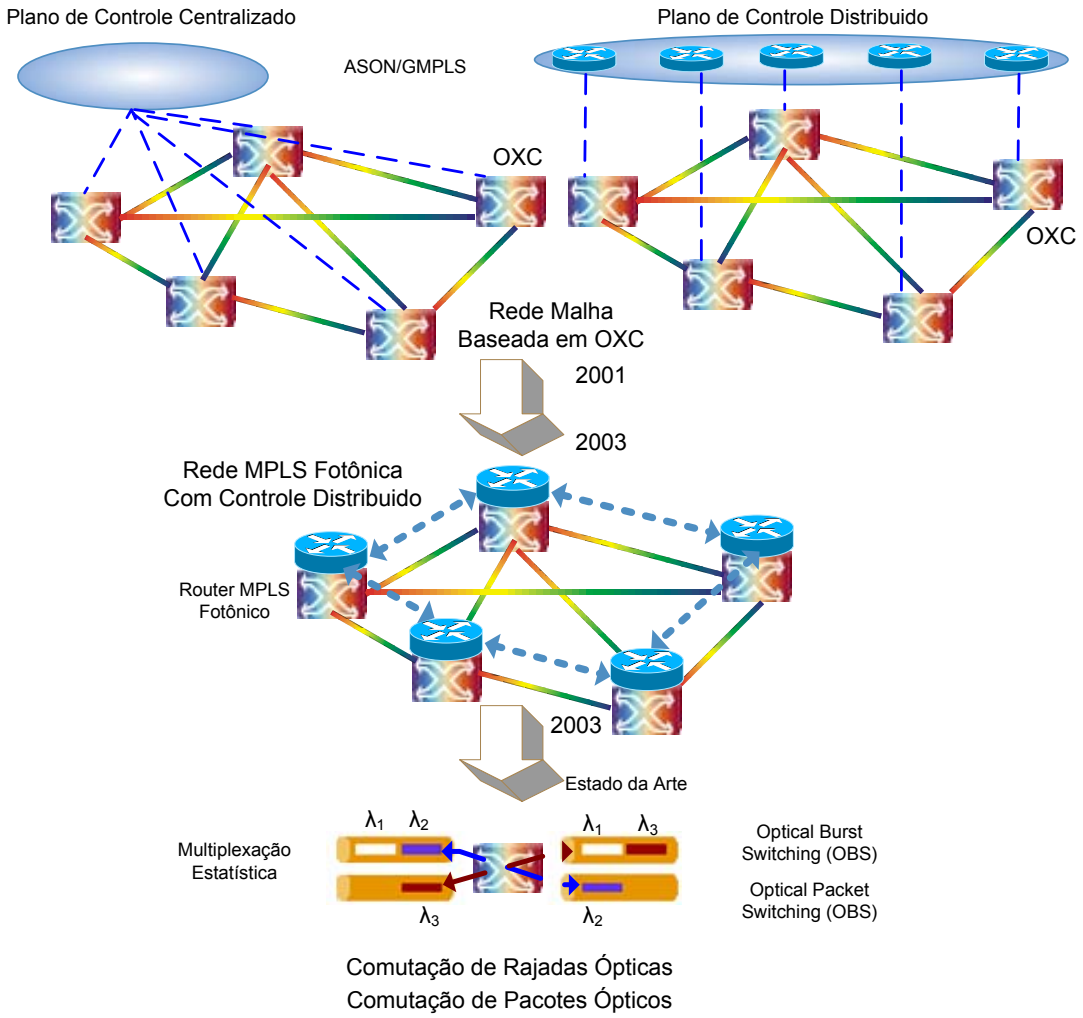


Figura **2.22** - Segunda geração das redes de transporte fotônicas.

Um avanço significativo é a automatização do processo de estabelecimento de rota. Processos de sinalização precisam ser introduzidos no domínio óptico para viabilizar estas redes ditas "dinâmicas", e conhecidas também como ASON ou ASTN (*Automatic Switched Transport Nework*) [NORTEL, 2001]. A introdução de um Plano de Controle é necessária para permitir o transporte de IP diretamente sobre WDM. Este trabalho de Tese tem como cenário uma rede do tipo OCS.

Na comutação óptica de pacotes [XU, 2001], a informação contida em cabeçalhos específicos (rótulos) pode ser usada para que se decida como o pacote será comutado em cada nó da rede. O comprimento do *payload* define a quantidade de dados que está sendo

transmitida em cada pacote, o que resulta numa granularidade mais fina. Assim, a tecnologia WDM está evoluindo para tecnologias como OBS e OPS, as quais suportam diretamente IP sobre WDM. Ambas tecnologias de comutação têm sido testadas como protótipos e estão em processo de otimização contínua, sendo ainda bastante custosa a sua implementação. Em compensação, estas redes utilizam eficientemente os recursos de largura de banda quando comparado com o OCS, pelo uso da multiplexação estatística.

Em redes OPS [RENAUD, 1997], a entidade de comutação básica é o pacote. A comutação de pacotes ópticos requer memória óptica. A memória óptica efetiva ainda não existe, e isto representa uma séria dificuldade para o desenvolvimento desta técnica. A carga útil é opticamente retardada usando fibras de retardo (FDL), segmentos de fibra, de comprimento proporcional, para emular os processos de memória [JUNYENT, 2006]. Posteriormente, a informação é comutada desde a porta de entrada para a porta de saída do nó. No momento, redes OPS suportam pacotes de tamanho fixo devido a problemas de sincronismo. Aqui o cabeçalho e a carga útil são enviados juntos. Ao alcançar um nó, o cabeçalho é extraido e processado eletronicamente.

Em redes OBS, a entidade de comutação básica é a rajada (*burst*) o qual contém um certo número de pacotes IP com destinos comuns. Um caminho óptico existe só pela duração do *burst*. O cabeçalho e a carga útil (*payload*) são transmitidos em separado com um intervalo de tempo pequeno entre ambos, permitindo que a parte de controle reserve primeiro os recursos a serem utilizados pelo *burst* de carga útil. Usualmente comutação óptica de rajadas requer um mecanismo de gerência de recursos rápido para minimizar as colisões de rajadas em um nó.

2.5.3 Evolução dos mecanismos de Encaminhamento sobre WDM

Acima da OTN, porém, os esforços estão focados principalmente nos mecanismos de encaminhamento. Como temos visto, nos primeiros estágios, roteadores IP eram interconectados usando serviços *leased-line* para produzir configurações ponto a ponto (IP sobre SDH). Posteriormente, foram desenvolvidos roteadores IP eletrônicos para taxas da ordem dos terabits por segundo, para interconectar estes com enlaces DWDM de grande capacidade (IP sobre SDH sobre DWDM). Logo, foi interessante ter conexões de roteadores usando rotas e canais virtuais sobre redes do tipo malha (IP sobre ATM), o qual colocou as bases para a engenharia de tráfego na rede.

Para implementar gerência integrada de camada 2 e 3, e assim integrar IP com ATM e outras tecnologias de camada de enlace, foi desenvolvido o MPLS, que oferece capacidade de comutação orientada à conexão com base em protocolos de roteamento e sinalização IP.

O próximo passo na evolução do backbone IP envolve IP sobre DWDM e MPLS fotônico. Comprimentos de onda são usados como rótulos, acomodando pacotes IP que trafegam pela mesma rota. O roteador MPLS fotônico comuta os caminhos ópticos. Assim, roteadores IP reconhecem roteadores MPLS fotônicos [CINCOTTI, 2006] [YAMANAKA, 2003], e integram operações de roteamento e sinalização. A Figura 2.23 mostra a evolução dos diferentes mecanismos de encaminhamento para permitir IP diretamente sobre WDM.

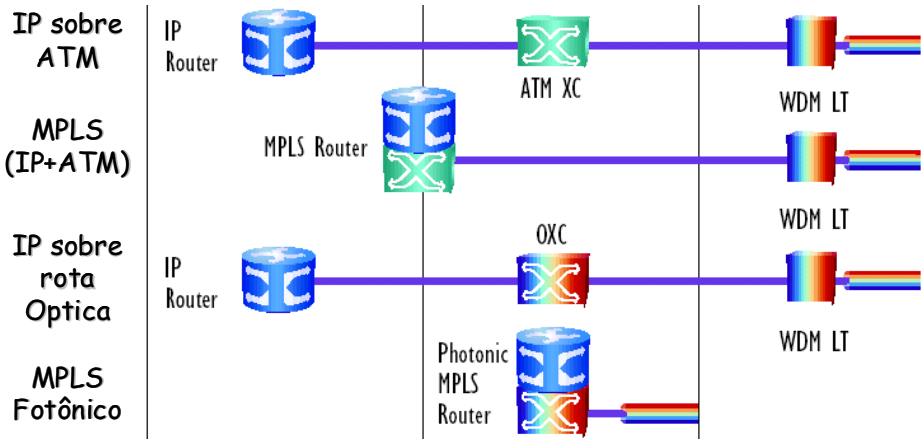


Figura **2.23** - Evolução dos mecanismos de encaminhamento (Modificado [Sato, 2002]).

2.5.4 Arquitetura da rede IP sobre WDM

Para a transmissão e comutação de datagramas IP, de natureza assíncrona e de tamanho variável, sobre uma rede todo-óptica baseada em comutação de circuitos ópticos (canais ópticos ou comprimentos de onda), de capacidades fixas e de natureza síncrona, é necessário atender certos requisitos.

As características que são desejáveis para adaptar datagramas IP a serem transmitidos sobre redes OTN baseadas em WDM são:

- Delimitação e sincronização da informação;
- Mecanismos de Proteção;
- Eliminar o excesso de *overhead*;
- Capacidades de monitoração de desempenho e erro;
- Engenharia de Tráfego e QoS.

Desempenho através de engenharia de tráfego inclui dois aspectos: orientado ao tráfego e orientado a recursos. Na orientação ao tráfego se objetiva minimizar o número de pacotes perdidos, maximizar a vazão (*troughput*) da rede e introduzir QoS. Quando a engenharia de tráfego está mais orientada a recursos procura-se aperfeiçoar a eficiência no uso dos recursos da rede. Um balanço entre tais objetivos é o desejado.

A Figura 2.24 apresenta a desejável eliminação de *overhead* pela supressão de camadas intermediárias e alguns benefícios que podem ser obtidos ao transmitir IP diretamente sobre OTN.

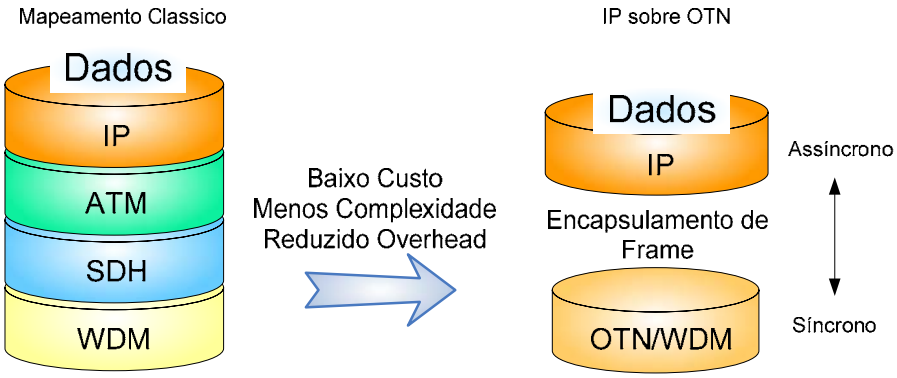


Figura **2.24** – Arquitetura IP sobre OTN

Como temos visto, a infra-estrutura de transporte está se movimentando na direção dos serviços da Internet e das respectivas necessidades de largura de banda. Embora WDM tenha sido muito utilizada para incrementar a capacidade de transporte, em cenários IP/OTN algumas funcionalidades de rede são implementadas diretamente sobre a camada óptica através de um Plano de Controle responsável pelas funções de roteamento e sinalização. É consenso entre fabricantes, provedores e pesquisadores que um plano de controle, centrado em IP, é necessário para a rede óptica dar suporte de aprovisionamento dinâmico, engenharia de tráfego e recuperação de caminho óptico. Contudo, ainda permanece a questão de como os roteadores IP devem interagir com a OTN para alcançar conectividade fim-a-fim.

2.5.5 Plano de Controle IP/WDM

Em redes ópticas comutadas por circuitos cada elemento da rede que pertence ao plano de transporte pode ser controlado por um plano de controle. Os protocolos associados estão sendo padronizados pela OIF, IETF e ITU-T [SAHA, 2003]. O plano de controle pode ser

configurado como centralizado, onde todo o controle está centralizado numa única entidade administrativa; ou distribuído, onde o controle é distribuído em cada um dos nós da rede. As Figuras 2.25 e 2.26 apresentam estas configurações.

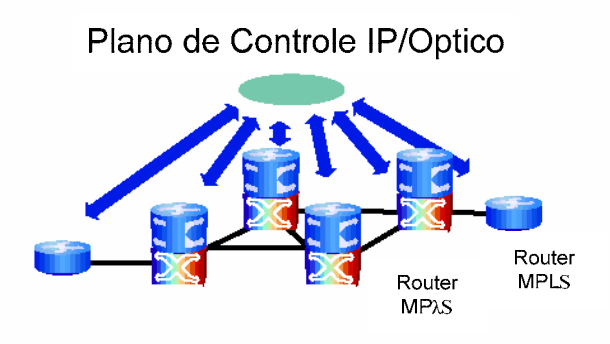


Figura **2.25** - Plano de Controle Centralizado.

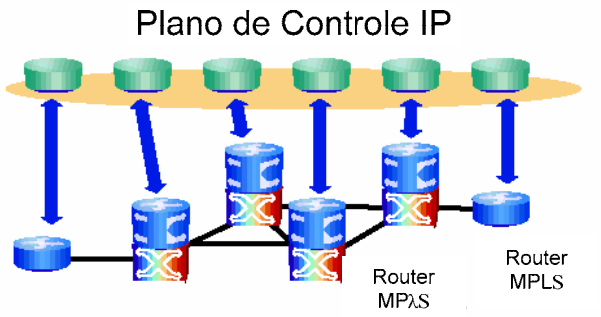


Figura **2.26** - Plano de Controle Distribuído.

2.5.5.1 Funções do Plano de Controle

As principais funções do plano de controle são:

- ***Descoberta do vizinho***: Função pela qual um elemento de rede determina automaticamente os detalhes de sua conectividade a todos seus vizinhos do plano de dados. Esta informação inclui a identidade dos vizinhos, a identidade das terminações do enlace, etc.
- ***Encaminhamento***: O encaminhamento cobre dois aspectos:
  1. Estabelecimento automático da topologia e a descoberta de recursos, que permite aos agentes de controle ter uma visão local da conectividade do plano de dados e a disponibilidade dos recursos na rede. Este procedimento implica num mecanismo para inundar a informação de conectividade do enlace para todos os agentes de controle da rede.

2. O cálculo do caminho, que é um procedimento pelo qual um agente de controle determina um caminho para uma conexão usando a topologia disponível e a informação dos recursos.

- ***Sinalização***: Indica a sintaxe e a semântica da comunicação entre agentes de controle no estabelecimento e manutenção das conexões. Para tal, se faz uso de protocolos de comunicação. Tais protocolos, atualmente, buscam ser abertos e padronizados.
- ***Gerência de recursos locais***: Encarregado da administração dos recursos localmente disponíveis e controlado por um agente específico, que também tendem a serem padronizadas por protocolos específicos (por exemplo, SNMP).

A OTN é incapaz do processamento individual de pacotes. A interação entre roteadores IP e a OTN demanda uma interface de roteamento e sinalização bem definida conhecida como Interface Usuário-Rede (UNI: *User-Network Interface*). Por outro lado, sub-redes ópticas de diferentes domínios e provedores, pertencentes à OTN, interagem por meio de uma interface de roteamento e sinalização bem definida conhecida como Interface Rede-Rede (NNI: *Netwok-Network Interface*) [RAJAGOPALAN, 2000] [METZ, 2000] [OIF, 2000]. Estes aspectos de arquitetura são apresentados na Figura 2.27

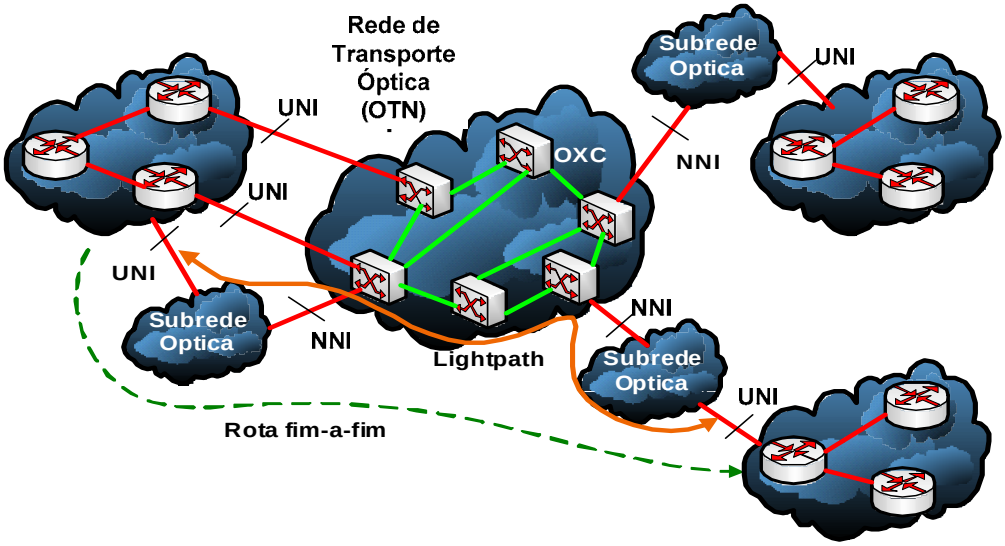


Figura **2.27** - Interfaces na Arquitetura IP/OTN-WDM

A base para a infra-estrutura todo-óptica é construída sob o conceito de roteamento de comprimento de onda (*wavelength routing*) [ROUSKAS, 2002]. Uma rede deste tipo consiste de comutadores de comprimento de onda OXCs (*optical cross-connects*)

interconectados por um conjunto de enlaces de fibra formando uma topologia malha arbitrária. Os serviços que esta rede oferece a redes clientes estão sob a forma de conexões lógicas que são implementadas usando *lightpaths*.

A OTN, em síntese, provê conectividade ponto-a-ponto entre estes roteadores cliente, geralmente IP, com *lightpaths* de largura de banda fixa. O conjunto de *lightpaths* define a topologia da rede virtual interconectada. Esta topologia pode ser estática, que neste caso pode ser provisionada manualmente pelo administrador, não sendo necessários protocolos de sinalização para a interface IP-OTN.

Para a topologia mudar dinamicamente serão necessários protocolos de sinalização tanto para a UNI quanto para a NNI. Outro serviço que a OTN oferece ao cliente é a recuperação automática de caminho óptico nos casos de falhas de rede, tema que será abordado em extenso no Capítulo 4 e centro deste trabalho de Tese.

2.5.6 Modelos de Implantação de Rede Óptica

Tem-se três modelos de rede: o modelo *Overlay*, o modelo *Peer* e o modelo híbrido [RAJAGOPALAN, 2000] [METZ, 2000] [COMELLAS, 2003].

No modelo *overlay* os protocolos de roteamento e sinalização das redes IP são independentes dos correspondentes protocolos da OTN. Este modelo apresenta uma relação cliente-servidor, onde a rede IP (cliente) requisita serviços de transporte da rede OTN (servidor). A vantagem do modelo *overlay* é a sua implementação relativamente simples. Sua desvantagem é que requer a criação e gerência de adjacencias de roteamento sobre a rede óptica. A Figura 2.28 apresenta a arquitetura deste modelo.

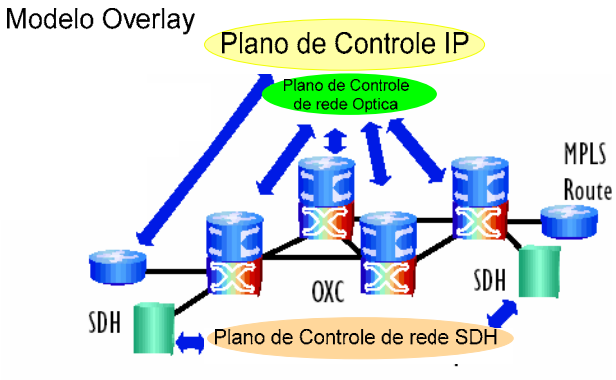


Figura **2.28** - Arquitetura do Modelo *Overlay*

No modelo *Peer*, as redes IP e óptica são tratadas como uma única rede integrada, com gerência e engenharia de tráfego unificada. Os OXC são tratados como qualquer outro roteador pelo plano de controle. Do ponto de vista de roteamento e sinalização, não existe diferença entre as interfaces UNI e NNI ou qualquer outra interface *roteador-roteador* [METZ, 2000].

No modelo *Peer*, um único protocolo de roteamento roda sobre ambos os domínios das redes (IP e óptico), assim cada camada tem pleno conhecimento da outra. Esse plano de controle único é possível a partir do advento do GMPLS. A colaboração de ambas camadas nos processos de roteamento leva a otimização do desempenho da rede. A desvantagem desse modelo é a necessidade de informação de roteamento específica para redes ópticas a ser conhecida pelos roteadores. A Figura 2.29 apresenta a arquitetura do modelo *Peer*.

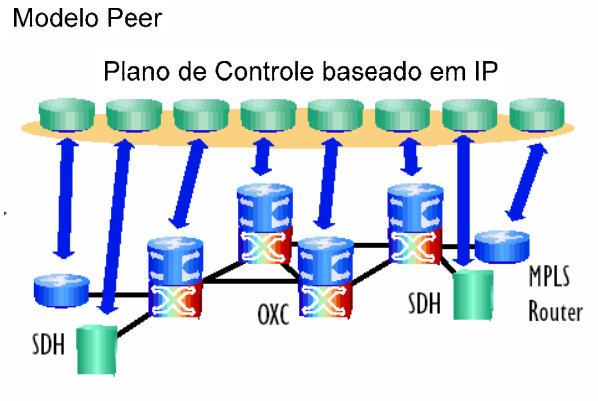


Figura **2.29** - Arquitetura do modelo *Peer*.

No modelo híbrido (interdomínio ou *augmented*), há instâncias de roteamento separadas nos domínios IP e óptico, porém a informação de uma instância de roteamento é repassada por meio da outra instância de roteamento. Por exemplo, endereços IP serão transportados pelos protocolos de roteamento ópticos para permitir que a informação seja alcançada pelos clientes IP. Este modelo combina o melhor dos modelos de interconexão *Peer* e *Overlay*. É mais simples de implementar que o modelo *Peer* e não requer gerência de interfaces de roteamento sobre a rede óptica, como acontece no modelo *Overlay*.

2.5.7 Serviços de Transporte Ópticos

Os serviços de transporte ópticos podem ser classificados como *Permanent, Soft Permanent* e Comutado. É chamado de *Permanent* quando os serviços são estabelecidos a partir do sistema de gerência da rede com protocolos de gerência (NMI). É dito *Soft Permanent* quando os serviços são estabelecidos desde o sistema de gerência, o qual utiliza

protocolos de sinalização e roteamento (NNI e NMI). Por último, é dito comutado (*Switched*) quando os serviços são estabelecidos pelo cliente sob demanda, através de protocolos de sinalização e roteamento (UNI e NNI).

2.6 REDES ÓPTICAS COMUTADAS AUTOMATICAMENTE (ASON)

Os organismos de padronização em redes ópticas definiram um primeiro modelo de rede chamado de ASON (*Automatic Switched Optical Network*), desenvolvido pelo grupo de estudo 15 da ITU-T na Rec.8080, em resposta à demanda dos membros da ITU para criar uma definição completa da operação das redes de transporte comutadas automaticamente, principalmente no que diz respeito a seu plano de controle [JAJSZCZYK, 2005] [BLACK, 2002] [TOMSU , 2002].

Enquanto redes baseadas em tecnologia SDH oferecem só capacidade de transporte, a ASON permitirá o estabelecimento e liberação de canais ópticos de forma automática. Para atingir esta funcionalidade a definição de um plano de controle óptico é necessária, o qual será o responsável por realizar as funcionalidades de sinalização e roteamento.

Diferente das propostas da IETF (MPλS, GMPLS), onde os padrões para o plano de controle evoluem a partir de protocolos já existentes, a ITU projetou a arquitetura desde o princípio. Assim, enquanto GMPLS está fortemente associado com as redes IP, os membros da ITU, que vêm do mundo das *operadoras,* agregam em seus projetos os conceitos de protocolos usados em redes de transporte de telecomunicações, tais como SDH e ATM.

ASON não é um conjunto de protocolos, é uma arquitetura que define os componentes num plano de controle e as interações entre esses componentes. Sendo uma arquitetura de referência, ASON não é diretamente implementada [LARKIN, 2002].

Os padrões relacionados com ASON são:

- Arquitetura para ASON (G.8080, formalmente conhecida como G.ason);
- Controle de conexão e chamada (G.7713 - G.dccm), o qual também da cobertura aos aspectos de sinalização;
- Arquitetura e requisições para roteamento na ASON (G.7715 - G.rtg);
- Técnicas de descoberta automática (G.7714 - G.disc).

2.6.1 Arquitectura lógica ASON

A arquitectura lógica de uma rede ASON é formada por 3 planos funcionais: o Plano de Transporte, o Plano de Controle e o Plano de Gerência.

Plano de Transporte (*Transport Plane*)

Este plano é formado por uma rede de transporte óptica (OTN) que provê canais ópticos unidirecionais ou bi-direcionais entre usuários e detecta informação do estado das conexões (detecção de falhas, qualidade do sinal, etc).

Plano de Controle (*Control Plane*)

Suporta o estabelecimento/eliminação das conexões como resultado de uma requisição dos clientes da rede (conexão comutada) ou de uma solicitação do sistema de gerência (NMS: *Network Management System*), em conexões *soft-permanents*.

Plano de Gerência (*Management Plane*)

Faz as funções de gerência (gerência de falhas, configuração, contabilidade e segurança) para os planos de transporte e de controle.

A arquitetura ASON é apresentada na Figura 2.30.

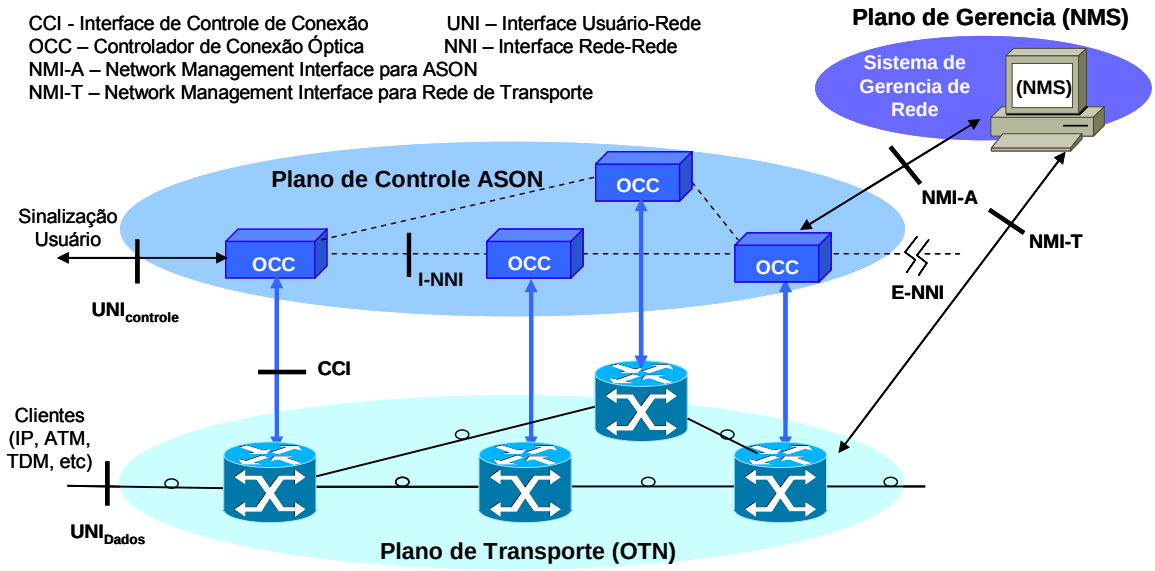


Figura **2.30 - A**rquitetura ASON

2.6.2 Plano de Controle ASON

O plano de controle óptico de uma ASON tem como função principal dotar de inteligência a rede de transporte óptica [ITU-T - G.872, 2001], permitindo, através de protocolos de roteamento e sinalização, o aprovisionamento (estabelecimento e eliminação) dinâmico e flexível de canais ópticos, engenharia de tráfego (TE) para RWA, proteção/restauração óptica automática, qualidade de serviço e redes privadas virtuais ópticas (OVPN) [JUNYENT, 2004].

O plano de controle pode estar baseado em protocolos IP ou em ATM. A IETF sugeriu basear o plano de controle em protocolos de roteamento e sinalização IP, particularmente no plano de controle MPλS. Posteriormente foi proposto o GMPLS [MANNIE, 2004], o qual tomou como base os protocolos *Link Management Protocol* (LMP) [LANG, 2005] como protocolo de descoberta do vizinho; o *Open Shortest Path First* (OSPF) [KOMPELLA, 2005], ou *Intemediate System-Intermediate System* (IS-IS) [KOMPELLA2, 2005] como protocolos de descoberta de recursos e topologia da rede óptica; e o *Resource Reservation Protocol-Traffic Engineering* (RSVP-TE) [DRAKE, 2005] ou *Constraint-Based Routing Label Distribuition Protocol* (CR-LDP) [ASHWOOD-SMITH, 2002], como protocolos de sinalização. Também, se tem proposto basear o plano de controle em protocolos ATM, como o *Private Optical NNI* (PONNI ou PNNI) [PARETA, 2002] [SÁNCHEZ, 2003].

2.6.3 Multiprotocol Lambda Switching (MPλS)

Para viabilizar a conjugação do MPLS e da tecnologia de transporte óptica em uma única rede são necessárias adaptações nos comutadores MPLS (chamados de LSR: Label Switch Router) e nos comutadores ópticos (OXC). Desta forma, as redes tendem a convergir para o modelo de duas camadas com uma adaptação conveniente do IP para inclusão de QoS, características de engenharia de tráfego e mecanismos de proteção e restauração, através de um plano de controle [MURTHY, 2002].

O MPλS [AWDUCHE, 2001] descreve um plano de controle ASON centrado em IP baseado numa extensão do MPLS direcionado para redes DWDM, tornando os elementos da rede aptos a suportar altas taxas de dados. MPλS fornece também uma estrutura orientada à conexão para o protocolo IP, tornando mais fácil a incorporação de QoS e engenharia de tráfego na Internet e outros serviços IP.

Sob a influência das técnicas desenvolvidas para o MPLS, esta proposta considera a tecnologia OXC para administrar o aprovisionamento em tempo real dos canais ópticos e permitir o uso de semântica uniforme para gerência de rede e operações de controle em redes híbridas, com elementos de rede OXCs e roteadores de comutação de rótulos. MPλS permitirá gerência da largura de banda no canal óptico e o seu aprovisionamento dinâmico, assim como sobrevivência da rede por meio de capacidades melhoradas de proteção e restauração.

Da mesma forma que MPLS, MPλS se baseia apenas em rótulos para definir o próximo salto. Assim, não é necessário subir até a camada de rede para processar endereços IP. Esse rótulo funciona como um índice na tabela de roteamento e é muito mais eficiente que as tabelas tradicionais. O comprimento de onda, usado como rótulo, é o identificador único e possibilita a roteadores e comutadores realizar as funções de encaminhamento.

O plano de controle MPλS tem topologia fixa e é separado do canal de dados. O plano de controle para OXC usa protocolos IP estendidos para distribuir a informação de estado relevante da rede de transporte óptica, incluída a informação de estado da topologia. Esta informação de estado é usada por um sistema de roteamento baseado em restrições, para calcular os caminhos dos canais ópticos ponto a ponto. O plano de controle de OXC usa um protocolo de sinalização de MPLS para os canais ópticos ponto a ponto. Dessa forma, pacotes IP podem ser diretamente transportados sobre redes DWDM.

Uma diferença básica entre MPLS e MPλS é o nível de granularidade: MPλS controla *lambdas*, enquanto que MPLS controla fluxos de pacotes, que podem ser transportados em *lambdas*.

Posteriormente ao MPλS, surgiu o GMPLS (G*eneralized MultiProtocol Label Switching*) como uma solução de convergência tecnológica, de engenharia de tráfego e QoS para a rede de transporte.

2.6.4 Generalized Multiprotocol Label Switching (GMPLS)

O GMPLS [MANNIE, 2004] é um conjunto de protocolos estendidos de MPLS e MPλS em um plano de controle comum, tanto para redes ópticas como eletrônicas, que é necessário para a convergência na próxima geração de redes IP sobre DWDM. GMPLS é um desenvolvimento da IETF e, como tal, usa um plano de controle baseado em IP. O

Grupo de trabalho CCAMP (*Common Control and Management Plane*) cuida das atualizações e melhorias deste paradigma.

GMPLS estende MPLS e MPλS incluindo também a comutação por divisão no tempo para dar suporte a tecnologias como SONET/SDH [PAPADIMITRIOU, 2003]; além de aprimorar o plano de controle para tecnologias de comutação de comprimentos de onda (*lambdas*), espacial (porta/fibra) e pacotes/células.

A generalização proporciona um plano de controle ASON comum e padronizado, necessário para a evolução de redes ópticas abertas e interoperáveis. Um plano de controle comum simplifica as operações e a gestão, o que reduz o custo das operações e proporciona uma ampla faixa de cenários de desenvolvimento.

O principal foco de GMPLS é o plano de controle das diversas camadas de comutação, que permite hierarquias para o transporte da informação. O plano de controle e o plano de transporte de dados se encontram fisicamente desagregados, como mostrado na Figura 2.31.

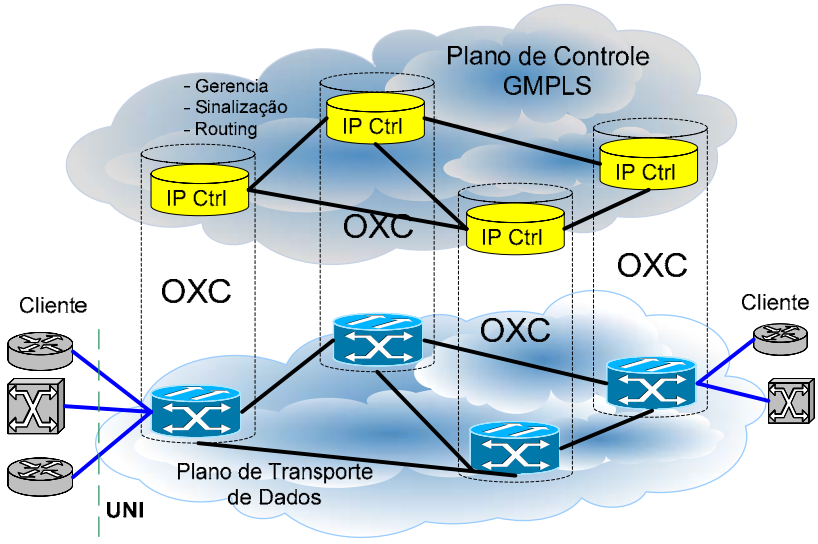


Figura **2.31** - Plano de controle e plano de transporte de dados.

Para incluir os diferentes tipos de comutação (TDM, *lambda* e porta/fibra), foram estendidas certas funções providas por MPLS para incorporar um novo conjunto de interfaces nos LSR. Estas interfaces se classificam em:

- Interfaces PSC (*packet switch capable*), que reconhecem os limites de pacotes e enviam dados com base na informação do cabeçalho do pacote. Por exemplo, interfaces de roteadores que encaminham dados baseados no cabeçalho do pacote IP ou cabeçalho *shim* MPLS;
- Interfaces L2SC (*layer*-2 *switch capable*), que reconhecem os limites de quadros/células e podem enviar dados em função do conteúdo do seu cabeçalho. Como as interfaces Ethernet que usam o cabeçalho MAC ou interfaces ATM baseados na informação dos VPI/VCI;
- Interfaces TDM (*time-division multiplexer capable*), que encaminham os dados em *slots* de tempo, como as interfaces *cross-connect* (XC) SDH/SONET, os multiplexadores *add*/*drop* (ADM), as interfaces TDM G.709, as interfaces PDH etc;
- Interfaces LSC (*lambda switch capable*), que encaminham dados em comprimentos de onda, como as interfaces *photonic cross-connect* (PXC) ou *optical cross-connect* (OXC);
- Interfaces FSC (*fiber-switch capable*), que encaminham dados com base na posição em que são recebidos no espaço físico (porta), como as interfaces PXC/OXC operando ao nível de uma ou múltiplas fibras.

Os domínios das interfaces usadas em GMPLS são apresentados na Figura 2.32.

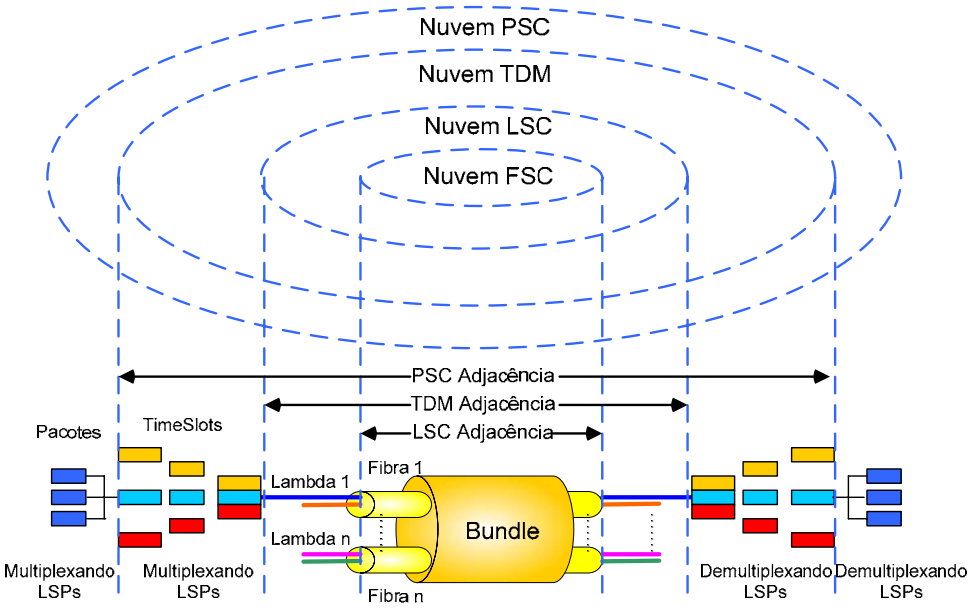


Figura **2.32** - Domínios das interfaces em GMPLS (Modificado [BANERJEE1, 2001]).

Em GMPLS, um circuito só pode ser estabelecido entre interfaces do mesmo tipo. Genericamente, todos os distintos tipos de circuitos que podem ser estabelecidos entre duas interfaces do mesmo tipo são denominados LSP. Um LSP pode se aninhar dentro de outro criando uma hierarquia de LSPs, como apresentado na Figura 2.33. No alto da hierarquia encontram-se as interfaces FSC, seguidas das interfaces LSC, as interfaces TDM, as interfaces L2SC e, por último, as interfaces PSC.

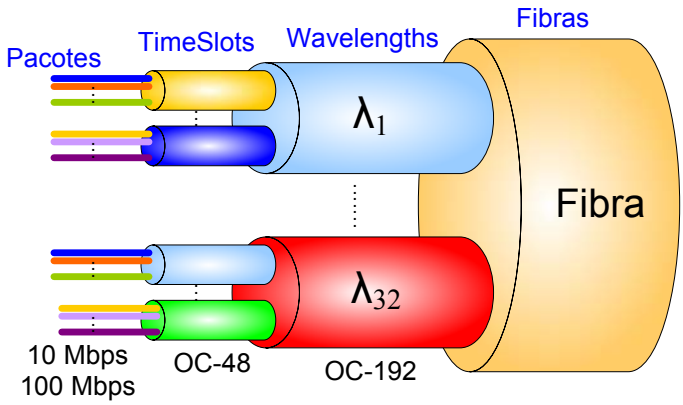


Figura **2.33** - Hierarquia de LSPs

Os LSPs que entram e saem do domínio do transporte óptico nos mesmos LSR podem ser agregados e encapsulados em um único LSP. Esta agregação permite conservar o número de *lambdas* utilizados no domínio MPLS. A hierarquia de LSPs também ajuda a tratar a natureza discreta da largura de banda óptica, o qual permite aproveitar melhor a capacidade do canal óptico.

Um LSR e um OXC exibem várias relações isomórficas, as quais permitem reutilizar algoritmos do modelo do plano de controle MPLS-TE. A distribuição da informação de estado da topologia, o estabelecimento dos caminhos óptico, as funções de engenharia de tráfego, as capacidades de proteção e restauração seriam facilitadas pelo plano de controle de engenharia de tráfego do MPLS generalizado.

Assim, um OXC com um plano de controle MPLS-TE se parece com um LSR. A fibra física entre um par de OXCs representaria um único enlace na topologia da rede. Os comprimentos de onda ou canais individuais seriam análogos aos rótulos. Protocolos de roteamento, como IS-IS ou OSPF, com extensões de engenharia de tráfego adicionais específicas de redes ópticas, podem ser usados para distribuir a informação sobre a

topologia óptica, assim como a informação sobre a largura de banda disponível e os canais disponíveis por fibra. Um protocolo de sinalização de MPLS, tal como RSVP estendido, pode ser usado para a gestão dos caminhos de canal óptico [BANERJEE2, 2001].

Existem algumas diferenças e limitações, como a fusão de rótulos no domínio óptico. Um OXC não pode ainda unir vários comprimentos de onda em um único *comprimento de onda*. Outra diferença é que um OXC não pode realizar o equivalente das operações de trocar rótulos no domínio óptico.

Um exemplo de implementação de uma arquitetura ASON com plano de Controle GMPLS é a rede CARISMA implementada pelo Grupo CCABA e o Grupo de Comunicações Ópticas (GCO) da *Universitat Politecnica de Catalunya* [CARISMA, 2006], e apresentada na Figura 2.34. A arquitetura desta rede está baseada num anel dual de fibras ópticas (fibra de serviço e fibra de proteção) com 12 comprimentos de onda disponíveis no anel e três nós ópticos com capacidade OADM de 4 canais WDM *add-drop*. Cada canal WDM tem capacidade de até 2,5 Gbps e três destes canais podem alcançar até 10 Gbps.

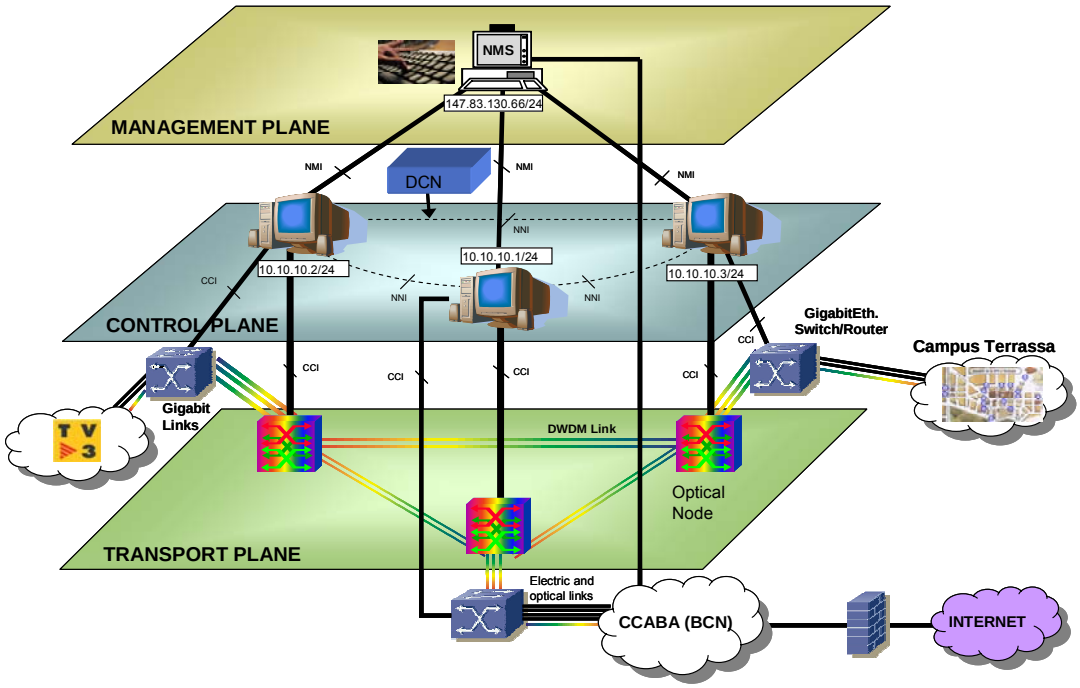


Figura **2.34** – Arquitetura da Rede CARISMA [CARISMA, 2006]

2.7 COMENTÁRIOS E CONCLUSÕES

Neste Capítulo foi apresentada uma visão geral das redes de transporte de telecomunicações com uma descrição básica dos sistemas de comunicações ópticas, sua evolução histórica, tanto nos aspectos de arquitetura como de tecnologias, para concluir com o estado da arte da arquitetura.

Dentro deste contexto se apresentaram as arquiteturas multicamada, baseadas em múltiplas tecnologias de rede em pilha que se têm mostrado ineficientes e que as operadoras ainda mantêm por tentar preservar o investimento feito em equipamentos e tecnologia.

Neste cenário são analisados parâmetros de rendimento. Esta análise revela que, desde uma perspectiva de *overhead*, a arquitetura IP/ATM/SDH (~22% de *overhead*), apresenta um mapeamento extremamente ineficiente, além da necessidade de gerenciar duas redes com tecnologia dissimilar (IP e ATM). No entanto, ATM permite engenharia de tráfego e QoS, características que muitas operadoras de redes ainda consideram suficiente para compensar o alto *overhead* inserido.

Embora a arquitetura IP/SDH apresente menos *overhead* (~6%), e tenha melhor escalabilidade (10 Gbps) que IP/ATM (622 Mbps), SDH precisa de encapsulamento adicional para a delimitação de pacotes (PPP/HDLC), além de não prover muita flexibilidade em termos de capacidade de expansão. Esta é uma das motivações para a migração das redes *backbone* IP para transporte baseado em tecnologia WDM. Para eliminar a camada SDH, a sua capacidade de transporte com suas características de proteção e multiplexação, deverão ser feitas na camada óptica.

A disponibilização da tecnologia MPLS, com sua capacidade de gerenciamento de tráfego e de comutação orientada à conexão com base em protocolos de roteamento e sinalização IP poderá ser empregada na substituição da camada ATM e permitirá que redes IP sem conexão se orientem a conexão através dos LSPs e da adição de um rótulo no cabeçalho do pacote. Assim, alguma camada de adaptação é ainda necessária entre as camadas IP/MPLS e OTN para negociar questões como *framing*, controle de fluxo, correção de erro, etc., e assim eliminar por completo a camada SDH. Neste contexto, o protocolo GFP se apresenta como uma proposta viável.

Nesse sentido, a OTN permitirá acomodar diferentes clientes (IP, ATM, etc) em redes WDM, através de um Plano de Controle ASON, na rede óptica para facilitar os processos de *internetworking* entre o cliente e a rede de transporte. Uma ASON com plano de controle GMPLS é uma das soluções que permitirão um tráfego fluido de IP sobre WDM, e que incorporará capacidades de *networking* (roteamento e sinalização), gerenciando-as de maneira unificada.

Aspectos relativos ao roteamento e à sobrevivência ante falhas, de alta importância para a consolidação da proposta IP/WDM com ASON/GMPLS sobre OTN, também vêm sendo propostos e discutidos nos fóruns de padronização e na academia e serão desenvolvidos em detalhe nos próximos capítulos.

Capítulo 3

"Onde está o caminho para a morada da luz?..."
Jó 38:19a

3 ALOCAÇÃO DE ROTA E COMPRIMENTO DE ONDA (RWA)

3.1 INTRODUÇÃO

A rede WDM pode ser descrita como um modelo em duas camadas: a camada OTN, constituída pelos elementos de rede ópticos (topologia física) e pelo conjunto de "*lightpaths*" (topologia virtual); e a camada Cliente, formada por qualquer tecnologia que possa utilizar-se da rede WDM como tecnologia de transporte (Figura 3.1). A camada OTN fornece transparência ao cliente no serviço de comutação de circuito.

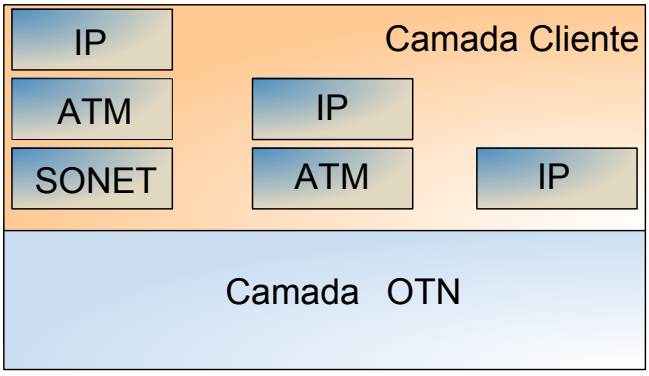


Figura 3.1 - Modelo de camadas da rede de transporte

Uma das funções principais da camada OTN é providenciar requisições de *lightpaths* das aplicações da camada superior, definindo as rotas e reservando os comprimentos de onda para tais solicitações, bem como configurar apropriadamente os estados de todos os dispositivos ópticos envolvidos. Assim, a alocação de rota e comprimento de onda (*Routing and Wavelength Assignment* - RWA) é um problema extremamente relevante a considerar em redes roteadas por comprimento de onda (*wavelength-routed network*)

especialmente quando não existe conversão de comprimento de onda na rede [GONG, 2003].

3.1.1 Redes roteadas por comprimento de onda

A arquitetura de redes roteadas por comprimento de onda consiste de dois tipos de nós: *optical cross-connects* (OXCs), o qual interconecta as fibras na rede, e os nós *edge*, os quais provêm a interface entre sistemas não-ópticos (*routers IP, switches ATM*, etc) e o núcleo da rede (Figura 3.2), como também foi apresentado no Capítulo anterior.

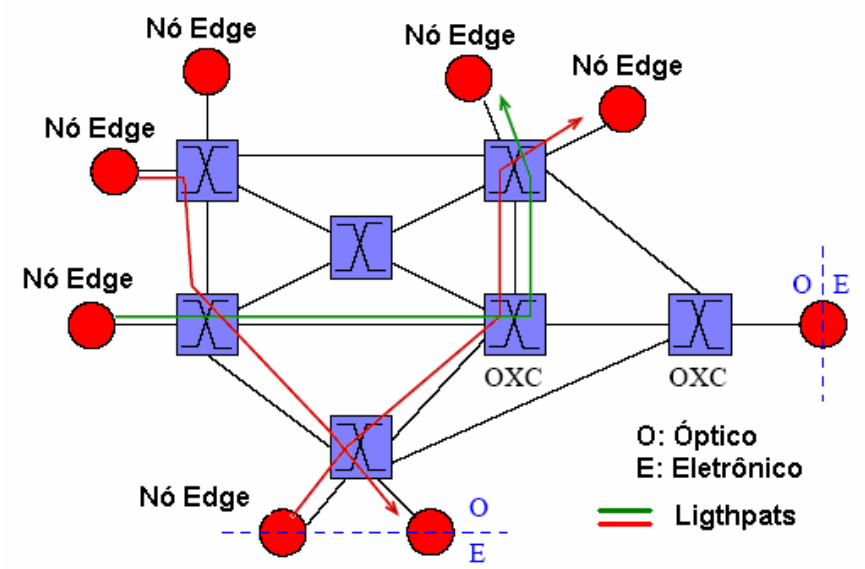


Figura 3.2 - Arquitetura de redes roteadas por comprimento de onda

Os serviços que as redes roteadas por comprimento de onda oferecem a sistemas finais conectados aos nós *edge* estão na forma de conexões lógicas implementadas usando *lightpaths* [ROUSKAS, 2001]. Nestas redes o conceito de caminho óptico descreve uma rota óptica estabelecida entre dois nós, criado pela alocação de um comprimento de onda por toda a rota [CHOI, 2000]. Para todo este trabalho consideraremos que:

CAMINHO ÓPTICO (*lightpath*) = ROTA + COMPRIMENTO DE ONDA

O *caminho óptico* provê um circuito comutado (*circuit-switched*) entre dois nós da topologia de rede. Porém, em redes WDM, o número de comprimentos de onda disponível nos enlaces de fibra limita o número de conexões fim-a-fim. Cada comprimento de onda é alocado a um canal sem consideração da largura de banda requerida. A granularidade de largura de banda é restrita à utilização de largura de banda de um comprimento de onda.

Assim, o comprimento de onda ocupado desde a fonte até o destino depende da disponibilidade dos comprimentos de onda nos enlaces intermediários. Nas redes sem conversão de comprimento de onda, o *caminho óptico* deve usar o mesmo comprimento de onda desde a origem até o destino. Isto é chamado de restrição de continuidade de comprimento de onda (*wavelength-continuity constraint*) [MUKHERJEE, 1997] [THIAGARAJAN, 1999] [RAMASWAMI,1997]. Para as conexões cujas rotas compartilham um enlace comum são alocados diferentes comprimentos de onda [RAMASWAMI, 1995].

Então, redes WDM impõem restrições adicionais na alocação do comprimento de onda. Se um nó é equipado com conversores de comprimento de onda, então a restrição de continuidade de comprimento de onda desaparece, e o problema de roteamento só se limita ao número de canais disponíveis em cada enlace. Porém, se um *caminho óptico* opera no mesmo comprimento de onda através de todos os enlaces de fibra que percorre, um algoritmo de RWA é indicado para satisfazer as restrições de continuidade de comprimento de onda. Estas restrições levam a uma ineficiente utilização dos canais e resultam numa alta probabilidade de bloqueio (taxa entre o número de conexões bloqueadas pelo número total de conexões solicitadas).

3.2 FUNDAMENTOS SOBRE ALGORITMOS DE RWA

O objetivo do algoritmo de RWA é a seleção de uma rota e de um comprimento de onda de maneira a satisfazer uma dada requisição de conexão, visando maximizar o vazão e otimizando a alocação de rotas e comprimentos de onda para um dado padrão de tráfego, mantendo um bom desempenho para a rede como um todo.

De uma forma geral, os algoritmos de RWA baseiam-se em três princípios de funcionamento distintos (MURTHY, 2002):

1 - Escolher, inicialmente, a melhor rota e logo selecionar o comprimento de onda mais adequado disponível, considerando-se a rota estabelecida. Se não houver nenhum comprimento de onda disponível para a rota em questão, repete-se o procedimento anterior para a "segunda melhor" rota, e assim por diante, até especificar um par "rota/comprimento de onda" de modo a atender à requisição do cliente. Se não for possível, nega-se o atendimento da mesma por indisponibilidade de recursos.

2 – Selecionar em primeiro lugar o comprimento de onda mais adequado, para só então escolher a melhor rota disponível para alocação com tal comprimento de onda. Seguindo o mesmo raciocínio do algoritmo anterior, tenta-se primeiro efetuar a alocação com a melhor rota e, caso isso não seja possível, continua-se a tentar, sucessivamente, com as outras rotas. Caso não se tenha rota disponível para atender a requisição com o comprimento de onda determinado, repetem-se os mesmos passos anteriores para o segundo comprimento de onda mais adequado, e assim por diante. Se, após estas tentativas de atendimento da requisição com os diversos comprimentos de onda, não for possível estabelecer um par "comprimento de onda/rota" válido, a requisição deve ser negada por indisponibilidade de recursos.

3 – Considerar, simultaneamente, de acordo com alguma ponderação específica, as determinações da rota quanto do comprimento de onda a ser alocado de modo a se atender a requisição, não realizando, assim, a determinação inicial de qualquer um deles. Apesar de esta última abordagem tender a uma alocação mais racional dos recursos da rede, uma vez que leva ambos em consideração (com as devidas ponderações) simultaneamente, tem-se que ela, geralmente, acarreta uma maior sobrecarga de processamento e, conseqüentemente, maior demora no atendimento das requisições.

Algoritmos de RWA baseados em controle centralizado não são muito adequados para redes mais amplas. Para esse tipo de redes, o controle distribuído mostra-se como uma alternativa viável capaz de superar as deficiências apresentadas pelos algoritmos centralizados [MURTHY, 2002]. Existem vários protocolos de controle distribuído para a realização do roteamento de comprimento de onda. De uma maneira geral, tem-se que os pedidos de conexão que, necessariamente, devem fazer uso de caminhos (rotas) mais longos, com maior número de saltos para serem atendidos, estão sujeitos a uma probabilidade de bloqueio (não atendimento por indisponibilidade de recursos) maior do que aqueles que utilizam caminhos mais curtos (menor número de saltos). Assim, a justiça no atendimento às diversas requisições de conexão, com diferentes comprimentos de rota (número de saltos), é um problema de relativa importância nas redes WDM, devendo ser levado em consideração na elaboração de um algoritmo eficiente de RWA.

Um outro parâmetro que pode ser utilizado como base de comparação entre diferentes algoritmos de RWA é a eficiência com que estes atendem a um mesmo conjunto de

requisições de conexão, o qual, por sua vez, pode ser representado por uma matriz de demanda de requisições (matriz de tráfego).

Dentro os muitos algoritmos existentes, um algoritmo que estabeleceu as bases para algoritmos de roteamento mais sofisticados foi o algoritmo de *Dijkstra*.

3.2.1 O Algoritmo de *Dijkstra*

O Algoritmo de *Dijkstra* (1959) é um algoritmo que calcula o caminho de custo mínimo entre nós (vértices) de um grafo. Escolhido um nó como raiz da busca, este algoritmo calcula o custo mínimo deste nó para todos os demais nós do grafo. Ele é bastante simples e com um bom nível de desempenho [DIJKSTRA, 1959] [UFSC, 2005] [DROZDEK, 2002] [GOLDBARG, 2000].

Este algoritmo parte de uma estimativa inicial para o custo mínimo e vai sucessivamente ajustando esta estimativa. Ele considera que um nó estará fechado quando um caminho de custo mínimo já tiver sido obtido desde o nó tomado como raiz da busca até ele. Caso contrário o nó estará aberto.

3.2.1.1 Estrutura do Algoritmo de *Dijkstra*

Uma versão do algoritmo de *Dijkstra* é dada na Tabela 3.1:

Tabela 3.1 - Algoritmo de *Dijkstra*

```
DijkstraAlgorithm (digraph ponderado simples, first vértice)
        for todos os vértices v
                currDist(v) = ∞;
        currDist(first) = 0;
        toBeChecked = todos os vértices;
        while toBeChecked não esta vazio;
                v = um vertice em toBeChecked com currDist(v) mínimo;
remove v de toBeChecked;
for todos os vértices u adjacentes a v e em toBeChecked
                        if currDist(u) > currDist(v) + peso (aresta(vu))
          currDist(u) = currDist(v) + peso (aresta(vu));

                  predecesor (u) = v;
```

Uma maneira mais simples de apresentar o algoritmo de *Dijkstra* é apresentado a seguir:

Seja **G(V,A)** um grafo orientado, onde V são os vértices de G, e A seus arcos. Seja ***s*** um vértice de **G**:

a).Atribua valor zero à estimativa do custo mínimo do vértice s (a raiz da busca) e infinito às demais estimativas;

b).Atribua um valor qualquer aos precedentes (o precedente de um vértice *t* é o vértice que precede *t* no caminho de custo mínimo de *s* para *t*);

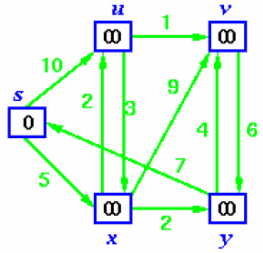
c).Enquanto houver vértice aberto:

- Seja k um vértice ainda aberto cuja estimativa seja a menor dentre todos os vértices abertos;
- Feche o vértice k;
- Para todo vértice j ainda aberto que seja sucessor de k faça:
  - Some a estimativa do vértice k com o custo do arco que une k a j;
  - Caso esta soma seja melhor que a estimativa anterior para o vértice j, substitua-a e anote k como precedente de j.

A seqüência da Figura 3.3 ilustra o Algoritmo de *Dijkstra* [UFSC, 2005]:

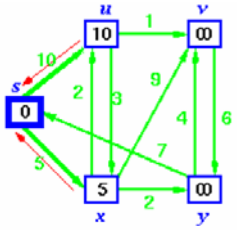
a) Inicialmente todos os nodos tem um custo infinito, exceto s (raiz da busca) que tem valor 0:

Nós	s	u	v	x	y
Estimativas	*0*	∞	∞	∞	∞
Precedentes	-	-	-	-	-



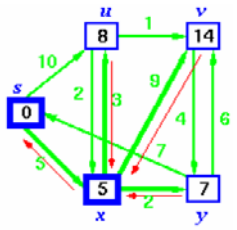
b) Selecione *s (vértice aberto de estimativa mínima), feche s e recalcule as estimativas de u e x*

Nós	s	u	V	x	y
Estimativas	*0*	*10*	∞	*5*	∞
Precedentes	*s*	*s*	-	*s*	-



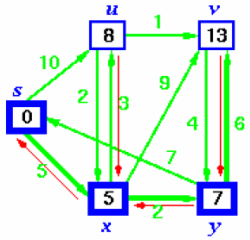
c) Selecione x (vértice aberto de estimativa mínima), feche x, e recalcule as estimativas de u,v e y.

Nós	s	u	v	x	y
Estimativas	*0*	*8*	*14*	*5*	*7*
Precedentes	*s*	*x*	*x*	*s*	*x*



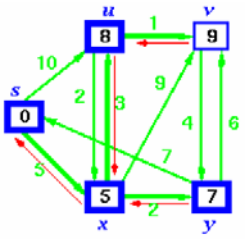
d) Selecione y (vértice aberto de estimativa mínima), feche y, e recalcule a estimativa de v

Nós	s	u	v	x	y
Estimativas	*0*	*8*	*13*	*5*	*7*
Precedentes	*s*	*x*	*y*	*s*	*x*



e) Selecione u (vértice aberto de estimativa mínima), feche u, el recalcule a estimativa de v

Nós	s	u	v	x	y
Estimativas	*0*	*8*	*9*	*5*	*7*
Precedentes	*s*	*x*	*u*	*s*	*x*



f) Selecione v (vértice aberto de estimativa mínima), e feche v

Nós	s	u	v	x	y
Estimativas	*0*	*8*	*9*	*5*	*7*
Precedentes	*s*	*x*	*u*	*s*	*x*

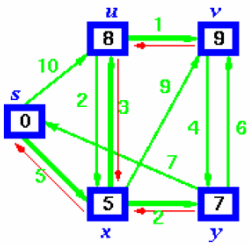


Figura 3.3 - Funcionamento do Algoritmo de *Dijkstra*

Quando todos os vértices tiverem sido fechados, os valores obtidos serão os custos mínimos dos caminhos que partem do vértice tomado como raiz da busca até os demais vértices do grafo. O caminho propriamente dito é obtido a partir dos vértices chamados acima de precedentes. Para exemplificar, considere o caminho de custo mínimo que vai de s até v, cujo custo mínimo é 9. O vértice precedente de ***v*** na última das tabelas acima é ***u***. Sendo assim, o caminho é:

$s \rightarrow \ldots \rightarrow u \rightarrow v$

Por sua vez, o precedente de ***u*** é ***x***. Portanto, o caminho é:

$s \rightarrow \ldots \rightarrow x \rightarrow u \rightarrow v$

Por último, o precedente de ***x*** é o próprio vértice ***s***. Logo, o caminho de custo mínimo é:

$$s \rightarrow x \rightarrow u \rightarrow v$$

Como apresentado, o algoritmo de *Dijkstra* computa apenas um único caminho de custo mínimo entre um dado par de vértices. Para se obter todos os caminhos de custo mínimo entre dois vértices é necessário modificar a forma de anotação dos precedentes. A modificação no passo 3 indicada a seguir é suficiente para permitir o cálculo de todos os caminhos por um processo similar ao descrito acima

Para todo vértice j ainda aberto que seja sucessor de k faça:

- a soma da estimativa do vértice k com o custo do arco que une k a j;
- caso esta soma seja melhor que a estimativa anterior para o vértice j, substitua-a e anote k como precedente único de j;
- caso esta soma seja igual à estimativa anterior para o vértice j, adicione k ao conjunto dos precedentes de j;

Supondo que o peso do arco (y,v) no grafo acima fosse 2, haveriam dois caminhos de custo mínimo do vértice ***s*** para ***v***. Esta duplicidade resulta em dois precedentes para o vértice ***v***:

Nós	***s***	***u***	***v***	***x***	***y***
Estimativas	0	8	9	5	7
Precedentes	s	x	u,y	s	x

Sendo assim, os dois caminhos são dados por:

(s → ... → u → v) e (s → ... → y → v)

Seguindo as precedências para ***u*** e ***y*** nestes dois casos são obtidos os dois caminhos:

(s → x → u → v) e (s → x → y → v)

3.3 CLASSIFICAÇÃO DOS ALGORITMOS DE RWA

As redes WDM roteadas por comprimento de onda são, por natureza, redes comutadas a circuitos. Nessas redes, uma requisição ou pedido de conexão cria a necessidade de que um canal de comunicação (conexão) seja estabelecido desde um nó, chamado de nó origem, até um outro nó, chamado de nó destino. Tal conexão, então, é utilizada para a transmissão de dados da origem para o destino e vice-versa, sendo liberada quando não é mais necessária.

Em uma rede WDM sem conversão de comprimento de onda, uma conexão é estabelecida por meio de um *caminho óptico*, identificado por um caminho físico (rota) e um comprimento de onda. A imposição de continuidade no comprimento de onda determina que deve ser alocado o mesmo comprimento de onda ao longo de todos os *links* da rota origem-destino.

Tal imposição degrada o desempenho da rede como um todo, na medida em que aumenta a probabilidade da ocorrência de bloqueio de pedidos de conexão. A probabilidade de bloqueio de conexão é definida, como foi visto, como a porcentagem de conexões rejeitadas por número de requisições de conexão [MURTHY, 2002]. Assim, uma conexão pode utilizar uma rota apenas se a mesma for contínua no comprimento de onda. Em um ambiente de tráfego dinâmico, no qual conexões são solicitadas e encerradas dinamicamente de maneira aleatória, pode ser que, porventura, ocorra que se tenha uma rota disponível para atender a uma determinada requisição, porém a mesma acabe sendo bloqueada por não possuir um comprimento de onda que esteja disponível em todos os *links* ao longo do caminho.

Sempre que surge uma nova requisição de conexão é utilizado um algoritmo de RWA para determinar um *caminho óptico* que atenda à mesma. Nesse momento, um bom algoritmo se faz necessário para aumentar o desempenho da rede em termos da diminuição da probabilidade de bloqueio de conexões.

De acordo com o exposto acima, os algoritmos de RWA possuem, basicamente, duas partes independentes: um módulo de seleção de rotas e um módulo de seleção de comprimentos de onda. A escolha da rota é baseada em algum critério de custo como a quantidade de saltos, por exemplo. A determinação do comprimento de onda é feita tendo por base algum critério, por exemplo, o fator de uso (porcentagem de uso) dos diferentes comprimentos de onda na rede como um todo.

Dado que existem vários algoritmos distintos tanto para a escolha das rotas quanto para a seleção do comprimento de onda, existem também, conseqüentemente, enorme variedade de propostas para a realização de ambos, ou seja, algoritmos de RWA. Tais algoritmos procuram determinar o melhor par "rota/comprimento de onda" de modo a atender adequadamente uma requisição de conexão, diferenciando-se, basicamente, em suas políticas para escolha de cada um desses elementos individualmente. Assim, tem-se que os

algoritmos de roteamento de comprimento de onda (WR) podem ser classificados com base em seus métodos de:

- Algoritmos de seleção de rotas, e
- Algoritmos de alocação comprimentos de onda.

Tais métodos podem ser realizados um após o outro, em qualquer ordem ou, ainda, pode-se calcular ambos (rota e comprimento de onda) conjuntamente. Em qualquer caso, a ordem de seleção determinada acarreta diferenças quanto aos seus desempenhos.

3.4 ALGORITMOS DE SELEÇÃO DE ROTA

De um modo geral, os algoritmos de seleção de rota podem ser classificados em três categorias [MURTHY, 2002]:

- Roteamento Fixo (*fixed routing* – FR),
- Roteamento Alternativo (*alternate routing* – AR), e
- Roteamento à Exaustão (*exhaust routing* – ER).
- Roteamento Adaptativo (*adaptive routing*)

Tal classificação é baseada na restrição (caso exista) sobre a escolha das rotas dentro do universo de todas as possíveis.

No método de rotas fixas, apenas uma rota é fornecida para cada par de nós e a rota mais curta é a escolhida. Quando uma solicitação de conexão chega a um par de nós, este procura em sua rota pré-definida qual o comprimento de onda está disponível.

No método de roteamento alternativo, duas ou mais rotas são fornecidas para cada par de nós. Ao haver uma solicitação de conexão a um par de nós, é feita uma verificação da disponibilidade de cada uma dessas rotas, em uma ordem pré-definida.

No método de roteamento por exaustão, todas as rotas possíveis são verificadas para o par de nós. O estado da rede é representado por meio de grafos e o algoritmo do caminho-mais-curto é utilizado para encontrar a melhor rota. O método por exaustão apresenta

melhor desempenho que os outros dois, mas apresenta uma complexidade bem maior. Abaixo são apresentados mais detalhes destes algoritmos de seleção de rota:

3.4.1 Roteamento Fixo (FR)

Nos algoritmos do tipo roteamento fixo (FR), para cada par de nós *p*, apenas uma rota candidata R^p é fornecida. Tem-se que as rotas candidatas para cada um dos pares de nós da rede são fixas e previamente determinadas (isto é, são calculadas *off-line*), não podendo, portanto, ser alteradas de acordo com mudanças nas condições de tráfego da rede.

3.4.2 Roteamento Alternativo (AR)

Nos algoritmos do tipo roteamento alternativo (AR), para cada par de nós *p*, é fornecido um conjunto de *K* rotas candidatas, as quais são denotadas por R_0^p, R_1^p, ... , R_{K-1}^p e correspondem a um subconjunto de todas as possíveis rotas para o par de nós em questão. Estas rotas são, também, calculadas a priori (*off-line*). Quando uma solicitação de conexão é feita para um par *p*, uma das rotas candidatas em R^p será selecionada, a menos que a requisição seja negada.

3.4.3 Roteamento à Exaustão (ER)

Ao contrário dos anteriores, nos algoritmos do tipo roteamento à exaustão (ER) não há restrição sobre a rota a ser selecionada. Para um dado par de nós *p*, é escolhida uma rota dentre todas as possíveis.

3.4.4 Roteamento Adaptativo (*adaptive routing*)

Nos algoritmos do tipo roteamento adaptativo, lighpaths são estabelecidos adaptativamente baseados no estado presente da rede. Este algoritmo é mais tolerante a falhas e apresenta uma baixa probabilidade de bloqueio.

3.5 ALGORITMOS DE ALOCAÇÃO DE COMPRIMENTO DE ONDA

Dependendo da ordem em que os diferentes comprimentos de onda são testados, os algoritmos de seleção de comprimento de onda podem ser genericamente separados em quatro tipos:

- Mais Utilizado (*most used* – MU),

- Menos Utilizado (*least used* – LU),
- Ordem Fixa (*fixed order* – FX), e
- Ordem Aleatória (*ramdom order* – RN).

De acordo com o tipo de algoritmo, tem-se que a ordem de busca dos comprimentos de onda pode, ou não, depender do fator de uso dos mesmos na rede.

Pelo método "mais utilizado", o comprimento de onda livre é definido fazendo uma busca do mais utilizado para o menos utilizado. De forma contrária, o método "menos utilizado" busca encontrar o comprimento de onda livre começando a busca pelo menos utilizado, aumentando assim a chance de rapidamente encerrar a busca. No método de ordem fixa, os comprimentos de onda podem receber índices e a busca obedecer a ordem deste índice. No método de ordem randômica, é feita uma busca em todos os comprimentos de onda livres de forma aleatória.

Os dois primeiros métodos são preferidos quando se trata de uma rede de controle centralizado. Os dois outros métodos são utilizados em redes com controle distribuído. O método que apresenta melhor desempenho é o "mais utilizado" [MURTHY, 2002].

3.5.1 Mais Utilizado (MU)

O algoritmo MU prioriza a alocação do comprimento de onda mais utilizado, ou seja, aquele que está sendo usado no maior número de *links* na rede. Desta forma, os comprimentos de onda são testados na ordem decrescente de sua utilização. Desse modo, o algoritmo MU procura alocar os *lightpaths*, sempre que possível, com o mesmo comprimento de onda, deixando, assim, um bom número de rotas contínuas no comprimento de onda (devido aos comprimentos de onda não alocados) disponíveis para os próximos pedidos de conexão. Para funcionar corretamente, tal algoritmo necessita conhecer informações reais ou estimadas a respeito do estado global da rede, de modo a determinar o fator de uso de cada um dos diferentes comprimentos de onda. Com isso, tem-se que o algoritmo MU mostra-se mais apropriado para implementações centralizadas, sendo mais facilmente adaptável que para implementações distribuídas.

3.5.2 Menos Utilizado (LU)

De maneira oposta, o algoritmo LU dá preferência para que seja alocado o comprimento de onda menos utilizado, ou seja, aquele que é usado no menor número de *links* na rede. Desse modo, tem-se que os comprimentos de onda são testados em ordem crescente de utilização. Com isso, tal algoritmo procura balancear o fator de uso dos diferentes comprimentos de onda, distribuindo uniformemente a carga entre os mesmos.

A idéia intuitiva por trás deste algoritmo é que, por meio da tentativa de alocação da conexão com o comprimento de onda menos utilizado, poder-se-á encontrar uma rota mais curta (com menor número de saltos) do que se fosse empregado o comprimento de onda mais utilizado, deixando, assim, um maior número de *links* disponíveis para uso pelas requisições de conexão futuras. Assim, como o algoritmo anterior (MU), o LU também precisa que sejam conhecidas informações reais ou estimadas acerca do estado global da rede, de modo a comparar os fatores de uso dos diferentes comprimentos de onda. Tal algoritmo é, igualmente, mais adequado para implementações centralizadas do que para implementações distribuídas.

3.5.3 Ordem Fixa (FX)

O algoritmo FX procura o universo de comprimentos de onda em uma ordem fixa. Todos os comprimentos de onda são indexados e testados na ordem crescente de seus índices, sendo alocado, assim, o primeiro que estiver disponível na rota em questão (para o caso de se determinar, em primeiro lugar, a rota que será utilizada) ou, então, o primeiro que possuir uma rota que seja nele contínua (para o caso de se escolher, primeiramente, o comprimento de onda). Assim, algoritmo FX não depende dos fatores de uso dos comprimentos de onda e, conseqüentemente, não tem a necessidade de que se tenham disponíveis informações sobre o estado global da rede. Pela escolha do primeiro comprimento de onda disponível, este algoritmo procura alcançar um desempenho comparável à do MU, podendo, porém, ser facilmente implementado em arquiteturas tanto centralizadas quanto distribuídas.

3.5.4 Ordem Aleatória (RN)

Por último, tem-se o algoritmo RN, o qual testa o conjunto de comprimentos de onda em uma ordem aleatória, por meio da atribuição de índices aos mesmos e do sorteio, igualmente provável, dos índices dos comprimentos de onda que tentará se alocar quando

da tentativa de atendimento de uma requisição de conexão qualquer. Tal algoritmo também é independente dos fatores de uso dos comprimentos de onda (não precisa de informações a respeito do estado global da rede) e, nesse sentido, mostra-se adequado tanto para implementações centralizadas quanto distribuídas. A idéia do RN é, de maneira similar à que acontece no algoritmo LU, distribuir uniformemente a carga sobre os diferentes comprimentos de onda.

3.6 ALGORITMOS DE RWA

Tendo visto os vários algoritmos individuais existentes para seleção de rotas e de comprimentos de onda, poderemos compreender mais claramente os algoritmos de alocação de rotas e comprimentos de onda (RWA), responsáveis por desempenhar ambas as funções.

Nos quatro primeiros algoritmos, apresentados a seguir, é estabelecida inicialmente a rota com base em alguma métrica relativa ao custo da mesma, para logo selecionar, dentre o universo de comprimentos de onda disponíveis, aquele que será alocado ao longo desta rota, utilizando, para tal, algum algoritmo de seleção de comprimento de onda.

O último algoritmo de RWA descrito, por sua vez, realiza a determinação simultânea da rota e do comprimento de onda associado. Nesse caso, tem-se que a métrica utilizada na determinação do custo de uma rota apresenta certa dependência, também, com o comprimento de onda que está sendo considerado. Assim, é associado um valor de custo a cada par "rota/comprimento de onda" e aquele, dentre todos os pares, que possuir o menor valor é o escolhido para a alocação.

3.6.1 Roteamento Fixo (*Fixed Routing* – FR)

O algoritmo de roteamento fixo (FR) é o mais simples dentre todos. Para cada par de nós p na rede, é calculada, *a priori*, uma rota fixa R^p (normalmente a menor rota). Desse modo, quando ocorre uma requisição para que seja estabelecida uma conexão entre o par de nós p, o algoritmo verifica se há algum comprimento de onda que esteja disponível ao longo de todos os *links* de R^p. Se não houver comprimento de onda disponível, a requisição é bloqueada. Se houver apenas um comprimento de onda disponível, a requisição é, então, atendida com o mesmo. Caso contrário se houver mais de um comprimento de onda

disponível, a seleção de qual comprimento de onda será alocado dentre eles é feita por meio de algum algoritmo específico de seleção de comprimento de onda.

A principal vantagem deste algoritmo está na sua rapidez de execução, a qual faz com que as conexões demorem menos em ser estabelecidas. Por outro lado, o mesmo resulta, geralmente, em um desempenho de rede muito baixa, uma vez que testa uma única rota para cada par de nós *p* dado, mesmo tendo em vista que podem existir várias rotas para esse par. Desse modo, quando ocorre a solicitação de uma conexão, podem não existir comprimentos de onda disponíveis na rota R^p, podendo, existir outras rotas ligando o mesmo par de nós que disponham de comprimentos de onda não utilizados. Em tal caso, entretanto, se tem que o pedido de conexão seria negado.

Em condições de baixas requisições de conexão (carga leves), com pouco uso dos recursos da rede, o algoritmo FR apresenta um resultado melhor, à medida que a probabilidade de se achar um comprimento de onda disponível na rota fixa é alta. Todavia, com o aumento da carga submetida à rede, o desempenho do algoritmo começa a decair. Com relação a esse aspecto, ocorre que o desempenho da rede é bastante influenciada por fatores como a topologia e a conectividade da mesma. Em uma rede densamente conectada, na qual há várias rotas possíveis para se ligar um par de nós, o algoritmo FR alcança um resultado de desempenho muito pobre.

3.6.2 Roteamento Fixo Alternativo (*Fixed Alternate Routing* – FAR)

O algoritmo de roteamento fixo alternativo (FAR) é uma combinação do algoritmo FR, com o algoritmo de roteamento alternativo (AR). Para cada par de nós *p*, é estabelecido um conjunto de *K* rotas candidatas, calculadas *a priori* (*off-line*), as quais correspondem a um subconjunto de todas as possíveis rotas para o par de nós em questão e são denotadas por R_0^p, R_1^p, ... , R_{K-1}^p. Quando é feita uma requisição para o par de nós *p*, tem-se que as rotas candidatas do mesmo são testadas, em uma ordem fixa, até que se encontre alguma com um custo finito (as métricas mais utilizadas são a quantidade de saltos e o atraso). Se não houver nenhuma rota com custo finito dentre as candidatas, isto é, se não houver nenhum comprimento de onda disponível em qualquer das rotas, então a solicitação de conexão será bloqueada. Caso contrário, se houver mais de um comprimento de onda disponível na rota escolhida, um deles é especificado por meio de um algoritmo de seleção de comprimento de onda.

Apesar de ser um algoritmo um tanto mais complexo que o FR, o FAR ainda mantém as características relativas à simplicidade e rapidez do tempo de estabelecimento de conexões. Apresenta, ainda, desempenho superior à do algoritmo FR, uma vez que tem a possibilidade de efetuar uma escolha, para cada par de nós, dentre mais de uma rota candidata. Entretanto, devido ao fato de que as rotas fornecidas para um dado par de nós poderem não incluir todas as rotas possíveis, tem-se que o desempenho deste algoritmo não é a melhor possível.

3.6.3 Roteamento à Exaustão (*Exhaust Routing* – ER)

Teoricamente, a utilização do algoritmo de roteamento à exaustão resulta em um desempenho maior do que a dos algoritmos anteriores (FR e FAR). Em tal algoritmo, não se determina previamente as rotas candidatas a testar para cada par de nós. Ao invés disso, mantém-se a informação de estado da rede na forma de um grafo. Tal informação de estado é dinâmica, mudando continuamente de acordo com as condições dinâmicas de tráfego. Quando surge uma nova requisição de conexão para o par de nós p, o algoritmo determina a melhor rota, baseado em algum critério de custo, dentre todas as candidatas.

Assim, devido ao fato de explorar o universo das possíveis rotas, o algoritmo procura elevar a taxa de aceitação das conexões. A rede pode ser modelada como um grafo com W subgrafos, cada um correspondendo a um comprimento de onda específico. Assim, um algoritmo convencional de determinação do menor caminho (por exemplo, o Algoritmo de Dijkstra) pode ser utilizado para se estabelecer a rota de menor custo em cada um dos subgrafos de modo que a melhor possa ser escolhida, que junto com o comprimento de onda correspondente atenderá a requisição.

Se o custo de uma rota é mensurado exclusivamente pelo número de saltos, tem-se que o algoritmo de procura pela menor distância (*breadth-first search algorithm*) pode ser utilizado para se determinar o menor caminho. Dado que o algoritmo ER leva em consideração todas as rotas possíveis, o mesmo resulta em um melhor desempenho da rede. Apesar de tal mérito, ele possui algumas desvantagens. A complexidade de tempo para o pior caso (*worst-case time complexity*) do algoritmo é maior e, conseqüentemente, a execução do mesmo é mais lenta. Este algoritmo mostra-se mais adequado à implementação centralizada do que à distribuída.

3.6.4 Roteamento pelo Caminho Menos Congestionado (LCR)

O algoritmo de roteamento pelo caminho menos congestionado (*Least Congested Path Routing* – LCR) seleciona a rota com o menor nível de congestionamento entre um par de nós *p*. O congestionamento de uma rota é determinado pelo número de comprimentos de onda disponíveis para uso ao longo da rota como um todo. Quanto maior o número de comprimentos de onda livre, menos congestionada é a rota. O algoritmo a seguir é baseado na abordagem de roteamento alternativo.

Para cada par de nós *p*, é selecionado um conjunto de *K* rotas candidatas (um subconjunto de todas as rotas possíveis para o par de nós em questão), as quais são calculadas previamente e denotadas por R_0^p, R_1^p, ... , R_{K-1}^p. Quando é feita uma solicitação de conexão para o par de nós p, calcula-se o custo de cada uma das *K* rotas candidatas, onde o custo de uma rota é definido com base no seu grau de congestionamento. Caso mais de uma rota apresente o mesmo custo, tem-se que a rota com o menor número de saltos é preferida. Uma vez selecionada a rota, pode-se utilizar um dos algoritmos de seleção de comprimento de onda de modo a determinar o comprimento de onda a ser alocado na mesma. A razão intuitiva por trás da seleção da rota menos congestionada é a seguinte: o algoritmo tenta manter tantas rotas contínuas em comprimento de onda quantas possíveis, o que irá ajudar a satisfazer várias requisições futuras. Espera-se que tal algoritmo apresente um desempenho superior ao dos algoritmos FR e FAR. Entretanto, devido ao fato do mesmo basear-se no roteamento alternativo, tem-se que o seu desempenho, em termos da probabilidade de bloqueio de conexões, é pior do que a apresentada pelos algoritmos baseados na abordagem de roteamento à exaustão.

3.6.5 Seleção Conjunta de Rota e Comprimento de Onda (JWR)

Todos os algoritmos anteriores revistos selecionam a rota e o comprimento de onda de maneira independente, um após o outro. Apesar dos algoritmos expostos efetuarem a seleção, inicialmente, da rota, para só então determinarem o comprimento de onda a ser utilizado no caminho, tem-se que o contrário também é possível (primeiro o comprimento de onda e, logo, a rota a ser alocada), levando a um novo conjunto de algoritmos.

Ao contrário de todos esses, o algoritmo de seleção conjunta de rota e comprimento de onda (*Joint Wavelength-Route Selection* – JWR) atribui um custo a cada par "rota – comprimento de onda", selecionando, então, aquele com o menor custo dentre todos. Tem-

se que a função de atribuição de custo a esses pares de rota/λ leva em consideração fatores como o *status* de utilização do comprimento de onda na rede, a quantidade de saltos e o nível de congestionamento (número de comprimentos de onda disponíveis) na rota.

O algoritmo JWR também utiliza uma abordagem baseada no roteamento alternativo. Para cada par de nós *p*, é calculado *off-line* um conjunto de *K* rotas candidatas, denotadas por R_0^p, R_1^p, ... , R_{K-1}^p, as quais representam um subconjunto de todas as rotas possíveis para esse par de nós. Denota-se por $A(\omega_i)$ o número de *links* nos quais o comprimento de onda ω_i está disponível no momento. Adicionalmente, denota-se por $L(R_f^p)$ o número de saltos e por $F(R_f^p)$ o número de comprimentos de onda disponíveis na rota R_f^p. Assim, tem-se que o custo de cada um dos pares "rota – comprimento de onda" é dado pela expressão (1).

$$C(\omega_i, R_f^p) = \alpha_1 \cdot A(\omega_i) + (1-\alpha_1) \cdot \{\alpha_2 \cdot [W - F(R_f^p)] + (1-\alpha_2) \cdot L(R_f^p)\}, \quad 0 \le \alpha_1 \, e \, \alpha_2 \le 1 \quad (1)$$

Valores adequados para as constantes α_1 e α_2 podem ser escolhidos de modo a se obter diferentes funções de custo. O estabelecimento de um valor alto para α_1 ($\alpha_1 = 1$), por exemplo, dará preferência à escolha do comprimento de onda mais utilizado primeiro. Por outro lado, um valor pequeno para α_1 ($\alpha_1 = 0$) irá preferir a rota de menor custo, ignorando o nível de utilização atual dos comprimentos de onda. Assim, o JWR tenta combinar as vantagens dos algoritmos MU, FAR e LCR.

3.7 CONSIDERAÇÕES NO PROJETO DE RWA

Considerações tais como o custo das rotas, a justiça e eqüidade no atendimento de requisições e a forma como o plano de controle está constituído são importantes no projeto de RWA em uma rede roteada por comprimento de onda, e são tratadas a seguir.

3.7.1 Considerações acerca do Custo das Rotas

Fatores como a quantidade de saltos, o atraso ou, ainda, o congestionamento são considerados como o custo de uma rota. Se não há nenhum comprimento de onda disponível em todos os *links* de uma dada rota, então o custo da mesma é definido como sendo infinito; caso contrário, tal custo é finito. A quantidade de saltos de uma rota corresponde ao número de *links* que a mesma possui. No caso de atraso, associa-se a cada *link* um valor de custo proporcional à distância (ou atraso) do mesmo. Desse modo, para a

obtenção do custo total de uma rota, então, basta somar os custos de cada um de seus *links* componentes. Por sua vez, o congestionamento de uma rota tem como parâmetro o número de comprimentos de onda utilizados na mesma. Tem-se que quanto maior o número de comprimentos de onda disponíveis, menor será o congestionamento.

3.7.2 Justiça / Eqüidade no atendimento de requisições

Uma importante preocupação a levar em conta no atendimento de uma requisição em uma rede WDM é a diferença existente entre as probabilidades de bloqueio de conexões cujas rotas apresentam tamanhos diferentes (diferente número de saltos). Geralmente, tem-se que um algoritmo de RWA favorece o estabelecimento das conexões com um menor número de saltos. Dito de outra maneira, as solicitações de conexão com rotas grandes são bloqueadas com maior freqüência do que as rotas de menor tamanho, o que leva a uma condição de assimetria no atendimento das requisições (problema da injustiça).

De modo a otimizar a eqüidade/justiça no atendimento dos pedidos de conexão com diferentes tamanhos de rota, é necessária a implementação de mecanismos apropriados de controle para regular a admissão das requisições. Para esse objetivo, associa-se uma probabilidade de bloqueio a cada par origem-destino de nós (a cada pedido de conexão). Define-se, ainda, um índice de desempenho global para a rede, o qual consiste em uma média entre todas as probabilidades de bloqueio de conexão, ponderadas pelas respectivas intensidades do tráfego de requisições referente aos diferentes pares origem-destino da rede. Essa medida global, denominada probabilidade média de bloqueio da rede, reflete o desempenho da rede como um todo, ao passo que as probabilidades de bloqueio individuais de cada solicitação correspondem ao grau de serviço oferecido a um cliente em particular. Logo, tem-se que todas as medidas (globais e individuais) devem ser levadas em consideração na avaliação de um algoritmo de RWA.

Um algoritmo que resulta em uma alta variância entre as probabilidades de bloqueio individuais é dito injusto. Devido ao problema da injustiça, tal algoritmo não é desejável, mesmo que seja capaz de proporcionar um bom desempenho de bloqueio à rede como um todo. Por outro lado, tem-se que, à medida que se aumenta a taxa de aceitação das requisições com rotas maiores, é esperada uma degradação na resposta global da rede. Em outras palavras, a melhoria da justiça no atendimento às diferentes solicitações de conexão pode ser alcançada ao custo de uma perda no rendimento global. Desse modo, qualquer

algoritmo que atue no sentido de aumentar a eqüidade/justiça no atendimento às diversas requisições deve assegurar que a perda no desempenho global seja a mínima possível.

No caso de se tratar de um algoritmo distribuído, tem-se que o problema gerado pela reserva de recursos (reserva de um comprimento de onda em um *link*, por exemplo) que é efetuada pelas diferentes requisições de conexão, é responsável por aumentar ainda mais a diferença entre as performances das conexões individuais. O problema da reserva de recursos surge enquanto se procura alguma rota com comprimento de onda disponível para atender uma determinada solicitação. Nesse sentido, mostra-se imperativo que um algoritmo de roteamento distribuído utilize algum mecanismo para aumentar a justiça no atendimento aos pedidos de conexão com diferentes tamanhos de rota.

Comutadores OXC com conversão de comprimento de onda podem ser empregados em nós estratégicos da rede de modo a reduzir a probabilidade de bloqueio das conexões com muitos saltos. Um conversor de comprimento de onda, dispositivo capaz de substituir o comprimento de onda de um sinal de entrada por um outro, ameniza a imposição de continuidade no comprimento de onda nos nós conversores. Apesar dos conversores proporcionarem um aumento no desempenho das conexões com rotas mais longas, tem-se que tais dispositivos não resolvem o problema da injustiça de um modo geral. Isso devido ao seu posicionamento não ótimo, além do fato de que os pedidos de conexão que utilizam rotas mais curtas beneficiam-se, igualmente, da presença dos mesmos. Além disso, esses dispositivos influenciam significativamente no aumento tanto do custo quanto da complexidade da rede.

Uma outra abordagem que pode, possivelmente, aumentar o desempenho das requisições com maior quantidade de saltos é o re-roteamento de comprimento de onda. Tal mecanismo movimenta um pequeno conjunto de *lightpaths* existentes para novos comprimentos de onda de modo a liberar uma rota contínua em comprimento de onda para o atendimento de uma nova requisição de conexão. Do mesmo modo que os conversores de comprimento de onda, a utilização do re-roteamento resolve o problema da injustiça apenas parcialmente. Além disso, tem-se que tal abordagem também aumenta a complexidade e o custo de operação da rede. Quando se utiliza um algoritmo de roteamento distribuído, então, esses dois fatores (complexidade e custo) tornam-se ainda maiores.

Além da característica de aumentar o grau de justiça no atendimento às diferentes solicitações de conexão da rede, tem-se que um algoritmo de melhoria da justiça deve, preferencialmente, possuir as seguintes propriedades:

- A perda no desempenho global deve ser mantida dentro de limites aceitáveis;
- A utilização dos canais de comprimento de onda (*links* com comprimento de onda associado) deve ser alta;
- O algoritmo deve mostrar-se adequado às redes com diferentes graus de conectividade. Em particular, o mesmo deve ser útil para redes esparsamente conectadas, nas quais o problema da injustiça é mais gritante.
- O algoritmo deve ser necessariamente flexível para permitir a escolha de um determinado compromisso (*trade-off*) entre o nível de justiça pretendido e a perda no desempenho global da rede;
- A penalidade acarretada nas requisições de rotas curtas não deve ser tão alta que torne as suas probabilidades de bloqueio mais altas do que as das requisições de rotas longas. Em outras palavras, tem-se que as conexões de tamanho (número de saltos) mais reduzido não devem ser sobrepenalizadas;

3.7.3 Controle Centralizado e Controle Distribuído

Os algoritmos RWA podem ser projetados para Planos de Controle estabelecidos de forma centralizada ou distribuída.

No caso do controle centralizado, assume-se que um elemento que centraliza o controle na rede está disponível. O controlador faz um acompanhamento do estado da rede e é responsável por selecionar as rotas e comprimentos de onda das requisições, assim como enviar sinais de controle para os nós envolvidos nos processos de estabelecimento e liberação dos "*lightpaths*". Nenhum dos nós da rede sabe qual é o estado atual de toda a rede em um determinado momento. Os algoritmos centralizados normalmente são utilizados em pequenas redes, não sendo escaláveis para redes maiores.

Um nó pode usar um esquema distribuído de busca rápida na seleção da rota e do comprimento de onda para atender uma requisição. Podem ser usadas também, rotas pré-

definidas e realizada a busca de comprimentos de onda livres nos enlaces da rota selecionada. Os nós enviam mensagens de controle aos seus vizinhos, solicitando reserva de comprimento de onda dos enlaces diretamente conectados a eles. Estando a rota definida e o comprimento de onda reservado, um sinal de controle é enviado a vários nós para configurar o chaveamento nos nós de roteamento para o estabelecimento dos "*lightpaths*". Da mesma forma, para liberar um "*caminho óptico*", um sinal de controle é enviado do nó origem para os demais. Os protocolos de controle distribuído são utilizados com o propósito de se obter simplicidade e escalabilidade.

Requisições de conexões com grandes saltos demoram mais para ser atendidas. Isso ocorre principalmente quando o controle distribuído é usado, devido a maior possibilidade de haver conflito na reserva de comprimentos de onda e pela falta de justiça entre conexões com diferentes números de saltos envolvidos na conexão.

3.8 OUTRAS PROPOSTAS PARA RWA

Na prática, muitos algoritmos de RWA estão baseados no método de roteamento alternativo (*alternate routing*) para prover diversas possíveis rotas entre um par de nós e melhorar a resposta de bloqueio.

Existem propostas algorítmicas que consideram outros fatores que influenciam o rendimento da rede que, às vezes, são negligenciados, tais como o número de saltos das outras possíveis rotas alternativas e a posição de cada enlace na rede. Com base nestes fatores, um novo algoritmo de RWA denominado *Less Influence Path First* (LIPF) é proposto em [GONG, 2003].

Outra proposta [KRISHNASWAMY, 2001] considera o problema de maximizar o número de *lightpaths* que podem ser estabelecidos em uma rede óptica, dada uma matriz de conexão (um conjunto estático de demandas) e o número de comprimentos de onda que a fibra suporta em uma rede sem conversão de comprimento de onda. O problema de estabelecer todas as conexões da matriz de tráfego usando poucos comprimentos de onda também foi tratado por [BANERJEE, 1996] e [BARONI, 1998]. Assim, este problema de maximização do número de *lightpaths* (Max-RWA) e o posterior problema de minimizar o número de comprimentos de onda (Min-RWA), é formulado como um Programa Linear Inteiro (*integer linear programme* – ILP) para redes de tamanho pequeno (alguns nós).

Para redes de dezenas de nós foram desenvolvidos algoritmos baseados em soluções obtidas por Relaxação LP (*LP-relaxation*) da formulação ILP. Redes tais como NSFNET e EONNET serviram de cenário para esta proposta.

Modelos com programação linear inteira (ILP) são populares na literatura, pois eles permitem a descrição formal dos problemas. Na prática, entretanto, escalabilidade para redes com dezenas de nós e centenas de demandas surgem constantemente. Em muitos casos os ILP´s são computacionalmente intratáveis [WALDMAN, 2004]. No trabalho de Karcius [KARCIUS, 2004], em uma rede de grande dimensão como a NSFNET, usando-se, por exemplo, software de otimização CPLEX numa Intel Pentium IV/1,6 Ghz, foi excedida a capacidade de memória do equipamento. Então, para o atendimento destes casos deverão ser desenvolvidas heurísticas para encontrar soluções a estas características, problemas normalmente encontrados na realidade das redes ópticas.

3.9 ALGORITMOS DE RWA ESTÁTICOS E DINÂMICOS

Algoritmos de RWA disponíveis na literatura podem ser classificados segundo a forma como o tráfego é assumido. Assim temos:

a) Tráfego Estático (*off-line*)

No caso da demanda de tráfego estático, um conjunto de conexões para o par fonte-destino é pré-estabelecido. Estes pares são escolhidos baseados na estimativa de requisitos de tráfego entre um nó e outro. O objetivo é fazer as alocações de rotas e de comprimentos de onda da demanda existente de tal forma que seja minimizado o número de comprimentos de onda utilizados. O grande desafio é maximizar o número de solicitações satisfeitas, mantendo-se um número de comprimentos de onda fixo. Este problema é conhecido como o problema do estabelecimento dos "*lightpaths*" estáticos (*Static Lightpath Establishment* – SLE). Tem-se mostrado que o problema SLE é intratável, ou seja, o único algoritmo conhecido que encontra uma solução otimizada requer um tempo exponencial não factível para uma situação de alocação de comprimentos de onda em uma rede de alta velocidade.

b) Tráfego Dinâmico,

No caso da demanda de tráfego dinâmico, as requisições de conexões chegam a, e partem desde a rede uma-a-uma de maneira randômica. Este tipo de tráfego gera os mais variados

modelos de situações em uma rede de transporte. Durante a operação da rede pode ser necessário retirar algum *caminho óptico* já existente e estabelecer novos *lightpaths* em resposta à mudança do padrão de tráfego da rede ou falha de algum componente. Diferentemente do problema colocado no caso do RWA estático, as soluções para o problema do RWA dinâmico devem ser computacionalmente simples, já que a requisição deve ser processada em tempo real. Quando surge uma nova requisição, a rota e o comprimento de onda devem ser alocados de tal forma que seja maximizado o número de requisições futuramente atendidas. Em geral, os esquemas de roteamento dinâmico acarretam em maiores probabilidades de bloqueio. Os algoritmos para RWA dinâmico são bem menos sofisticados do que os algoritmos para RWA estático, já que não se tem conhecimento das requisições futuras, enquanto que no RWA estático todas as conexões são conhecidas *a priori*.

Para o caso estático, as métricas de desempenho geralmente usadas são consideradas em uma das seguintes categorias [CHOI, 2000]:

- Número de comprimentos de onda requeridos;
- Probabilidade de bloqueio de conexão;
- Custo do enlace;

Assim, para os algoritmos de RWA *off-line*, o interesse é focado em minimizar o número requerido de comprimentos de onda de maneira a maximizar o número de conexões acomodadas se o número de comprimentos de onda é limitado.

Para os algoritmos de RWA dinâmicos, o objetivo é minimizar a probabilidade de bloqueio. É necessário que estes algoritmos sejam simples e rápidos. A proposta desta Tese pertence a esta classificação, sendo aqui desenvolvido um algoritmo de RWA dinâmico orientado a sobrevivência baseado em heurísticas simples e um algoritmo genético rápido.

No *paper* de [CHOI, 2000], é feito um *overview* de algoritmos RWA sob condição de tráfego estático, e realizada uma classificação por algumas de suas características funcionais. A Figura 3.4 apresenta esta classificação. O problema de RWA é dividido em dois sub-problemas: roteamento e alocação de comprimento de onda, e cada um deles é sub-dividido em duas funções: procura e seleção.

Em problemas de roteamento, tomar todos os possíveis pares fonte-destino não é prático, pois o número de espaços de estado aumenta exponencialmente com o número de nós e enlaces. Aqui, a função busca é usualmente realizada por técnicas conhecidas, tais como algoritmos de caminho mais curto (*shortest-path algorithm*) e suas variações. Em *k-shortest path algorithm* (na qual mais de uma rota é disponível), a função de seleção é realizada por algoritmos de otimização seqüenciais ou combinatórios. Algoritmos seqüenciais (*greedy algorithm*) são dos mais simples, nos quais a seleção para cada caminho óptico é feita seqüencialmente. Esta técnica precisa de duas funções: ordem de seleção e regra de seleção.

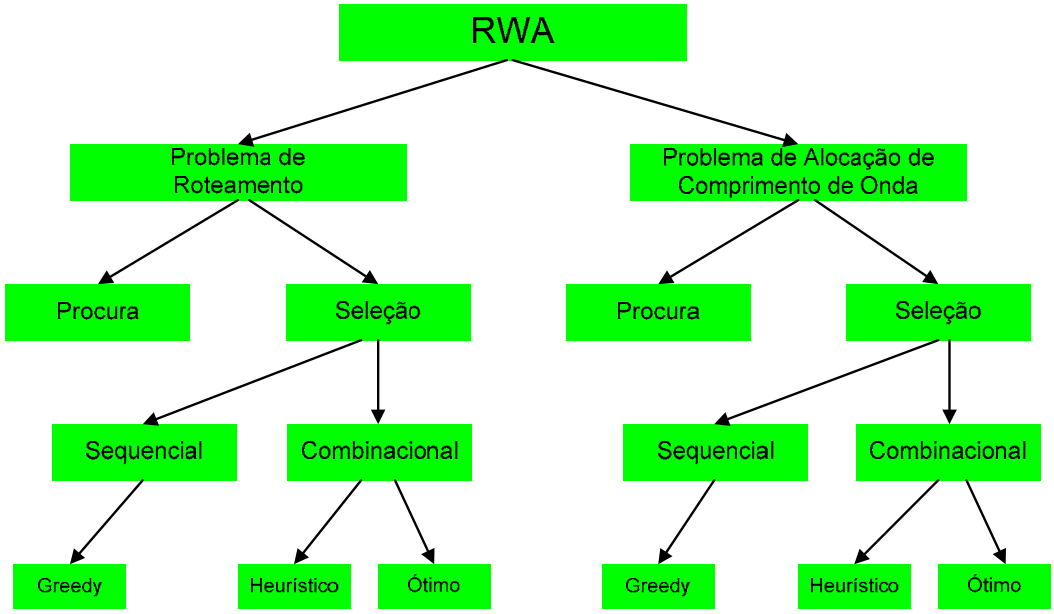


Figura 3.4. Classificação funcional de algoritmos de RWA (modificado [CHOI, 2000])

A ordem de seleção é a seqüência de seleção de *lightpaths* a ser roteado (ou a ser alocado). A regra de seleção é o critério de decisão para escolher um dos candidatos disponíveis. Por outro lado, técnicas de seleção combinacional consideram a interdependência de roteamento de *caminho óptico*.

Os métodos combinacionais são divididos em duas aproximações: mecanismos ótimos e heurísticos. A aproximação ótima usa todas as possíveis combinações da interdependência. Os métodos Heurísticos reduzem o espaço de combinação. A seleção ótima alcança o melhor resultado, mas o custo da complexidade computacional é crítico.

Um número de algoritmos heurísticos tais como algoritmos genéticos, *Simulated Annealing* (ou arredondamento aleatório - *random rounding*), e TABU tem sido propostos e provêm bom desempenho, enquanto o tempo de computação não é exponencialmente incrementado [CHOI, 2000].

Em trabalhos considerando algoritmos genéticos, Sinclair [SINCLAIR, 1993] usa uma codificação *bit-string* compacta das tabelas de roteamento com operadores convencionais, mas empregando uma função de penalidade para eliminar *loops* de roteamento infinito.

Em [SHIMAMOTO, 1993] é abordado o roteamento dinâmico em redes de circuitos comutados. Um indivíduo, no seu algoritmo, é representado como uma cadeia (*string)* de índices em uma tabela de busca dos k-caminhos mais curtos (*k-shortest paths*) para cada par de nós. No trabalho de Mann [MANN, 1995], roteamento estático é abordado usando uma representação similar ao de Shimamoto, mas codificado como bits antes que como inteiros.

Em trabalhos sobre alocação de comprimentos de onda, em [TAN, 1995] se descreve algumas aproximações de solução baseadas em GA (*Genetic Algorithm*) para redes de transporte transparentes multi-comprimento de onda, no qual combina-se um *bit-string* GA para a seleção de rota com uma heurística para alocação de fibra e comprimento de onda. Posteriormente, em [SINCLAIR, 1998] e [SINCLAIR2, 1998] é desenvolvido um GA híbrido para roteamento, escolha de fibra e alocação de comprimento de onda usando uma representação orientada a objetos e operadores específicos ao problema. Em contraste, Abed [ABED, 1996] aplica um *bit-string* GA para projetar a topologia lógica de uma rede LAN ou MAN usando alocação de comprimento de onda em uma única fibra óptica.

3.10 RWA COM CONVERSÃO DE COMPRIMENTO DE ONDA

O desempenho das redes WDM pode ser melhorado se os nós intermediários da rede possuírem recursos de conversão de comprimento de onda [RAMAMURTHY, 1998], [BARRY, 1996], [SUBRAMANIAN, 1996]. Uma rede que suporta conversão plena em todos os nós (conversão ubíqua) é funcionalmente equivalente a uma rede comutada por circuito. Ou seja, a requisição de caminhos ópticos é rejeitada somente quando não há capacidade disponível no caminho.

Como foi dito, este trabalho só enfocará a problemática de RWA nas redes sem conversão de comprimento de onda já que, em muitos casos, não é viável economicamente ter conversores em cada um dos nós por ser estes muito onerosos. Para amenizar a viabilidade econômica, projetistas consideram ter alguns nós com recursos de conversão. Então, as questões neste tipo de redes são:

a) Quantos nós de uma rede devem ter capacidade de conversão?

b) Onde estes conversores devem estar localizados na rede?

c) Que tipo de conversão o nó deve ter?

d) Quantos conversores deve um nó ter?

3.11 COMENTÁRIOS E CONSIDERAÇÕES FINAIS

Neste Capítulo foram vistos diferentes propostas para RWA em redes WDM roteadas por comprimento de onda. Para redes IP/OTN com WDM um caminho dinâmico é estabelecido pelo plano de controle com base na execução de um algoritmo de RWA, o qual, de maneira geral, se encarrega de selecionar a "melhor" rota e um canal óptico disponível. Porém, a imposição de continuidade no comprimento de onda aumenta a probabilidade de bloqueio das conexões, degradando, conseqüentemente, o desempenho da rede.

Outra importante preocupação a levar em conta no atendimento de uma requisição é a diferença existente entre as probabilidades de bloqueio de conexões cujas rotas apresentam tamanhos diferentes (número de saltos). Aspectos tais como justiça/eqüidade precisam ser considerados.

Assim, para um algoritmo de RWA selecionar a "melhor" rota é necessário levar em conta a combinação de diversos fatores (número de saltos, largura de banda, tráfego, qualidade de serviço, etc.). Estes fatores "administrativos" definem o chamado "custo" dos enlaces, que fará parte determinante na seleção da rota. Um adequado comprimento de onda disponível estabelecerá, assim, o caminho solicitado. Esta informação deve ser logo distribuída para todos os nós da rede através de protocolos de roteamento e sinalização no plano de controle, para o estabelecimento do *caminho óptico* e atualização de tabelas. Cada um destes passos precisa ser cuidado e otimizado.

Capítulo 4

"E há de ser que todo aquele que invocar o nome do Senhor será salvo; ....
e entre os SOBREVIVENTES aqueles que o Senhor chamar".
JI 2:32

4 SOBREVIVÊNCIA

4.1 INTRODUÇÃO

A sobrevivência de redes, particularmente no contexto das redes ópticas, tem motivado forte interesse em *operadoras* e pesquisadores pela necessidade de implementação de mecanismos que agreguem confiabilidade à rede. Hoje em dia a transmissão de aplicações críticas tais como a transmissão de mídias em tempo real, negócios sobre a rede, tele-medicina, operações bancárias e financeiras, etc. precisam, além de segurança, de sistemas de proteção/restauração adequados que garantam continuidade do serviço.

Sobrevivência (*Survivability*) se refere à capacidade da rede de transferir o serviço interrompido sobre a capacidade de reserva da rede para driblar uma contingência de falha [CHOI, 2005]. Isto é um requisito crítico para as redes IP sobre WDM.

O projeto de uma rede de telecomunicações que permita manter um nível aceitável de serviço quando a ocorrência de uma falha é um dos mais importantes desafios para os operadores de redes. O objetivo principal da sobrevivência de uma rede é restaurar o tráfego afetado por uma falha. Assim, a relevância da sobrevivência está relacionada com a confiabilidade do serviço que se fornece.

Nos EE.UU, por exemplo, se uma rede tiver uma queda do serviço por mais de 30 minutos, que afete a 30.000 ou mais clientes deve ser reportado à FCC [MANCHESTER2, 2004]. Além do descrédito que isto representa para o provedor do serviço, a insegurança nos clientes levará à busca de novas soluções. Logo, *operadoras* vêm dando muita importância a este tema, oferecendo sobrevivência como importante valor agregado na sua estratégia de mercado.

A eleição de um esquema de sobrevivência é uma negociação entre a utilização dos recursos da rede (custo) e o tempo de interrupção do serviço. Para ajudar nesta negociação, os provedores dos serviços de rede esperam oferecer diferentes ofertas de serviços ou níveis dos mesmos.

Assim, pode-se classificar os caminhos num pequeno conjunto de níveis de serviço. Entre outras coisas, estes níveis de serviço definem as características de confiabilidade do caminho. O nível de serviço associado com um caminho dado mapeia-se com um ou mais esquemas de proteção e restauração durante o estabelecimento do caminho. Um diferenciador entre estes níveis de serviço é o tempo de interrupção do serviço no caso de falhas da rede, que se define como o tempo transcorrido entre a aparição da falha e a restauração do mesmo. A eleição do nível de serviço (ou esquema de proteção/restauração) pode ser dada pelos requisitos de serviço das distintas aplicações.

Os contratos feitos com sistemas digitais síncronos consideram 0,01% do tempo (~52 minutos por ano) como tempo máximo permitido para que o sistema fique inoperante entre um cliente e uma central de telefonia. O dobro deste tempo pode ser aceito para a interconexão entre dois clientes passando por uma central.

Os possíveis componentes que podem falhar nas redes WDM são enlaces, fibras, nós e canais (comprimentos de onda). O corte de uma fibra causa uma falha de enlace. Quando um enlace falha, todas as fibras que o constituem falharam. Uma falha de nó pode ser causada devido a falhas no OXC e um canal pode falhar devido a falhas nos comutadores associados ao OXC [MURTHY, 2002] ou a falhas nos *lasers* de emissão de um comprimento de onda dado.

As falhas encontradas com mais freqüência em sistemas de comunicações ópticas são as rupturas acidentais de condutores de fibra e os defeitos nos dispositivos de comutação [DONGYUN, 2000]. Para superar estas contingências, a técnica mais usada é a pré-configuração de reserva de capacidade para cada caminho de trabalho e comutar para estes recursos reservados, para manter a continuidade do serviço quando acontecer uma falha. O procedimento parece intituivo, porém o desenvolvimento de uma efetiva e eficiente aproximação para alocar reserva de capacidade é ainda uma questão aberta para os pesquisadores.

A Tabela 4.1 apresenta dados típicos de taxas de falhas em elementos de rede (transmissor, receptor, fibra, etc.), e os respectivos tempos para a sua reparação segundo estatísticas levantadas pela *Telcordia* e apresentadas nos trabalhos de Zhang e To, [ZHANG, 2004] [TO,1994].

Tabela 4.1 – Taxas de Falhas e Tempos de reparação.

Métrica	**Estatísticas *Telcordia***
Equipamento MTTR	2 h
Corte de fibra MTTR	12 h
Taxa de corte de fibra	4,39/ano/1000 milhas
Taxa de falha do TX	10.867 FIT
Taxa de falha do RX	4311 FIT

Onde MTTR (*Mean Time To Repair*) é o tempo médio para reparos, e FIT (*Failure-in-Time*) é a média do número de falhas que acontecem em 109 horas. Atributos de qualidade costumam ser apresentados na forma de MTTR e no Tempo Médio entre Falhas (MTBF: *Mean Time Between Failure*).

Na nomenclatura de sobrevivência, o *caminho óptico* que transporta o tráfego numa operação normal é conhecido como *caminho óptico* primário, *caminho óptico* de trabalho ou *caminho óptico* de serviço. Quando um caminho primário falha, o tráfego é re-roteado sobre um novo *lightpath* conhecido como caminho óptico *backup* ou caminho óptico de proteção.

4.1.1 Ameaças ao Sistema da Rede

Os termos “falhas”, “acidentes” ou “ataques” [FISHER, 1997], são eventos que representam uma possível ameaça ao sistema, geralmente difícil de diferenciá-los entre si.

As falhas são eventos potencialmente destrutivos causados por deficiências no sistema ou em elementos externos do qual o sistema é dependente. Falhas podem ser causadas por erros de *software*, problemas no hardware ou dados corrompidos.

Os acidentes correspondem a toda gama de desastres geralmente causados por eventos externos ao sistema. Desastres naturais e erros humanos estão nesta categoria. É o maior problema nas redes de comunicações.

Os ataques ao sistema geralmente são causados por pessoas. Os problemas que mais se destacam incluem intrusões, escutas (*probes*) e interrupção do serviço (*denial of service*). A técnica adotada para solucionar os ataques é o emprego de mecanismos de segurança, que restringem os recursos oferecidos pelo sistema. Este tipo de problema concerne mais à área de segurança de rede e não serão abordados neste trabalho.

De qualquer maneira os sistemas nem sempre podem esperar pela identificação da causa do problema para tomar alguma medida devido à urgência em restabelecer o fluxo de transmissão da informação à sua normalidade. A função dos sistemas sobreviventes é reagir e se recuperar do problema ocorrido independentemente da identificação da causa.

O sistema deve ter a capacidade em manter os serviços essenciais e atender seus requisitos, mesmo que parte do sistema fique incapacitada. Uma estratégia seria manter os serviços mais importantes durante um problema, enquanto que os serviços não essenciais podem ser interrompidos e recuperados posteriormente. Nesta abordagem é importante a diferenciação dos serviços.

4.1.2 Controle do Mecanismo de Sobrevivência: Centralizado ou Distribuído

Um esquema de sobrevivência pode ser controlado de maneira centralizada ou distribuída. Um controle distribuído é preferido quando a rede de transporte é muito extensa. Um protocolo de controle distribuído precisa necessariamente de algumas mensagens de controle para a troca de informação entre os nós. Um controle centralizado é uma boa alternativa quando as dimensões da rede não são muito longas e a quantidade de nós é reduzida.

4.1.3 Demanda de Tráfego Estática ou Dinâmica

A demanda de tráfego pode ser estática ou dinâmica. Numa demanda de tráfego estático um conjunto de demandas de conexão é dado *a-priori*. O objetivo é alocar caminhos com capacidade de proteção para todas as demandas minimizando a capacidade reserva requerida. Este problema é relevante na fase de planejamento para determinar a capacidade necessária no futuro com base nas demandas atuais e as esperadas.

No caso de tráfego dinâmico as demandas chegam à rede de uma maneira aleatória. Uma vez estabelecida a proteção para a requisição esta é mantida por um tempo aleatório antes

de ser terminada. Aqui, o objetivo é minimizar a probabilidade de bloqueio das demandas do cliente.

4.2 CRITÉRIOS DE SELEÇÃO DE ESQUEMAS DE SOBREVIVÊNCIA

Para fazer uma adequada escolha entre vários mecanismos de recuperação devem ser observados os seguintes critérios:

Robustez: Os esquemas de recuperação com caminhos pré-estabelecidos, não poderão recuperar as falhas da rede que afetem simultaneamente os caminhos de trabalho e de proteção. Assim, se deve eleger idealmente estes caminhos para que sejam tão disjuntos quanto possível, de maneira que qualquer caso de falha simples não afetará a ambos caminhos [MANNIE, 2002].

A robustez de um esquema de recuperação também se determina pela quantidade de largura de banda reservada para recuperação – a medida que a quantidade compartilhada de largura de banda de proteção se incrementa usando os métodos clássicos (a largura de banda reservada diminui), o esquema de recuperação chega a ser menos robusto às falhas. Claramente, é necessária uma maior capacidade se pretende-se um maior grau de recuperação da falha. Assim, o grau em que a rede está protegida é determinado pela política que define a quantidade de largura de banda reservada.

Tempo de recuperação: Em geral, são desejados esquemas de proteção e restauração que possam agir rapidamente ante a contingência de uma falha. A proteção local (de enlace) será geralmente mais rápida que os esquemas fim-a-fim.

Os objetivos do tempo de recuperação para a comutação de proteção SONET/SDH (não inclui o tempo de detecção de falha) está especificado em 50 ms de acordo com [ITU-T G.841, 1996] levando em conta as restrições quanto à distância, número de conexões implicadas, e no caso de proteção melhorada em anel, o número de nós do anel.

Compartilhamento de Recursos: A proteção de enlace 1+1 e 1:N, e a proteção do caminho extremo-a-extremo, requerem caminhos de recuperação dedicados com limitada possibilidade de compartilhar recursos: o 1+1 não permite compartilhamento, 1:N permite algum compartilhamento de recursos de proteção e suporte de tráfego extra. A flexibilidade está limitada devido às restrições da topologia [MANNIE, 2002].

4.3 ETAPAS NA SOBREVIVÊNCIA DE UMA REDE

A recuperação de uma falha da rede tem lugar em várias etapas que incluem a detecção da falha, a localização da falha, a notificação, a recuperação (proteção/restauração) e o restabelecimento do tráfego.

A detecção da falha depende da tecnologia e sua implementação. Em geral, as falhas são detectadas por mecanismos de nível mais baixo (p.e. SONET/SDH usa *Loss-of-Light* (LOL)). Quando um nó detecta uma falha, pode-se enviar um alarme até uma entidade, a qual tomará as ações apropriadas, ou o alarme pode-se propagar a um nível mais baixo (p.e. SONET/SDH AIS).

A localização da falha pode-se conseguir via protocolos. Por exemplo, no plano de controle GMPLS (*Generalized Multiprotocol Label Switching*), é usado o protocolo LMP para a localização do problema.

A notificação da falha também pode-se obter via protocolos de sinalização. Por exemplo, no mesmo GMPLS, usando a notificação GMPLS RSVP-TE/CR-LDP.

Na recuperação basicamente se tem dois tipos de mecanismos: proteção e restauração.

4.3.1 Mecanismos de Recuperação

Se recursos *backup* (rotas e comprimentos de onda) para um *caminho óptico* são pré-calculados e reservados, então temos estabelecido um esquema de proteção para o respectivo *caminho óptico*. Por outro lado, se uma falha acontece e recursos *backup* têm de ser obtidos dinamicamente para cada conexão interrompida, então nesse caso temos um esquema de restauração [RAMAMURTHY, 2003].

Os mecanismos de restauração utilizam os recursos da rede mais eficientemente que os mecanismos de proteção, pois não necessitam alocar recursos previamente. Neste mecanismo, o canal óptico de restauração será estabelecido somente quando a falha de um enlace afetar o caminho primário da conexão. Os mecanismos de proteção alocam previamente os recursos e, conseqüentemente, prejudicam a aceitação de conexões futuras. Apesar disto, os mecanismos de proteção oferecem um tempo de recuperação consideravelmente menor do que os de restauração e garantem a respectiva recuperação, coisa que os esquemas de restauração não podem garantir completamente.

Em proteção, capacidade reserva é estabelecida geralmente durante a alocação do caminho. Em restauração, a capacidade reserva que ainda é disponível depois da ocorrência da falha, é usada para re-roteamento da conexão perdida [WANG, 2002].

Proteção e restauração podem ser aplicadas localmente (enlace) ou extremo-a-extremo (caminho). Tratada localmente, a proteção e restauração se enfocam na proximidade local da falha com o objetivo de reduzir o retardo no serviço de recuperação. Por exemplo, na proposta extremo-a-extremo no GMPLS, os nós origem e destino do caminho LSP (*Label Switched Path*) se encarregam de controlar a recuperação.

4.3.1.1 Esquemas de Proteção

Esquemas de proteção podem ser classificados como proteção em anel (*ring protection*) e proteção em malha (*mesh protection*). Esquemas de proteção em anel incluem APS (*Automatic Protection Switching*) e SHR (*Self-Healing Rings*) [ZHANG, 2004]. Tanto proteção em anel como em malha podem ser divididos em dois grupos: proteção de caminho e proteção de enlace.

Na proteção de caminho (*path protection*), o tráfego é re-roteado através de um caminho *backup* toda vez que acontece uma falha de enlace no caminho de trabalho. Os caminhos *backup* e de trabalho devem ser disjuntos para que uma única falha de enlace não possa perjudicar ambos os caminhos.

Na proteção de enlace (*link protection*), o tráfego é re-roteado só ao redor do enlace afetado. A proteção de caminho leva a um eficiente uso dos recursos *backup* e baixo retardo de propagação fim-a-fim. Para a recuperação do caminho, proteção de enlace provê um curto tempo de comutação para proteção.

Tem-se também introduzido o conceito de sub-caminho de proteção (*sub-path protection*) numa rede em malha, dividindo um caminho primária numa seqüência de segmentos e protegendo cada segmento separadamente. A proteção de sub-caminho óptico é um mecanismo alternativo que reduz o tempo de restauração da conexão. Esta proteção, proposta por Ou [OU, 2002] e Zhang [ZHANG, 2003], proporciona tempos de restauração menores, pois a sinalização da falha não necessita percorrer todo o caminho óptico para iniciar os procedimentos de recuperação. Em contrapartida, este mecanismo prejudica a eficiência dos recursos da rede.

Outra técnica é feita dividindo a rede em diferentes domínios, no qual um segmento de *caminho óptico* num domínio deve ser protegido pelos recursos do mesmo domínio [ANAND, 2002]. Comparado com proteção de caminho, proteção de sub-caminho pode alcançar alta escalabilidade e tempos de recuperação rápidos com um pequeno sacrifício no uso de recursos [ZHANG, 2004].

Os esquemas de proteção de caminho, sub-caminho e enlace podem ser dedicados ou compartilhados. Em proteção dedicada são usados comprimentos de onda *backup* dedicados só para o caminho de trabalho a ser protegida. Já quando são usados caminhos *backup* compartilhados, comprimentos de onda podem ser usados por diferentes caminhos de trabalho desde que estes não formem parte do mesmo grupo de enlaces com risco compartilhado.

4.3.1.2 Esquemas de Restauração

Restauração dinâmica pode também ser classificada como restauração de caminho, sub-caminho ou enlace [WANG, 2002].

Na restauração de caminho quando um enlace falha, os nós fonte e destino de cada conexão que atravessa o link em falha são informados do problema. Os nós fonte e destino de cada conexão independentemente descobrem um caminho *backup* fim-a-fim. Na restauração de sub-caminho, quando um enlace falha o nó *upstream* do respectivo enlace é quem detecta a falha e descobre um caminho *backup* desde ele (o nó *upstream*) até o correspondente nó destino, para cada conexão interrompida. Na restauração de enlace os nós finais do *link* que tem falhado, dinamicamente, descobrem um caminho ao redor do enlace para cada conexão que atravessa o *link*.

Os esquemas de recuperação são apresentados na Figura 4.1.

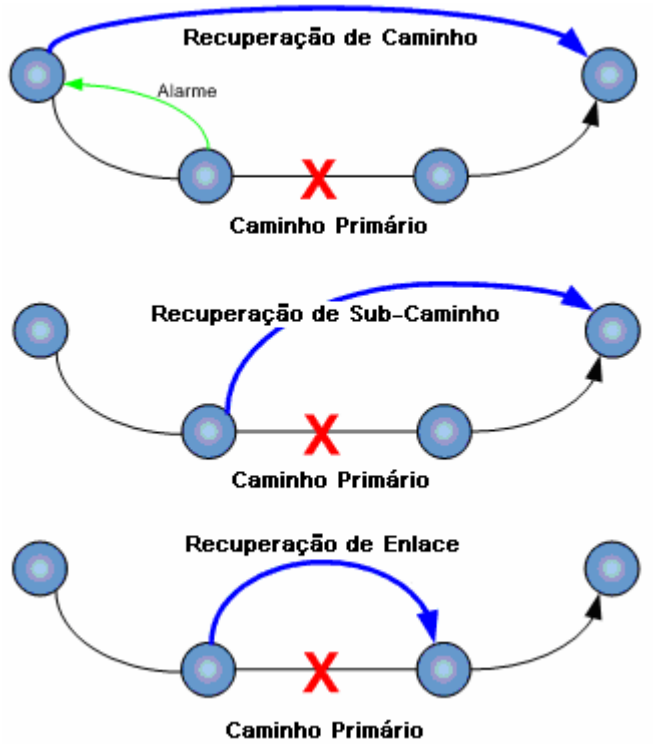


Figura 4.1 - Esquemas de recuperação: Caminho, Sub-Caminho e Enlace.

Entre estes três tipos de recuperação, a recuperação de enlace é a mais rápida e a de caminho é a mais lenta. A Figura 4.2 apresenta um resumo dos esquemas de sobrevivência.

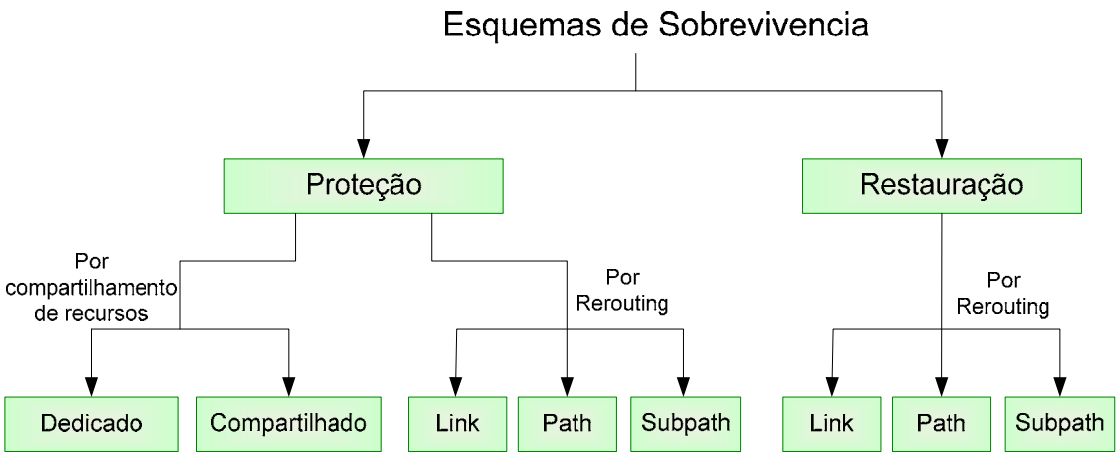


Figura 4.2 - Esquemas de Proteção e Restauração para redes em malha WDM

Geralmente, esquemas de restauração são mais eficientes no uso da capacidade da rede devido ao fato que este tipo de esquema não aloca capacidade reserva e provê resiliência contra diferentes classes de falhas; porém esquemas de proteção têm rápido tempo de recuperação e garante a respectiva recuperação, coisa que os esquemas de restauração não podem como um todo garantir.

4.4 EVOLUÇÃO DA SOBREVIVÊNCIA NA REDE DE TRANSPORTE

Redes de Transporte legadas compreendem a funcionalidade para prover transporte, multiplexação, comutação, supervisão e sobrevivência da camada de serviço. O núcleo da rede de transporte está atualmente num período de transição, evoluindo desde redes SONET/SDH baseados em TDM, para redes ópticas baseadas em WDM com transporte, multiplexação, roteamento/comutação, supervisão e sobrevivência suportados na camada óptica [ZHENG, 2004]. Os serviços de rede também estão em transição, migrando de serviços baseados em voz para serviços baseados em pacotes.

Estes acontecimentos têm levado os operadores de rede a reconsiderar os seus mecanismos de sobrevivência tradicionais. Arquiteturas de rede com sobrevivência foram desenvolvidas com base no paradigma *Circuit-Switched*/TDM. Com a expansão da Internet e aplicações multimídia tem sido necessária a migração para redes comutadas por pacotes/DWDM, com a necessária evolução para novos esquemas de sobrevivência na rede.

4.4.1 Sobrevivência baseada em APS (*Automatic Protection Switch*)

A classe mais simples de mecanismos para sobrevivência de uma rede no evento de uma falha num elemento de rede ou link é o APS. O esquema APS envolve a reserva de um canal de proteção (dedicado ou compartilhado) com a mesma capacidade do canal primário a ser protegido. As diferentes técnicas APS são caracterizadas pelos seguintes critérios:

- A topologia: Linear ou *Anel* (*malha* não é suportada por APS);
- Se o canal de proteção transporta uma cópia *backup* do tráfego permanentemente ou só quando requerido para proteção;
- Se o canal de proteção é compartilhado entre canais de trabalho que podem potencialmente necessitar proteção;
- Se ambas as direções de transmissão comutam (comutação bidirecional) para canais de proteção quando uma falha acontece numa direção, ou só a direção afetada comuta (comutação unidirecional); e
- Se a rede automaticamente reverte o tráfego para os canais de trabalho depois de esta ter sido restaurada (*revertive switching*), ou continua a seguir usando o canal de proteção (*non-revertive switching*).

4.4.1.1 APS em Topologias Ponto-a-Ponto

As topologias Ponto-a-Ponto são usualmente utilizadas num sistema que precisa só de caminhos que conectem dois nós entre si. Na proteção linear a entidade a ser protegida segue uma rota ponto-a-ponto.

No paradigma *Circuit-Switched*/TDM, o APS é o protocolo usado para proteção em redes SONET/SDH contra falhas de nós e enlaces em redes ponto-a-ponto.

Em qualquer esquema APS, o elemento de rede que detecta a condição de falha também inicia a ação de comutação de proteção, e é chamado de *tail-end node*. O outro extremo da proteção é chamado de *head-end node*. A função principal do nó *head-end* é dividir o sinal elétrico do enlace de trabalho afetado (faz uma cópia duplicada do sinal) e alimentá-lo no canal de proteção. Esta operação é chamada de função *bridge*. Assim, o APS provê proteção por redirecionamento automático do tráfego afetado pela falha para rotas alternativas. Tem-se aqui três tipos de mecanismos básicos de proteção: 1+1 , 1:1 e 1:N

Em proteção 1+1 o *bridge* está sempre presente. Em proteção 1:1 ou 1:N o nó *tail-end* faz um *upstream* requisitando o *bridge*. Em SONET/SDH esta sinalização é transmitida em 2 bytes de *overhead*, os quais constituem o canal de sinalização APS. Os critérios típicos para iniciar um APS são:

- Detecção de uma falha (LOS: *Loss-of-signal*, LOF: *Loss-of-Framing*);
- Falha de Sinal (excessiva taxa de erro de bit – BER);
- Degradação de sinal (Alto BER relativo);
- Comandos iniciados externamente desde o OSS (Sistema Operativo).

Estes critérios formam uma hierarquia de prioridades, com comandos desde o OSS (funções de manutenção, por exemplo) com a maior prioridade, seguida de detecção de falhas.

Proteção 1+1

Aqui, um sinal SONET/SDH é transmitido através de dois caminhos disjuntos desde uma fonte até um destino. O destino decide qual sinal vai receber baseado no melhor entre os dois sinais, estas indicações são providas pela subcamada de seção (*multiplex section sublayer*). Na prática, cada caminho fica protegido por um outro caminho dedicado

(*protection section*). Comutação de proteção unidirecional não precisa de um canal de APS para coordenar *endpoints*; porém, um canal de APS é necessário para comutar proteção bidirecional [CAVENDISH, 2000] [ITU-T G.841, 1996].

Tipicamente, em SONET/SDH, o canal de proteção é um OC-n completo. Como apresentado na Figura 4.3, quando o elemento de rede detecta que o tráfego que chega a partir do canal de proteção é melhor do que o do canal de trabalho, este comuta para tomar o tráfego desde o canal de proteção.

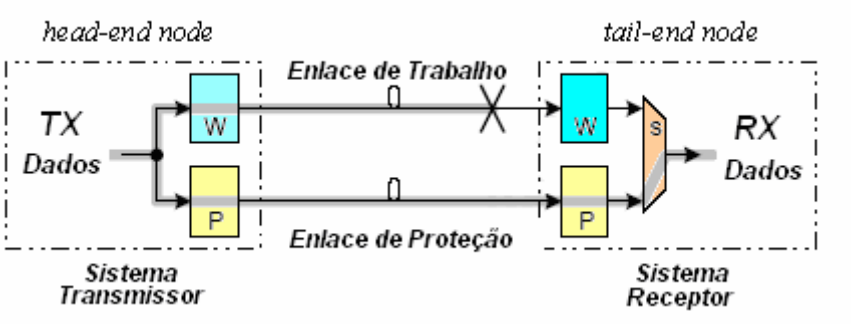


Figura 4.3 - Proteção 1+1 APS

Proteção 1:1

Em proteção 1:1, dois caminhos disjuntos são também usados, com a diferença que o sinal SONET/SDH é transmitido só por uma via, o chamado caminho de trabalho (*working section*). O outro caminho, chamado de caminho de proteção, fica ocioso, porém pode também ser usado para transporte de tráfego não protegido, conhecido como tráfego extra (*extra traffic*), o qual é interrompido quando a fibra de proteção é necessária quando acontecer uma queda de enlace. O processo de retirar o tráfego extra é chamado de *traffic squelching.*

Proteção 1:N

Em proteção 1:N, N fibras de serviço são protegidas por um único caminho de proteção. Dado que N caminhos primários compartilham um único caminho de proteção, um canal de APS é necessário para coordenar a comutação quando acontecer uma falha. Aqui também tráfego extra pode ser transportado pelo caminho de proteção.

Quando uma falha acontece o *tail-end* informa ao *head-end* que precisa da operação de comutação para a linha de proteção. Este examina o estado atual do sistema de proteção e a

prioridade da condição para cada enlace de trabalho requisitando proteção, logo faz a comutação para o enlace de proteção. A Figura 4.4 apresenta este esquema.

O esquema 1:N APS amplia grandemente a disponibilidade do sistema contra falhas de uma única fibra. Este esquema é muito mais eficiente do que 1+1. Uma limitação existe, porém, quando é aplicado a algumas fibras que formam o sistema 1:N no mesmo cabo, ali não haverá sobrevivência quando acontecer o corte desse cabo.

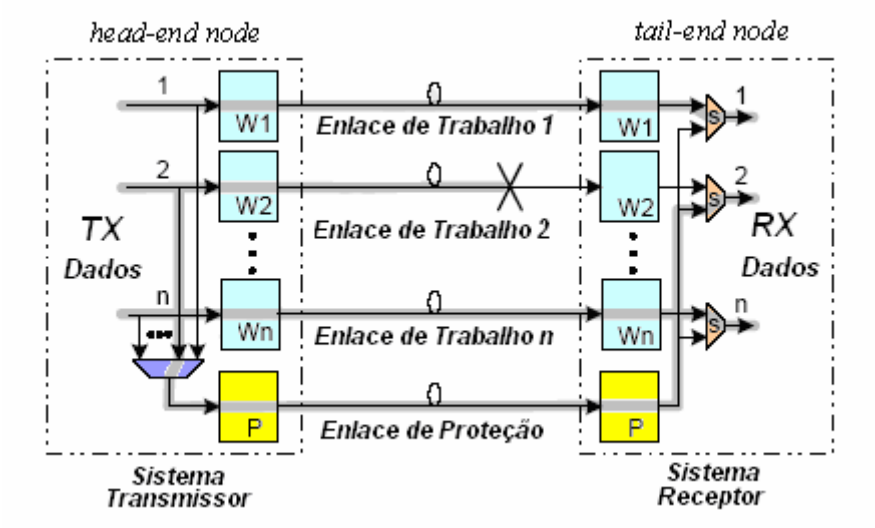


Figura 4.4 - Proteção 1:N APS

4.4.2 Sobrevivência em Topologias em Anel

Com a normalização da tecnologia SONET/SDH são também estabelecidas novas topologias de sobrevivência baseadas em anéis de proteção. Tecnicamente os anéis são extensões da tecnologia APS e são muito mais simples de entender do que os esquemas de sobrevivência para as redes *em malha*, embora estas últimas sejam mais eficientes. Uma estimação da arquitetura instalada de 1990 a 2004 nos diz que mais de 100.000 terminais ADM para anel SONET foram implantadas só nos Estados Unidos [GORSHE, 2005]. Isto nos mostra que esta topologia é de muita importância e estará ainda presente como uma tecnologia legada por um longo tempo. Têm-se dois tipos de proteção em anéis SDH:

- Anel de proteção dedicado MS (*multiplex section (MS) dedicated protection Rings*), chamado também de SNCP (*Sub-Network Connection Protection*) [MANCHESTER1, 1999]. Em SONET a denominação muda para UPSR (*Unidirectional Path Switched Ring*) [BLACK, 2002]. É usado roteamento unidirecional e proteção em nível de caminho; e,

- Anel de proteção compartilhada MS (*MS shared protection rings*), conhecida também como MSPRings. Em SONET a denominação muda para BLSR (*Bidirectional Line Switched Rings*) [BLACK, 2002]. É usado roteamento bi-direcional e proteção em nível de linha do tipo *loopback*.

4.4.3 Sobrevivência em Redes em Anel com MultiplexaçãoWDM

Os mecanismos de proteção em anel da arquitetura SONET/SDH tem sido considerado satisfatórios devido ao seu sistema simples de controle ante falhas e ao rápido serviço de recuperação [MURTHY, 2002]. Isto motivou que algumas operadoras continuassem com as redes anel, porém agora introduzindo tecnologia WDM. Conceitualmente o panorama é o mesmo, os comutadores de comprimento de onda são interconectados numa topologia *anel* similar. A maior diferença está nas capacidades de roteamento, comutação e conversão de comprimento de onda das redes em anel WDM [CAVENDISH, 2000].

Uma das propostas para sobrevivência em redes anel com multiplexação WDM é um *padrão* desenvolvido pelo grupo da IEEE 802.17 [IEEE 802.17, 2004] chamado de RPR (*Resilient Packet Ring*). Este protocolo de nível 2 foi desenvolvido para proporcionar serviços de transmissão de pacotes não orientados a conexão entre elementos de um anel SDH. Apresenta duas opções para recuperação de falhas:

- Faz um curto-circuito físico ao detectar uma falha;
- Avisa as estações que tomam as medidas para não encaminhar tráfego pela rota afetada.

4.4.4 Sobrevivência em Redes Malha com multiplexação WDM

Uma das vantagens de redes em *malha* WDM sobre as redes em anel baseadas no legado SONET/SDH é que as redes em malha WDM são capazes de suportar diferentes esquemas de proteção e podem ser mais eficientes. Particularmente, usando-se proteção de caminho compartilhado, as redes em *malha* WDM podem requerer só 40-60 % de capacidade extra para proteger a rede de qualquer falha simples, comparado com o 100% de capacidade de reserva usado pelos esquemas de proteção baseados em anéis SONET/SDH [RAMAMURTHY, 2003].

Num esquema de proteção compartilhado, os recursos de rede ao longo da rota *backup* podem ser compartilhados entre vários caminhos primários de diferentes conexões (sempre

que não compartilhem os mesmos enlaces). Assim, só uma rota primária (do conjunto de rotas primárias capazes de compartilhar o caminho *backup*), em caso de uma falha, desviará seu tráfego para o caminho de proteção. Da maneira geral, é assumido que [ZHANG, 2004]:

- Falhas de enlace é o cenário dominante em falhas de rede;
- Tem-se uma única falha de enlace num determinado tempo, e esta é reparada antes que a próxima falha aconteça. A probabilidade de múltiplas falhas acontecerem num determinado intervalo de tempo é remota.

4.5 PROTEÇÃO COMPARTILHADA EM REDES EM MALHA WDM

As atuais e grandes necessidades de largura de banda para o transporte de dados vêm sendo suportadas pelo avanço da tecnologia fotônica, com destaque nas tecnologias WDM e *Optical Cross-connects* (OXC). A tecnologia WDM permite a centenas de *lightpaths* serem multiplexados numa mesma fibra se alcançando capacidades efetivas na ordem dos Terabits por segundo. A grande quantidade de tráfego de informação é encaminhada pelos OXCs os quais, quando interconectados em topologia em malha, são controlados por um Plano de Controle (centralizado ou distribuído).

Nesta topologia, a sobrevivência também tem bastante relevância para o desenho robusto da rede. Devido ao potencialmente grande volume de informação que é transportado por um enlace de fibra, a ocorrência de uma falha pode ter desastrosas conseqüências tanto para a rede de transporte como para as redes clientes. A adoção de proteção compartilhada em redes WDM com topologia em malha pode alcançar 100% de recuperação ante uma única falha e com uma considerável redução da redundância em termos de consumo de capacidade da rede [HO, 2004].

Comparada com as redes ópticas legadas, três características são destacáveis nas redes ópticas WDM comutadas por comprimento de onda: demanda de tráfego dinâmico, controle distribuído e topologia em malha. A sobrevivência nestas redes tem muitos requisitos, incluindo eficiência na capacidade e recuperação rápida ante falhas, existindo entre ambas sempre um compromisso. Por outro lado, e se considerando uma única falha num determinado tempo, a capacidade destas redes para compartilhamento *backup* pode ser realizada em três níveis [LEI, 2003]:

Nível 1: Quando dois caminhos entre a fonte e o destino tem enlaces completamente disjuntos, eles podem compartilhar os mesmos recursos (o mesmo comprimento de onda, por exemplo) do mesmo caminho backup.

Isto é apresentado na Figura 4.7, onde os caminhos primários 1 e 2 estão completamente disjuntos, logo os seus caminhos *backup* podem compartilhar os mesmos enlaces e o mesmo comprimento de onda.

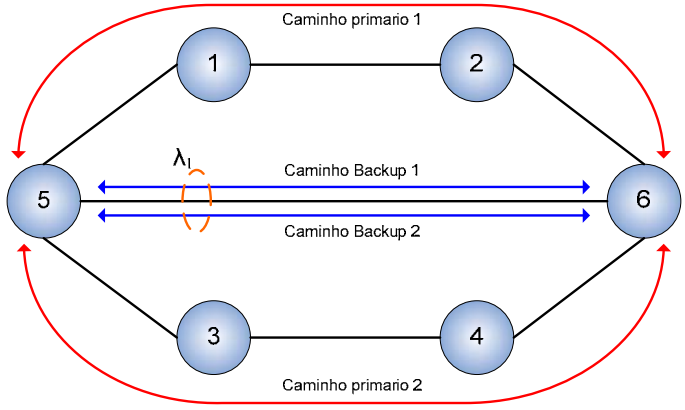


Figura 4.5 - Compartilhamento backup Nível 1.

Nível 2: O compartilhamento de recursos backup para requisições distintas que não têm enlaces comuns nos seus caminhos de trabalho também é possível.

A diferença com o nível 1 é que os caminhos de trabalho não têm os mesmos nós fonte-destino. Na Figura 4.8 os caminhos de trabalho (1-2, 3-4) não iniciam nos mesmos nós, mas os seus caminhos *backup* podem se compartilhar completamente, nos enlaces necessários.

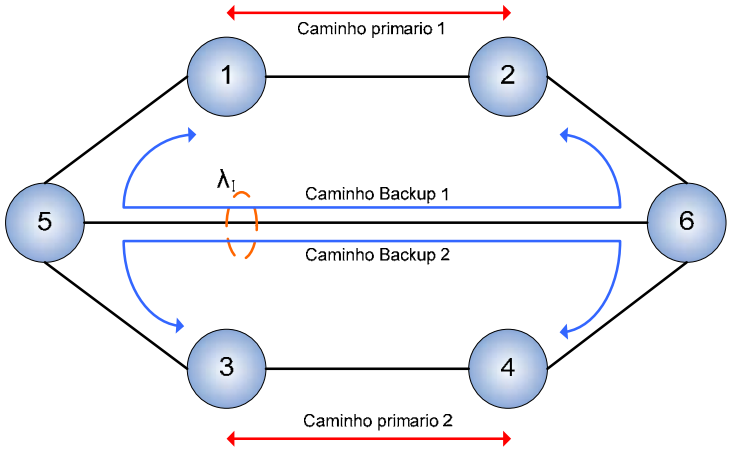


Figura 4.6 - Compartilhamento backup Nível 2.

Nível 3: O compartilhamento de recursos backup, mesmo que estes formem parte de demandas cujos caminhos de trabalho têm enlaces em comum, também é possível.

Na Figura 4.9 o caminho *backup* 1 seria usado para recuperar o enlace 1-3 do caminho primário 1. O caminho *backup* 2 seria usado para recuperar o enlace 1-2 do caminho primário 2.

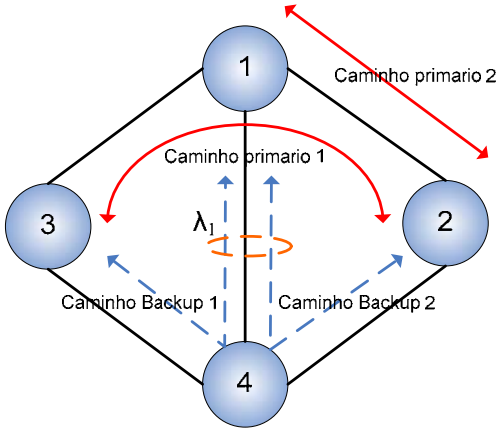


Figura 4.7 - Compartilhamento backup Nível 3

Embora os caminhos primários 1 e 2 tenham um enlace comum (o enlace 1-2), seus respectivos caminhos *backup* podem ainda compartilhar o mesmo enlace 1-4 e o mesmo comprimento de onda, pois uma única falha de enlace não prejudicará o serviço.

Compartilhamento *backup* de nível 1 e nível 2 podem ser aplicados tanto em sobrevivência baseada em caminho quanto em sobrevivência baseada em enlace. O nível 3 só pode ser aplicado a recuperação baseada em enlace.

O compartilhamento *backup* de nível 1 pode ser aplicado tanto em esquemas de proteção como em esquemas de restauração. Já o nível 2, normalmente, pode ser aplicado só para restauração [LEI, 2003]. Porém, novos esquemas de sobrevivência, como o apresentado nesta Tese, pretendem aproveitar ao máximo a capacidade de compartilhamento de rota *backup*.

4.6 RECUPERAÇÃO DE FALHA EM REDES MULTICAMADAS

No caso de multicamada o mecanismo de recuperação deve operar numa escala de tempo de resposta ascendente. A Tabela 4.2 apresenta vários mecanismos com seus respectivos tempos de recuperação numa rede multicamada [CAVENDISH, 2000].

Tabela 4.2 – Tempo de Recuperação de vários mecanismos de Sobrevivência.

Tecnologia		Detecção	Restabelecimento	Detalhes
WDM	WDM-OMS/OCh	1-10 ms	10-30 ms	Anel/P-P
SONET /SDH	SONET/SDH	0,1 ms	50 ms	Anel
	APS 1+1	0,1 ms	50 ms	P-P
	FDDI	0,1 ms	10 ms	Anel
	STM	0,1 ms	100 ms	
ATM	ATM PV-C/P 1+1	0,1 ms	10 ms * N	N=# hops
	ATM PNNI SPV-C/P SV-C/P	40 s	1-10 s	
IP	BGP	180 s	10-100 s	
	IGRP e OSPF	40 s	1-10 s	
	IS-IS	40 s	1-10 s	
	RIP	180 s	100 s	

Da Tabela 4.2 pode se ver que embora o tempo de re-estabelecimento em WDM seja mais rápido do que na tecnologia SDH, a detecção da falha leva mais tempo a ser feita. A recuperação de falhas introduzidas desnecessariamente nas camadas altas (ou seja, quando já se tem um mecanismo nas camadas inferiores) pode originar instabilidade das rotas e congestionamento de tráfego, devendo ser evitada. A verificação da persistência de problemas pode ser usada nas camadas superiores para permitir uma reação antecipada das camadas inferiores ante falhas.

4.7 SOBREVIVÊNCIA EM REDES GMPLS

Uma série de esquemas de sobrevivência tem sido proposta pelo IETF para o projeto de normalização do plano de controle GMPLS. Os diferentes esquemas têm distintas capacidades de compartilhamento com seus conseqüentes efeitos na sua eficiência.

Para o desenvolvimento de um plano de controle comum, tanto para redes ópticas como para as redes eletrônicas, são necessários mecanismos que permitam uma gerência inteligente de falhas por meio de protocolos de sinalização, roteamento e gerência de enlaces. Em nível de conexão a gerência de falhas em GMPLS é abordada em quatro passos primários: Detecção, Localização, Notificação e Mitigação.

A detecção de falhas deveria ser realizada na camada mais próxima à falha, a camada físico-óptica. Uma medida clássica de detecção de falhas nesta camada é a detecção de perda de luz (LOL, *loss of light*). Outras técnicas baseadas na relação sinal/ruído óptico (OSNR), a taxa de erro de bit (O-BER) óptica, dispersão, diafonia e atenuação têm sido desenvolvidas.

A localização de falhas requer a comunicação entre os nós para determinar onde aconteceu a falha. Uma conseqüência de se utilizar LOL para a detecção de falhas é que esta se propaga no sentido de *downstream* ao longo de todo o caminho da conexão, permitindo a todos os nós de *downstream* detectar a falha.

O protocolo LMP inclui um procedimento de localização de falhas projetado tanto para redes transparentes (*all-optical*) quanto para opacas (opto-eletrônicas). Este mecanismo se embasa no envio de mensagens *ChannelFail* de LMP entre nós adjacentes sobre um canal de controle, separado dos canais de dados. Esta separação do plano de controle e de dados permite que se use um único conjunto de mensagens para a localização de falhas, independentemente do esquema de codificação do plano de dados.

Quando detectada e localizada a falha é utilizada a proteção e restauração para mitigar o problema. A proteção e a restauração se têm abordado tradicionalmente utilizando duas técnicas: comutação de caminho e comutação de enlace. Na comutação de caminho a falha é tratada nos extremos do caminho (nós inicial e final). Na comutação de enlace a falha é tratada no nó de trânsito no qual se detectou a falha.

A comutação de caminho pode-se sub-dividir em proteção de caminho, com pré-alocação de caminhos de proteção e em restauração de caminho, onde as conexões são re-roteadas, tanto dinamicamente como também utilizando caminhos pré-calculados (mas não pré-alocados). A comutação de enlace pode-se dividir em proteção *span*, onde se comuta o tráfego para um canal paralelo alternativo e restauração de enlace, onde o tráfego se

comuta para uma rota alternativa entre os dois nós (isto implica atravessar nós intermediários adicionais).

Para utilizar a proteção devem existir mecanismos que possam:

- Distribuir as propriedades relevantes do enlace, como a largura de banda de proteção e as capacidades de proteção;
- Estabelecer caminhos secundários através da rede;
- Sinalizar um *comutador* desde o caminho primário ao secundário e o contrário.

4.7.1 Mecanismos de proteção GMPLS

Os mecanismos de proteção em GMPLS são os seguintes:

- Proteção 1+1: os dados da carga se transmitem simultaneamente sobre dois caminhos separados e se utiliza um seletor no nó de recepção para eleger o melhor sinal;
- Proteção M:N: são compartilhados M caminhos de *backup* pré-alocados entre N caminhos primários; porém, os dados não se replicam no caminho de *backup*, mas são alocados e transmitidos por ele só quando falha o caminho primário;
- Proteção 1:N: se compartilha um caminho *backup* pré-alocado entre N caminhos primários;
- Proteção 1:1: se pré-aloca um caminho *backup* dedicado para um caminho primário.

As proteções 1:N e 1:1 são casos especiais da proteção M:N.

4.7.1.1 Proteção Span ou Proteção de Enlace

A Proteção *span* é aplicada entre dois nós adjacentes e se embasa na comutação para um canal ou enlace de *backup* quando acontece uma falha. Como parte das extensões de roteamento GMPLS, o tipo de proteção do enlace se anuncia para que se possa utilizar a proteção *span* no cálculo da rota. Uma vez selecionada a rota, se faz a sinalização da conexão utilizando RSVP-TE ou CR-LDP.

Cada nó que proporciona uma proteção *span* dedicada 1+1 deve replicar os dados em dois canais separados. Isto requer utilizar o dobro da largura de banda da conexão entre o par de nós e a capacidade de replicar os dados em ambos os canais. Quando se detecta uma falha no nó de recepção, este deve comutar do canal de trabalho para o canal de proteção.

Na proteção *span* compartilhada M:N se tem que detectar as falhas antes de realizar a comutação já que os dados não se encontram replicados nos canais primário e de *backup*. Quando se localiza uma falha, o nó de *downstream* pode iniciar uma proteção *span* local enviando uma mensagem de *refresh* RSVP Path. As mensagens de *refresh* do caminho são elementos de RSVP que permitem aos nós intermediários atualizar o estado de um LSP. Isto permite realizar a comutação do canal primário para o de reserva. A troca prévia da configuração de proteção compartilhada utilizando LMP minimiza a possibilidade de um conflito no canal de *backup* (rótulo) quando é feita a comutação de proteção. A Proteção de Enlace é apresentada na Figura 4.10.

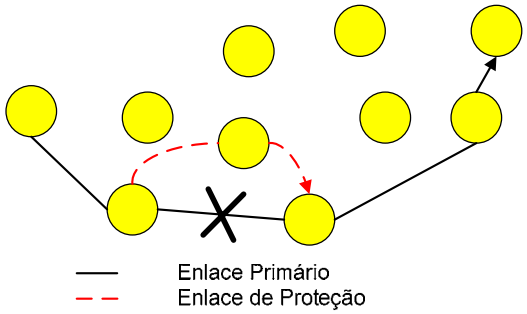


Figura 4.8 - Proteção de Enlace

4.7.1.2 Proteção de Caminho

A proteção de caminho é feita nos nós finais (iniciador e terminador) e requer a comutação para um caminho alternativo quando acontece uma falha.

Quando se tem calculado os dois caminhos, a fonte gera duas conexões roteadas explicitamente com os bits «dedicado 1+1» e «não protegido» ativos, respectivamente, no vetor de bits de proteção da correspondente mensagem de sinalização. O estabelecimento indica que estes dois caminhos desejam reservas compartilhadas. Para a proteção de caminho 1+1, a conexão se transmite simultaneamente sobre os dois caminhos separados e se utiliza um seletor no nó terminador para selecionar o melhor sinal. Em cada nó onde os dois caminhos se ramificam deve-se replicar os dados em ambos os ramos. Nos nós nos quais se unem os caminhos deve-se eleger os dados de um caminho com base na integridade do sinal.

Na proteção de caminho M:N, pré-estabelecem-se M caminhos distintos para a proteção compartilhada dos N caminhos principais. Estes caminhos secundários são utilizados para a comutação rápida quando o caminho principal falha. Mesmo que os recursos para estes

caminhos de *backup* estejam pré-alocados, o tráfego de baixa prioridade pode utilizar estes recursos tendo em conta que o respectivo tráfego será bloqueado se acontecer uma falha no caminho primário. A proteção de caminho é apresentada na Figura 4.11.

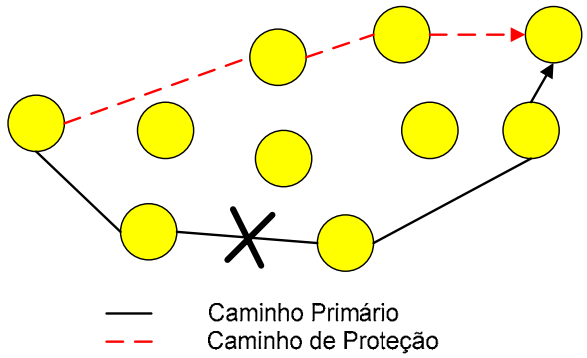


Figura 4.9 - Proteção de Caminho

4.7.2 Mecanismos de restauração em GMPLS

A restauração é projetada para reagir rapidamente ante falhas, utilizando a largura de banda eficientemente, mas normalmente requer o estabelecimento de recursos e o cálculo de rotas dinamicamente; por essa razão, leva mais tempo em comutar para um caminho alternativo do que as técnicas de proteção. A restauração pode ser implementada na fonte ou num nó intermediário uma vez que o nó responsável tenha sido notificado mediante os mecanismos de notificação mencionados anteriormente ou utilizando mensagens de erro padrões.

4.7.2.1 Restauração de linha

Para suportar a restauração de linha é selecionado um novo caminho num nó intermediário. Isto leva o tráfego a atravessar nós adicionais de trânsito. A restauração de linha pode ser benéfica para as conexões que atravessem múltiplos saltos e/ou longas distâncias, já que a latência na notificação da falha pode ser consideravelmente reduzida. Neste caso só se re-roteiam segmentos da conexão em lugar do caminho completo.

A restauração de linha pode romper as requisições caso esteja definida uma rota explícita para a conexão. As restrições utilizadas para rotear a conexão podem ser enviadas para que um nó intermediário que faz a restauração de linha possa calcular uma rota alternativa apropriada.

4.7.2.2 Restauração de caminho

A restauração de caminho comuta o tráfego para uma rota alternativa ao redor da falha, onde o novo caminho é selecionado no nó fonte. Pode-se otimizar o processo de restauração, por exemplo, pré-calculando rotas alternativas e salvando-as para uso futuro. Um caminho restaurado pode reutilizar nós do caminho original e/ou incluir nós intermediários adicionais. Os recursos dos nós de *downstream* são reutilizados (compartilhados) sempre que seja possível e os recursos dos nós intermediários que já não são necessários são liberados. Este compartilhamento de recursos aumenta as probabilidades da conexão para conseguir os recursos requeridos quando o re-roteamento está em progresso. Se os recursos são calculados e pré-alocados, o re-roteamento é mais rápido já que tais recursos estão garantidos, a não ser que falhem ou que estejam utilizados por conexões de maior prioridade.

Os esquemas de restauração podem ser divididos em 4 categorias [MANNIE2, 2002] em função do cálculo do caminho de restauração, a reserva de recursos de restauração e a função de alocação do canal de restauração serem feitos antes ou depois da falha. Os cinco mecanismos de sobrevivência são apresentados na Tabela 4.3 [LEI, 2003].

O desempenho de um esquema de sobrevivência introduz vários aspectos. Em [LEI, 2003], as categorias apresentadas na Tabela 4.3 são comparadas em dois aspectos: eficiência de capacidade e tempo de interrupção do serviço, se considerando uma única falha.

Tabela 4.3 - Alguns esquemas de Sobrevivência para GMPLS

Categoria	**Funções**			
	Cálculo de Caminho	Reserva de recursos	Alocação de Canal	Crossconnect
Proteção	Antes	Antes	Antes	Antes
Restauração1	Antes	Antes	Antes	Depois
Restauração2	Antes	Antes	Depois	Depois
Restauração3	Antes	Depois	Depois	Depois
Restauração4	Depois	Depois	Depois	Depois

Análise do tempo de interrupção do serviço

O tempo de interrupção do serviço consiste, geralmente, de duas partes: Tempo de gerenciamento da falha (T_M) que inclui o tempo para detecção, localização e notificação da falha; e o tempo de recuperação da falha (T_R), o qual deve incluir o tempo para o nó fonte

comutar o tráfego desde o caminho primário com falha para o caminho *backup* (T_S) e incluir o Tempo de cálculo da rota de recuperação (T_C), assim como o Tempo de configuração da rota de recuperação (T_{setup}), dependendo do esquema de sobrevivência selecionado.

O T_{setup} consistiria do Tempo de alocação de canal (T_A) e o Tempo de configuração do OXC (T_O), dependendo do esquema de recuperação selecionado. Estas relações são apresentadas na Figura 4.12.

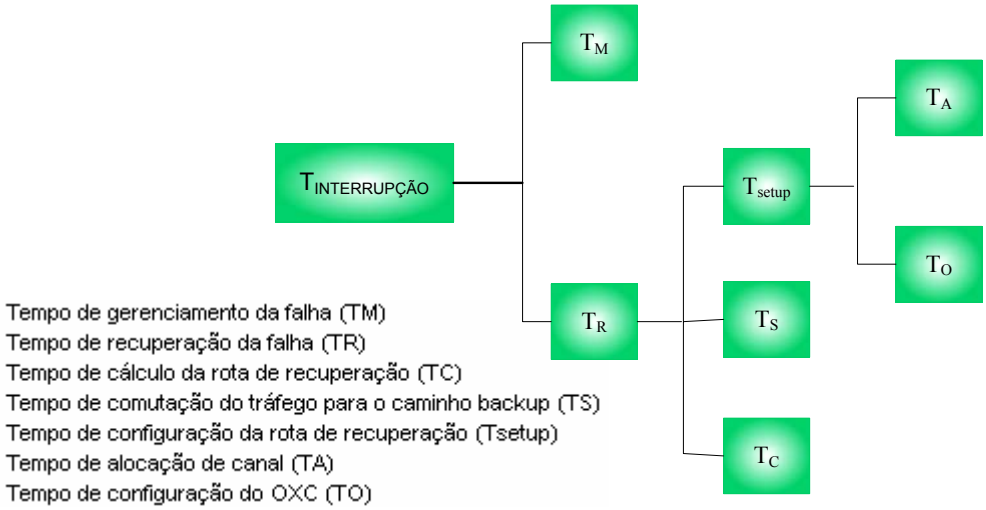


Figura 4.10 – Composição do Tempo de Interrupção de Serviço.

Assim, para *Restauração4* o Tempo de Interrupção de Serviço depois de uma falha ocorrer seria:

$$T_{INTERRUPÇÃO} = T_M + T_S + T_C + T_A + T_O$$

Para *Restauração2* e *Restauração3*, dado que a rota de recuperação tem sido pré-calculada antes da falha, o Tempo de Interrupção de Serviço depois de uma falha ocorrer seria:

$$T_{INTERRUPÇÃO} = T_M + T_S + T_A + T_O$$

Para *Restauração1*, dado que o cálculo da rota de recuperação e a alocação de canal tem sido pré-calculada antes da falha, o Tempo de Interrupção de Serviço seria:

$$T_{INTERRUPÇÃO} = T_M + T_S + T_O$$

Para *Proteção*, dado que todas as funções têm sido calculadas antes da falha, o Tempo de Interrupção de Serviço seria:

$$T_{INTERRUPÇÃO} = T_M + T_S$$

Assim, comparando os Tempos de Interrupção de Serviço de cada um destes mecanismos, se tem que:

Restauração4 > Restauração3 = Restauração2 > Restauração1 > Proteção

Além disto, dado que o tempo de notificação de uma falha de um esquema de sobrevivência baseado em enlace é geralmente mais curto do que num esquema de sobrevivência baseado em caminho, o Tempo de Interrupção de Serviço dos esquemas de sobrevivência baseados em enlace são mais curtos do que os baseados em caminho.

4.8 RWA SOBREVIVENTE (S-RWA)

Numa rede WDM em malha com comprimento de onda contínuo implementando proteção de caminho fim-a-fim, o problema de se encontrar um par de caminhos primário-*backup* com enlaces disjuntos e alocar um adequado comprimento de onda para cada caminho é conhecido como o problema de Alocação de Rota e Comprimento de Onda Sobrevivente (S-RWA).

Geralmente, um par de caminhos fonte-destino com o menor custo é estabelecido para o transporte do tráfego de dados. De maneira similar ao custo de um caminho primário não protegido, definido como a soma dos custos de todos os enlaces nele contidos, o custo do par primário-*backup* é a soma dos custos dos caminhos individuais.

Quando se procura por um esquema de proteção compartilhado, o custo de um par primário-*backup* pode apresentar diferentes configurações em função das prioridades e políticas que são estabelecidas para a criação dos caminhos. Aqui geralmente é priorizada a diversidade e a capacidade de compartilhamento visando à otimização de recursos ou a probabilidade de bloqueio, em detrimento de outros critérios (tempo de computação, por exemplo).

O par pode ser selecionado, tanto a partir de um conjunto pré-planejado de rotas alternadas, ou calculado dinamicamente. Dependendo das considerações de engenharia de tráfego, diferentes funções de custo podem ser aplicadas aos enlaces da rede, tais como aplicar valor constante (para minimizar a distância do salto), pelo comprimento do enlace (para minimizar o retardo), fração da capacidade disponível nos enlaces (para balanço da carga na rede), custo de rede (custo operacional, custo do equipamento, etc.) nos enlaces (para minimizar o custo) e assim por diante [ZHANG, 2004].

O problema de alocar o comprimento de onda (WA) pode ser considerado depois de ter sido estabelecido a rota do par primário-*backup*. Diferentes heurísticas têm sido propostas. O problema de WA pode também ser considerado juntamente com o cálculo da rota do par primário-*backup*, problema que tem sido provado ser NP-completo [ZHANG2, 2003]. Quando uma rede tem capacidade de conversão total de comprimento de onda, o assunto é reduzido a um problema de roteamento ótimo, o qual pode ser solucionado usando um dos diferentes algoritmos já existentes.

Além de heurísticas S-RWA, aproximações baseadas em programação linear (LP) são também usadas para tratar o problema. Aproximações LP podem ser usadas tanto para pré-calcular um conjunto de rotas candidatas quanto para calcular um par de rotas primário-backup em forma dinâmica, *on-demand*. Embora um esquema baseado em LP não seja muito escalável, por causa do cálculo intensivo necessário, ele pode ser usado para projetar eficientes algoritmos heurísticos.

A sobrevivência em redes IP-sobre-WDM, tratada nesta proposta, pode ser implementada tanto na camada WDM quanto na camada IP/GMPLS. Na camada WDM, cada caminho óptico primário é protegido por um outro caminho óptico geralmente disjunto. Na camada IP/GMPLS, cada LSP primário é protegido por um outro LSP. A proteção WDM proporciona um tempo de restauração menor do que a proteção IP/GMPLS, já que não depende de sinalização e temporização para a detecção da falha [BICUDO, 2005]. Como o mecanismo de proteção IP não tem acesso aos sensores/receptores ópticos que monitoram uma provável interrupção da portadora, estes precisam do envio periódico de mensagens *HELLO* para detectar a falha.

Um mecanismo integrado para permitir a sinalização do evento de falha da camada WDM para a camada IP, foi proposto por Zheng [ZHENG, 2003]. Mesmo assim, o tempo de restauração da proteção IP será superior ao da proteção WDM. Como um único canal óptico pode transportar até milhares de conexões LSPs, o desempenho da camada IP/GMPLS continua prejudicado pela sobrecarga computacional associada ao grande número de procedimentos necessários à recuperação da falha. A proteção WDM, em contrapartida, executa o procedimento somente uma vez para cada canal óptico. A desvantagem da proteção WDM é o isolamento entre recursos primários e de proteção, dado que, uma vez que um canal óptico é reservado para recuperação, este não será

cogitado como um recurso disponível. Na proteção IP/GMPLS este isolamento não ocorre, pois LSPs primários e de recuperação coexistem em um mesmo canal óptico.

Alcançar um tempo de restauração equivalente às redes SONET/SDH é necessário para a substituição desta tecnologia, ainda utilizada em telecomunicações. Para este objetivo é necessário o desenvolvimento de mecanismos de proteção WDM. Apesar de a proteção IP ser mais eficiente que a proteção WDM, a proteção WDM é a única capaz de atingir os 50 milisegundos das redes SONET/SDH [BICUDO, 2005].

4.8.1 Alocação de Reserva de Capacidade

Como se pode intuir a partir do conteúdo apresentado, o projeto de redes sobreviventes requer margens de capacidade; ou seja, reserva de recursos (comprimentos de onda e enlaces de fibra). Assim, qualquer projeto de algoritmo deveria objetivar a minimização dos recursos reservados. Técnicas de compartilhamento de recursos são muito usadas para reduzir a capacidade de reserva requerida.

O problema da alocação de reserva de capacidade (*spare capacity assignment*) tem sido formulado como um Programa Linear Inteiro (ILP: *integer linear program*). Dado que ILP é computacionalmente intratável [MURTHY, 2002], soluções baseadas em rápidas heurísticas que produzem soluções aproximadas são preferidas. Assim, um modelo de fluxo multi-objetivo (*multicommodity*) apresentado em [XIONG, 1999], [GROVER, 1999], [MURAKAMI, 1995], [IRASCHKO, 1996], [CAENEGEM2, 1997], [HERZBERG, 1995], [HERZBERG2, 1997], [OH, 2000], [DOUCETTE, 2001], usa um conjunto de caminhos pré-definidos para todas as demandas formando assim o espaço de busca com o objetivo de minimizar o custo de alocação de reserva de capacidade.

Um esquema de aproximação de K caminhos curtos para limitar o comprimento do conjunto de caminhos candidatos é usado em [XIONG, 1999], [GROVER, 1999], [IRASCHKO, 1996], [CAENEGEM2, 1997]. O método de Relaxamento de Lagrangian é usado em [DOSHI, 1999], [MEDHI, 2000] visando simplificar o problema original. Muitas Heurísticas têm sido apresentados na literatura [XIONG, 1999], [GROVER, 1999], [CAENEGEM, 1998], [CAENEGEM2, 1997], [MEDHI, 2000].

Em [PATEL, 2003] é apresentado um estudo comparativo de custos de mecanismos de alocação de reserva de capacidade e seu desempenho. A análise experimental mostra que a

topologia de rede, o padrão de demanda (ou matriz de tráfego) e o número de saltos por rota primária tem um significativo impacto no custo econômico da alocação de reserva de capacidade oferecida por um esquema sobre outro.

Posteriormente foram propostos mecanismos de sobrevivência visando uma rede que possa combinar as vantagens de redundância e resiliência da topologia em anel e as vantagens de eficiência e escalabilidade da topologia em malha. Dentre estas propostas, existem as que oferecem uma abordagem na camada IP/GMPLS como os algoritmos BIRA e HIRA proposto por Zheng et al. [ZHENG e MOHAN, 2003] e o algoritmo de Kodialam et al. [KODIALAM e LAKSHMAN, 2001], visando a versatilidade, maior granularidade e flexibilidade de configuração desta camada. Outras têm um enfoque mais voltado para a recuperação na camada WDM como em [WANG et al., 2002], [RAMAMURTHY e MUKHERJEE, 1999] e [ZHANG e MUKHERJEE, 2004], que proporcionam um tempo de recuperação menor, devido à menor granularidade e por não ser necessário sinalização extra. No trabalho de Ou *et al*. [OU et al., 2002] e Zhang et al. [ZHANG, 2003] são apresentados esquemas de proteção de sub-caminho como uma alternativa viável para reduzir o tempo de restauração, já que a sinalização não necessita percorrer toda extensão do caminho óptico para ser iniciado o procedimento de recuperação.

No desenvolvimento de Mohan e Murthy [MOHAN, 1999] [MURTHY, 2002] é considerado o problema do estabelecimento confiável de conexões para recuperação rápida de falhas em redes WDM roteadas por comprimento de onda com demanda de tráfego dinâmico. Aqui é usado o método de roteamento alternativo (*alternate routing*), onde cada par fonte-destino usa um conjunto de K rotas alternativas (rotas candidatas) pré-calculadas *off-line*. Neste trabalho se tem a seguinte notação:

'*link*' → enlace físico
'*wlink*' → canal-comprimento de onda num enlace físico
R_p e R_b → rotas candidatas primária e backup
w_p e w_b → comprimento de onda usado por um caminho óptico primário e backup
$< R_p; w_p >$ → *lightpath* primário (L_p)
$< R_b; w_b >$ → *lightpath* backup (L_b)

O par rota-comprimento de onda candidato com o menor custo é escolhido. O custo do *lightpath* primário (L_p) é dado pelo número de saltos ou *wlinks* usados por este.

Então, o custo de uma conexão usando o *lightpath* primário-backup < L_p; L_b > é dado por:

$$C(L_p; L_b) = C_p(L_p) + C_b(L_b; L_p);$$

O *pseudo-código* usado por esta proposta é dado a continuação:

Function $C_p(L_p)$
Begin
    custo ← *0;*
    Para cada wlink w_l *de* L_p *fazer*
    custo ← *custo + custo_do_Primário*(w_l)
    Return(custo)
End.
Function $C_b(L_b; L_p)$
Begin
    custo ← *0;*
    Para cada wlink w_l *de* L_b *fazer*
    custo ← *custo + custo_do_Backup*(w_l;R_p)
    Return(custo)
End.

Neste contexto, são analisados pelos autores três método de alocação de comprimento de onda: PDBWA-S, PDBWA-D e PIBWA (*primary independent backup wavelength assignment*). Este último é interessante, pois a diferença dos dois primeiros não impõe restrições no uso dos comprimentos de onda para os *lightpaths* primário e backup, de maneira que ambos os caminhos poderiam usar comprimentos de onda diferentes, oferecendo assim um melhor desempenho em termos de probabilidade de bloqueio que os dois primeiros, porem introduzindo maior complexidade que estes.

Considerando um *lightpath* primário L_p com custo finito, tem-se K-1 possíveis rotas *backup*, cada uma com W possíveis comprimentos de onda. Então, para este L_p há (K-1)W possíveis caminhos *backup*. Para calcular C_b de um *lightpath backup* para o dado caminho óptico primário (L_p), é necessário o custo de cada um dos *wlinks* no *lightpath* backup. Se o *wlink* é livre, então seu custo é 1. Se não está disponível é infinito, do contrario é 0.

Para definir este custo são necessárias O(H) unidades de tempo. Assim, para um dado *lightpath* primário num dado comprimento de onda, escolher o melhor caminho em qualquer comprimento de onda requer $O(KH^2W)$ unidades de tempo. Então, processar cada

caminho óptico primário em cada comprimento de onda para determinar o mínimo custo do par primário-*backup* terá uma complexidade de $O(K^2H^2W^2)$.

Este algoritmo é muito atrativo pelo uso da técnica de multiplexação *backup* que faz mais eficiente o uso dos recursos, melhorando o desempenho da rede. O uso do esquema de roteamento alternativo de alguma maneira reduz a complexidade respeito de outros esquemas, porem pode limitar o desempenho em termos de probabilidade de bloquieo.

Este desempenho poderia ser melhorado pela adoção de uma aproximação baseada em roteamento adaptativo (*adaptive routing*), onde caminhos ópticos são estabelecidos adaptativamente baseados no estado presente da rede. Mas, instancias de tal problema são do tipo NP-completo [YUAN, 2004], assim, é desejável ir para soluções baseadas em aproximações heurísticas com um razoável tempo de computação.

4.9 USO DE HEURÍSTICAS BASEADAS EM ALGORITMO GENÉTICO

Problemas de projeto e otimização para redes sobreviventes freqüentemente requerem algoritmos de tipo não-polinomiais (NP). Instâncias de tais problemas são difíceis de abordar com os métodos exatos da programação matemática, devido ao longo tempo de processamento e requisitos de memória computacional. Assim, pesquisadores têm optado por técnicas heurísticas.

Por outro lado, algoritmos evolucionários, em especial os Algoritmos Genéticos, tem chamado grande atenção por sua aplicação na solução de problemas complexos e de otimização em diferentes campos da ciência, incluindo as Telecomunicações, e em particular as redes ópticas comutadas por comprimento de onda [SINCLAIR1, 1998] [SINCLAIR2, 1998] [SINCLAIR3, 1993] [SINCLAIR4, 1999] [BISBAL, 2004], porém, em algumas aplicações resultam inviáveis pelo tempo de execução que demanda o processo computacional.

Uma poderosa alternativa para problemas específicos é a modelagem híbrida baseada em Heurísticas e Algoritmos genéticos, que combina a melhor heurística para a solução do problema dentro da estrutura robusta que oferece o algoritmo genético.

Aproximações baseadas puramente em GA podem levar a uma longa latência de configuração devido ao processo randômico para obter a primeira geração de indivíduos

toda vez que acontece uma nova solicitação do cliente. O uso de algoritmos heurísticos pode ajudar a otimizar estes processos, estabelecendo uma base de população de rotas primárias e de proteção, de maneira a se ter uma convergência rápida na obtenção do par mais adequado para tal solicitação.

Assim, para cada solicitação de comprimento de onda, e visando reduzir a complexidade computacional, o algoritmo híbrido procura:

a) Por um conjunto de rotas principais candidatas;

b) Suas correspondentes rotas de proteção (disjuntas das rotas principais);

Estes conjuntos de rotas serão pré-calculadas e usadas para formar o espaço de busca para o GA. Assim, se pretende que o mecanismo possa distribuir tráfego mais equitativamente e o compartilhamento de caminhos de proteção possam ser aprimorados.

A Figura 4.14 apresenta um exemplo do que se espera do planejamento de reserva de capacidade para proteção compartilhada usando heurísticas. Aqui, em caso de acontecer uma falha, um único caminho de proteção (mecanismos de proteção clássicos 1:1 ou 1:N) não conseguiria satisfazer todos os requisitos de tráfego. Porém, usando estas heurísticas seria possível.

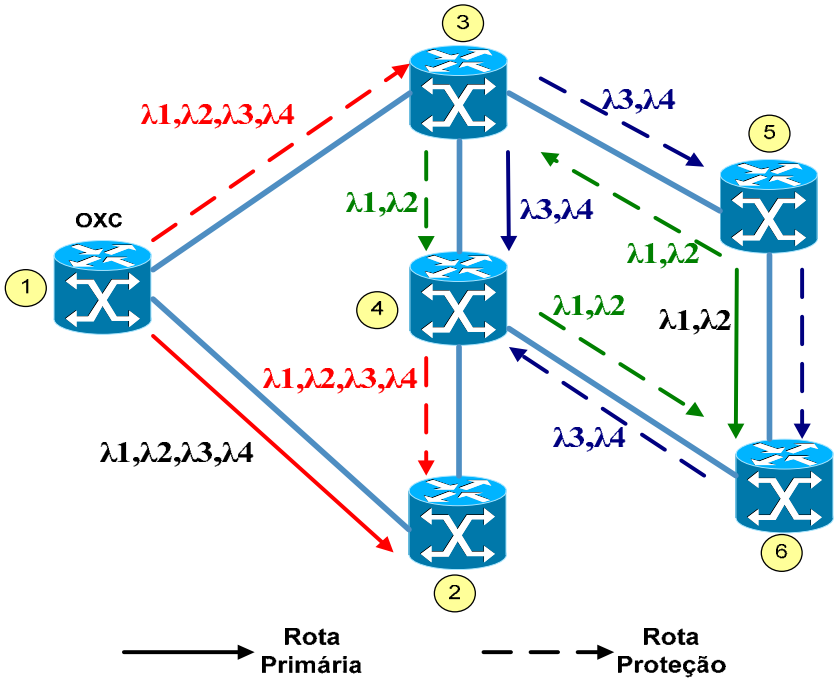


Figura 4.11 - Proteção compartilhada para diversas Rotas de Trabalho.

No exemplo, para a proteção de rota de trabalho 1-2 têm-se reservadas as rotas *backup* 1-3-4-2 e 1-3-5-6-4-2, assim o tráfego pode ser otimamente balanceado nessas duas rotas de proteção em caso de falha na rota primária. Assim, a proposta deste trabalho pretende ser mais eficiente quando comparado a um único caminho de proteção. A Tabela 4.4 mostra os requisitos de tráfego, caminhos de Trabalho, caminhos de Proteção e comprimentos de onda do exemplo anterior.

Tabela 4.4 - Requerimentos de Tráfego, caminhos de Trabalho e caminhos de Proteção.

Rotas		**Tráfego**	**Caminhos**	
Fonte	Destino	**(Nº de Lambdas)**	Rota de Trabalho λ_{Work}	Rota Backup λ_{Prot}
1	2	4	1-2, λ_1	1-3-4-2, λ_1
			1-2, λ_2	1-3-4-2, λ_2
			1-2, λ_3	1-3-5-6-4-2, λ_3
			1-2, λ_4	1-3-5-6-4-2, λ_4
3	4	2	3-4, λ_3	3-5-6-4, λ_3
			3-4, λ_4	3-5-6-4, λ_4
5	6	2	5-6, λ_1	5-3-4-6, λ_1
			5-6, λ_2	5-3-4-6, λ_2

Embora a aproximação híbrida Heurístico/Algoritmo Genética seja promissora, esta tem algumas limitações. Dado que esta é uma forma de procura estocástica guiada, não existe garantia de que um valor ótimo global possa ser alcançado. Em compensação, uma boa solução aproximada pode ser conseguida.

Em [BISBAL, 2004], por exemplo, é proposta uma heurística baseada em roteamento adaptativo usando um algoritmo genético, chamado de FT-GRWA (*fault tolerance GA-based Routing and Wavelength Assignment*), o qual oferece um bom desempenho a um razoável tempo de execução, quando comparado com o esquema PIBWA [MOHAN, 1999] [MURTHY, 2002]. Porem, os processos de busca randômica da primeira população resultam num significativo retardo.

Em [LE , 2005] é proposto um algoritmo híbrido baseado na técnica de agentes móbiles e algoritmos genéticos para proteção de caminho em redes WDM com sobrevivência usando um esquema de compartilhamento backup e diferentes comprimentos de onda para os

lightpaths primário e backup, como no método PIBWA [MOHAN, 1999] [MURTHY, 2002]. Neste mecanismo, os agentes móbiles, implementados pelo esquema de roteamento baseado em formigas (*ant-based*) [NGO, 2004], se encarregam de explorar o estado da rede, atualizando assim as tabelas de rotas, o qual permite definir a primeira população para o algoritmo genético sem necessidade de criação aleatória, o qual leva a uma otimização no tempo de execução e melhora o desempenho do algoritmo FT-GRWA. O pseudo código deste processo é mostrado a seguir:

{Atualiza tabela de roteamento do nó fonte}
Se o novo ciclo é diferente de qualquer outro disponível no listado de ciclos do nó fonte, Then
    Se o número de ciclos no listado de ciclos é menor que P Then
        Inserte seu agente novo ciclo no listado
    Else
        Substitua um ciclo existente com o agente novo ciclo baseado na política FIFO
    End if
End if

Aqui, o ciclo é formado por os dois caminhos, primário e backup, disjuntos entre si, constituindo um individuo da população. Os resultados obtidos na simulação apresentam uma baixa probabilidade de bloqueio e um relativo curto tempo na execução do algoritmo. A complexidade deste algoritmo híbrido é O(G.P.N.(P+W)), onde G é o número de gerações e P a população, ambos parâmetros do GA, N representa o número de nós da rede e W o número total de comprimentos de onda por enlace. Aqui, os autores não consideram o tempo de computação gasto pela heurística dos agentes móbiles.

4.10 COMENTÁRIO FINAL

O projeto de uma rede de telecomunicações que permita manter um nível aceitável de serviço quando da ocorrência de uma falha é um dos mais importantes desafios para os operadores de redes.

A sobrevivência de redes, particularmente no contexto das redes ópticas, tem motivado forte interesse nos *operadoras* e pesquisadores pela necessidade de implementação de mecanismos que agreguem confiabilidade à rede, e isto é um requisito crítico para as redes IP sobre WDM. Capacidade de recuperação de falhas na camada óptica é conseguida usando proteção, onde uma requisição cliente é atendida com dois caminhos em lugar de um: um caminho de trabalho e um caminho *backup*, ambos disjuntos entre si.

O método de proteção mais simples é conhecido como proteção dedicada, e usa um caminho óptico *backup* por cada caminho de trabalho. De maneira a usar os recursos mais eficientemente, técnicas de multiplexação de caminho *backup* são introduzidas para permitir que dois ou mais caminhos de trabalho possam compartilhar o mesmo caminho de reserva, com a restrição que seus respectivos caminhos de trabalho não pertençam ao mesmo SRLG.

Problemas de projeto e otimização baseados nesta técnica freqüentemente requerem algoritmos de tipo NP, porém difíceis de abordar com os métodos exatos da programação matemática devido ao longo tempo de processamento Assim, pesquisadores tem optado por técnicas heurísticas específicas.

Por outro lado, algoritmos evolucionários, em especial os GAs, têm ganhado grande interesse por sua aplicação na solução de problemas complexos e de otimização em campos como as Telecomunicações, e em particular as redes ópticas. Porém, em algumas áreas a sua aplicação resulta inviável pelo tempo de execução que demanda o processo computacional.

Uma poderosa alternativa para problemas específicos relativos à sobrevivência e a RWA é apresentada neste trabalho, usando modelagem híbrida baseada em Heurísticas e Algoritmos genéticos, que combinam soluções heurísticas dentro da estrutura robusta que oferece o algoritmo genético, orientando-o à multiplexação de caminho backup.

Capítulo 5

"Porque o Senhor é bom; a sua benignidade dura para sempre,
e a sua fidelidade de GERAÇÃO em GERAÇÃO".
SI 100:5

5 ALGORITMOS GENÉTICOS

5.1 INTRODUÇÃO

Algoritmos evolucionários, e muito em especial os algoritmos genéticos, tem despertado grande interesse por sua aplicação na solução de problemas complexos e de otimização em diferentes campos da ciência, incluindo as Telecomunicações. Aplicações nesta última área incluem projeto de redes, roteamento de chamadas, alocação de rota e comprimento de onda (RWA), gerência de rede etc.

Este Capítulo revisa os fundamentos teóricos dos algoritmos genéticos, ferramenta que será usada neste trabalho.

5.2 CONCEITOS BÁSICOS

5.2.1 Algoritmo

Um algoritmo é um método repetitivo para resolver problemas, baseado em uma seqüência codificada de instruções para manipulação de símbolos. Um algoritmo gera um "processo algorítmico", projetado intencionalmente ou não e que consiste na obediência a uma estrutura única, ramificada, recursiva ou iterativa, que vai-se desenvolvendo em série/paralelo, com rotinas e sub-rotinas invocadas quando necessárias. O nome algoritmo deriva de al-Jwarizmi, matemático árabe do século IX.

5.2.2 Heurística

Segundo ANSI/IEEE Padrão 100-1984, a heurística trata de métodos ou algoritmos de busca durante a resolução de problemas; assim, as soluções se descobrem pela avaliação do

progresso alcançado na procura de um resultado final. É comum usar o termo como adjetivo, caracterizando técnicas pelas quais se melhora o resultado de um problema.

5.2.3 Algoritmos Evolucionários

Os algoritmos evolucionários se subdividem em subáreas: algoritmos genéticos (GA) [MITCHELL, 1993], programação evolucionária (EP), estratégias evolutivas (ES), programação genética (GP) [SINCLAIR2, 1999], classificação de sistemas (CS), entre outros [FOGEL, 1998]. Nas últimas décadas, o algoritmo genético (GA) tem mostrado ser uma ferramenta prática e robusta de otimização e busca. Estes algoritmos estão baseados nos mecanismos de evolução das espécies, que levam à sobrevivência do mais apto pelo processo de busca e seleção natural.

5.2.4 Processos Estocásticos

Os processos estocásticos são aqueles onde não se pode ter certeza de que os dados estimados serão iguais aos dados reais, apenas tem-se uma estimativa dos valores esperados. Processos estocásticos são caracterizados por serem constituídos de variáveis aleatórias indexadas pelo tempo. A principal finalidade dos processos estocásticos é a de compreender o comportamento da trajetória de um sistema objetivando fazer previsões e/ou controlar o futuro do sistema.

5.3 ALGORITMOS GENÉTICOS

O Algoritmo Genético é um método para a solução de problemas de otimização que é baseado na seleção natural, o processo que conduz a evolução biológica. Combina a sobrevivência do mais apto entre estruturas de seqüências com uma troca de informações estruturada, porém com certa aleatoriedade. Assim, o Algoritmo Genético modifica repetidamente a população de indivíduos. Sobre sucessivas gerações, a população “evolui” para uma solução ótima. O Algoritmo Genético pode ser aplicado para solucionar uma variedade de problemas de otimização que não são adequadamente satisfeitos por algoritmos de otimização padrão, incluindo problemas no qual a função objetivo é descontínua, não-diferenciável, estocástica, ou altamente não-linear.

Os GAs foram introduzidos em 1975 por John Holland da Universidade de Michigan [GOLDBERG, 1989], com o intuito de formalizar matematicamente e explicar rigorosamente processos de adaptação em sistemas naturais e desenvolver sistemas

artificiais (simulados em computador) que reproduzam os mecanismos originais encontrados em sistemas naturais. O tema central de sua pesquisa em algoritmos genéticos foi a robustez, isto é, o balanço entre a eficiência e a eficácia.

Um GA gera uma seqüência de populações usando mecanismos de seleção, e aplica *crossover* e mutação como mecanismos de busca. Um GA é uma técnica de busca randômica global no espaço de solução do problema e, usualmente, permite a captura em uma otimização local [GEN, 2000].

Por serem uma analogia da seleção natural de Darwin, os algoritmos genéticos adotaram um vocabulário derivado da genética. Assim, um conjunto de soluções candidatas é denominado de população; cada solução candidata é denominada indivíduo ou cromossomo, que por sua vez é formada por genes. Cada iteração do algoritmo genético é chamada de geração; a combinação de dois (ou mais) indivíduos para se criar novos indivíduos é dito de recombinação ou *crossover*; e a modificação aleatória de um indivíduo é chamada de mutação.

O Algoritmo Genético diferencia-se dos algoritmos de otimização padrão em duas maneiras, como sumariza na Tabela 5.1:

Tabela 5.1 – Paralelo entre um Algoritmo Padrão e o GA

Algoritmo Padrão	Algoritmo Genético
Gera um único ponto a cada iteração. A seqüência de pontos aproxima a uma solução ótima.	Gera uma população de pontos a cada iteração. A população aproxima a uma solução ótima.
Seleciona o próximo ponto na seqüência por cálculo determinístico.	Seleciona a próxima população por cálculo que envolve escolha randômica.

5.3.1 Terminologia usada em GA

Os principais termos, a serem utilizados neste trabalho são:

Genes: Parâmetros a serem otimizados. Assim como na evolução natural, formam o bloco básico de uma otimização por meio de GA. No caso de codificação binária (mais comum), os genes são formados por alelos (bits).

Cromossomo: ou código-indivíduo Uma solução possível do problema. É formado por um conjunto de genes. Em cada um estarão representados todos os parâmetros a serem otimizados.

População Inicial: Um conjunto finito de cromossomos ou indivíduos. A partir desta população os GA tentarão evoluir para uma melhor solução do problema.

Gerações: Populações consecutivas de cromossomos. A partir da população inicial, sucessivas gerações de cromossomos serão geradas, analisadas, cruzadas e propagadas ou descartadas.

Pais: A partir da população inicial, pares de cromossomos (pais) serão escolhidos. Suas características serão combinadas gerando novos cromossomos filhos.

Filhos: A partir dos pais e através do processo de cruzamento genético, uma população de filhos é gerada, substituindo os pais na próxima geração.

Cruzamento (*crossover***)**: ou recombinação. Tendo sido escolhidos os dois pais, há uma mistura em seus códigos genéticos. Na forma mais comum, cruzamento simples, sorteia-se um ponto qualquer no cromossomo e troca-se os genes a partir daquele ponto, gerando assim dois filhos.

Mutação: De forma aleatória, escolhe-se um gene e se altera alguma característica sua. Para representação binária do cromossomo, inverte-se o valor do bit. Obviamente, a probabilidade associada a este operador é baixa, do contrário teríamos uma procura essencialmente aleatória.

Função de Avaliação: também chamada de função *fitness,* provê uma medida de desempenho com respeito a um conjunto particular de parâmetros.

Função de Aptidão (custo): define o foco da otimização. Cada indivíduo na população deve possuir um valor de função de aptidão. Essa função será a responsável pela ligação entre o problema físico e o Algoritmo Genético.

A função de aptidão e a função de avaliação devem ser distintas. A função de aptidão transforma a medida da função de avaliação em alocação de oportunidades reprodutivas. A avaliação de um cromossomo é independente da avaliação de qualquer outro cromossomo. Já a aptidão é sempre definida de acordo com outros membros da atual população.

5.3.2 Componentes de um GA

Um algoritmo genético para a abordagem de um determinado problema sempre deve possuir os seguintes componentes [MICHALEWICZ, 1996]

1) Uma representação genética (código) para soluções candidatas ou potenciais (processo de codificação);
2) Uma maneira de criar uma população inicial de soluções candidatas ou potenciais;
3) Uma função avaliação que faz o papel da pressão do ambiente, classificando as soluções em termos de sua adaptação ao ambiente (sua capacidade de ser uma solução ao problema);
4) Operadores genéticos para alterar a composição dos indivíduos em uma população (em geral, *crossover* e mutação);
5) Valores para os diversos parâmetros usados pelo algoritmo genético (tamanho da população, probabilidades de aplicação dos operadores genéticos, etc.).

Neste trabalho, por exemplo, a codificação é numérica não binária, onde os números se correspondem com cada nó da rede. A população inicial de soluções candidatas não é aleatória, ela é gerada por heurísticas. A função avaliação é linear (embora os problemas a solucionar sejam de natureza não linear), e simples de maneira a se ter eficiência na otimização. Os operadores genéticos usados são basicamente os de *crossover* e mutação. Os valores para os diversos parâmetros também foram adequadamente definidos. Tudo isto será tratado no próximo Capítulo.

Bons resultados podem ser obtidos com o uso de algoritmos genéticos, mesmo quando o problema a ser resolvido é NP - difícil ou NP-completo, ou possui um espaço de busca descontínuo, não-linear, não-diferenciável, discreto, multimodo ou com presença de ruído. É nesses tipos de problemas que os algoritmos genéticos têm mostrado um desempenho superior às técnicas convencionais, como o método do gradiente ou busca aleatória [MICHALEWICZ, 2000].

5.4 IMPLEMENTAÇÃO DE UM ALGORITMO GENÉTICO

O desempenho dos algoritmos genéticos depende de vários fatores, como a codificação das soluções candidatas, o mecanismo de seleção, os operadores e a configuração dos parâmetros. A otimização de um problema através de algoritmos genéticos se processa da seguinte forma:

5.4.1 Codificação das Soluções Candidatas

Diferente dos métodos tradicionais de otimização, os algoritmos genéticos trabalham com a codificação das variáveis em vez das próprias variáveis do problema. Dessa forma, uma codificação adequada é necessária para o sucesso do algoritmo genético. Além disso, os algoritmos genéticos trabalham com uma população de soluções ao invés de uma única solução [GOLDBERG, 1989].

A maioria dos algoritmos genéticos usa soluções candidatas codificadas em um arranjo de bits com tamanho fixo e ordem dos bits bem definida. A codificação binária é a forma mais comum de codificação, de fato, no seu trabalho original, Holland e seus alunos concentraram-se nesse tipo de codificação. Entretanto, recentemente, vários outros tipos de codificação foram usados, como a codificação usando números reais, caracteres e até mesmo outros tipos de arranjos, como árvores.

Mecanismo de Seleção

Após decidir sobre a codificação das soluções candidatas, o segundo passo é escolher como o algoritmo genético fará a seleção, a escolha das soluções candidatas que irão ser usadas na criação de novas soluções e quantas novas soluções serão criadas.

O propósito da seleção é fazer com que os indivíduos mais aptos na população tenham algum tipo de prioridade na escolha para reprodução, aumentando a probabilidade de transmitir seu código genético às próximas gerações. A seleção deve ser balanceada com os operadores de *crossover* e mutação. Uma seleção muito forte faz com que indivíduos sub-ótimos dominem a população, reduzindo a diversidade necessária para progressos futuros. Por outro lado, uma seleção muito fraca resulta numa evolução muito lenta.

Por conveniência, se decompõe o processo de seleção em três passos [GOLDBERG, 1989] [BACK, 2000]:

1. Mapear a função aptidão para a função avaliação (*fitness*);
2. Criar uma distribuição de probabilidades proporcional à avaliação;
3. Selecionar amostras de acordo com essa distribuição.

5.4.2 Função Avaliação

A função aptidão é definida como:

$$\Im : A_x \rightarrow \Re$$

Onde: A_x é o espaço das variáveis do problema (espaço de busca). A função aptidão tipicamente mede algum custo a ser minimizado ou alguma recompensa a ser maximizada. A definição da função aptidão depende da aplicação, mas há algumas linhas gerais que devem ser seguidas na escolha da função aptidão:

- A função aptidão deve refletir as características mais relevantes a serem otimizadas. Os algoritmos genéticos são notoriamente oportunistas e há muitos casos de algoritmos otimizando uma função aptidão que não representa a característica desejada;
- A função aptidão deve exibir alguma regularidade no espaço representado pela codificação das soluções candidatas;
- A função aptidão deve prover informação suficiente para guiar a busca do algoritmo genético. Funções que dão quase o mesmo valor para cada solução candidata exceto para o ótimo devem ser evitadas.

A função avaliação (*fitness function*) mapeia os valores da função aptidão para um intervalo não-negativo. É a função avaliação que é usada em última análise pelo algoritmo genético e não a função aptidão. Ela pode ser definida como:

$$\Phi : A_x \rightarrow \Re_+$$

A função avaliação é usada para o ajuste quando se utiliza um método de seleção proporcional à avaliação do indivíduo. Neste caso, a função avaliação é usada para se mapear a função aptidão em um intervalo não-negativo.

A função de avaliação deve também ser relativamente rápida. Isto é tipicamente verdade tanto para um método de otimização como na proposta deste trabalho. Como um algoritmo genético trabalha com uma população de soluções potenciais, este incorre o custo de avaliar-se esta população. Além disto, a população é substituída (em parte ou totalmente) a cada geração. Os membros da população reproduzem e sua cria deve ser então avaliada, e todos estes processos podem levar a pouca eficiência na solução se não se tem uma adequada função avaliação.

5.4.3 Método de Seleção e Procedimento de Amostragem

Dentre os métodos de seleção mais comuns, pode-se citar:

Roulette Wheel - Método de seleção proposto por Holland, o qual usa uma seleção proporcional à função avaliação. O número esperado de vezes que um indivíduo será selecionado para reprodução é proporcional à sua avaliação dividida pela avaliação média da população. Para cada indivíduo é dada uma fatia de uma roleta (*roulette wheel*), proporcional à sua avaliação. Essa roleta é girada N vezes, onde N é o número de indivíduos da população. A cada giro, o indivíduo marcado na roleta é selecionado para a reprodução. Este método estocástico resulta no número esperado de filhos para cada indivíduo, mas de forma estatística. Quando se usa uma população com poucos indivíduos, o número alocado de filhos para cada indivíduo pode ficar longe de seu valor esperado [PAVANI, 2003].

Stochastic Universal Sampling - Melhora o método Roulette Wheel, minimizando a diferença entre o número alocado de filhos para cada indivíduo e o seu valor esperado [BAKER, 1987].

Rank Selection - Método de seleção proposto para evitar uma convergência prematura do algoritmo genético. Os indivíduos de uma população são ordenados segundo sua avaliação e o número esperado de vezes que um indivíduo será selecionado para reprodução depende da sua posição em relação aos demais indivíduos e não da sua avaliação. Após essa ordenação, o procedimento de amostragem poderia ser o *Stochastic Universal Sampling*.

Tournament Selection - Método de seleção proposto para ser computacionalmente mais eficiente que o *Rank Selection*, pois não necessita ordenar toda a população de acordo com a avaliação de cada indivíduo. Dois (ou mais) indivíduos são selecionados aleatoriamente da população e o "melhor" indivíduo nesse conjunto é selecionado para reprodução.

5.4.3.1 Ajuste

Os mecanismos de seleção que fazem uma seleção proporcional à avaliação do indivíduo, como o *Stocasthic Universal Sampling* e o *Roulette Wheel*, precisam de um mecanismo de regulação da competição dos indivíduos durante a execução do algoritmo genético, chamado de ajuste (*scaling*). Neste caso, a função avaliação é uma composição entre a função aptidão e a função de ajuste g:

$$\Phi(a_i(t)) = g(f(a_i(t)))$$

Onde:

$a_i(t) \in A_x$

$g(f(a_i(t))) \in \Re_+$

No início da execução do algoritmo genético há uma tendência de alguns super indivíduos (aqueles que têm uma avaliação muito superior aos demais) dominarem o processo de seleção.

Neste caso, o ajuste deve reduzir a avaliação desses indivíduos para evitar uma convergência prematura do algoritmo genético. No final da execução do algoritmo genético, a população já quase convergiu, de forma que a diferença de avaliação entre os indivíduos da população é muito pequena, diminuindo assim a velocidade de convergência. Neste caso, o ajuste deve aumentar a diferença entre as avaliações dos diferentes indivíduos que compõem essa população, para continuar a recompensar os melhores indivíduos com maiores probabilidades de seleção para reprodução.

Além disso, esse ajuste também é necessário quando a meta do algoritmo genético é minimizar a função aptidão, visto que maiores valores da função avaliação correspondem a menores valores da função aptidão. Portanto, problemas de minimização devem ser transformados no seu problema de maximização equivalente, dado que a probabilidade de se selecionar um determinado indivíduo é proporcional à sua avaliação.

5.4.4 Operadores Genéticos

5.4.4.1 Cruzamento

Os indivíduos selecionados pelo mecanismo de seleção são copiados para o *mating pool* (lugar de acasalamento). Agora vem a fase da recombinação (*crossover*), onde os indivíduos (pais) presentes no *mating pool* são combinados de alguma forma para gerar novos indivíduos (filhos). A idéia por trás da recombinação é que dados dois (ou mais) indivíduos que tem uma avaliação boa, mas por diferentes razões, o ideal seria que se combinassem as melhores propriedades desses indivíduos em um único.

Em linhas gerais, dois ou mais indivíduos (pais) são selecionados no *mating pool*. Esses indivíduos são combinados com uma probabilidade igual a $P_c \in [0,1]$ (parâmetro que indica

a probabilidade de ocorrer a recombinação) para gerar um ou mais novos indivíduos. Esses novos indivíduos vão formar a população dos filhos. Com probabilidade igual a $(1 - P_c)$, os pais são copiados diretamente para a população dos filhos. O operador de recombinação é dependente da codificação dos indivíduos.

5.4.4.2 Mutação

Após a fase de recombinação, cada indivíduo da população dos filhos pode sofrer mutação. A mutação introduz pequenas variações aleatórias nos genes de um indivíduo com probabilidade $P_m \in [0,1]$. Se os indivíduos usam uma representação binária, a mutação pode ser alcançada, por exemplo, mudando-se um bit aleatoriamente. Nas outras codificações, a mutação é um pouco mais complexa e depende dos limites do problema.

5.4.5 Métodos de Substituição de População

Após as fases de seleção, de recombinação e de mutação, os indivíduos presentes na população dos filhos devem ser inseridos na população, substituindo, de alguma forma, seus pais. Há basicamente dois métodos em que essa substituição pode ocorrer:

1) A população dos filhos substitui completamente a população dos pais, ou seja, os filhos não competem com os pais. Esse método é conhecido como *nonoverlapping* ou geracional;
2) A população dos filhos compete com a população dos pais pela sobrevivência. Esse método é conhecido como *overlapping*. A escolha de quais indivíduos serão substituídos pode ser aleatória ou determinística.

Nesta última, a quantidade de intersecção entre pais e filhos é chamada de *generation gap*. Esse parâmetro controla qual a fração da população será substituída a cada geração. Se o *generation gap* é de 100%, então toda a população é substituída.

Além disso, tanto no modelo *overlapping* como no modelo geracional pode ser interessante adotar uma estratégia de substituição elitista: sempre se mantém o(s) melhor(es) indivíduo(s) para a próxima geração. Isso é muito importante se o algoritmo genético é usado para otimizar uma função e o aptidão é achar o ótimo global dessa função.

5.4.6 Configuração dos Parâmetros

A última decisão para se implementar um algoritmo genético é como atribuir os valores para seus vários parâmetros, tais como o tamanho da população, a probabilidade de recombinação, a probabilidade de mutação, etc. Esses parâmetros tipicamente interagem um com outro de maneira não-linear, de forma que não se pode otimizar um independentemente de outro.

De maneira geral, a maioria das pessoas usa os parâmetros que funcionaram bem em experiências anteriores. Na literatura, se podem encontrar diversos valores para esses parâmetros. Por exemplo, em [DE JONG, 1975] se indica que a população deve ter de 50 a 100 indivíduos, a probabilidade de recombinação deve ser de 0,6 e a probabilidade de mutação por bit deve ser de 0, 001.

Contudo, não existem princípios gerais que podem ser formulados *a priori* sobre a configuração dos parâmetros de um algoritmo genético, em vista da variedade dos tipos de problema, codificações e critérios de desempenho que são possíveis nas diferentes aplicações. Mais ainda, o tamanho da população, as probabilidades de recombinação e mutação devem mudar no curso da simulação, caso se busque um desempenho ótimo. Dado esse problema, existe ainda muita pesquisa voltada para estratégias em que os parâmetros do algoritmo genético se adaptam durante sua execução [BACK2, 2000].

O ciclo do GA é repetido até que o critério de otimização seja alcançado, conforme pode ser visto num esquema básico do GA apresentado na Figura 5.1.

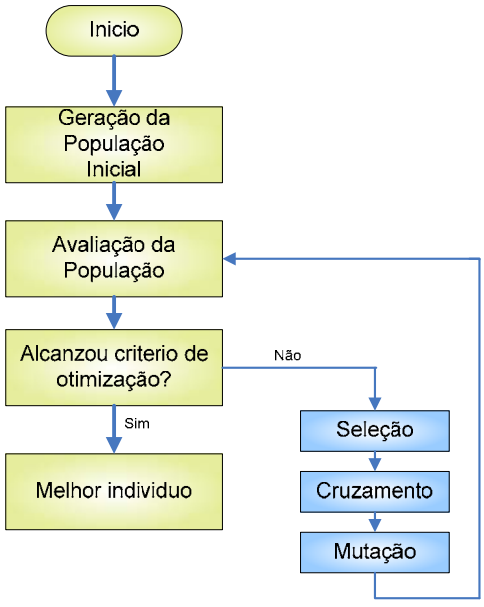


Figura 5.1 - Etapas de um algoritmo genético

Outro fator importante a destacar é que os algoritmos genéticos não necessitam de nenhuma informação auxiliar além do valor da função avaliação, embora tais informações possam ser usadas para acelerar a convergência do algoritmo.

Outra grande diferença é que os algoritmos genéticos usam regras probabilísticas para guiar a busca, o que possibilita escapar de pontos de ótimo locais, proporcionando uma robustez em uma vasta gama de problemas de otimização. Ao contrário dos métodos clássicos, os algoritmos genéticos conseguem obter um equilíbrio entre dois objetivos aparentemente conflitantes: o aproveitamento das melhores soluções, sem causar uma convergência prematura, e a exploração do espaço de busca, sem tornar a busca totalmente cega e aleatória.

5.4.7 Pseudocódigo de um algoritmo genético simples

O pseudocódigo de um algoritmo genético simples é apresentado na Tabela 5.2.

Tabela 5.2 - Pseudocódigo de um algoritmo genético simples

```
BEGIN /* Algoritmo Genético Simples */
Gerar população inicial e calcular a função de avaliação de cada indivíduo
WHILE NOT Concluído DO
BEGIN /* Produzir nova geração */
FOR Tamanho população/2 DO
BEGIN /*Ciclo Reprodutivo */
Selecionar dois indivíduos da anterior geração para o crossover (probabilidade de seleção
proporcional à função de avaliação do indivíduo)
Cruzamento dos dois indivíduos obtendo dois descendentes
Efetuar mutação dos dois descendentes com certa probabilidade
Calcular a função de avaliação dos dois descendentes mutados
Inserir os dois descendentes mutados na nova geração
END
IF a população tem convergido THEN
Concluído:= TRUE
END
END
```

No próximo Capítulo será apresentado o Pseudocódigo do algoritmo genético da proposta, com o detalhe de cada uma das linhas.

5.5 QUANDO NÃO UTILIZAR GA

É importante ressaltar que devido ao fato dos algoritmos genéticos serem uma ferramenta de busca e otimização de propósito geral, eles somente devem ser usados quando soluções clássicas ou dedicadas não existem, não se aplicam, não otimizam os processos ou falham

quando aplicadas. De maneira geral, os algoritmos genéticos não devem ser usados quando:

1) O espaço de busca não é muito grande, o que origina uma busca exaustiva da solução ótima;
2) A solução ótima deve ser necessariamente encontrada, pois não há garantias que o algoritmo genético encontre a solução ótima;
3) O espaço de busca é suave ou unimodal, pois um algoritmo baseado no método do gradiente [MICHALEWICZ, 2000] será muito mais eficiente do que um algoritmo genético para explorar a suavidade do espaço de busca;
4) Se o espaço de busca é conhecido, possibilitando o uso de heurísticas específicas ao domínio da aplicação;
5) Se uma solução deve ser obtida após um dado intervalo de tempo ou há restrições de tempo real, pois embora os algoritmos genéticos possam obter uma solução sub-ótima em um curto intervalo de tempo, não há garantias de que essa solução será obtida após um certo número fixo de iterações.

5.6 JUSTIFICATIVA PARA A ESCOLHA DO GA NESTA TESE

Existem outros algoritmos inspirados na teoria evolutiva de Darwin, que assim como os algoritmos genéticos envolvem reprodução, variação aleatória, competição e seleção de indivíduos na população. Esses algoritmos são por exemplo: *Tabu Search* (TS) [GLOVER, 1990] e *Simulated Annealing* (SA) [KIRKPATRICK, 1983]. A escolha do método de otimização mais adequado para cada problema depende essencialmente das características do problema em consideração.

Para problemas lineares com restrições lineares, programação linear parece ser o mais adequado. Se o problema puder ser dividido em diferentes etapas, o mais adequado poderia ser programação dinâmica. Para problemas não-lineares com restrições lineares ou não lineares (como são os problemas de RWA com restrições não lineares SRLG, por exemplo), o melhor seria a escolha de um método de otimização não-linear, tais como *Tabu Search*, *Simulated Annealing* ou Algoritmos Genéticos. Por que então se escolheu GA para este trabalho?. Características, tais como robustez, versatilidade, eficiência e simplicidade pesaram para a eleição deste método de otimização.

Tratando-se de robustez, ainda que apresentem uma taxa de convergência apenas boa, pois não se pode garantir a obtenção do máximo, os GAs são normalmente robustos para convergirem para a região de máximo.

Quanto à versatilidade, GAs são capazes de lidar com diferentes tipos de problemas sem grandes mudanças no programa principal. Para o programa é transparente a forma como é calculada a função custo (função *fitness*). Como não necessita de informações adicionais da função, pode facilmente ser usado para diferentes funções.

Na eficiência do algoritmo, os resultados são satisfatórios quando comparado com outros métodos (ILPs por exemplo). Com GAs usando apenas os operadores básicos, problemas de complexidade média podem ser resolvidos.

A relativa simplicidade, comparada com os demais métodos de otimização, é uma grande vantagem para a escolha de GA em diferentes áreas. Tanto a simplicidade de entendimento do processo quanto de programação do algoritmo devem ser destacadas.

5.7 CONSIDERAÇÕES FINAIS

Os GAs são ferramentas de otimização, com características marcantes de robustez, versatilidade, simplicidade e eficiência. Os principais cuidados quanto ao uso deste algoritmo dizem respeito à escolha da função custo, que orientará a busca por soluções mais ótimas, e à codificação adotada, a qual irá definir a precisão do algoritmo.

Embora os algoritmos evolucionários tenham sucesso nos problemas de procura de propósito geral e procedimentos de otimização, e seja uma boa aproximação para problemas específicos, em algumas aplicações resultam inviáveis pelo tempo de execução que demanda o processo computacional. Em particular, o GA é um método genérico que precisa ser customizado para a problemática específica que se deseja abordar. Assim, o projeto para o mecanismo de codificação dos indivíduos, o tamanho da população, o número de gerações (iterações), o critério de parada (*stopping*) e os diferentes operadores podem ser adaptados às características do problema em questão para otimizar o tempo de computação.

Nesta proposta é formulado um GA adaptado às necessidades de execução em tempo real em que são feitas as funções que se desejam otimizar, a saber RWA e Sobrevivência. Além do mais, a alternativa adotada neste trabalho, que é a modelagem híbrida baseada em Heurísticas e Algoritmos genéticos, propiciará o estabelecimento de uma rápida convergência no valor mais ótimo, proposta que será detalhada no próximo Capítulo.

Capítulo 6

"e os teus ouvidos ouvirão a palavra do que está por detrás de ti,
dizendo: ESTE É O CAMINHO, andai nele;
quando vos desviardes para a direita ou para a esquerda".
Is 30:21

6 PROPOSTA DE MECANISMO S-DRWA PARA REDES IP/WDM BASEADO EM HEURÍSTICA-GA

Em sobrevivência de redes ópticas comutadas por comprimento de onda, a proteção do caminho óptico se faz crítica pela necessidade de se determinar um caminho *backup* apropriado dentro de um curto período de tempo. Aproximações baseadas puramente em GA podem levar a uma longa latência de configuração devido ao processo randômico para obter a primeira geração de indivíduos quando acontece uma nova requisição.

O uso de algoritmos heurísticos, juntamente com GAs, podem ajudar a agilizar estes processos, além de estabelecer uma base de população de rotas primárias e de proteção, de maneira a ter-se uma convergência rápida para a obter o par adequado para tal requisição.

Com base nessas observações é proposto neste trabalho um novo algoritmo híbrido para RWA e proteção de caminho óptico (S-DRWA) baseado em heurística-algoritmo genético.

6.1 PROBLEMÁTICA

Com o rápido crescimento da Internet, o avanço da tecnologia WDM e a integração de várias tecnologias de comunicação e serviços, as redes de telecomunicações estão evoluindo para incluir aplicações que fazem uso de uma enorme largura de banda, e que precisam de ótima utilização dos recursos e capacidade de recuperação ante falhas na rede.

6.1.1 Otimização de Recursos: Problemática de RWA

A otimização no uso dos recursos parte da utilização de um bom algoritmo de RWA, com a adequada seleção de uma rota e de um comprimento de onda, de maneira a satisfazer

uma dada requisição de conexão, visando maximizar o *throughput* e mantendo um bom desempenho para a rede como um todo.

O problema de RWA pode ser formulado assim: dado um conjunto de *lightpaths* que precisam ser estabelecidos na rede, e dada uma limitação no número de comprimentos de onda, precisamos determinar as rotas e os comprimentos de onda que devem ser alocados para os *lightpaths* de modo que o máximo número de *lightpaths* possa ser estabelecido (ou a mínima probabilidade de bloqueio seja atingida). Assim, o desejável é:

a) Estabelecer todos os *lightpaths* usando o mínimo número de comprimentos de onda,

b) Estabelecer todos os *lightpaths* usando o mínimo número de saltos na rota;

c) Maximizar o número de *lightpaths* estabelecidos, sujeito a uma restrição no número de comprimentos de onda e/ou número de saltos no caminho.

6.1.2 Capacidade de recuperação: Problemática de Sobrevivência

Além da otimização na alocação de rotas e comprimentos de onda, um desafio crítico no projeto e gerência de redes ópticas é a sobrevivência. Quando uma simples falha acontece, tal como uma ruptura da fibra ou um defeito numa placa do comutador (*switch*), o resultado se traduz numa grande perda de dados e, lamentavelmente, a probabilidade de ocorrência de falhas não é pequena. Um relatório da FCC (*Federal Communications Commission*), por exemplo, reporta a ruptura de 136 fibras nas redes de transporte nos Estados Unidos em 1997 [FONSECA, 1998].

A sobrevivência de uma rede óptica depende de dois mecanismos que se encontram intimamente ligados entre si: a proteção para o caminho de dados e a recuperação do transporte de dados sobre o dito caminho de proteção.

Propostas para desenvolver apropriadas arquiteturas e estratégias que minimizem a perda de dados ante falhas, com uma rápida recuperação (com velocidades comparadas a SDH) são intensamente trabalhadas atualmente pelos grupos de pesquisa.

6.2 PROPOSTA: ALGORITMO HÍBRIDO HEURÍSTICO-GA (HGA)

Neste trabalho é proposto um novo mecanismo para alocação de rotas e comprimentos de onda (RWA) para caminhos de trabalho e de proteção compartilhada visando a

sobrevivência da rede, usando um esquema integrado baseado em Heurística-Algoritmo Genético. A aproximação heurística permitirá um menor esforço computacional e, portanto, um menor tempo de execução. O algoritmo genético oferecerá uma aproximação robusta e confiável para a solução desejada.

A proposta deste trabalho para a sobrevivência é baseada no planejamento de reserva de capacidade, visando encontrar o mínimo tamanho de reserva de recursos a ser alocado na rede óptica, de maneira a sobreviver a falhas dos elementos de rede e dispor assim de maiores recursos (comprimentos de onda) para o atendimento do maior número de requisições.

A dependência entre caminhos de trabalho e a correspondente reserva de capacidade no caso de proteção compartilhada (abordado nesta proposta) insere um maior grau de dificuldade ao problema.

6.2.1 Premissas

- Neste trabalho será assumida a possibilidade de ocorrência de uma única falha durante um dado intervalo de tempo, considerando que a probabilidade de duas falhas acontecerem simultaneamente é muito baixa [XIN, 2002];
- Este trabalho só considera falhas nos enlaces, e estima que os nós possuam redundância, com pouca probabilidade de falha.
- Dado que um dos interesses desta proposta é a otimização de recursos, assume-se que depois de uma falha no caminho de trabalho não é prioritário manter a mesma QoS no caminho de proteção, em termos de latência de propagação;
- Assim que acontecer uma falha na rede, um protocolo de sinalização será acionado para re-rotear o tráfego para os caminhos de *backup*;
- Requerimentos de largura de banda serão expressos em termos de comprimentos de onda.

6.2.2 Desenvolvimento proposto

Um mecanismo dinâmico para RWA visando sobrevivência é formulado em 3 passos para encarar as problemáticas consideradas:

1. Será desenvolvida uma aproximação heurística para selecionar caminhos candidatos a rotas de trabalho e suas correspondentes candidatas a rotas de

proteção, de maneira a alcançar ótimo desempenho, mantendo viabilidade computacional;

2. As requisições de tráfego serão distribuídas otimamente, sobre as rotas candidatas de trabalho e de proteção, usando algoritmo genético (GA);

3. Os comprimentos de onda serão alocados nas rotas de trabalho e nas rotas de proteção compartilhadas implicitamente pelo GA.

Assim, para cada solicitação de comprimento de onda, e visando reduzir a complexidade computacional, o algoritmo procura:

a) Por um conjunto de rotas principais candidatas;

b) Suas correspondentes rotas de proteção (disjuntas das rotas principais);

As heurísticas propostas visam simplificar a procura de rotas de trabalho e rotas de proteção e está baseada num algoritmo de roteamento mixto alternativo-adaptativo. É definido um conjunto de rotas de trabalho entre um nó fonte e um nó destino como um conjunto de rotas candidatas pré-calculadas por um esquema de roteamento alternativo. Logo, comprimentos de onda serão alocados as rotas de uma maneira adaptativa, em função da sua capacidade de compartilhamento pelo algoritmo genético, satisfazendo assim a requisição feita.

As heurísticas são executadas uma única vez, ou bem quando se tenha alguma mudança na topologia ou configuração da rede. O objetivo básico dos algoritmos heurísticos nesta proposta é originar um espaço de busca para o GA, eliminando a necessidade de uma recursiva criação aleatória da primeira geração, próprio do GA clássico, poupando assim precioso tempo computacional.

6.2.2.1 Grupo de Enlaces de Risco Compartilhado (SRLG).

Para a abordagem do problema de caminho de proteção compartilhado será usado o conceito de SRLG (*Shared Risk Link Group* – Grupo de Enlaces de Risco Compartilhado). Um SRLG é definido como um grupo de enlaces que compartilham um mesmo componente de rede, cuja falha vem comprometer todos os *links* do grupo.

No início das redes de transporte óptica, a identificação dos SRLGs não foi tomada com a devida importância ou não era realizada eficientemente, até gerência e distribuição de SRLGs ter recebido atenção da IETF [PAPADIMITRIOU, 2001] e dos fabricantes [SEBOS, 2001].

Através da aproximação por algoritmos genéticos serão consideradas restrições não lineares, as quais serão introduzidas pelo compartilhamento dos enlaces de proteção entre os SRLG. Com a consideração de restrições SRLG no planejamento de reserva de capacidade *backup*, a alocação de comprimentos de onda em cada rota de proteção compartilhada será feita antes das falhas acontecerem, visando-se obter uma curta latência de restauração na rede.

Os caminhos de proteção poderão compartilhar enlaces se e somente se suas correspondentes rotas de trabalho formem parte de diferentes SRLGs. Um problema será diferenciar que fibras pertencem a grupos de risco compartilhado, pois caminhos lógicos disjuntos podem fisicamente não ser disjuntos.

Negligenciar restrições SRLG no projeto de RWA/sobrevivência leva a que a alocação de comprimento de onda para caminhos *backup* tenha que ser feita dinamicamente depois de acontecida uma falha [DOSHI, 1999], fazendo busca de caminhos alternativos para todos os caminhos pertencentes ao enlace defeituoso. Como conseqüência se terá um elevado retardo de propagação da sinalização no plano de controle, principalmente nas redes de transporte de largo alcance, o qual contribuiria significativamente com a latência da restauração. Pretende-se, com a consideração de SRLGs no projeto, que os comprimentos de onda sejam alocados para cada caminho *backup* no estágio de criação do caminho primário, o qual redundará em uma menor latência de recuperação ante falhas.

6.2.3 Cenário de desenvolvimento do trabalho

A problemática da sobrevivência é abordada neste trabalho considerando um cenário formado por uma rede óptica transparente de transporte de dados IP/WDM, em uma rede em topologia em malha (*mesh*). Cada nó óptico da rede caracteriza um roteador-comutador de comprimento de onda. Cada enlace inclui duas fibras unidirecionais, com uma fibra em cada direção. Cada fibra tem a capacidade de receber a multiplexação de "n" comprimentos de onda.

O plano de controle da rede OMEGA (CPqD - Brasil), foi emulado em nosso laboratório da UnB (LABCOM) [PASTOR1, 2004]. Uma versão com plano de controle centralizado foi desenvolvida e nomeada de SIMOMEGA [CRISPIM, 2006]. Para avaliação e validação da nossa proposta de Tese foram considerados o *testbed* SIMOMEGA, e as topologias das redes OMEGA e NFSNet. Maiores detalhes destas redes são apresentados nos Anexos.

6.3 IMPLEMENTAÇÃO DAS HEURÍSTICAS

1) É pré-estabelecido um conjunto de rotas de trabalho para cada par fonte-destino, para o qual será usado um algoritmo de roteamento fixo Alternativo (vide Capítulo 3), baseado no algoritmo de Dijkstra modificado ou *k-shortest path first*;

2) Para cada rota de trabalho serão procuradas rotas disjuntas que conformarão o conjunto de rotas de proteção. Para tal será usado um algoritmo de busca de rotas de proteção baseado em árvores de busca.

Na prática, o tamanho do conjunto de rotas de proteção pré-candidatas para sua respectiva rota de trabalho está tipicamente entre 2 e 6 rotas [ZHOU 1, 2002].

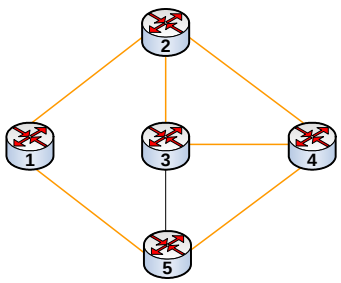
6.3.1 Algoritmo de Dijkstra modificado - Caminhos Primários

Neste algoritmo tem-se que:

- Buscar-se-á sempre os caminhos com o menor número de saltos;
- Se alguns dos enlaces dos caminhos mais curtos estiveram saturados, se procurará em aqueles de um salto a mais;
- Nesses outros caminhos verifica-se que o número de rotas de proteção decresce (pois o número de *links* disponíveis diminui).

Por exemplo, para o *Lightpath* 1 – 2, tem-se as seguintes rotas:

1-2
1-5-3-2
1-5-4-2
1-5-3-4-2
1-5-4-3-2



6.3.2 Algoritmo de Árvores de busca - Rotas de Proteção ou Backup

Foi desenvolvido um algoritmo para a busca de rotas de proteção para cada rota de trabalho baseado em árvores de busca. Dado que se busca a otimização de recursos, será assumido que depois de uma falha no caminho de trabalho não é prioritário manter a mesma latência de propagação.

Pretende-se reduzir a redundância de largura de banda pela otimização do compartilhamento de largura de banda de proteção entre distintos SRLGs. Assim, são selecionados os caminhos de proteção baseados na sua capacidade de compartilhamento e no seu menor número de saltos, logo que possível. Estes vêm a ser os enlaces de *backup* mais comuns que podem ser compartilhados pelos caminhos de trabalho pertencentes a diferentes SRLGs.

Para isto, uma árvore será gerada desde o grafo correspondente à topologia da rede considerando todos os caminhos entre os nós fonte-destino, eliminando os nós intermediários e enlaces que formam parte do caminho de trabalho, deixando o nó fonte como a raiz da árvore. Por exemplo, para a rota primária 1-2-4, pelo uso do algoritmo de árvores de busca serão eliminados todos os saltos para o nó 2, e os caminho óptico *backup* serão: 1-5-4 e 1-5-3-4. A Figura 6.1 apresenta este cenário.

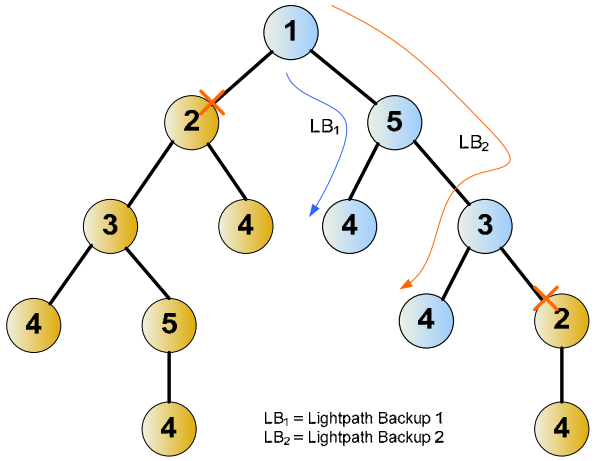


Figura 6.1 - Algoritmo de árvores de busca

Assim, tem-se um conjunto de rotas de proteção para cada rota de trabalho ou rota primária, considerando os caminhos disjuntos à dita rota. Para uma requisição entre os nós 1-2, considerando-se só o caminho primário de um salto 1-2, se tem o seguinte conjunto de rotas *backup*:

Lightpath 1-2:

- Caminho Primário: 1-2
- Candidatos a *Backups*: 1-5-3-2
  1-5-4-2
  1-5-3-4-2
  1-5-4-3-2

6.4 IMPLEMENTAÇÃO DO ALGORITMO GENÉTICO

O algoritmo genético opera sobre uma população de soluções potenciais pré-estabelecidas aplicando o princípio de sobrevivência dos mais aptos para produzir melhores aproximações. De forma geral, a estrutura do algoritmo genético a ser implantado é como se segue:

1) Parte-se de um espaço de busca formado pelo conjunto de rotas de trabalho e seus respectivos conjuntos de rotas de proteção, pré-selecionados pelas heurísticas aplicadas previamente;
2) Uma requisição de caminho óptico é feita pelo cliente da rede;
3) É selecionada uma população inicial P específica para tal requisição;
4) É feita a avaliação da população de rotas obtidas. Se foi alcançado o critério de otimização, então se tem a rota de trabalho e a rota de proteção para a requisição introduzida; com alocação implicita de comprimento de onda, do contrário;
5) São aplicados os operadores de cruzamento e mutação, e é feita uma nova seleção de P indivíduos baseados na sua aptidão. Assim, repete-se o passo 4, até obter-se as melhores aproximações, ou ser atingido um número pré-estabelecido de gerações.

Um diagrama de blocos do algoritmo proposto, considerando tanto as heurísticas como o algoritmo genético, é apresentado na Figura 6.2.

O *caminho óptico* selecionado e a tabela de *lightpath* atualizada são entregues ao plano de controle da rede óptica (por exemplo, uma rede ASON com plano de controle GMPLS). Para uma arquitetura de rede distribuída, um protocolo de roteamento de *gateway* interior (tal como OSPF-TE ou ISIS-TE) fará a difusão do caminho e atualizará as tabelas dos outros nós. Um protocolo de sinalização (um RSVP-TE, por exemplo) será encarregado da reserva dos recursos para o estabelecimento do c*aminho óptico*.

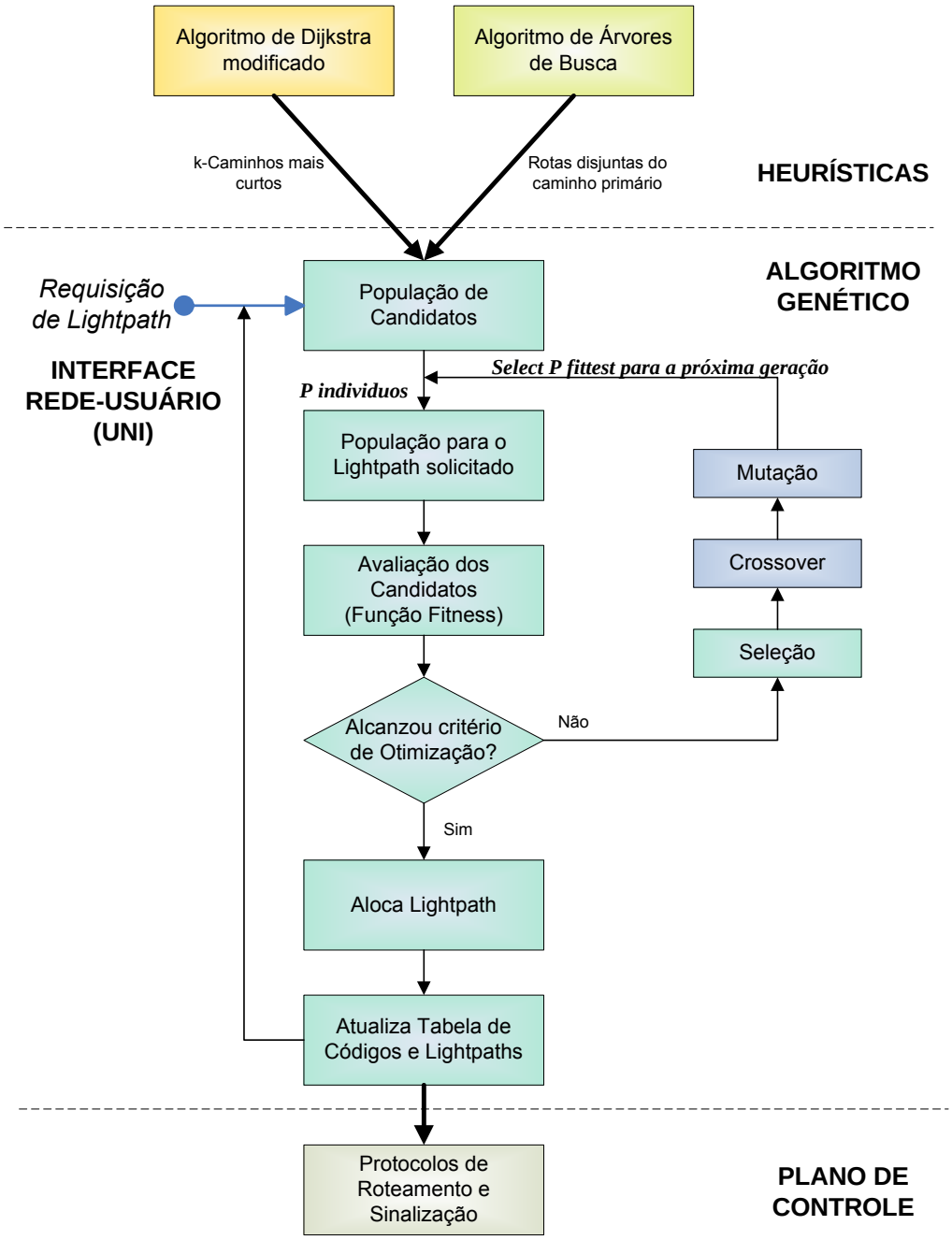


Figura 6.2 – Diagrama de blocos do algoritmo proposto.

A maneira como foi feita a implementação do algoritmo genético é apresentada a seguir.

6.4.1 Codificação dos indivíduos candidatos

No algoritmo proposto um indivíduo candidato (ou Cromossomo**)** é representado por meio de um código simbolizado por números inteiros onde cada número do código identifica um nó do *caminho óptico*. Cada código é formado por uma rota primária e por uma rota de *backup*, sendo estas rotas disjuntas.

Estes cromossomos formam parte da população inicial do GA. Em princípio o algoritmo genético deve, dada a requisição fonte-destino, reconhecer quais códigos formam parte da população específica para a respectiva solicitação.

Por exemplo, considerando a topologia da rede OMEGA, e supondo uma requisição para um caminho óptico protegido entre os nós 2 e 5, como mostrado na Figura 6.3, se teria como população inicial específica os cromossomos que começam no 2 e terminam no 5.

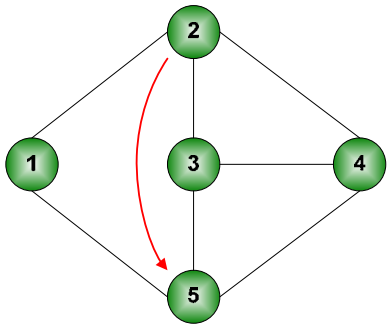


Figura 6.3 – Busca do Caminho óptico para a requisição 2 -5

Assim, ter-se-ia a seguinte população inicial:

2-1-5-2-3-5
2-1-5-2-4-5
2-1-5-2-4-3-5
2-1-5-2-3-4-5
2-3-5-2-1-5
2-3-5-2-4-5
2-4-5-2-1-5
2-4-5-2-3-5
2-4-3-5-2-1-5
2-3-4-5-2-1-5

Para obter a rota primária desde o código procura-se, a partir da origem para a direita, o valor de destino. Uma vez encontrado este valor de destino, tem-se a rota primária. O restante do cromossomo é a rota *backup* correspondente à respectiva rota primária. A Figura 6.4 apresenta, por exemplo, o código-indivíduo 2-1-5-2-4-3-5 e nela implicitamente o par Rota Primária-*Backup*.

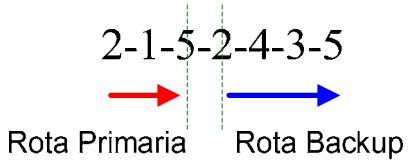


Figura 6.4 – Código-indivíduo: representação implícita do par Rota Primária-*Backup*

Posteriormente, o algoritmo classificará esta informação de entrada considerando que os códigos com maior aptidão são aqueles que têm a rota primária com o menor número de saltos e que à sua vez tenham a maior capacidade de compartilhamento na sua rota de proteção (backup).

6.4.2 Pseudo-código do GA

A população inicial é dada pelas heurísticas. Esta população é ainda filtrada em função do par s-d (origem-destino) da requisição cliente, tendo assim uma população especifica P. Esta evolui por meio dos operadores genéticos de cruzamento e mutação, obtendo-se novos indivíduos na população. Estes cromossomos são novamente avaliados em função da sua aptidão. O processo se repete até o melhor cromossomo ser selecionado ou a condição de parada ser atingida.

Seja:

G = número máximo de gerações;
C = melhor custo do candidato a *lightpath* (par primário-*backup*);
P = número de indivíduos da população específica.

Assim, o pseudocódigo do GA é formulado como apresentado na Tabela 6.1.

Tabela 6.1 - Pseudo-código do GA desta proposta

{População dada pelas heurísticas}
t=0
Seleciona população P para o lightpath solicitado
Avaliação de Fitness
C=melhor custo entre os nós s-d
while (t<G AND não se tenha alcançado o critério de otimização)
do crossover e avaliação fitness dos filhos
do mutação e avaliação fitness dos filhos
Select P fittest para a próxima geração
C=C+1;
t=t+1;
end while
Aloca Lightpath
Atualiza Tabela de Códigos e Lightpaths

6.4.3 Desenvolvimento passo-a-passo do Algoritmo Genético proposto

k-shortest path first

Obtem-se as rotas candidatas a Caminho Primário.

Algoritmo de Árvores de busca

Obtem-se as rotas disjuntas ao Primário, candidatos a Caminho de Proteção.

Código - Indivíduo ou cromossomo {rota primária + rota de proteção).

{População dada pelas heurísticas}

t=0

Seleciona população específica para o lightpath solicitado

Dos cromossomos que formam parte da população geral do GA serão selecionados os códigos específicos para a requisição *s-d*. Em princípio o algoritmo genético deve, dada a requisição fonte-destino, reconhecer quais cromossomos formam parte da população específica para dita solicitação.

Avaliação do Fitness

Para obter o melhor desempenho para os processos de roteamento e proteção, a função de avaliação deve considerar os cromossomos com as rotas primárias com o menor número de saltos e com as rotas de proteção que usem o menor número de comprimentos de onda disponíveis, isto é, os caminhos com a maior capacidade de compartilhamento.

Toda vez que um indivíduo é criado sua aptidão tem de ser avaliada. Neste estágio do algoritmo não só é feita a avaliação do candidato, como também é chamada a alocação implícita do comprimento de onda.

O indivíduo é avaliado em função do seu menor custo. O código-indivíduo com o menor número de saltos e que use um menor número de comprimentos de onda

livres terá o menor custo. Um canal é dito livre se não é usado nem por um caminho óptico primário nem por um caminho óptico de proteção. Se um canal está sendo usado por um ou mais caminhos ópticos de proteção, este poderia ser usado por um novo caminho de proteção sem ter que usar um novo canal livre, desde que seu caminho primário seja de diferente SRLG aos outros caminhos primários cujos caminhos de proteção desejam-se compartilhar.

Custo do Caminho de Trabalho ou Caminho Primário (C_w):

Seja C_w o custo do caminho primário. O C_w é definido pelo número de saltos, assumindo-se que se têm disponíveis ao menos um comprimento de onda livre na rota primária. Se alguns *lambdas* estão disponíveis o comprimento de onda de menor índice é alocado ao caminho óptico. Se não se têm comprimentos de onda disponíveis, então o C_w é considerado infinito.

Custo do Caminho de Proteção ou Backup (C_p):

Dado um enlace L, seja $C_{L,\,w}$ o custo de cada enlace com comprimento de onda w, onde:

w = 0, 1,.....W, são os comprimentos de onda na fibra deste enlace.

Sejam:

C_p : Custo do *lightpath* de proteção

C_{pw} : Custo do *lightpath* de proteção candidato com λ=w

$C_{L,\,w}$: Custo no enlace L do *lightpath* de proteção com λ=w

Então: $C_{pw} = \sum_{L \in Path} C_{L,w}$ .....(Eq. 6.1)

Para a alocação do custo no caminho de proteção serão analisados cada um dos seus enlaces e os pesos serão alocados com as seguintes considerações:

$C_{L,\,w} = 1$ → Se o λ no enlace não tem sido usado anteriormente no mesmo enlace;

$C_{L,\,w} = 0$ → Se o λ no enlace já foi usado e pode ser compartilhado, ou seja, o λ é usado por um conjunto de caminhos de proteção ψ, e o seu *caminho óptico* primário está em diferente SRLG com as rotas primárias de cada caminho de proteção no respectivo conjunto ψ;

$C_{L,\,w} = \infty$ → Nos outros casos;

Se o C_{pw} é considerado o melhor candidato, então $C_{pw} = C_p$;

Assim, o custo total (C_T) ou Função *Fitness* será dado por:

$$C_T = C_w + C_p + h_w(I) \text{.....(Eq. 6.2)}$$

Onde:

h_w = número de saltos da rota de trabalho;

I = número de nós do indivíduo candidato;

O termo $h_w(I)$ pretende privilegiar os indivíduos com o menor número de saltos no caminho primário. Como resultado, a Equação 6.2 mostra uma equação linear, que apresenta pouca complexidade, o qual redunda num menor tempo computacional na execução do algoritmo.

C= melhor custo entre os nós s-d

Estabelece o critério de parada (*stopping*). Como será apresentado posteriormente este valor é ajustado inicialmente a C=5. A rápida descoberta de uma boa rota é a chave para alcançar um curto tempo de computação.

Se ainda não se tem "o melhor" indivíduo, no estágio de avaliação se escolhe o 50% dos indivíduos com maior aptidão pelo mecanismo de seleção tipo *Stocasthic Universal Sampling*. Estes cromossomos são organizados em pares e assim são copiados para o *mating pool* (lugar de acasalamento) para reprodução (*crossover*).

while (t<G AND não se tenha encontrado ainda o melhor lightpath)

do crossover e avaliação fitness dos filhos

Cruzamento (*Crossover*) ou Recombinação

O operador de *crossover* é aplicado a pares de cromossomos de forma a trocar suas características genéticas, como acontece na reprodução natural. O ponto de *crossover* é selecionado a partir da primeira coincidência com o nó origem. Os filhos são gerados pela troca dos elementos da segunda parte dos pais, como mostrado na Figura 6.5.

Na prática, a informação a ser cruzada corresponde à parte do código do caminho óptico de proteção, do qual nos interessa tomar os caminhos com o menor número de saltos e a maior capacidade de compartilhamento. Como resultado podem-se obter filhos válidos ou não válidos. Também, o filho resultante pode ser igual a outro já existente. No processo de seleção só será escolhido um de eles.

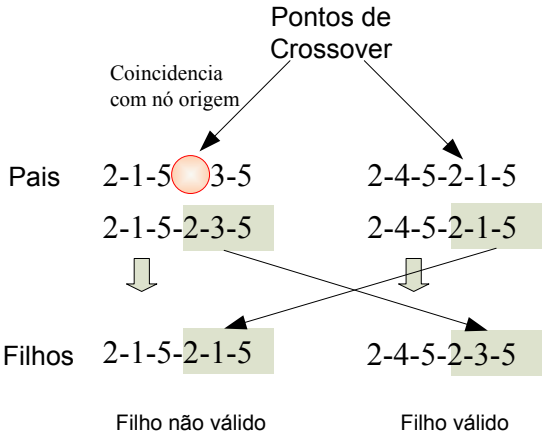


Figura 6.5 – Operação genética de Cruzamento.

Em resumo, no estágio de *crossover* são feitos os passos seguintes:

a) Aplicação do operador de cruzamento a um par de indivíduos;
b) Avaliação do custo dos P indivíduos obtidos (filhos);
c) Obter a média do *fitness* dos indivíduos da população.

***do* mutação e avaliação fitness dos filhos**

Mutação

O operador mutação faz uma troca randômica nas características genéticas de um indivíduo, permitindo ao GA obter indivíduos com novas características no espaço de busca. Neste algoritmo um nó do *lightpath* candidato, dito *"n"*, é aleatoriamente selecionado. A parte do caminho óptico entre o nó origem e o nó *"n"* permanece inalterável. Já a parte do indivíduo candidato que vai desde o nó *"n"* até um salto antes do nó destino é re-criado. O caminho óptico mutado deve também satisfazer os critérios de enlace disjunto, do contrário será uma rota não válida. A Figura 6.6 apresenta este processo para o caso em que se deseja obter o par primário-*backup* para uma requisição de caminho óptico entre os nós 5 e 1 da topologia OMEGA, por exemplo.

A mutação é feita pela troca de parte do código (certa parte correspondente ao caminho de proteção), podendo ser trocados um, dois ou três nós. A mutação, sendo um processo aleatório, pode originar indivíduos não válidos. No exemplo da Figura 6.6 se tem um indivíduo mutado que não corresponde à topologia da rede (não existe salto direto entre os nós 4 e 1).

O operador de mutação é aplicado entre os cromossomos cujo valor de *fitness* está abaixo de um dado valor (*baseline*). Este valor é o valor de aptidão médio de todos os

indivíduos da atual população, calculado no estágio de cruzamento. Obviamente, a probabilidade associada a este operador é baixa, do contrário teríamos uma procura essencialmente aleatória.

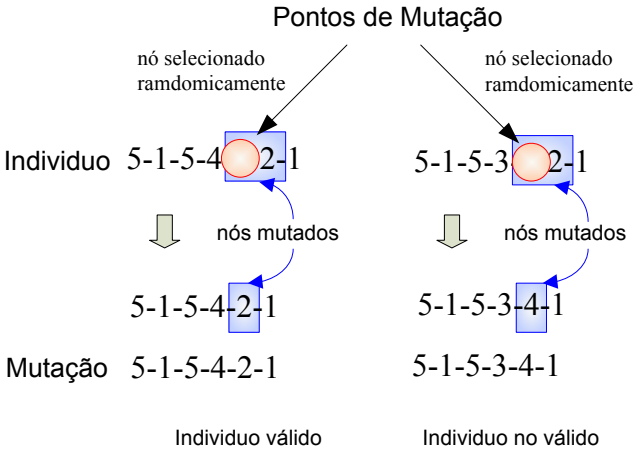


Figura 6.6 – Operação genética de Mutação.

Este processo tem mostrado experimentalmente ter menor probabilidade de bloqueio quando comparado com a técnica de aplicar mutação em indivíduos obtidos aleatoriamente, como em [BISBAL, 2004]. Então, no estágio de mutação são feitos os seguintes passos:

a) Aplicação do operador de mutação a 2 indivíduos escolhidos aleatoriamente dentre aqueles com valores de *fitness* abaixo da média (P-1 indivíduos);
b) Avaliação do custo dos 2P-1 indivíduos.

Select P fittest para a próxima geração

Depois de aplicar os operadores de *crossover* e mutação, o estágio de seleção escolhe os P indivíduos com maior aptidão entre os pais e os filhos que formarão parte da população da próxima geração. Este processo se repete até a condição de parada seja alcançada e o melhor indivíduo seja selecionado.

C=C+1;

Incrementa o valor do "melhor custo" C de maneira a se obter uma exigência menor para a avaliação da seguinte geração;

t=t+1;

Incrémenta t;

end while

Aloca Lightpath

Atualiza Tabela de Códigos e Lightpaths

6.4.4 Tabela de Códigos e *Lightpaths*

Esta tabela tem de ser atualizada depois de cada alocação de *caminho óptico*. Sempre considerando como referência a rede OMEGA, com 8 lambdas por fibra, se tem a seguinte configuração para a tabela de alocação λ-*Link* apresentada na Tabela 6.2.

Tabela 6.2 - Tabela de alocação λ-Link

	λ_1		λ_2		λ_3		λ_4		λ_5		λ_6		λ_7		λ_8	
Link	w	p	w	p	w	p	w	p	w	p	w	p	W	p	w	p
1-2																
1-5																
2-1																
2-3																
2-4																
3-2																
3-4																
3-5																
4-2																
4-3																
4-5																
5-1																
5-3																
5-4																

Nesta Tabela a 1ª coluna apresenta todos os *links* possíveis da rede. As colunas restantes apresentam a alocação dos comprimentos de onda tanto para os enlaces de trabalho, quanto para os enlaces de proteção. Esta separação é necessária devido ao fato que os comprimentos de onda nos enlaces de trabalho não podem ser compartilhados. Já os enlaces de proteção podem e devem, no possível, ser compartilhados.

A seguir um exemplo. Suponha uma série de requisições de c*aminho óptico* feitas pelas redes cliente e os respectivos "melhores" código-indivíduo selecionados pelo GA proposto. A Tabela 6.3 apresenta esta informação.

A Tabela 6.3 é só um exemplo no qual são apresentados alguns indivíduos que foram selecionados pela sua aptidão. Sendo o GA um processo estocástico nem sempre se terá a mesma estrutura inicial. Dada esta simulação de requisições cliente, e satisfeitas as

restrições do algoritmo proposto, a Tabela de alocação λ-*Link* apresentaria o seguinte conteúdo, mostrado na Tabela 6.4.

Tabela 6.3 - Informação de alocação de *Lightpaths* para as requisições dadas

Requisição de *Lightpath*	"melhor" indivíduo selecionado	*Lightpath* de Trabalho	*Lightpath* de Proteção
1-4	1-2-4-1-5-4	1-2-4	1-5-4
2-5	2-3-5-2-1-5	2-3-5	2-1-5
1-5	1-5-1-2-3-5	1-5	1-2-3-5
3-4	3-4-3-5-4	3-4	3-5-4
4-1	4-2-1-4-5-1	4-2-1	4-5-1
5-2	5-3-2-5-1-2	5-3-2	5-1-2

Supondo, agora, uma requisição de um cliente cuja rede se encontra conectada ao nó 4, e que deseja um *caminho óptico* com proteção para o envio de informação a outra rede conectada ao nó 5 da rede de transporte. Segundo os algoritmos de Dijkstra (*k-shortest path first*) e de árvores de busca, tem-se a seguinte população de entrada para o algoritmo genético: (4-5-4-3-5), (4-5-4-2-3-5), (4-5-4-2-1-5), (4-5-4-3-2-1-5), (4-3-5-4-5), (4-3-5-4-2-1-5), (4-2-3-5-4-5), (4-2-1-5-4-5), (4-2-1-5-4-3-5), (4-3-2-1-5-4-5).

Tabela 6.4 – Estado da Tabela de alocação λ-Link para o exemplo proposto

	λ_1		λ_2		λ_3		λ_4		λ_5		λ_6		λ_7		λ_8	
Link	w	p	w	p	w	p	w	p	w	p	w	p	w	p	w	P
1-2	x			x												
1-5		x	x													
2-1		x	x													
2-3	x		x													
2-4	x															
3-2	x															
3-4	x															
3-5	x															
4-2			x													
4-3																
4-5		x														
5-1		x		x												
5-3	x															
5-4		x		x												

O *Lightpath* desejado é selecionado ao considerar o custo de todos os candidatos. Este é o denominado custo satisfatório. No exemplo o menor custo seria C=7. Assim, o "melhor" candidato corresponde ao lightpath 4-5-4-3-5 com λ_2. Isto é apresentado na Tabela 6.5.

Tabela 6.5 – Avaliação dos candidatos a caminho óptico

Indivíduo	Custo Caminho de Trabalho (C_w)	Custo Caminho de Proteção (C_p)	Custo Total (C_T)	Resultado do GA
4-5-4-3-5	1	1+0	1+1+1(5)=7	O melhor
4-5-4-2-3-5	1	1+1+1	1+3+1(6)=10	
4-5-4-2-1-5	1	1+0+0	1+1+1(6)=8	
4-5-4-3-2-1-5	1	1+1+1+1	1+4+1(7)=12	
4-3-5-4-5	2	0	2+0+2(5)=12	
4-3-5-4-2-1-5	2	1	2+1+2(7)=17	
4-2-3-5-4-5	3	0	3+0+3(6)=21	
4-2-1-5-4-5	3	0	3+0+3(6)=21	
4-2-1-5-4-3-5	3	1	3+1+3(7)=25	
4-3-2-1-5-4-5	4	0	4+0+4(7)=32	

Definimos ***C= melhor custo entre os nós s-d,*** o custo satisfatório para obter o melhor indivíduo. Dado que o custo total vem dado por $C_T = C_w + C_p + h_w(I)$, o melhor custo, referência inicial para o algoritmo, seria dado por C=5, no qual se tem considerado o melhor valor esperado: um caminho de trabalho com um único salto e um caminho de proteção compartilhado também de um único salto.

Este algoritmo de S-RWA faz parte da operação de uma rede óptica transparente capaz de atuar automaticamente em caso de falha, redirecionando o tráfego para rotas de proteção em intervalos de tempo inferiores a 50 ms (com um pequeno número de nós no caso do sistema distribuído e valores maiores para um sistema de controle centralizado devido as taxas de transmissão da DNC - *Data Network Control*). Ao ser restaurado a falha, o sistema aguarda algum tempo para que a restauração seja confirmada e atua automaticamente sobre suas chaves ópticas para restaurar o caminho original, liberando novamente a rota de reserva para atender futuras falhas [SACHS, 2003].

6.5 ESTRUTURAS DE DADOS UTILIZADAS

O módulo de AG utiliza, para a representação em memória da topologia da rede, o conceito de grafos [BIGGS, 1974][BOLLOBAS, 1998][GODSIL, 2001][GOLDBARG, 2000] [DROZDEK, 2002].

Um grafo é uma estrutura abstrata que representa um conjunto de elementos chamados nós ou vértices (para a nossa rede os OXCs), e suas interdependências chamadas arestas ou arcos (para a nossa rede os "*enlaces"*). Desta forma, dado o conjunto N de vértices da estrutura e E o conjunto as ligações entre os vértices, um grafo pode ser representado por G=(N,E). Tem-se grafos não direcionados e grafos direcionados.

Um grafo não direcionado G_{nd} = (N,A) é um conjunto finito e não vazio de nós N, bem como um conjunto A de pares não ordenados {n1,n2} de nós distintos. Assim, a ordem de ligação entre os vértices não é importante. Um grafo direcionado G=(N,E) é um conjunto finito e não vazio de nós N, bem como um conjunto E de pares ordenados {n1,n2} de nós distintos. Aqui, a ordem de ligação entre os vértices tem importância.

Em um grafo G=(N,E) um arco e = (n1,n2) corresponde ao par de nós chamados de origem e destino respectivamente. Para um grafo não direcionado estes termos não são usados.

Num dado grafo o conceito de dois nós vizinhos é estabelecido se existe um arco "e", que pertence a E, com uma das seguintes condições: e = (n1,n2) ou e = (n2,n1).

Uma rede pode ser definida como R = (N,E,F) a partir de um grafo direcionado G=(N,E) atravessado por um fluxo F = {f1,f2,f3...fm} que circula em suas "m" arestas. Numa dada rede, dois nós são destacados: o nó origem e o nó destino. Para o modelo computacional implementado, um caminho em um grafo direcionado G=(N,E) é uma seqüência não vazia de arcos, que interligam os nós origem e destino. A implementação prática de grafos exige que cada elemento, seja vértice ou arco, tenha informações associadas ao mesmo.

Para a implementação em questão foi estudado e usado como modelo a biblioteca GTL - *Graph Template Library*, que pode ser vista como a extensão da STL *Standard Template Library* para grafos e seus algoritmos fundamentais. Além de grafos, o modelo implementado incorpora estruturas como tabelas *hash*, *containers* com funcionalidades específicas para cadeias (*strings*) e outras [DROZDEK, 2002][CRISPIM, 2006].

6.6 ANÁLISE DA COMPLEXIDADE DE UM ALGORITMO

Tem-se basicamente dois tipos:

- Espacial: Este tipo de complexidade representa o espaço de memória usado para executar o algoritmo, por exemplo.
- Temporal: Este tipo de complexidade é o mais usado podendo dividir-se em dois grupos:
    - Tempo (real) necessário à execução do algoritmo.
    - Número de instruções necessárias à execução.

6.6.1 Complexidade do Tempo

A **complexidade do tempo** de um problema é o número de passos que se toma para resolver uma instância de um problema, a partir do tamanho da entrada utilizando o algoritmo mais eficiente à disposição. Intuitivamente, caso se tome uma instância com entrada de longitude n que pode resolver-se em n^2 passos, se diz que esse problema têm uma complexidade em tempo de n^2. Supostamente, o número exato de passos depende da máquina em que se programa, da linguagem utilizada e de outros fatores. Para não ter que falar do custo exato de um cálculo se utiliza a *notacão O*. Quando um problema têm custo dado em tempo $O(n^2)$ em uma configuração de computador e linguagem, este custo será o mesmo em todos os computadores, de maneira que esta notação generaliza a noção de custo independentemente do equipamento utilizado [HARTMANIS, 1965]. São usadas três perspectivas no estudo da complexidade algorítmica.

- Melhor caso: é representado por Ω( ). Método que consiste em assumir que vai acontecer o melhor caso. Pouco usado. Tem aplicação em poucos casos.

- Caso médio: é representado por Θ( ). Este método é dos três o mais difícil de determinar pois necessita de análise estatística e como tal muitos testes. No entanto é muito usado pois é também o que representa mais corretamente a complexidade do algoritmo.

- Pior caso: é representado por *O*( ). Consiste basicamente em assumir o pior dos casos que podem acontecer, sendo muito usado e sendo normalmente o mais fácil de determinar. Se dissermos que um determinado algoritmo é representado por g(x) e a sua complexidade *Caso Pior* é n, será representada por g(x) = O(n).

Capítulo 7

"vê se há em mim algum caminho perverso,
e guia-me pelo caminho eterno"
SI 139:24

7 IMPLEMENTAÇÃO E AVALIAÇÃO DA PROPOSTA

7.1 ASPECTOS COMPUTACIONAIS DA IMPLEMENTAÇÃO

O mecanismo baseado em heurística-algoritmo genético para S-DRWA (*Survivability Dynamic Routing and Wavelength Assigment*), que denominamos HGA, foi implementado diretamente no plano de controle da rede de transporte SIMOMEGA e testado sobre as topologias das redes OMEGA e NSFNet. Um dado cliente pode ter acesso aos serviços do Sistema através da *UNI-Web* [PASTOR3, 2005] ou através de uma interface caractere desenvolvida sob o serviço *telnet*.

O ambiente IDE (*Entorno Integrado de Desenvolvimento*) utilizado para implementar o mecanismo HGA foi o *KDevelop KDE/C++* versão 3.1, disponível sob a licença GPL (*General Public License*) [KDEVELOP, 2006], no sistema operacional Linux, distribuição FEDORA 5. A linguagem usada para implementação do mecanismo foi o C++.

7.1.1 Funcionalidades do Mecanismo

As seguintes funcionalidades estão presentes:

Criação: para a criação de uma rota de trabalho com proteção, e com alocação de comprimento de onda de forma implícita, têm-se os seguintes passos:

a) Verificação léxica e sintática da solicitação recebida;
b) Cálculo do indivíduo melhor adaptado e posterior alocação de um comprimento de onda a este indivíduo (ver Capítulo 6). Neste contexto, o sistema pode indicar a impossibilidade da criação de tal rota. A informação das requisições aceitas

(ROK) e as bloqueadas (RNOK), bem como os detalhes dos caminhos de trabalho e proteção alocados são apresentadas no arquivo de log (*log2.txt)*.

c) Uma vez definido o indivíduo, a informação é enviada para os OXCs mediante os sets das portas e aguardar os set_acks respectivos.

Execução: para a execução do sistema são necessárias as seguintes informações:

1) Topologia da rede (nós e conectividade por fibra);
2) Comprimentos de onda em cada fibra (recursos da rede);
3) Estado atual da rede (quais rotas e comprimentos de onda estão ocupados).

De uma forma resumida, a implementação tem a seguinte lógica:

a) O algoritmo Dijkstra modificado é executado uma única vez para calcular todas as possibilidades de conexão de um nó para todos os outros nós da topologia (ver Capítulo 6);
b) Para cada conjunto de rotas são achados os respectivos conjuntos de rotas de proteção (ver Capítulo 6);
c) São criadas populações especificas; em função dos possíveis caminhos de um dado nó origem para um nó destino. As populações são compostas por indivíduos, que correspondem ao par caminho de trabalho/caminho de proteção;
d) As populações são armazenadas em um *container* de alto desempenho para busca indexada.

A rota principal (e a rota de proteção) é o conjunto interligado de enlaces já definidos pela topologia. Assim, o caminho óptico é dado pela respectiva rota acrescida de um comprimento de onda comum em todos os enlaces.

Nesse modelo, a representação do caminho corresponde a: nó1, porta de entrada1, porta de saída1; nó2, porta de entrada1, porta de saída2,.... etc.

7.1.2 Diagrama de Classes

A Figura 7.1 representa o diagrama UML simplificado das principais classes envolvidas no Sistema de Controle e do algoritmo HGA.

O conceito de grafo está implementado intrinsecamente. A classe *No* implementa o vértice ou nó, a *Arco* o arco. Assim, todo o grafo fica representado na classe *Topologia*. As demais classes dão suporte ao algoritmo de S-DRWA proposto.

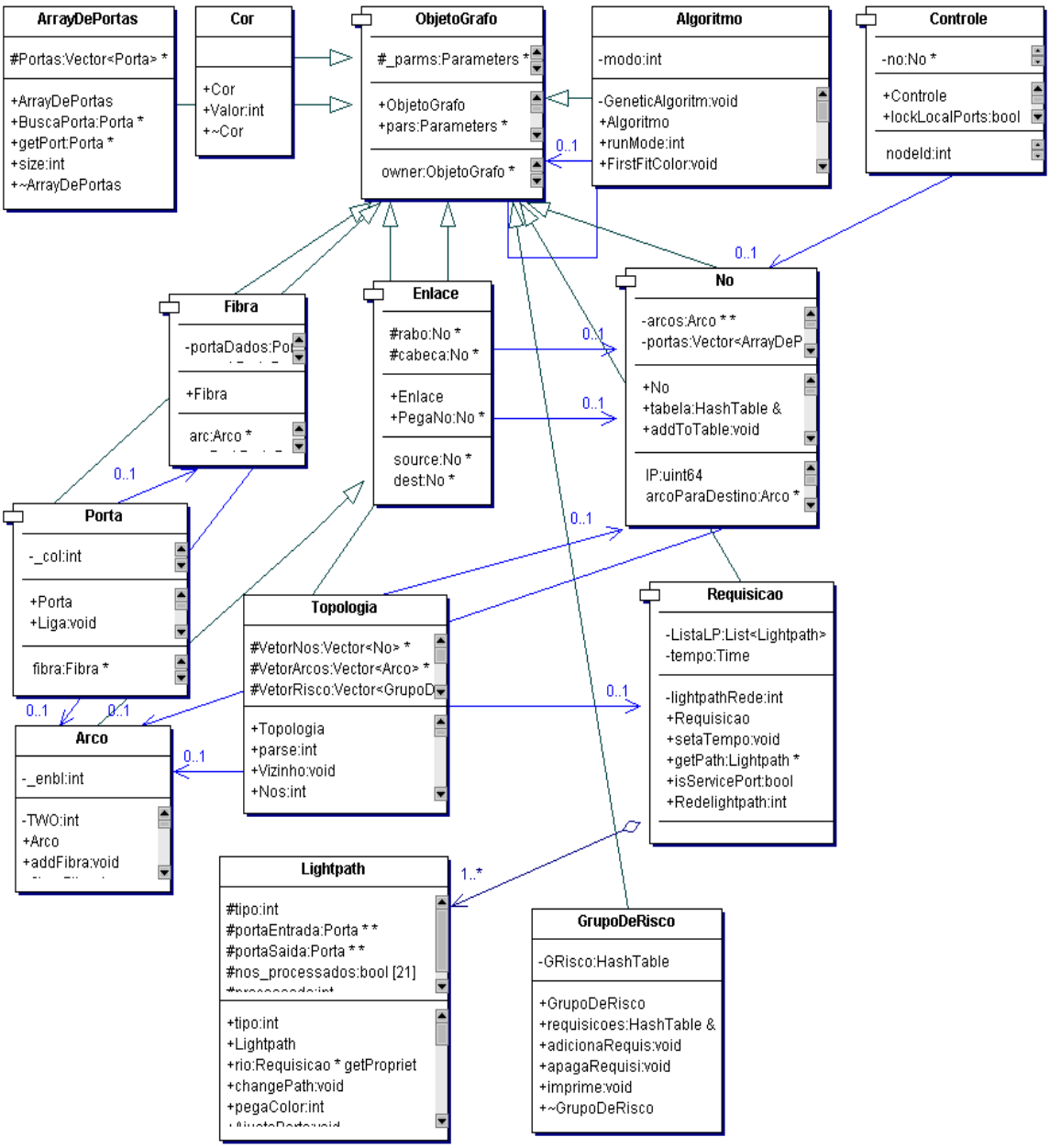


Figura 7.1 – Diagrama de Classes.

7.1.2.1 Definições básicas das Classes

ArrayDePortas: Tem como objetivo armazenar os estados de cada porta de um dado OXC e implementar os seus métodos. Nesta implementação foi utilizada a abstração das portas 0,1,2,3, sendo que a porta 3 é destinada para a função de ADD/DROP. As principais funcionalidades desta classe dizem respeito a implementar os mecanismos de inclusão,

consulta e exclusão de portas. Assim, concebeu-se uma solução computacional para elementos ópticos com múltiplas portas.

Cor: Esta classe implementa o conceito de cor, que representa os comprimentos de onda disponíveis na rede. As principais funcionalidades correspondem à inclusão, alteração e exclusão de cores (limites da rede em termos de comprimento de onda);

ObjetoGrafo: Classe que corresponde ao principal elemento da abstração da solução. Assim, qualquer outra classe que seja utilizada se remete ao ObjetoGrafo para obter um ID único em todo o sistema. As principais funcionalidades correspondem a inclusão, alteração e exclusão de objetos no sistema.

Algoritmo: Esta classe corresponde ao cerne da solução. Nela são implementados os métodos relativos às heurísticas, assim como os relativos ao GA. Esses métodos foram descritos detalhadamente na apresentação da proposta.

Controle: É a classe que armazena os dados de um OXC, bem como implementa os métodos necessários à operacionalização e controle do mesmo.

Fibra: Esta classe implementa a abstração de uma fibra óptica.

Enlace: Classe que representa a implementação do conceito de arco, que corresponde à interconexão de dois OXCs.

Nó: Implementa a abstração de um OXC acrescida das funcionalidades necessárias à implementação das funções do mesmo.

Porta: Esta classe corresponde a uma dada porta, que comporá um *array* de portas de um dado elemento óptico.

Topologia: Implementa o armazenamento de toda a topologia, bem como possui as funções típicas de manipulação de grafos.

Requisição: Representa uma dada solicitação de caminho óptico. Nesta classe cada requisição tem um único ID, bem como os controles internos de tempo de criação e eliminação.

Arco: Esta classe corresponde a implementação do conceito de um par de fibras TX/RX.

LightPath: Implementa o conceito de um dado caminho associado a um comprimento de onda.

GrupoDeRisco: essa classe armazena os arcos que fazem parte de um dado grupo de risco compartilhado e implementa as funções pertinentes à manipulação do mesmo.

7.1.3 Análise dos Comandos na UNI

Através de uma interface de serviço *telnet* o usuário ou o administrador gera uma *cadeia* com a síntese do comando desejado, a qual é logo enviada para o sistema de controle. Acoplado ao sistema de controle existe um tradutor capaz de efetuar as análises léxica e sintática do comando recebido. Assim, caso aconteça algum erro nesses dois estágios, a solicitação é negada e o erro é informado. Após o sucesso dos dois estágios anteriores, o comando é traduzido para uma seqüência lógica de eventos, que implementam a semântica da solicitação.

A análise léxica se baseia no fato que certas seqüências de caracteres devem ser tratadas como um único símbolo. Por exemplo: identificadores, constantes, palavras-chave (BEGIN, END, IF...), um ou mais brancos, caracteres duplos (:=, <> ...) etc.

O analisador léxico (ou *SCANNER*) agrupa os caracteres terminais em entidades únicas (*TOKENS*). A saída do *SCANNER* é uma sequência de pares da forma: (*TIPO DO TOKEN*, *INFORMAÇÃO*). O primeiro componente é uma categoria sintática (*IDENTIFICADOR, CONSTANTE*..) e o segundo uma cadeia que contém a informação relativa ao *TOKEN* (123, X, aux...).

Um exemplo específico de comando na rede SIMOMEGA é o seguinte:

```
> action create 1 2
```

Ao receber este *cadeia* os identificadores são mapeados em TOKENS (“action”, “create”, “1” e “2”), que servem como base para a análise da sintaxe do comando. A cadeia de *tokens* produzida pelo analisador léxico forma a entrada para o analisador sintático (*PARSER*), que examina o tipo de cada *token* para determinar se certas convenções da linguagem são obedecidas. O *parser* produz a representação adequada da estrutura sintática da cadeia de t*okens* recebidos e então dispara o conteúdo semântico.

7.1.4 Arquivo de definição de topologia

A topologia da rede para o modelo implementado é informada estaticamente a todos os computadores pelo gerente da mesma através do arquivo “5nodes.dat”.

Neste arquivo, entre outras informações, constam os nós pertencentes à rede e suas potencialidades, suas interligações e definição dos aspectos macro da infra-estrutura. Assim, pode-se implementar tanto uma rede em malha como em anel.

Um extrato deste arquivo de topologia da rede OMEGA é mostrado na Figura 7.2. Este arquivo é submetido a um *PARSER*. Na parte superior são mostrados os nós e suas respectivas capacidades em *lambdas*. O início é indicado pelo *TOKEN TOPOLOGY*.

5nodes.dat Página

```
# Topologia da Rede de Transporte
# Based on this data any node should be able to extract all its neighbours
TOPOLOGY

#       ID      C1:C2xNET-PORTS  C1:C2xDATA-PORTS
NODE    1       1:8x3            1:8x1
NODE    2       1:8x3            1:8x1
NODE    3       1:8x3            1:8x1
NODE    4       1:8x3            1:8x1
NODE    5       1:8x3            1:8x1

#       ID    ARC(SRG) NODE.PORT NODE.PORT
FIBER   1     1        1.1       5.0
FIBER   2     1        5.0       1.1
FIBER   3     2        1.0       2.0
FIBER   4     2        2.0       1.0
FIBER   5     3        2.1       3.0
FIBER   6     3        3.0       2.1
FIBER   7     4        2.2       4.0
FIBER   8     4        4.0       2.2
FIBER   9     5        4.1       3.1
FIBER   10    5        3.1       4.1
FIBER   11    6        3.2       5.1
FIBER   12    6        5.1       3.2
FIBER   13    7        4.2       5.2
FIBER   14    7        5.2       4.2
END

CONNECTION default PRIORITY MUST-PROTECT

ACTION
PROTECTION-TYPE          HGA
PROTECTION-COLOR         ANY
PROTECTION-PORT          ANY
MESH                     YES
MESH-MIN                 1
MESH-MAX                 16
PATH-TOL                 10
VIEW-ROUTES              YES
VIEW-SUMMARY             YES
VIEW-LINKS               YES
END
```

Figura 7.2 - Arquivo de Topologia da Rede OMEGA

O *TOKEN FIBER* evidencia o início do contexto de interligação entre os nós. Assim, cada fibra possui uma identificação única e pertence a um dado grupo de risco. Como os equipamentos possuem portas para interligação com os demais (0,1,2...), tais conexões também devem ser evidenciadas para a origem e destino respectivamente. Este grupo de informações é encerrado pelo *TOKEN END*.

Finalmente, vem o módulo que trata das características gerais da rede e do sistema. O ACTION é o *TOKEN* que dá início ao mesmo e o END delimita o final. A Figura 7.3 apresenta o arquivo de topologia para a rede NSFNet (ver também Anexo D).

```
# Topology database - NSFNet
# Topologia da rede NSFNet – 14 nodes
TOPOLOGY

#               ID      C1:C2xPORTA-REDE        C1:C2xPORTA-DADOS
NODE            0               1:8x3                   1:8x1
NODE            1               1:8x3                   1:8x1
NODE            2               1:8x3                   1:8x1
NODE            3               1:8x3                   1:8x1
NODE            4               1:8x3                   1:8x1
NODE            5               1:8x4                   1:8x1
NODE            6               1:8x2                   1:8x1
NODE            7               1:8x3                   1:8x1
NODE            8               1:8x2                   1:8x1
NODE            9               1:8x3                   1:8x1
NODE            10              1:8x4                   1:8x1
NODE            11              1:8x3                   1:8x1
NODE            12              1:8x3                   1:8x1
NODE            13              1:8x3                   1:8x1

#               ID  ARCO(SRG)    NODE.PORTA      NODE.PORTA
FIBER           1       1               0.0             1.0
FIBER           2       1               1.0             0.0
FIBER           3       2               0.1             2.0
FIBER           4       2               2.0             0.1
FIBER           5       3               0.2             3.0
FIBER           6       3               3.0             0.2
FIBER           7       4               1.1             2.1
FIBER           8       4               2.1             1.1
FIBER           9       5               1.2             7.0
FIBER           10      5               7.0             1.2
FIBER           11      6               2.2             5.0
FIBER           12      6               5.0             2.2
FIBER           13      7               3.1             4.0
FIBER           14      7               4.0             3.1
FIBER           15      8               3.2             11.0
FIBER           16      8               11.0            3.2
FIBER           17      9               4.1             5.1
FIBER           18      9               5.1             4.1
FIBER           19      10              4.2             6.0
FIBER           20      10              6.0             4.2
FIBER           21      11              5.2             8.0
FIBER           22      11              8.0             5.2
FIBER           23      12              5.3             9.0
FIBER           24      12              9.0             5.3
FIBER           25      13              6.1             7.1
FIBER           26      13              7.1             6.1
FIBER           27      14              7.2             10.0
FIBER           28      14              10.0            7.2
FIBER           29      15              8.1             10.1
FIBER           30      15              10.1            8.1
FIBER           31      16              9.1             12.0
FIBER           32      16              12.0            9.1
FIBER           33      17              9.2             13.0
FIBER           34      17              13.0            9.2
FIBER           35      18              10.2            12.1
FIBER           36      18              12.1            10.2
FIBER           37      19              10.3            13.1
FIBER           38      19              13.1            10.3
FIBER           39      20              11.1            12.2
FIBER           40      20              12.2            11.1
FIBER           41      21              11.2            13.2
FIBER           42      21              13.2            11.2
END

CONNECTION default PRIORITY MUST-PROTECT
ACTION
PROTECTION-TYPE         HGA
PROTECTION-COLOR        ANY
PROTECTION-PORT         ANY
MESH                    YES
MESH-MIN                1
MESH-MAX                32
PATH-TOL                10
VIEW-ROUTES             YES
VIEW-SUMMARY            YES
VIEW-LINKS              YES
END
```

Figura 7.3 - Arquivo de Topologia para a Rede NSFNet

A Figura 7.4 apresenta parte da topologia da rede NSFNet e a maneira como foram configuradas as portas de cada um dos 14 nós e seus correspondentes arcos (21 enlaces com pares de fibras, em sentidos opostos) para os testes da nossa proposta.

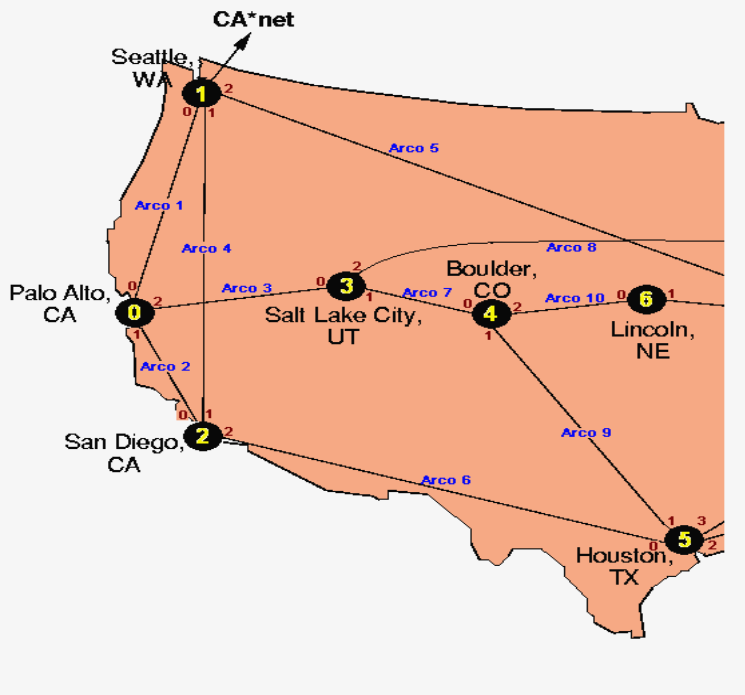


Figura 7.4 – Configuração da topologia da rede NSFNet para os testes

7.1.5 Solicitações para a criação de caminhos

Para solicitar um caminho ao Plano de Controle da rede de Transporte é usado um modelo Cliente-Servidor através da Interface Usuário-Rede (UNI). A comunicação entre a rede cliente e o plano de controle é feita via uma sessão *Telnet* desde a UNI. Assim, a partir da linha de comandos no *terminal* iniciamos uma sessão *telnet* no server *node1* (controlador da rede SIMOMEGA), na porta 1002, como mostrado na Figura 7.5.

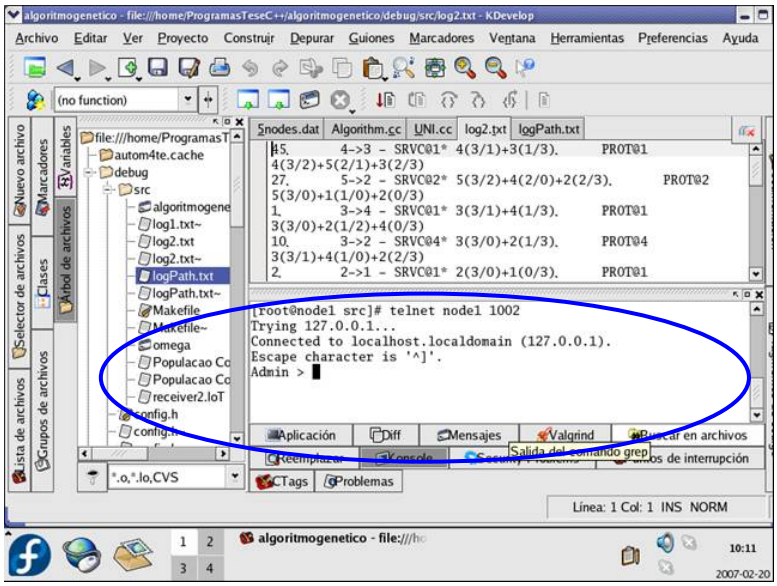


Figura 7.5 – Início de uma sessão *Telnet* desde a *Console* do *KDevelop*

No ambiente de serviço da UNI, proporcionada por Telnet, podemos solicitar, por exemplo, a criação de um caminho entre os nós 3 e 2 com o comando ***action create***, assim:

```
Admin> ac cr 3 2
```

Neste caso a UNI invoca a função ***create***. Esta função tem a seguinte lógica:

1. Toma-se o nó origem e destino respectivamente;
2. Monta-se a requisição com os parâmetros básicos da topologia (carregados do arquivo 5nodes.dat);
3. Fixa o proprietário da requisição;
4. Chama o algoritmo HGA para obter o caminho solicitado.

Se a requisição não foi aceita, é emitida uma mensagem de erro para o solicitante da mesma. Caso contrário, é enviada uma mensagem SETPORT para cada nó que faz parte do *ligthpath*. A requisição é armazenada na tabela de requisições do controlador.

O SETPORT ocasiona a comutação do respectivo nó, na chave e *lambdas* estipulados no comando. Após a comutação de suas chaves o nó que recebeu o comando envia um SETPORT_OK para o controlador. Assim, após receber o SETPORT_OK de todos os nós que fazem parte do respectivo caminho, o controlador armazena a requisição atendida, efetua a consistência das informações dos nós que enviaram o OK, estabelece o respectivo *Ligthpath* para LP_ACTIVE e, por último, remete um ROK (*Request OK*) para o solicitante da requisição.

Caso algum dos nós não consiga comutar suas chaves ele envia um SETPORT_NOK para o controlador e este desfaz com os demais as comutações. Desta forma, é enviado um UNSET_PORT para os nós e um RNOK (*Request Not OK*) para o solicitante do caminho.

Como podem existir várias requisições simultâneas ao controlador, o mesmo implementa um buffer que armazena as mesmas e as atende num conceito de FIFO (*First In First Out*). A requisição quando é completamente atendida é configurada no estado REQUEST_FINAL, caso contrário é configurada para REQUEST_PENDING.

No caso do caminho de proteção, as chaves não são configuradas no estado apropriado, mas é apenas registrado que determinadas portas do OXC estão associadas com a rota de

proteção. O resultado da alocação para a requisição solicitada é mostrado no *shell* do *Terminal* e armazenado no arquivo *log2.txt,* como mostrado a seguir, na Figura 7.6.

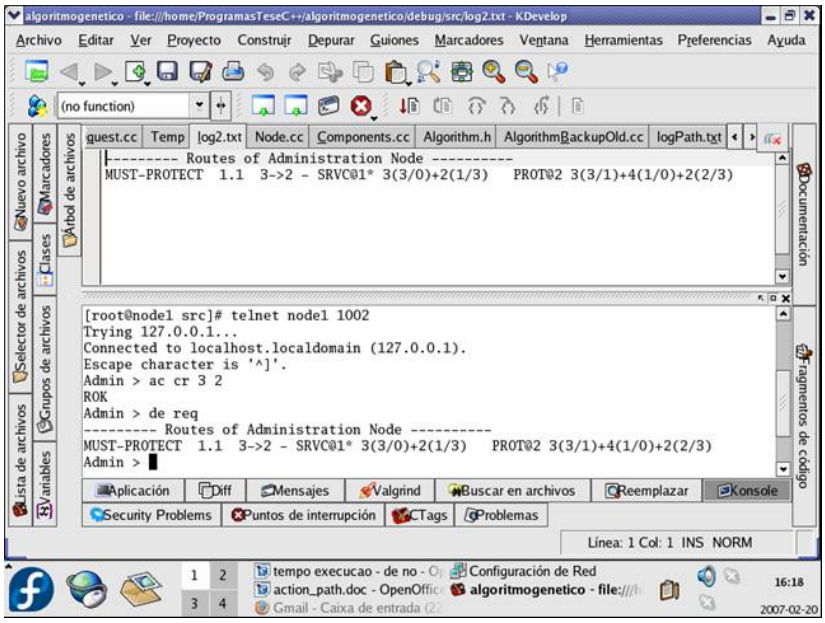


Figura 7.6 – Uso do comando ACTION CREATE e alocação do caminho solicitado

A indicação 1.1 indica que esta é a primeira requisição realizada e atendida pelo controlador, 3->2 mostra que a rota liga o nó 3 com o nó 2. SRVC@1* indica que a rota é de serviço (SRVC), e utiliza o comprimento de onda 1 (SRVC@1). O asterisco indica que a rota está ativa. Posteriormente são indicados os passos intermediários e, entre parênteses, informadas as portas ópticas de entrada e de saída de cada nó intermediário. No exemplo: 3(3/0)+2(1/3) indica que a rota parte do nó 3 e chega até o nó 2. No nó 3 a porta de entrada é a 3 (ADD) e a porta de saída a 0 da topologia. No nó 2 a porta de entrada é a 1 da topologia e a de saída é a 3 (DROP).

PROT@2 é a rota de proteção da rota 1, uma rota disjunta da rota de serviço, e que é formada pelos nós 3-4-2, usando o comprimento de onda 2. As portas constantes no exemplo podem ser diretamente inspecionadas no arquivo de topologia.

Também é possível criar rotas de maneira estática com o comando ACTION PATH. Este comando tem a seguinte sintaxe:

ac pa <rota de trabalho>@<lambda> MP @ <lambda> <rota de proteção>

Por exemplo:

```
ac pa 1 2 4@6 MP @7 1 5 4
```

Neste exemplo é criado um *caminho óptico* do nó 1 para o nó 4, passando pelo nó 2, com comprimento de onda 6, devendo o caminho ser protegido com comprimento de onda 7 usando a rota que vai desde o nó 1, passando pelo nó 5, até o nó 4. Isto é apresentado na Figura 7.7, além do resultado da requisição provida pelo algoritmo.

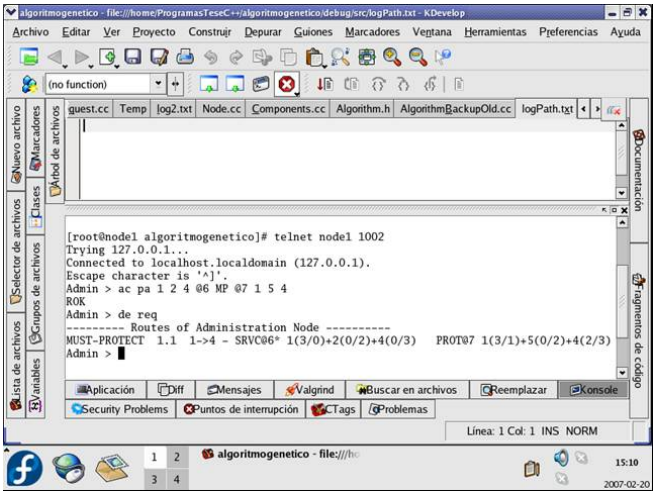


Figura 7.7 – Uso do comando ACTION PATH e alocação do caminho solicitado

7.1.6 Lógica para tratamento de uma falha no enlace

No SIMOMEGA, quando um enlace apresenta um problema, existe uma detecção automática da ausência de luz na respectiva entrada do OXC e então é emitida uma mensagem PORT_FAIL (*trap*), através da rede DNC (*Data Network Control*), para o sistema de controle. De posse desta mensagem, o sistema comuta as chaves para o caminho de proteção respectivo.

7.2 AVALIAÇÃO DO DESEMPENHO DO ALGORITMO HGA PROPOSTO

Com o objetivo de testar a consistência deste algoritmo foram utilizados um gerador de demandas e um comando de criação de requisições aleatórias.

7.2.1 Gerador de Demandas

O gerador de demandas foi escrito na linguagem C/C++ para Linux e é capaz de gerar solicitações de caminhos ópticos automaticamente, seguindo um modelo probabilístico, simulando a existência de clientes reais. O programa também faz a coleta de informações

necessárias para medição do desempenho do mecanismo. Para tal é usado um modelo de tráfego dinâmico no qual requerimentos cliente de conexão à rede serão feitos segundo um processo de Poisson com uma taxa de chegada de λ chamadas/s.

Um processo de Poisson [PAXSON, 1995] descreve o número de chegadas de entidades observadas no intervalo de tempo (0, t]. O processo de Poisson possui a seguinte função de distribuição de probabilidade:

$$P(Xt = x) = \frac{(\lambda t)^x e^{-\lambda t}}{x!}, x = 0,1,...$$

O tempo de retenção de sessão será exponencialmente distribuído com tempo de retenção média de *t* segundos. Os requerimentos de conexão serão distribuídos aleatoriamente em todos os nós da rede. A distribuição exponencial é bastante utilizada para modelar os tempos de serviço (é dizer, a distribuição do tamanho dos pacotes).

Para η sessões abertas na rede, o total da carga de tráfego (E) será dada por:

$$E = \eta \times \lambda \times t\left(erlangs\right)$$

Modificando os parâmetros η, λ, e t pode se ter controle sobre a carga.

A interação entre o gerador de demandas e o plano de controle foi montada utilizando um modelo Cliente/Servidor. O gerador de demandas (cliente) se comunica com o plano de controle (servidor) para solicitar a criação de um caminho óptico. O servidor, por sua vez, trata a solicitação e devolve informação para o cliente indicando se a solicitação foi atendida ou se houve bloqueio.

7.2.2 Comando de criação de requisições aleatórias

Com este comando as rotas são criadas em forma dinâmica e aleatória. Para efeitos de avaliação de desempenho é feita criação randômica através do comando *action ramdom* (*ac ra*). A sintaxe é a seguinte:

Admin> *ac ra <número de requisições> <delay>*

Por exemplo:

Admin> ac ra 60 1

Cria 60 requisições aleatórias com um retardo entre requisições de 1 ms. Isto é apresentado na Figura 7.8.

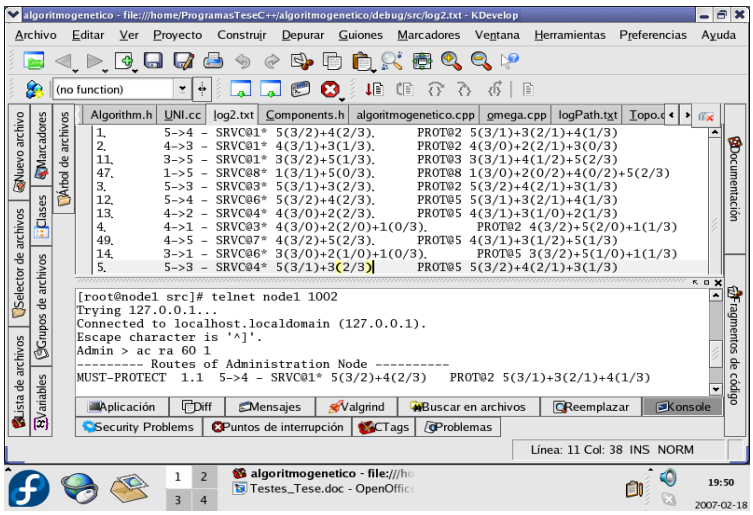


Figura 7.8 – Uso do comando ACTION RAMDOM e alocação aleatória de caminhos.

Os resultados de cada série de requisições são apresentados no arquivo *log2.txt*. Este arquivo é do tipo *apend*. Assim, quando é feita a execução randômica, automaticamente é acrescido o resultado das requisições atendidas e das recusadas. Para saber quais requisições foram atendidas, digitar o comando: *de req* (*debug request*).

```
Admin> de req
```

Se o retorno for ROK, será computado como aceita. Caso receba RNOK será computada como bloqueada. Isto é mostrado na Figura 7.9.

Para saber como estão as ocupações de cada porta com suas rotas e comprimentos de onda é usado o comando *de no* (*debug node*). Esta opção permitirá ao administrador ou usuário a criação de novas rotas de maneira estática. Por exemplo:

```
Admin> de no
```

Este comando pode ser chamado várias vezes para ver o resultado da ocupação das portas. Isto é apresentado na Figura 7.10**.**

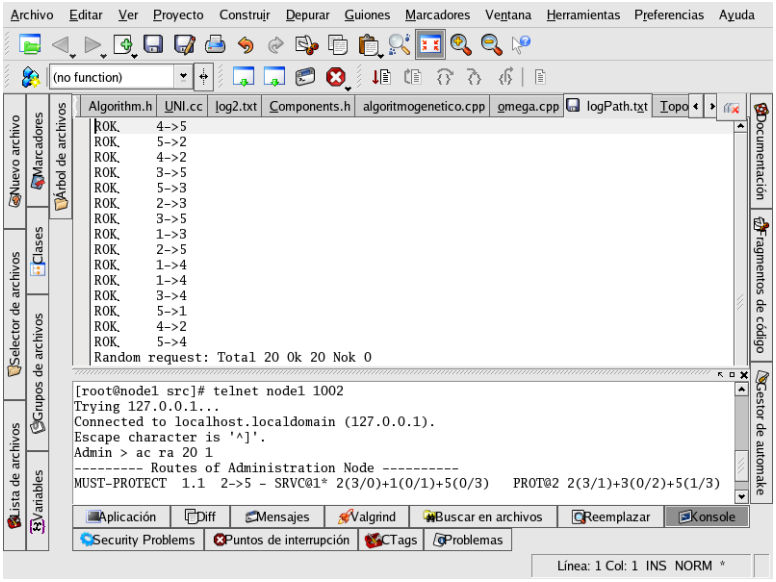


Figura 7.9 – Resultados mostrados pelo comando DEBUG REQUEST

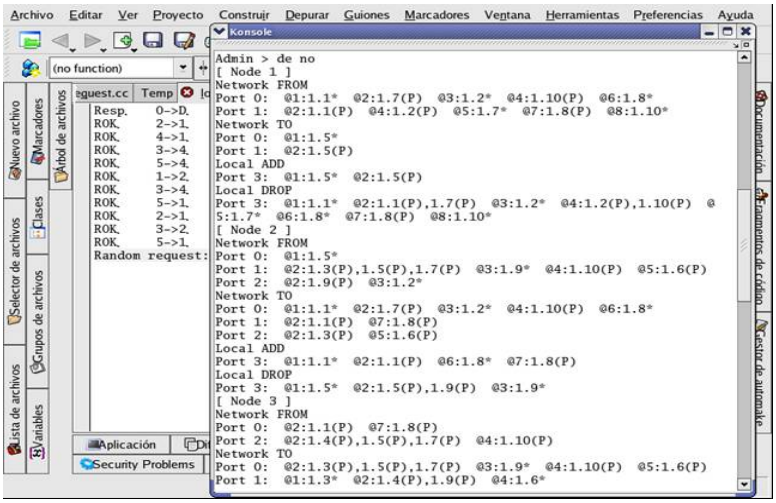


Figura 7.10 – Resultados mostrados pelo comando DEBUG NODE

7.2.3 Parâmetros de avaliação de desempenho

Neste trabalho foram avaliados os seguintes parâmetros:

a) Complexidade do algoritmo
b) Probabilidade média de bloqueio;
c) Tempo médio de execução;
d) Taxa de redundância da rede e capacidade de compartilhamento.

A avaliação de desempenho do mecanismo HGA foi feito no plano de controle da rede SIMOMEGA em uma PC com processador Pentium III 447 MHz e 384 MB de RAM, sob o sistema operacional Linux - distribuição FEDORA 5.

Para mostrar o desempenho do nosso mecanismo HGA foram feitas comparações com os diversos mecanismos apresentados na Tabela 7.1. Sobre a topologia da rede OMEGA foi comparado com o mecanismo do *testbed* SIMOMEGA [CRISPIM, 2006], apresentado no Anexo C; e sobre a topologia da rede *NSFNet*, com os algoritmos PIBWA [MOHAN, 1999] [MURTHY, 2002], apresentado nesta Tese em *4.8.1*, e com o algoritmo híbrido de Le, et.al. [LE, 2005], apresentado em *4.9*.

Tabela 7.1 – Mecanismos a serem comparados com a proposta HGA

MECANISMO	RWA	PROTEÇÃO	TOPOLOGIA	COMPLEXIDADE
SIMOMEGA [CRISPIM, 2006]	Roteamento Alternado: Dijkstra + First-Fit	Compartilhado tipo 1:N	OMEGA	
PIBWA [MURTHY, 2002]	S-DRWA com Roteamento Alternado baseado em Heurística com técnica de multiplexação *backup*		NSFNet	$O(K^2xH^2xW^2)$
HIBRIDO-LE [LE , 2005]	S-DRWA com Roteamento Adaptativo com Heurística baseada em Agentes Móbiles – GA, com técnica de multiplexação *backup*		NSFNet	$O(Gx(PxWxN^2 +P^2xN)$

7.3 COMPLEXIDADE DO ALGORITMO HGA

O processo para a obtenção da população entregada pelas heurísticas é feita usando O(N+N) unidades de tempo. Porem, dado que isto acontece uma única vez para todas as requisições estima-se que, diante dos processos recursivos do GA por cada requisição, seu custo computacional não terá muito impacto no tempo de execução total. Assim, a complexidade do mecanismo HGA há de recair na complexidade do algoritmo genético.

7.3.1 Complexidade do Algoritmo Genético proposto

A complexidade de avaliar o custo da população específica é P vezes a complexidade de avaliar o custo de cada individuo. O custo de cada indivíduo é obtido em dois passos:

a) Cálculo do custo do caminho primário: complexidade O(WxN).

b) Cálculo do custo do caminho backup: No pior dos casos, todos os comprimentos de onda (W) em todos os enlaces usados pelo caminho backup (um máximo de N) são examinados. Cada enlace pode ser compartilhado por outro caminho backup, em cujo caso, todos os enlaces (como máximo, N) do correspondente caminho primário serão também examinados. Assim, a complexidade para o custo do caminho backup estará dado por: $O(WxN^2)$ unidades de tempo.

Então, a complexidade de avaliar o custo de um indivíduo será: $O(WxN) + O(WxN^2) = O(WxN^2)$ e, a complexidade de avaliar o custo da população específica será então:

$$O(PxWxN^2).$$

A complexidade de se examinar todos os pares de indivíduos no estagio de *crossover* será $Px(P-1)/2$ vezes a complexidade de examinar um par de indivíduos. Esta operação inclui a criação do filho (dois por cada par), a confirmação da validade do indivíduo criado, e se este é diferente da população já existente. Estes passos são feitos usando O(N) unidades de tempo. Posteriormente procede-se à avaliação *fitness* do filho, cuja complexidade é O(PxWxN). Assim, a complexidade do estagio de *crossover* é dado por $O((Px(P-1)/2)xN + PxWxN)$, o que resulta em $O(P^2xN + PxWxN)$.

No estagio de mutação só dois indivíduos são mutados, porem esta operação requer igualmente de O(N) unidades de tempo. Assim, a complexidade que insere a mutação, considerando também a avaliação *fitness* do indivíduo, é dado por O(2P-1)x(N+WxN) ou simplesmente O(PxWxN).

Assim, a complexidade de cada iteração é o somatório da complexidade das etapas de *crossover* e mutação: $O(P^2xN + PxWxN) + O(PxWxN) = O(P^2xN + PxWxN)$, o qual, multiplicado por cada geração G representa:

$$O(Gx(P^2xN + PxWxN)).$$

Finalmente, a complexidade total do nosso algoritmo HGA estará dada por:

$$O(PxWxN^2).+ O(Gx(P^2xN + PxWxN)) = O(Gx(P^2xN + PxWxN^2))$$

A Tabela 7.2 apresenta uma comparativa de complexidade com os outros mecanismos analisados.

Tabela 7.2 – Comparativa da complexidade do HGA com PIBWA e HIBRIDO-LE

MECANISMO	COMPLEXIDADE
PIBWA [MURTHY, 2002]	$O(K^2xH^2xW^2)$
HIBRIDO-LE [LE , 2005]	$O(Gx(PxWxN^2 + P^2xN)$
HGA Proposto	$O(Gx(P^2xN + PxWxN^2))$

7.4 PROBABILIDADE MÈDIA DE BLOQUEIO

Após cada simulação foi calculada a probabilidade de bloqueio. O cálculo da probabilidade de bloqueio é dado pelo número de conexões bloqueadas sobre o total de requisições de conexões. A probabilidade de bloqueio é obtida pela Equação 7.1, assim:

$$P_b = \frac{\sum RNOK}{\sum Total\,\mathrm{Re}\,q} \quad \text{.....(Eq. 7.1)}$$

7.4.1 Probabilidade Média de Bloqueio

A Tabela 7.3 apresenta a Probabilidade Média de Bloqueio do algoritmo proposto. Os resultados foram obtidos usando-se o comando de criação de requisições aleatórias ACTION RAMDOM, executando-se até 10 testes por cada requisição, eliminando os valores extremos e obtendo o valor com maior freqüência. É importante lembrar que o algoritmo de HGA entrega tanto caminhos de trabalho como caminhos de proteção como um único indivíduo, por cada requisição dos clientes.

Observa-se nesta tabela uma boa probabilidade de bloqueio entre 25 e 35 requisições, sendo que em alguns testes foi alcançada uma probabilidade de 0.

Tabela 7.3 – Probabilidade de Bloqueio Média para o algoritmo HGA

Nº Requisições	ROK	RNOK	Probabilidade de Bloqueio
5	5	0	0,000
10	10	0	0,000
15	15	0	0,000
20	20	0	0,000
25	24	1	0,040
30	28	2	0,067
35	32	3	0,086
40	36	4	0,100
45	37	8	0,178
50	38	12	0,240

A Figura 7.11 mostra a curva da probabilidade média de bloqueio. Para valores acima das 50 solicitações se alcança a máxima resposta do sistema (38 requisições atendidas), levando o sistema ao seu ponto de saturação.

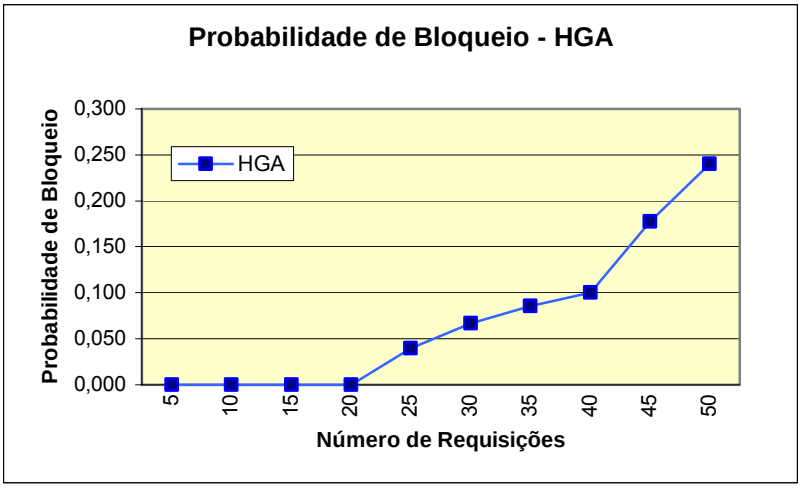


Figura 7.11 – Probabilidade de bloqueio obtida com o mecanismo HGA.

7.4.2 Probabilidade Média de Bloqueio como função de G e P

Foram também obtidos valores da probabilidade de bloqueio como uma função dos parâmetros G (número de gerações) e P (população) para uma carga de tráfego de 30 Erlangs. Foi avaliado o comportamento do algoritmo para a evolução de até 5 gerações, tanto para populações de 4 indivíduos como para a população máxima entregada pelas heurísticas. Os resultados são apresentados na Tabela 7.4

Tabela 7.4 – Probabilidade de Bloqueio como função de G e P

Nº Gerações	Probabilidade de Bloqueio	
	P=4	Pmax
1	0,267	0,167
2	0,100	0,067
3	0,067	0,033
4	0,033	0,033
5	0,033	0,033

A Figura 7.12 apresenta a probabilidade de bloqueio obtida como uma função dos parâmetros G e P. Observa-se que a probabilidade de bloqueio melhora quando G e P crescem, com tendência a se estabilizar. Esta análise é importante para definir o critério de parada do algoritmo. Assim, para P_{max} e considerando G=3 se terá um bom desempenho do

algoritmo, e podem então ser fixados como valores para população e critério de parada, respectivamente.

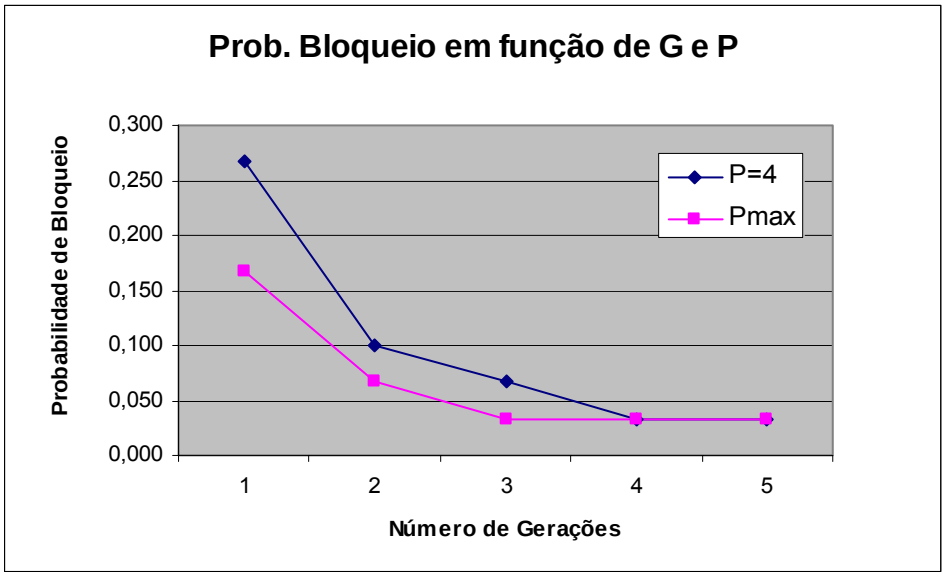


Figura 7.12 – Probabilidade de Bloqueio como função de G e P

7.4.3 Probabilidade de Bloqueio: HGA vs. algoritmo do SIMOMEGA

A Figura 7.13 apresenta o desempenho de bloqueio médio do algoritmo HGA proposto comparado com o algoritmo da rede SIMOMEGA. Observe o fato de que os resultados obtidos no SIMOMEGA correspondem a requisições atendidas para caminhos de serviço com proteção do tipo 1:N (ver anexo C para referência).

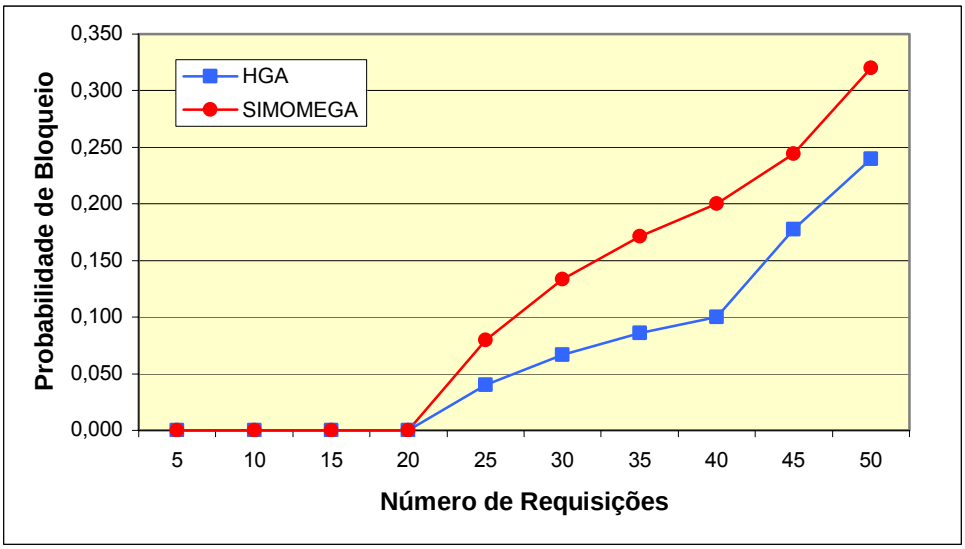


Figura 7.13 – Comparação das Probabilidades de bloqueio HGA – SIMOMEGA

Como é de se esperar, a probabilidade de bloqueio tende a aumentar com o número de requisições cliente. A curva mostrada na Figura 7.13 apresenta um bom desempenho do algoritmo de HGA, com valores de probabilidade de bloqueio muito abaixo dos resultados obtidos pelo algoritmo da rede SIMOMEGA.

Note-se, por exemplo, que para 35 requisições no HGA tem-se quase a mesma probabilidade de bloqueio do que para 25 requisições do SIMOMEGA.

7.4.4 Probabilidade de Bloqueio: HGA vs. PIBWA vs. HÍBRIDO-LE

A Tabela 7.5 mostra os valores da probabilidade média de bloqueio dos algoritmos PIBWA e HIBRIDO-LE, valores aproximados obtidos apartir dos resultados mostrados nos trabalhos publicados por [MOHAN, 1999][MURTHY, 2002] e [LE , 2005] respetivamente. Estes valores são contrastados com a nossa proposta HGA sobre a topologia da rede NSFNet. Observa-se que para cargas de tráfego maiores tem-se um melhor desempenho com o nosso mecanismo.

Tabela 7.5 – Probabilidade de Bloqueio dos algoritmos PIBWA, HIBRIDO-LE e HGA

Carga (Erlangs)	Pb PIBWA	Pb HÍBRIDO-LE	Pb HGA
35	0,02826	0,01174	0,01107
42	0,04087	0,01695	0,01593
49	0,05435	0,02445	0,02334
56	0,07348	0,03695	0,03179
63	0,09156	0,05087	0,04689

A Figura 7.14 evidencia graficamente estes resultados. Podemos deduzir, destes valores, que com o aumento da carga de tráfego na rede a capacidade de compartilhamento backup do nosso algoritmo consigue um melhor desempenho, liberando comprimentos de onda a serem alocados em novas requisições, melhorando assim a taxa média de bloqueio quando comparado com as outras propostas.

A certa similitude com a curva apresentada pela proposta de Le [LE , 2005] se pode interpretar como sendo devido às características hibridas de ambos os mecanismos.

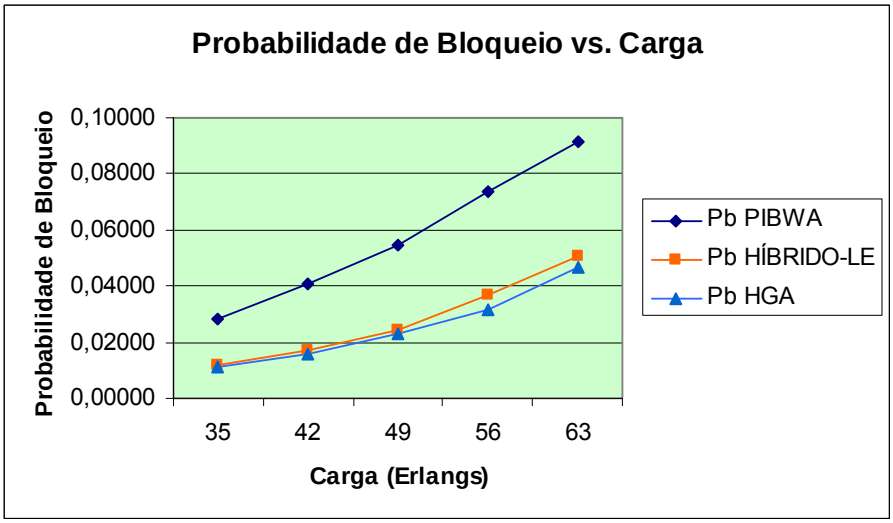


Figura 7.14 –Probabilidades de bloqueio: PIBWA, HIBRÍDO-LE e HGA

7.5 TEMPO MÉDIO DE EXECUÇÃO

O tempo médio de execução, como avaliador da velocidade de execução do algoritmo também é de interesse. Este tempo de execução do algoritmo é calculado como a razão entre o tempo de execução de uma série de requisições e o número de chamadas de dita série. A Equação 7.2 define este valor médio.

$$\bar{t}_m = \frac{\sum t_{execução-das-requisições}}{\sum N^o\, requisições} \quad \text{.....(Eq. 7.2)}$$

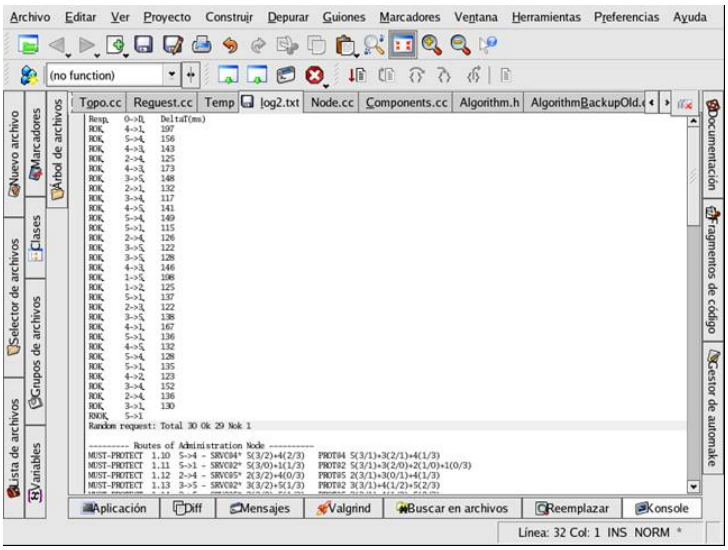


Figura 7.15 – Tempo de criação de cada um dos caminhos com proteção

O sistema guarda os tempos de execução, para a criação de cada um dos caminhos, no arquivo *log2.txt*. A Figura 7.15 apresenta esses tempos de criação dos caminhos com proteção para uma série de 30 requisições aleatórias.

7.5.1 Tempo médio de execução como função de G e P

A Tabela 7.6 apresenta o tempo médio de execução em função de G e P, considerando-se uma população de 4 indivíduos e logo a população máxima entregada pelas heurísticas. A Figura 7.16 permite ver como o tempo médio de execução vai-se incrementando com G.

Tabela 7.6 – Tempo médio de execução em função de G e P

Nº Gerações	Tempo Médio de Execução (ms)	
	P=4	Pmax
1	86,50	109,60
2	138,20	126,15
3	144,35	135,90
4	148,24	136,80
5	153,27	137,42

Observa-se que, para uma população menor (P=4), o tempo médio de execução na primeira iteração é muito menor, pois os indivíduos a avaliar não são muitos. Porém, nas seguintes gerações, os operadores de cruzamento e mutação vão exigir maior tempo de processamento do algoritmo, aumentando-se, portanto, o tempo necessário de execução.

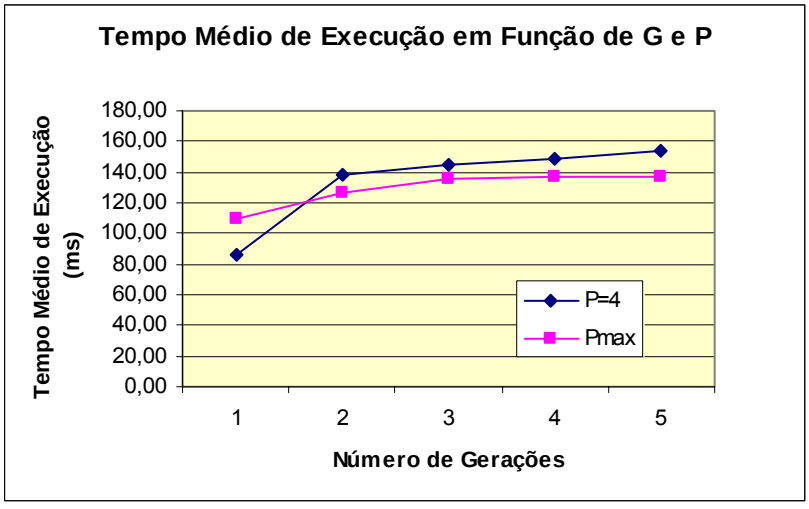


Figura 7.16 – Tempo médio de execução em função de G e P

Para P_{max} pode-se prescindir dos operadores genéticos, pois as heurísticas têm entregado ao algoritmo de GA todos os indivíduos (rotas de trabalho + proteção). Assim, esta pode

funcionar unicamente com o operador de seleção e a função de avaliação *fitness* (ver Capítulo 6), com o qual o tempo de execução tende a ser menor.

7.5.2 Probabilidade de Alocação de Indivíduos por Geração

A probabilidade de alocação de indivíduos por cada geração (para um tráfego de 30 Erlangs e considerando-se a população máxima dada pelas heurísticas), é apresentada na Figura 7.17. Observa-se que mais do 80% dos caminhos podem ser alocados na primeira iteração da evolução do algoritmo, o que demonstra que, em muitos casos um "muito bom caminho" pode ser achado na primeira iteração do algoritmo para o valor de custo mínimo.

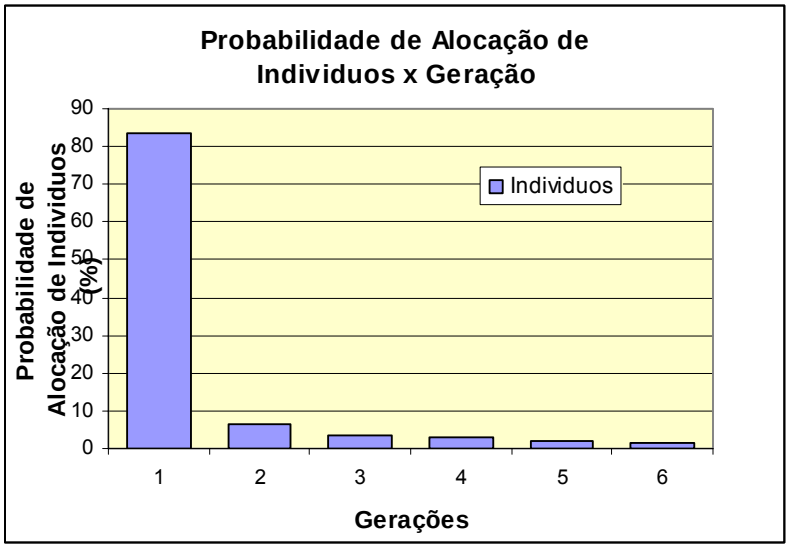


Figura 7.17 - Probabilidade de Alocação de Indivíduos por Geração no HGA

Esta estatística é importante para a definição do critério de parada do algoritmo, e mostra também que o incremento de G não tem um efeito significativo no tempo de execução médio.

7.5.3 Tempo médio de execução: HGA vs. SIMOMEGA

Para validar o tempo de latência deste algoritmo se apresenta, na Figura 7.18, o desempenho do tempo médio de execução do algoritmo HGA proposto comparado com o algoritmo da rede SIMOMEGA, para diferentes valores de tráfego (ver anexo C para referência).

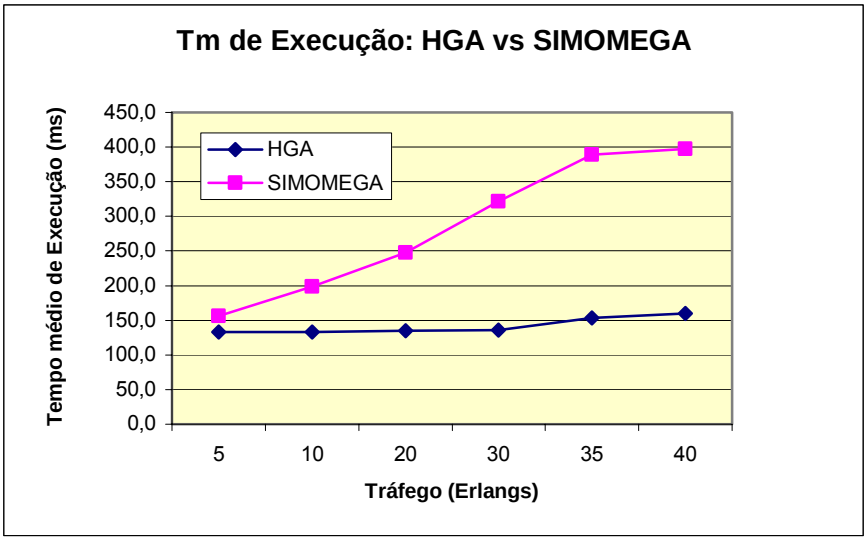


Figura 7.18 – Comparação do Tempo médio de Execução HGA – SIMOMEGA

A curva mostra que, para todos os casos, tem-se um tempo médio de execução muito menor com o algoritmo de HGA. Isto pode dever-se ao fato que à medida que o tráfego aumenta, uma capacidade de compartilhamento eficaz para os caminhos backup é necessária (como apresentado na proposta HGA), o qual, no SIMOMEGA, mostra-se pouco ótima pelo uso da proteção do tipo 1:N, que recursivamente tenderá a procurar caminhos de proteção num cenário com cada vez menos recursos, resultando num maior tempo médio de execução.

7.6 TAXA DE REDUNDÂNCIA DA REDE E CAPACIDADE DE COMPARTILHAMENTO

Outra métrica considerada neste trabalho é a taxa de redundância da rede R_r a qual vem definida como a razão entre a capacidade de reserva total e a capacidade de trabalho total, como mostrado na Equação 7.3 [ZHOU 1, 2002].

$$R_r = \frac{\sum_{(ij)\in L} B_{ij}}{\sum_{(ij)\in L} A_{ij}} \quad \text{.....(Eq. 7.3)}$$

Onde: A_{ij} : Soma total da largura de banda usando o enlace (i,j)

B_{ij} : Total da largura de banda reservada para caminhos *backup* que usam o enlace (i,j)

Para esta análise foi levantada a seguinte estatística. Considere-se 30 Requisições solicitadas desde a UNI e que foram alocadas pelo Algoritmo HGA (29 foram ROK e 1 NROK) (fonte: arquivo log2.txt).

Deve-se ter em conta, para esta análise, que o conjunto de caminhos de trabalho foi obtido pela heurística baseada no algoritmo de *Dijkstra*, é dizer, priorizando-se as rotas com o menor número de saltos e, portanto, de menor uso de enlaces. Já para o conjunto de caminhos de proteção interessa, não só uma menor quantidade de saltos, mas também a capacidade de compartilhamento que se possa obter.

```
[root@node1 ~]# telnet node1 1002
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
Admin > ac ra 30 1

1      3->2 - SRVC@1* 3(3/0)+2(1/3)          PROT@2 3(3/1)+4(1/0)+2(2/3)
2      4->5 - SRVC@1* 4(3/2)+5(2/3)          PROT@2 4(3/1)+3(1/2)+5(1/3)
3      5->1 - SRVC@1* 5(3/0)+1(1/3)          PROT@2 5(3/1)+3(2/0)+2(1/0)+1(0/3)
4      4->3 - SRVC@3* 4(3/1)+3(1/3)          PROT@2 4(3/0)+2(2/1)+3(0/3)
5      5->2 - SRVC@3* 5(3/0)+1(1/0)+2(0/3)   PROT@4 5(3/1)+3(2/0)+2(1/3)
6      5->1 - SRVC@5* 5(3/0)+1(1/3)          PROT@6 5(3/1)+3(2/0)+2(1/0)+1(0/3)
7      2->5 - SRVC@3* 2(3/0)+1(0/1)+5(0/3)   PROT@2 2(3/1)+3(0/2)+5(1/3)
8      4->3 - SRVC@4* 4(3/1)+3(1/3)          PROT@5 4(3/0)+2(2/1)+3(0/3)
9      5->1 - SRVC@7* 5(3/0)+1(1/3)          PROT@8 5(3/1)+3(2/0)+2(1/0)+1(0/3)
10     1->5 - SRVC@4* 1(3/1)+5(0/3)          PROT@5 1(3/0)+2(0/1)+3(0/2)+5(1/3)
11     4->3 - SRVC@6* 4(3/1)+3(1/3)          PROT@7 4(3/0)+2(2/1)+3(0/3)
12     3->5 - SRVC@6* 3(3/2)+5(1/3)          PROT@2 3(3/1)+4(1/2)+5(2/3)
13     4->3 - SRVC@8* 4(3/1)+3(1/3)          PROT@8 4(3/0)+2(2/1)+3(0/3)
14     3->2 - SRVC@5* 3(3/0)+2(1/3)          PROT@4 3(3/1)+4(1/0)+2(2/3)
15     3->4 - SRVC@3* 3(3/1)+4(1/3)          PROT@2 3(3/0)+2(1/2)+4(0/3)
16     3->2 - SRVC@7* 3(3/0)+2(1/3)          PROT@8 3(3/1)+4(1/0)+2(2/3)
17     1->2 - SRVC@6* 1(3/0)+2(0/3)          PROT@2 1(3/1)+5(0/1)+3(2/0)+2(1/3)
18     1->5 - SRVC@7* 1(3/1)+5(0/3)          PROT@8 1(3/0)+2(0/1)+3(0/2)+5(1/3)
19     2->3 - SRVC@1* 2(3/1)+3(0/3)          PROT@2 2(3/2)+4(0/1)+3(1/3)
20     1->4 - SRVC@1* 1(3/1)+5(0/2)+4(2/3)   PROT@2 1(3/0)+2(0/2)+4(0/3)
21     2->1 - SRVC@4* 2(3/0)+1(0/3)          PROT@8 2(3/1)+3(0/2)+5(1/0)+1(1/3)
22     5->4 - SRVC@3* 5(3/2)+4(2/3)          PROT@2 5(3/1)+3(2/1)+4(1/3)
23     2->1 - SRVC@1* 2(3/0)+1(0/3)          PROT@2 2(3/1)+3(0/2)+5(1/0)+1(1/3)
24     2->4 - SRVC@1* 2(3/2)+4(0/3)          PROT@4 2(3/1)+3(0/1)+4(1/3)
25     3->4 - SRVC@1* 3(3/0)+4(1/3)          PROT@4 3(3/2)+5(1/2)+4(2/3)
26     2->5 - SRVC@3* 2(3/1)+3(0/2)+5(1/3)   PROT@6 2(3/0)+1(0/1)+5(0/3)
27     3->5 - SRVC@1* 3(3/0)+5(1/3)          PROT@4 3(3/0)+4(1/2)+5(2/3)
28     5->2 - SRVC@6* 5(3/1)+4(2/0)+2(2/3)   PROT@4 5(3/0)+1(1/0)+2(0/3)
29     3->5 – RNOK
30     5->3 - SRVC@1* 5(3/1)+3(2/3)          PROT@2 5(3/1)+4(2/1)+3(1/3)
Random request: Total 30 Ok 29 NOk 1
```

A Tabela 7.7 apresenta os enlaces e os comprimentos de onda que foram alocadas para as 29 requisições aceitas.

Tabela 7.7 – Alocação de enlaces e comprimentos de onda pelo algoritmo HGA para 30 solicitudes de *Lightpath*

	λ_1		λ_2		λ_3		λ_4		λ_5		λ_6		λ_7		λ_8	
Link	**w**	**p**	**w**	**p**	**w**	**p**	**w**	**p**	**w**	**p**	**w**	**p**	**w**	**p**	**w**	**p**
1-2				▲	▲			■		▲	▲					▲
1-5	▲			▲	▲							▲	▲			
2-1	▲			▲	▲		▲					■				▲
2-3	▲			■				■		■				▲		●
2-4	▲			●												
3-2	▲			●				▲	▲			▲	▲			▲
3-4	▲			●	▲			●								▲
3-5				■				■		▲	▲					■
4-2				■				▲		▲	▲			▲		■
4-3				●	▲		▲				▲				▲	
4-5	▲			▲				▲								
5-1	▲				▲			●	▲			▲	▲			▲
5-3				●				▲								▲
5-4	▲				▲			▲			▲					

Lênda:
▲ Lambda 1 vez usada
■ Lambda 2 vezes usada
● Lambda 3 vezes usada

Assim, para estas 30 requisições, os caminhos de proteção usarão mais enlaces e, portanto, também mais comprimentos de onda do que os caminhos de trabalho, o qual é usual em todo algoritmo de RWA com sobrevivência. Isto é evidenciado na Tabela 7.8.

Tabela 7.8 – *Lambdas* usados pelos enlaces para os caminhos de trabalho e Proteção

Enlace	Comprimentos de Onda	
	Trabalho	Proteção
1-2	2	4
1-5	3	2
2-1	3	3
2-3	1	5
2-4	1	1
3-2	3	4
3-4	2	3
3-5	1	4
4-2	1	5
4-3	4	1
4-5	1	2
5-1	4	3
5-3	0	3
5-4	3	1
Total	29	41

A taxa de redundância da rede (R_r) depende muito da topologia da rede como do algoritmo de alocação de capacidade de reserva. Usando um esquema de proteção dedicada, R_r seria igual a 100%. Sem considerar explicitamente restrições SRLG o esquema de proteção

compartilhada proposto por [ALANYALI, 1999], obtem valores na ordem de 74% a 87% para uma rede de 32 nós.

Aplicando a Equação 7.3, tem-se para a proposta HGA:

$$Rr = 41/70 = 0{,}58$$, é dizer uma taxa de redundância de 58%

Pode-se considerar este um ótimo valor quando comparado com os resultados obtidos com o mecanismo apresentado no trabalho de [ALANYALI, 1999]. Em [ZHOU 1, 2002], foram obtidos valores similares à nossa proposta, porem o seu algoritmo, baseado em proteção multi-path, foi projetado para um cenário S-RWA estático, onde a reserva de recursos também é fundamental.

O que se deseja avaliar também é a capacidade de compartilhamento que se pode alcançar com um dado algoritmo. Assim, observa-se da Tabela 7.7 que, para o exemplo dado, 18 enlaces são re-usados pelo algoritmo de HGA por duas ou por três vezes, tendo-se compartilhado até 26 comprimentos de onda, o que representa 38,8% de capacidade de compartilhamento, liberando assim recursos, os quais poderão ser utilizados para alocar novas requisições.

É importante destacar que se usando um sistema de proteção sem compartilhamento seriam necessários, para este exemplo, reservar até 67 *lambdas* para os caminhos de proteção, (é dizer, 26 a mais do que os usados pelo algoritmo HGA), e necessários 18 enlaces adicionais, o qual levaria a elevar dramaticamente a probabilidade de bloqueio.

Capítulo 8

"Concluímos, pois, que o homem é justificado pela fé,
Independentemente das obras da lei"
Ro 3:28

8 CONCLUSÕES

8.1 ANÁLISE DOS RESULTADOS

Nas redes de transporte ópticas com restrição de comprimento de onda, cenário de desenvolvimento deste trabalho, conexões *multi-hops* são mais complicadas de se estabelecer do que aquelas de um único salto, dado que aquelas precisam de um maior número de canais a serem iguais em toda a extensão do caminho. Também, dependendo de fatores tais como a topologia de rede e o tráfego cursado, alguns enlaces podem apresentar maior congestionamento do que outros, de maneira que requisições que requeiram *lambdas* nestes enlaces terão uma alta probabilidade de ser bloqueados.

Por outro lado, os esquemas de sobrevivência estão evoluindo da proteção mais simples, a proteção dedicada, para técnicas de multiplexação de caminho *backup,* para permitir que dois ou mais caminhos de trabalho possam compartilhar o mesmo caminho de proteção, desde que seus respectivos caminhos de trabalho não pertençam ao mesmo SRLG.

Portanto, no projeto de algoritmos de S-DRWA não só é importante o desempenho enquanto à probabilidade de bloqueio, mas também a capacidade de compartilhamento dos caminhos *backup*, que redunda em uma ótima gestão dos recursos, liberando canais de comprimento de onda para novas alocações reduzindo, assim, a probabilidade de bloqueio.

Outro parâmetro de grande interesse é a complexidade computacional e o tempo de execução, assim como a diminuição da taxa de redundância, obtida pelo ação do algoritmo. O tempo de execução do algoritmo é um fator chave para o estabelecimento rápido de caminhos ópticos dinâmicos. Desta maneira se pode garantir uma latência adequada na rede.

Nos nossos testes foram avaliados valores de probabilidade de bloqueio como uma função dos parâmetros G (número de gerações) e P (população) na topologia da rede OMEGA. Foi avaliado o comportamento do algoritmo para a evolução de até 5 gerações, tanto para populações de 4 indivíduos como para a população máxima entregada pelas heurísticas. Observa-se que a probabilidade de bloqueio melhora quando G e P crescem, com tendência a se estabilizar. Está análise foi importante para definir o critério de parada do nosso algoritmo. Assim, para Pmax e considerando G=3 o mecanismo apresentou um bom desempenho sendo fixados como valores de população e critério de parada, respectivamente.

Lembre-se que o GA é um método genérico que precisa ser customizado para a problemática específica que se deseja abordar. Assim, o projeto para o mecanismo de codificação dos indivíduos, o tamanho da população, o número de gerações (iterações), o critério de parada (*stopping*) e os diferentes operadores foram adaptados às características do problema para otimizar o tempo de computação. Assim, é formulado um GA adaptado às necessidades de execução em tempo real em que são feitas as funções que se desejam otimizar, a saber RWA e Sobrevivência. Além do mais, a alternativa adotada neste trabalho, que é a modelagem híbrida baseada em Heurísticas e Algoritmos genéticos, tende ao estabelecimento de uma rápida convergência no valor mais ótimo

Desta maneira, a probabilidade de alocação de indivíduos por cada geração para o HGA mostrou que mais do 80% dos caminhos podem ser alocados na primeira iteração da evolução do algoritmo, o que demonstra que, em muitos casos um "muito bom caminho" pode ser achado na primeira iteração do algoritmo, tendo-se assim um reduzido tempo de computação e uma convergência rápida para o valor de coste mínimo (valor de *fitness* ótimo).

Na avaliação da probabilidade de bloqueio média do nosso algoritmo HGA comparada com outras propostas foram obtidos resultados satisfatorios. Tanto na comparação com o esquema utilizado pelo SIMOMEGA, numa rede com 5 nós; assim como no paralelo com as propostas PIBWA e HÍBRIDO-LE, numa topologia com 14 nós, o nosso algoritmo mostrou sua eficiência.

Assim, quando comparado com o algoritmo da rede SIMOMEGA, a qual implementa um algoritmo de RWA baseado em *Dijkstra* e *FirstFit*, e um mecanismo de proteção do tipo

1:N, o algoritmo de HGA apresenta um bom desempenho, com valores de probabilidade de bloqueio muito abaixo dos resultados obtidos pelo algoritmo da rede SIMOMEGA.

Na comparação com o algoritmo PIBWA, o qual implementa um algoritmo de RWA alternativo com sobrevivencia, o algoritmo de HGA mostra um desempenho superior, com probabilidade de bloqueio melhor aos resultados obtidos na proposta de [MURTHY, 2002].

Na análise sobre os resultados obtidos em [LE , 2005], observa-se valores muito similares, que vão-se diferenciando ligeramente com o aumento do tráfego. Esta similaridade se corresponde com as características híbridas heurístico-genéticos de ambos os algoritmos, porem, o diferencial na codificação do indivíduo e o tipo de heurística empregada dão ao nosso algoritmo um melhor desempenho a maiores cargas de tráfego.

Enquanto ao tempo médio de execução, como avaliador da velocidade de computação do algoritmo, se obtiveram também bons resultados. Quando avaliado em função de G e P observa-se que para uma população reduzida (P=4), o tempo médio de execução na primeira iteração foi muito menor, explicado pela relativamente pouca quantidade de indivíduos a avaliar. Porém, nas seguintes gerações, os operadores de cruzamento e mutação exigem da máquina um maior tempo de processamento do algoritmo, aumentando-se, portanto, o tempo necessário de execução.

Para populações maiores pode-se prescindir da funcionalidade dos operadores genéticos em favor de um menor tempo de execução. Isto é aconselhável nesta proposta, e se apresenta como uma variante, dado que as heurísticas têm entregado ao algoritmo de GA todos os indivíduos (rotas de trabalho + proteção). Assim, a parte GA do mecanismo pode funcionar unicamente com o operador de seleção e a função de avaliação *fitness* na complexa tarefa de selecionar os melhores caminhos com capacidade de compartilhamento e alocar os comprimentos de onda em forma implícita, obtendo-se um relativamente reduzido tempo de execução.

Para validar o tempo de latência do nosso algoritmo foi feito um paralelo com o desempenho do tempo médio de execução entregado pelo mecanismo do SIMOMEGA, para diferentes valores de tráfego. Para todos os casos, tem-se um tempo médio de execução mais reduzido com o nosso algoritmo. Isto pode dever-se ao fato que a medida que o tráfego aumenta, a capacidade de compartilhamento para os caminhos *backup*

implementada pela proposta do HGA começa a ser útil, permitindo ainda se obter recursos com menores iterações, enquanto que o SIMOMEGA, pelo uso da proteção do tipo 1:N, tenderá recursivamente a procurar caminhos de proteção num cenário com cada vez menos recursos, precisando assim de um maior tempo de execução.

O tempo de execução de um algoritmo também pode-se expresar em função da complexidade do algoritmo. O nosso algoritmo HGA apresenta uma complexidade dada por: $O(Gx(P^2xN + PxWxN^2))$, complexidade similar à proposta de [LE , 2005] e uma menor complexidade quando comparada com o algoritmo PIBWA de [MURTHY, 2002].

Outra métrica considerada neste trabalho, a taxa de redundância da rede, apresentou também um ótimo valor, quando comparado com os resultados do SIMOMEGA, com o esquema de proteção compartilhada proposto por Alanyali [ALANYALI, 1999] e com o trabalho de [ZHOU 1, 2002], alcançando uma taxa de redundância de 58%. Também, a capacidade de compartilhamento que se conseguiu alcançar com o nosso algoritmo esteve acima do 38%. Como conseqüência os recursos não usados podem ser alocados em novas requisições, diminuindo assim a probabilidade de bloqueio.

Portanto, por médio destes processos de avaliação e validação demonstramos que o algoritmo HGA para S-DRWA proposto neste trabalho é efetivo, obtendo-se uma baixa probabilidade de bloqueio e um relativamente baixo tempo de execução, com uma alta capacidade de compartilhamento de rotas de proteção.

Finalmente, vale destacar que das propostas revisadas nesta Tese, muitos dos artigos e trabalhos de pesquisa divulgados não apresentam suficiente informação de maneira a reproduzir o algoritmo com fins de avaliação. Detalhes da implementação, a necessidade de uma formulação mais adequada do algoritmo, a falta de uniformidade nas representações das variáveis e parâmetros envolvidos, etc. tornam difícil a avaliação e comparação das diferentes propostas na prática.

8.2 CONCLUSÕES DO TRABALHO

Esta Tese apresentou a criação, o desenvolvimento e a aplicação de um algoritmo híbrido heurístico-GA (HGA) para a otimização dos mecanismos de Alocação Dinâmica de Rota e Comprimento de onda visando Sobrevivência (S-DRWA), orientado à reserva de capacidade baseado em compartilhamento de rotas de proteção, e aplicado em redes de transporte IP sobre WDM.

Neste mecanismo, as heurísticas propostas fazem a seleção dos melhores caminhos de trabalho com seus respectivos caminhos *backup* e o Algoritmo Genético faz o aprovisionamento para o "melhor" par de rotas trabalho/proteção com a alocação do comprimento de onda adequado, estabelecendo assim o caminho com proteção requerido.

Para avaliação e validação desta proposta foram feitos testes de desempenho sobre protótipos e topologias de rede conhecidas. Os resultados obtidos foram comparados com propostas validadas internacionalmente, demonstrando nosso mecanismo um alto desempenho nos parâmetros de probabilidade de bloqueio, tempo médio de execução, complexidade computacional, taxa de redundância e capacidade de compartilhamento, perfilando-se esta proposta como sólida alternativa de solução para a problemática de S-DRWA.

8.3 TRABALHOS FUTUROS

Esta proposta de S-DRWA pode se estender para se obter novas funcionalidades. Propostas de trabalhos futuros são dadas a seguir.

8.3.1 Reconfiguração da rede para contornar o problema de bloqueio

Em redes de grande porte, pode dar-se o caso que uns *lightpaths* já estabelecidos estejam bloqueando rotas críticas que dificultam o estabelecimento de algumas novas rotas. Nestes casos, é desejável ter a possibilidade de reconfigurar a rede para alcançar uma situação ótima global, Porém a condição de não interromper as rotas de serviço já existentes o impede.

Uma estratégia para contornar este problema poderia consistir em duplicar a informação, dos caminhos que originam o bloqueio, por um tempo determinado por uma rota de proteção adequada, para logo o receptor comutar a dita rota de proteção, liberar a inicial, evitando assim a perda de informação, e permitir um re-ordenamento do tráfego. Adaptar o algoritmo para esta contingência será necessario.

8.3.2 Avaliação do algoritmo HGA em outros planos de controle

É de interesse avaliar e validar o aporte desta proposta em outros planos de controle, sejam estes centralizados, sejam distribuídos, com outras topologias ou modelos de rede, de maneira a ter um maior panorama da eficácia e utilidade deste algoritmo.

8.3.3 Interface de Configuração do Algoritmo

Dado que é de importância para a customização do algoritmo híbrido, principalmente a parte relativa ao GA, a configuração de certos parâmetros tais como o tamanho da população, o número de gerações, o critério de parada, etc., uma interface de configuração facilitaria esta funcionalidade.

ANEXOS

A. A REDE OMEGA

A Rede OMEGA-WRON (*Optical Metro network for Emerging Gigabit Applications-Wavelength Routing Optical Network*) é um *testbed* de rede óptica transparente em topologia malha com um plano de controle distribuído, baseado em roteamento de comprimento de onda RWA, orientado a conexão e com caminhos bidirecionais. O *testbed* OMEGA foi desenvolvido pela Fundação CPqD (Centro de Pesquisa e Desenvolvimento em Telecomunicações) de Campinas, SP – Brasil [ROSSI, 2002].

O plano de Controle distribuído da rede OMEGA foi também montado, para fins de pesquisa e desenvolvimento no laboratório "*LabCom"* do Departamento de Engenharia Elétrica da Universidade de Brasília [PASTOR1, 2004]. Posteriormente foi estabelecida em uma arquitetura centralizada e nomeada de SIMOMEGA [CRISPIM, 2006], como parte do convenio UnB/CDT-CPqD. Também se encontra um plano de controle da rede OMEGA no "*OpNeAR Lab*" da *University of Texas at Dallas* [OPNEAR, 2007] *sob o* projeto "*Differentiated Reliability in an Optical Test-bed*". Ambos os laboratórios desenvolvem as suas pesquisas independentemente.

Cada nó possui um dispositivo *add/drop* local; um módulo de comutadores ópticos (OXCs); amplificadores ópticos; *transponders* e um módulo de controle. Cada nó possui 4 portas, três dessas portas são conectadas com os nós adjacentes e uma é usada para o *add/drop*. Os comutadores ópticos, compostos por oito entradas e oito saídas, são responsáveis por redirecionar um dos oito comprimentos de onda desde uma porta de entrada para uma porta de saída. Nesta rede, os OXC não provêm conversão de *comprimento de onda*.

A.1. PLANO DE TRANSPORTE DA REDE OMEGA

A rede OMEGA é formada por cinco nós equivalentes funcionalmente com capacidade para se conectar com outros três nós da rede. Cada nó pode receber um comprimento de onda por uma porta e pode optar entre duas portas de saída para cada novo cliente. A Figura A.1 mostra a topologia desta rede. Como cada porta tem duas fibras (uma para

entrada e outra para saída), o comprimento de onda poderá retornar para o nó de origem, possibilitando também a montagem de uma rede funcional em anel bidirecional, como utilizado nas redes SDH, e que pode ser especialmente útil se deseja-se comparar desempenho entre as duas tecnologias. Cada nó possui também uma porta bidirecional para entrada e saída dos clientes locais (*add-drop*), capacitando a rede a permitir acesso a novos clientes desde qualquer nó.

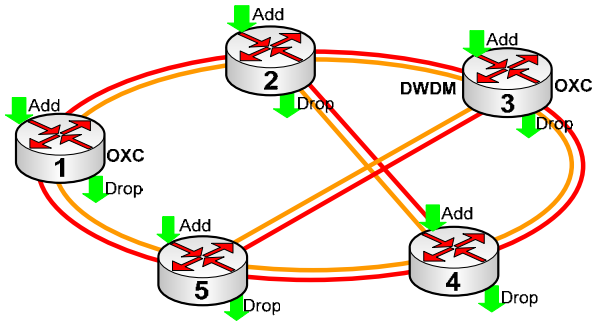


Figura **A.1** - Topologia da Rede OMEGA.

Além do OXC, cada nó possui um módulo com *transponders* que têm a função de adaptação dos comprimentos de onda dos clientes para os comprimentos de onda da grade ITU usada nesta rede. Esta rede tem também um módulo de amplificação óptica necessário para manter o nível de potência, compensando as perdas de inserção dos demais componentes. Cada um dos sete enlaces de fibra da Rede OMEGA compreende dois carretéis de 20 km de fibra monomodo (ITU-T G.652). Cada fibra é caracterizada em termos de dispersão, atenuação e PMD. A Figura A.2 mostra a estrutura física de um nó desta rede.

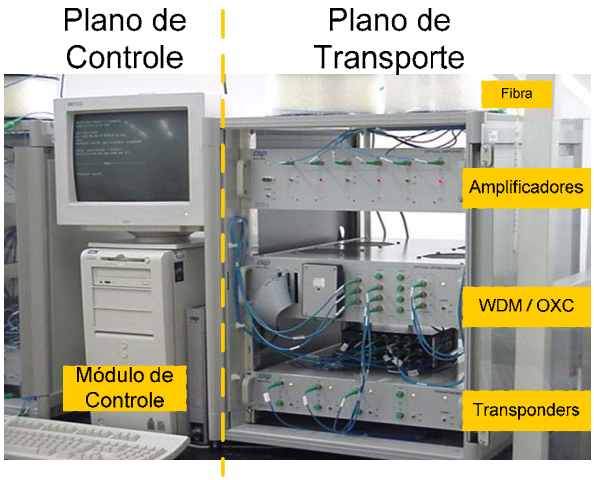


Figura **A.2** - Estrutura física de um nó da rede OMEGA

A Figura A.3 representa esquematicamente os elementos de cada nó, responsáveis pela multiplexão/demultiplexão (WDM), a conexão cruzada (OXC), a adaptação dos comprimentos de onda (*Transponders*) e as operações de derivação e inserção (OADM).

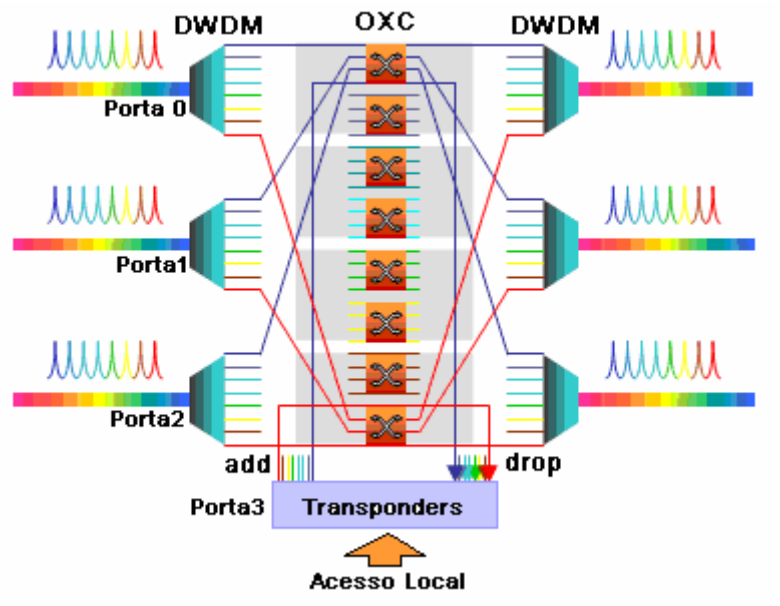


Figura **A.3** - Elementos de um nó óptico da rede OMEGA

A Tabela A.1 apresenta, de forma resumida, as características técnicas das chaves termo-ópticas 8 x 8 usadas na rede OMEGA [ROCHA, 2002].

Tabela A.1 - Características típicas da chave termo-óptica 8 x 8 fabricada pela NEL.

Item	Especificação
Portas Entrada/Saída	8 × 8 (não-blocante)
Janela de operação	1550 nm
Perda de inserção	<8dB
Uniformidade da perda	<2dB
Razão de extinção	>40dB
PDL	<0,5dB
Perda de retorno	>40dB
Velocidade de chaveamento	<3ms
Consumo de potência	<8W (Módulo PLC), 2,8W (circuito de controle)
Temperatura de operação	0 to 65℃
Controle de chaveamento	TTL (+5V)
Tensão de alimentação	+24V±5% / 0,85º (max)
Ventilação	Necessário ventilação forçada de ar (>1,5m/sec. recomendada)
Dimensões (W × D × H)	145 × 156 × 23 mm³

Nesta rede, a função de comutação possui três etapas:

1. Demultiplexação do sinal WDM separando os canais entre si;

2. Cada comprimento de onda entra individualmente em uma das portas do comutador óptico espacial que o direciona para uma das portas de saída;
3. Os comprimentos de onda são direcionados para uma fibra de saída já multiplexados.

Cada *cross-connect* da rede OMEGA foi projetado para usar três MUXs (1x8) e três DEMUXs (8x1) com espaçamento de canal de 200 GHz baseado na grade ITU-T, na faixa desde 1547,72 a 1558,98 nm. Estes comutadores são controlados por um PC, que usa interfaces TTL para tal função. Os comutadores ópticos têm um nível de *cross talk* de –35dB, e filtros com faixa de passo suficientemente larga para evitar o corte spectral (*spectral clipping*). A Figura A.4 mostra a configuração física do *optical cross-connect* (OXC) da rede OMEGA.

Figura A.4 - *Optical cross-connect* (OXC) da rede OMEGA.

A Tabela A.2 lista as características relativas a perdas e ganhos para cada dispositivo embutido no nó óptico.

Tabela A.2 - Características típicas dos dispositivos do nó óptico

Dispositivo	(dB)
Perda no Demux, $Loss_{demux}$	3
Perda no Comutador, $Loss_{sw}$	8
Perda no Mux, $Loss_{mux}$	3
Perda no Connector, $Loss_{con}$	0,5
Ganho no EDFA, G_{EDFA}	15 to 25

São utilizados amplificadores EDFA nas três portas de saída de cada nó. Cada amplificador amplifica todos os comprimentos de onda de uma só vez, o qual pode acarretar diferença

de amplificação entre os canais WDM, tendo-se a necessidade de ajustes para equalização da amplificação.

Um *transponder* ou adaptador de comprimento de onda, presente em cada nó da rede, permite inserir ou retirar até quatro sinais locais, aceitando entradas desde baixas taxas de transmissão até 2,5 Gbps, usando modulação direta. A Tabela A.3 apresenta a grade da ITU-T utilizada nesta rede. Estes canais correspondem às freqüências 192,3 THz até 193,7 THz, com espaçamento de 200 GHz por canal.

Tabela A.3 - Grade ITU-T utilizada pela rede OMEGA

193,1 THz	193,3 THz	193,5 THz	193,7 THz
λ4 = 1552,52 nm	λ3 = 1550,92 nm	λ2 = 1549,32 nm	λ1 = 1547,72 nm

192,3 THz,	192,5 THz	192,7 THz	192,9 THz
λ8 = 1558,98 nm	λ7 = 1557,36 nm	λ6 = 1555,75 nm	λ5 = 1554,13 nm

A.2. PLANO DE CONTROLE DA REDE OMEGA

A rede OMEGA apresenta uma arquitetura *Overlay* com plano de controle distribuído baseado em uma rede Ethernet onde trafega um protocolo proprietário desenvolvido no CPqD. Cada nó possui um computador PC com três placas *FastEthernet* e duas placas para o controle dos comutadores ópticos. O estado dos comutadores é controlado por computadores locais existentes em cada nó. Estes PCs se comunicam entre si através da mesma fibra óptica que é utilizada pelo plano de transporte, porém utilizando o comprimento de onda em 1310 nm, o qual é reservado para controle. Este sinal de controle trafega no sentido contrapropagante ao de transporte de dados. Assim, é necessário inserir acopladores WDM para separar o sinal de controle (janela de 1,3 μm) do sinal DWDM (janela de 1,5 μm). A Figura A.5 mostra o nome das portas Ethernet de cada computador e como estas portas estão interligadas atendendo a topologia física mostrada na Figura A.1.

O sinal de controle é gerado em cada nó em seu computador de controle e transmitido em um esquema ponto a ponto aos computadores de controle adjacentes. Todos os PCs tem a topologia da rede inserida manualmente, não estando ainda implementado nenhum algoritmo de descoberta de arquitetura. Porém, podem-se desabilitar portas de saída

automaticamente em função de informações de tráfego ou de impossibilidade de operação por falta de sinal.

Como toda arquitetura *Overlay*, as informações de topologia e recursos não são compartilhadas entre as camadas IP e WDM. Assim, é definida uma interface usuário-rede (UNI) para acesso entre as camadas. Por médio de linha de comandos, essa interface habilita um usuário a realizar aprovisionamento de caminho óptico, obter informação de estado da topologia e do protocolo de controle LMP [ROSSI, 2002]. A UNI server, que é executada em cada PC, aceita conexões de tipo *telnet* de qualquer computador remoto conectado à rede de controle. As rotas são aprovisionadas usando RSVP simplificado e a rede possui, ainda, um esquema de proteção do tipo 1:N [SACHS, 2003].

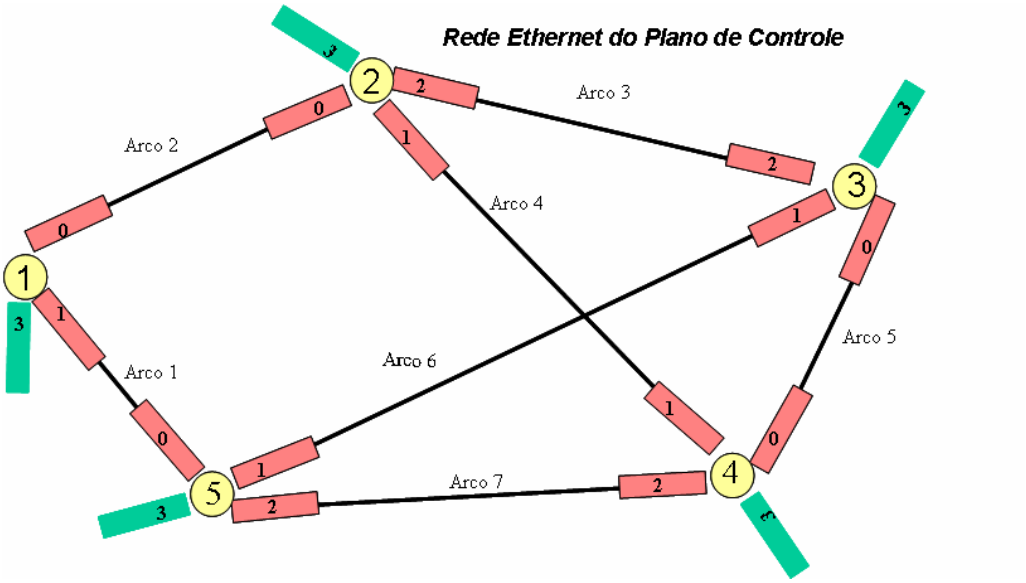


Figura A.5 - Portas Ethernet do sistema de controle.

Entre dois nós adjacentes são trocadas informações de controle. Automaticamente ou depois de alguma análise, ação ou correção, estas informações são divulgadas para nós adjacentes até que toda a rede esteja em um estado estável. Assim, foram criados vários tipos de mensagens trocadas entre roteadores.

Uma tabela dos recursos disponíveis já está armazenada em todos os nós no momento em que é solicitada uma nova conexão, pois a mesma foi inserida manualmente. Todos os computadores já possuem as rotas de menor caminho obtidas pelo algoritmo Dijkstra, executado sobre topologia disponível logo que o sistema de controle é colocado em execução. Sabendo o menor caminho disponível, bem como o comprimento de onda

associado, esta rota é atribuída conforme solicitação de um novo cliente. Além dessa possibilidade, é permitido determinar manualmente a rota e o comprimento de onda [PASTOR, 2004].

As rotas podem ser solicitadas manualmente através de uma interface UNI que aceita comandos simples. Se os computadores da rede OMEGA estiverem conectados a alguma rede de controle externa poderão ser acessados via "telnet".

A.3. RWA NA REDE OMEGA

Cada computador do plano de controle da rede OMEGA tem capacidade de calcular a rota para um dado cliente e enviar a mesma para que todos os roteadores façam a reserva desta rota, tomem conhecimento do novo cliente que ocupa uma dada banda em alguns enlaces e executem o chaveamento necessário alterando o estado das chaves envolvidas para atender este novo cliente.

O processo de criação de uma nova rota é feito a partir de qualquer um dos nós, sem que os clientes que já utilizam a rede sejam afetados. Uma tabela dos recursos já está disponível a todos os nós no momento em que é solicitada uma nova conexão. Todos os computadores já possuem as rotas de menor caminho obtidas pelo algoritmo *Dijkstra* executado sobre a tabela de rotas disponíveis logo que o programa é colocado em execução. Sabendo qual é a menor rota, bem como o comprimento de onda associado, o caminho é atribuído conforme solicitação de um novo cliente. Também é possível escolher manualmente a rota e o comprimento de onda [PARADISI, 2001].

O protocolo de aprovisionamento de caminho óptico é baseado no RSVP (*Resource Reservation Protocol*) simplificado desenvolvido especialmente para esta rede. O protocolo é responsável pela solicitação de reserva e posterior criação de uma nova conexão fim a fim sempre que houver uma nova demanda. As conexões existentes não são modificadas, e somente os recursos disponíveis são utilizados para as novas conexões. As conexões são desfeitas, também sob demanda, caracterizando uma rede orientada a conexão e capaz de garantir qualidade de serviço.

Quando uma nova demanda de tráfego é solicitada a partir de um dado nó (denominado de nó proprietário), este nó passa a ser o responsável pelo cálculo das rotas apropriadas (rota principal e rotas de proteção) e pela reserva destes recursos na rede. Para o cálculo das

rotas é utilizado um algoritmo RWA que escolhe a rota pelo caminho mais curto, usando o algoritmo de *Dijkstra*, e associa o comprimento de onda, usando o algoritmo *First-fit*, nesta rota.

Logo após o cálculo das rotas, o nó proprietário tenta fazer a reserva de recursos para a rota principal através da mensagem *LIGHTPATH_CREATE_TRY* que é enviada pelo canal de controle para o nó origem (nó onde a rota se inicia). O nó origem não corresponde, necessariamente, ao nó que está criando a rota. Esta mensagem informa a seqüência de nós intermediários e o comprimento de onda. Quando um nó da rota recebe esta mensagem, ele verifica a disponibilidade do recurso e, em caso de sucesso, reserva as portas do OXC (*Optical Cross-Connect*), configurando a chave no estado apropriado, para logo enviar a mesma mensagem para o próximo nó da rota. Durante este processo os nós intermediários atualizam seus bancos de dados com a nova reserva de recursos. Se, por outro lado, não existe disponibilidade do recurso, o nó responde com uma mensagem *LIGHTPATH_CREATE_FAIL* para o nó anterior. Este nó então libera qualquer recurso reservado para esta demanda e envia esta mensagem para o nó anterior na seqüência da rota principal. Quando o nó origem recebe a mensagem *LIGHTPATH_CREATE_FAIL*, ele conclui que a rota foi bloqueada e descarta o pedido de conexão correspondente. A Figura A.6 ilustra este procedimento.

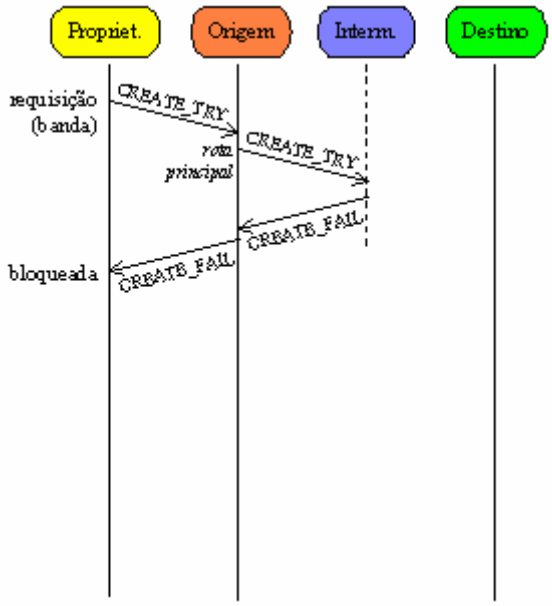


Figura A.6.: Mensagens de controle utilizadas para estabelecer um caminho óptico.

Por outro lado, quando uma mensagem *LIGHTPATH_CREATE_TRY* chega ao último nó da rota, este envia uma mensagem *LIGHTPATH_CREATE_DONE* para o nó origem indicando o sucesso na reserva da rota principal. Após a alocação da rota principal, as rotas de proteção (se houver) são alocadas usando um procedimento similar ao descrito acima. As únicas diferenças entre a alocação das rotas principal e de proteção são:

- Ao atingir o último nó da rota de proteção, em vez de enviar uma mensagem *LIGHTPATH_CREATE_DONE* para o nó de origem, é enviada uma mensagem *LIGHTPATH_CREATE_SUCCESS* para toda a rede (*broadcast*), e;

- As chaves não são configuradas no estado apropriado, mas é apenas registrado que determinadas portas do OXC estão associadas com a rota de proteção.

As chaves da rota de proteção serão configuradas no estado apropriado somente após uma falha na rede. Se o nó origem recebe a mensagem *LIGHTPATH_CREATE_SUCCESS*, ambos os caminhos, principal e de proteção, foram criados com sucesso. A Figura A.7 mostra o procedimento de criação das rotas principal e de proteção. Todo nó que recebe a mensagem *LIGHTPATH_CREATE_SUCCESS* atualiza seu banco de dados, incluindo a nova rota como recurso não disponível. Esta informação é usada pelos nós da rede ao rodarem o algoritmo de RWA para escolherem as rotas.

A.3.1. Procedimento para liberação de um caminho óptico

O caminho óptico criado tem um número de identificação (ID) composto pelo número do nó proprietário e um número seqüencial interno atribuído pelo próprio nó proprietário. Este ID é utilizado nas mensagens subseqüentes para comunicação de falhas, restauração ou liberação do recurso por solicitação do nó proprietário. Uma vez que o caminho óptico não é mais necessário, o nó proprietário envia uma mensagem *LIGHTPATH_DESTROY* para toda a rede. Ao receber esta mensagem, cada nó libera os recursos reservados para a conexão em particular e, correspondentemente, atualiza o seu banco de dados. Isto é apresentado na Figura A.7.

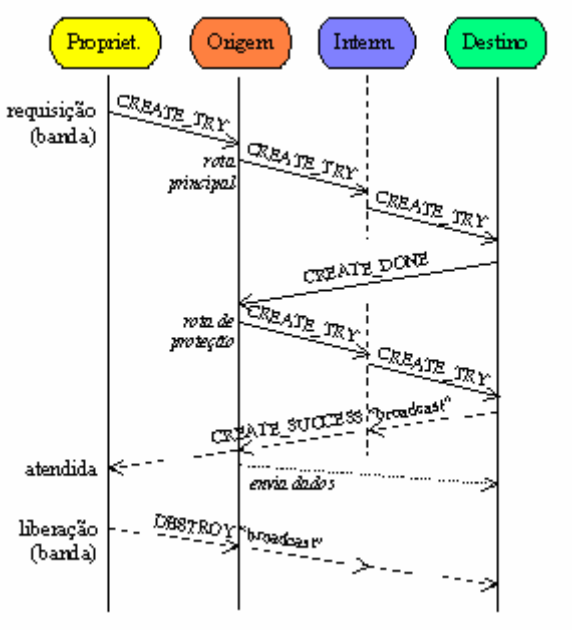


Figura A.7. Mensagens de controle para estabelecer e destruir um caminho óptico.

A.4. MECANISMO DE PROTEÇÃO DA REDE OMEGA

O mecanismo de proteção da rede OMEGA é baseado em um gerenciamento da integridade dos enlaces que denominamos LMP (*Link Management Protocol*). Este protocolo é bastante simples e se assemelha aos protótipos de mesmo nome, desenvolvidos pelo IETF, apenas na sua função principal. O LMP da rede OMEGA opera na camada de enlace e envolve um conjunto de mensagens trocadas entre nós vizinhos da rede. Uma mensagem HELLO é enviada continuamente para indicar que o enlace está operacional. Tipicamente é enviada uma mensagem HELLO a cada 5 milésimos de segundo.

A operação do LMP se baseia na troca de mensagens HELLO entre pares adjacentes de nós de rede. Quando a recepção do HELLO é interrompida por um intervalo de tempo ajustável, o sistema passa de um estado “UP” para o estado “FAIL”. Esta passagem para o estado FAIL é caracterizada pelo envio de mensagens de falha para toda a rede. A Figura A.8 apresenta o diagrama de estado do mecanismo de proteção e recuperação.

Ao receber a mensagem de falha, cada nó altera o estado das chaves ópticas para ativar a rota de reserva e repassa a mensagem de falha para os seus vizinhos. Se um nó não está envolvido com as rotas em questão, somente divulga a mensagem de falha para os seus vizinhos sem alterar o estado de suas chaves.

Foi adotada a ausência de 4 pacotes HELLO para que o sistema ecoe as mensagens de falha. A escolha do tempo entre pacotes HELLO (5 ms) e do número de pacotes (4

pacotes) que define a mudança de estado é função da velocidade das máquinas e das placas de rede utilizadas. Estes valores foram considerados adequados para equipamentos Pentium III - 866MHz com placas de rede de 100Mb/s Fast Ethernet. O kernel 2.4.2 do sistema operacional Linux foi modificado para utilizar *patch* de baixa latência. O LMP pode ser suspenso manualmente, sem que o alarme seja ecoado.

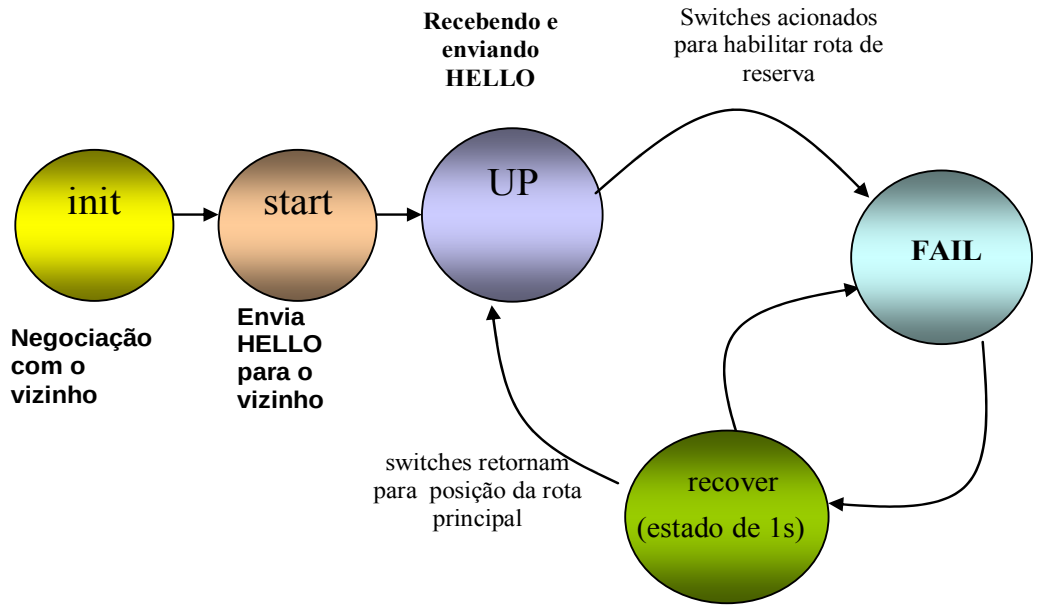


Figura A.8 - Diagrama de estado do mecanismo de sobrevivência da rede OMEGA.

B. EMULAÇÃO DO PLANO DE CONTROLE DA REDE OMEGA

Para operar como um *testbed* para trabalhos de pesquisa e implementação, foi emulado o plano de controle da rede OMEGA (Figura B.1) no laboratório *LabCom* do Departamento de Engenharia Elétrica da Universidade de Brasília. Foram usados cinco microcomputadores com configurações semelhantes para representar cada um dos nós ópticos da rede, e neles instalou-se o sistema operacional Linux Red Hat 9.0. A configuração física da rede de simulação inclui três placas Ethernet 10/100 Mbps por máquina, possibilitando uma topologia e funcionalidade similar à apresentada pela rede OMEGA.

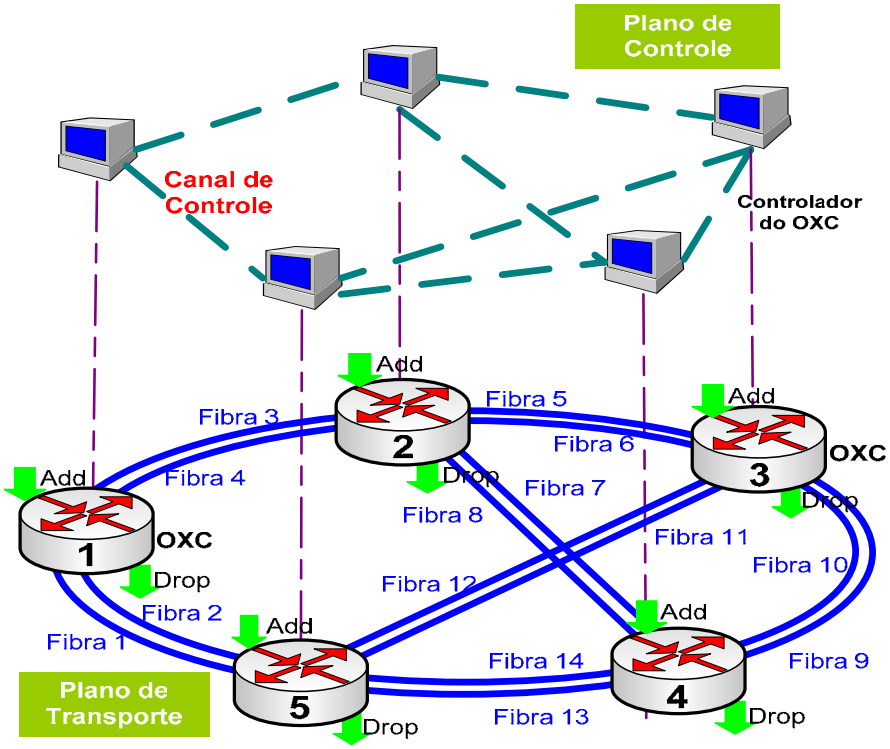


Figura B.1 – Arquitetura Física da rede OMEGA

A Figura B.2 ilustra a rede emulada com endereços IP (192.168.0.0/24). Nas máquinas foi instalado um cliente do programa ZEBRA 0.94, que é um aplicativo livre que gerencia protocolos de roteamento TCP/IP, tais como BGP-4, RIPv1, RIPv2 e OSPFv2 [PASTOR, 2004][CRISPIM, 2006].

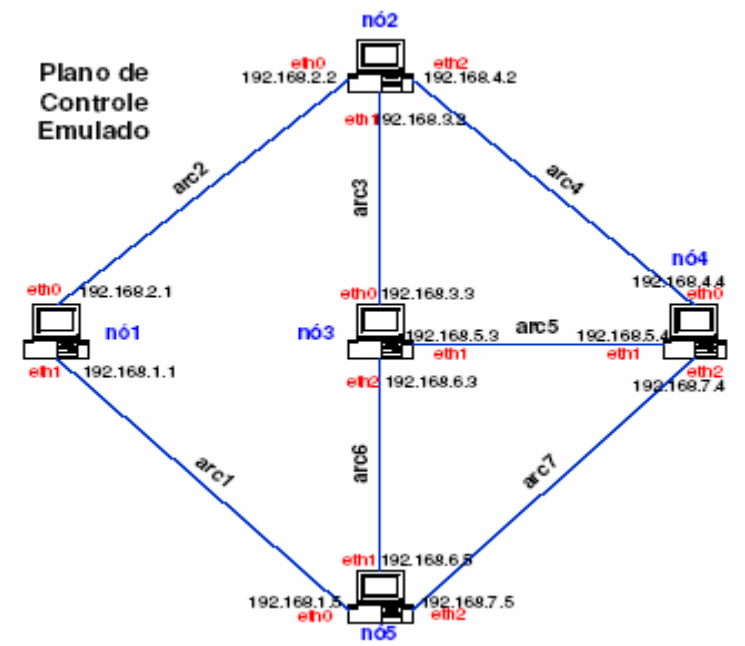


Figura B.2 – Configuração do Plano de controle emulado no Laboratório da UnB

Neste plano de Controle, mensagens *Hello* LMP (*Link Management Protocol*) são trocadas periodicamente entre os nós para validar os enlaces de controle e a integridade da sessão.

Para que os protocolos de controle pudessem operar, foi necessário o carregamento, em cada ponto da rede de controle, de um arquivo com a topologia da rede física OMEGA. Nesse arquivo, são fornecidas informações acerca da quantidade de nós, ligação das fibras e esquema de proteção adotado.

C. TESTBED SIMOMEGA

O desenvolvimento de um plano de controle centralizado a partir da arquitetura da rede OMEGA, baseado no sistema operacional Linux Fedora 4, foi nomeado de SIMOMEGA, [CRISPIM, 2006]. A solução centralizada desenvolvida nesse *testbed* é estruturada em três camadas: gerência, controle e simulação física.

C.1. ELEMENTOS DE REDE FÍSICOS

Dada a dificuldade da estruturação de uma rede com um maior número de nós, nesta rede foi adotado o princípio da simulação dos elementos físicos da rede existente no CPqD. Desta forma, a rede simulada tem cinco nós que representam os elementos ópticos da rede OMEGA.

A Figura C.1 apresenta o layout da simulação dos elementos físicos de um site através de três módulos de software, um para cada elemento.

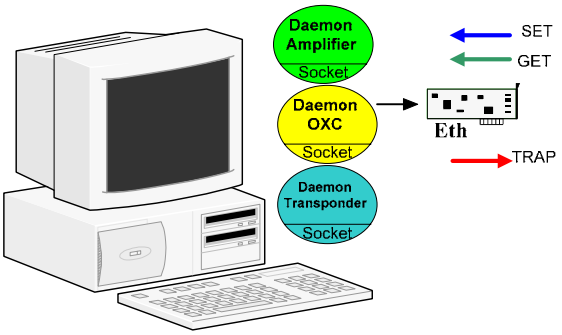


Figura C.1 - Simulação dos elementos físicos

C.2. ELEMENTOS LÓGICOS

Todos os programas que compõem o plano de controle deste *Testbed* foram estudados, validados e testados. Neste contexto, também se inserem os programas desenvolvidos para realizarem o teste dinâmico das funcionalidades relativas ao controle da rede óptica. A solução foi centralizada numa única máquina a qual recebe os dados e os processa de acordo com os protocolos envolvidos.

Para a gerência é usado um sistema no modelo web executado num único servidor http para uma melhor interação gráfica do usuário com o controle da rede. Além disto, o

referido sistema foi desenvolvido com o conceito de auditoria funcional, que tem como objetivo o registro, num banco de dados relacional, de todas as interações do usuário com o sistema de controle. A Figura C.2 apresenta uma visão completa da arquitetura implementada no SIMOMEGA.

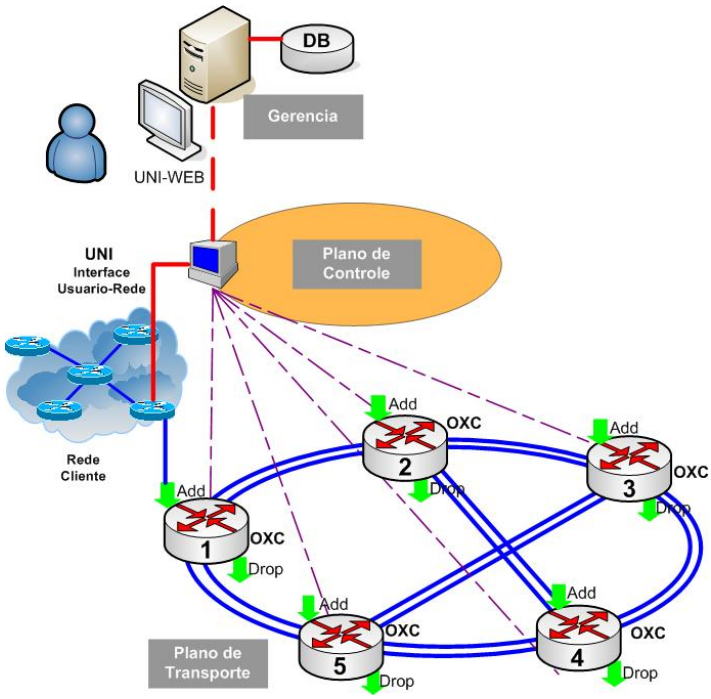


Figura C.2 - Arquitetura da Rede SIMOMEGA

C.3. ALGUNS TESTES NO SIMOMEGA

A Tabela C.1 apresenta os resultados entregados pelo sistema do SIMOMEGA para 30 requisições de caminhos de serviço, os tempos consumidos na criação de cada uma das rotas e o número de nós envolvidos em cada Lightpath. [CRISPIM, 2006, pag. 128]

Tabela **C.1** - Resultados entregados pelo SIMOMEGA para 30 requisições.

NumReq	Tempo - ms	Num. Nós	Lightpath
1	235	2	5->4 - SERVICE@1* 5(3/2)+4(2/3)
2	319	2	3->4 - SERVICE@2* 3(3/1)+4(1/3)
3	304	3	3->4 - SERVICE@3* 3(3/0)+2(1/2)+4(0/3)
4	304	4	3->2 - SERVICE@1* 3(3/2)+5(1/0)+1(1/0)+2(0/3)
5	240	2	5->3 - SERVICE@2* 5(3/1)+3(2/3)
6	257	2	2->1 - SERVICE@2* 2(3/0)+1(0/3)
7	364	3	2->5 - SERVICE@1* 2(3/2)+4(0/2)+5(2/3)
8	247	2	4->3 - SERVICE@1* 4(3/1)+3(1/3)
9	304	3	1->3 - SERVICE@3* 1(3/1)+5(0/1)+3(2/3)
10	295	3	4->3 - SERVICE@4* 4(3/0)+2(2/1)+3(0/3)
11	351	3	3->5 - SERVICE@4* 3(3/1)+4(1/2)+5(2/3)
12	370	3	5->2 - SERVICE@3* 5(3/2)+4(2/0)+2(2/3)
13	275	2	1->5 - SERVICE@2* 1(3/1)+5(0/3)
14	286	3	3->2 - SERVICE@5* 3(3/1)+4(1/0)+2(2/3)
15	307	3	4->5 - SERVICE@3* 4(3/1)+3(1/2)+5(1/3)
16	297	3	5->3 - SERVICE@5* 5(3/2)+4(2/1)+3(1/3)
17	426	4	3->5 - SERVICE@6* 3(3/0)+2(1/0)+1(0/1)+5(0/3)
18	435	4	1->5 - SERVICE@5* 1(3/0)+2(0/2)+4(0/2)+5(2/3)
19	344	3	4->3 - SERVICE@6* 4(3/2)+5(2/1)+3(2/3)
20	448	4	5->4 - SERVICE@4* 5(3/0)+1(1/0)+2(0/2)+4(0/3)
21	269	4	5->4 - SERVICE@6* 5(3/0)+1(1/0)+2(0/2)+4(0/3)
22	260	4	1->5 - SERVICE@7* 1(3/0)+2(0/1)+3(0/2)+5(1/3)
23	194	3	1->4 - SERVICE@8* 1(3/1)+5(0/2)+4(2/3)
26	434	3	5->4 - SERVICE@7* 5(3/1)+3(2/1)+4(1/3)
28	306	4	3->1 - SERVICE@8* 3(3/1)+4(1/2)+5(2/0)+1(1/3)
30	476	2	4->2 - SERVICE@2* 4(3/0)+2(2/3)

D. REDE NSFNet

Acrónimo inglés de *National Science Foundation's Network*, a NSFNET deu início a uma série de redes dedicadas à comunicação da pesquisa e da educação. Foi criada em 1986 pelo governo dos Estados Unidos (através da *National Science Foundation*) e esta baseada no protocolo TCP/IP, compatível com a ARPANET. Os enlaces originais de 56 kbps foram atualizados para 1.5 Mbps em 1988 e posteriormente a 45 Mbps em 1991.

De 217 redes conectadas no julho de 1988 para mais de 50.000 no Abril de 1995, quando o serviço de *backbone* foi retirado, a NSFNET cresceu exponencialmente estimulado pela expansão da Internet. Ao total, 93 paises foram conectados ao *backbone* de *NSFNet*. A Figura D.1 apresenta as interconexões e a topologia desta rede.

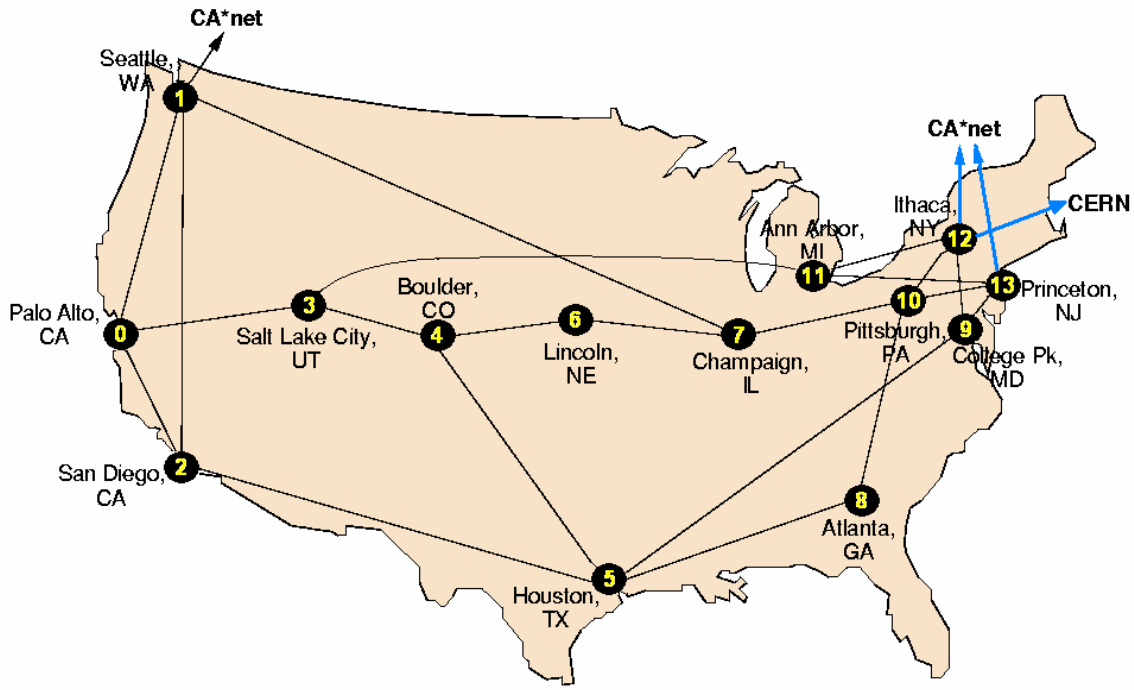


Figura D.1 - Interconexões e topologia da rede *NSFNet.*

REFERÊNCIAS BIBLIOGRÁFICAS

[ABED, 1996] Abed, M.A.A.; Ghanta, S.- "Optimizing logical topology of lightwave network architecture (LNA) using genetic algorithms" - Proc. 1996 - IEEE 15th Annual Intl. Phoenix Conf. on Computers and Communications – Scottsdale-Arizona – USA, March, 1996.

[ABILENE, 2005] http://abilene.internet2.edu/about/faq.html

[ALI, 2000] M. Ali, B. Ramamurthy, and J.S. Deogun. "Routing and wavelength assignment with power considerations in optical networks". Computer Networks, 2000.

[ALANYALI, 1999] M. Alanyali, and E. Ayanoglu, "Provisioning algorithms for WDM optical networks" IEEE/ACM Trans. Net., vol. 7, no. 5, Oct. 1999, pp. 767–778.

[ALFERNESS, 1999] Alferness R. C.; Bonenfant P. A.; Newton C. J.; Sparks K.A.; Varma E. L. A., "Pratical Vision for Optical Transport Networking". Bell Labs - Technical Journal, v.4, n.1, p.3-18, Janeiro – Março 1999.

[ANAND, 2002] V. Anand, S. Chauhan, and C. Qiao, "Sub-path Protection: A New Framework for Optical Layer Survivability and Its Quantitative Evaluation," Dept. of Comp. Sci. and Eng., SUNY Buffalo, Tech. rep. 2002-01, Jan. 2002.

[ANSI-105, 1995] ANSI T1.105-1995, "Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates and Formats." - 1995

[ASHWOOD-SMITH, 2002] P. Ashwood-Smith et al, "Generalized MPLS Signaling CR-LDP Extensions", IETF draft-ietfmpls-generalized-cr-ldp-, Abril 2002.

[AWDUCHE, 2001] Awduche, D. and Rekhte, Y.. "Multiprotocol Lambda Switching: Combining MPLS Traffic Engineering Control with Optical Crossconnects". IEEE Communications Magazine. - 2001.

[BACK, 2000] T. Back, D.B. Fogel, and Z. Michalewicz, editors. "Evolutionary Computation 1 – Basic Algorithms and Operators". Institute of Physics Publishing, 2000.

[BACK2, 2000] T. Back, D.B. Fogel, and Z. Michalewicz, editors. Evolutionary Computation 2 – Advanced Algorithms and Operators. Institute of Physics Publishing, 2000.

[BAKER, 1987] J.E. Baker. Reducing bias and inefficiency in the selection algorithm. In Genetic Algorithms and their Applications: Proceedings of the Second International Conference on Genetic Algorithms, pages 14–21. Erlbaum, 1987.

[BANERJEE, 1996] D. Banerjee and B. Mukherjee, "Practical approaches for routing and wavelength assignment in large all-optical wavelength routed networks," - IEEE J. Select. Areas Commun., vol. 14, 1996.

[BANERJEE1, 2001] Banerjee, A.; Drake, J.; Lang, J.P.; Turner, B.; Kompella, K.; Rekhter, Y.; Generalized multiprotocol label switching: an overview of routing and management enhancements, IEEE Communications Magazine, Volume: 39 Issue: 1, Jan 2001, pp. 144-150.

[BANERJEE2, 2001].Banerjee, A.; Drake, L.; Lang, L.; Turner, B.; Awduche, D.; Berger, L.; Kompella, K.; Rekhter, Y., Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques, IEEE Communications Magazine, Volume: 39 Issue: 7, Jul 2001, pp. 144-151

[BARRY, 1996] R. Barry and P. Humblet, “Models of blocking probability in all-optical networks with and without wavelength changers”, IEEE JSAC, vol. 14, no 5, pp. 868-880, Jun. 1996.

[BARONI, 1998] S. Baroni, P. Bayvel, and R. J. Gibbens, “On the number of wavelengths in arbitrarily-connected wavelength-routed optical networks,” - Optical Society of America, TOPS, vol. 20, pp. 195–204, 1998.

[BICUDO, 2005] Marco D. D. Bicudo, Otto Carlos M. B. Duarte “Um Mecanismo de Proteção em Redes WDM em Malha” - SBRC 2005 - Simpósio Brasileiro de Redes de Computadores - RJ – Brasil, 2005

[BIGGS, 1974] BIGGS, N. “Algebraic Graph Theory”. Cambridge University Press, 1974.

[BISBAL, 2004] D. Bisbal et al., “Dynamic Routing and Wavelength Assignment in Optical Networks by Means of Genetic Algorithms,” Photonic Networks Communications, vol. 7, no.1, pp. 43-58, 2004

[BLACK, 2002] Uyless Black, Optical Networks – Third Generation Transport Systems Prentice Hall, PTR, 2002.

[BODUCH, 2006] Boduch, M.; Fisher, K.; Leonov, O.; Grzyb, J.; Schmidt, T.; Saunders, R.; Ceuppens, L.; “Transmission of 40 Gbps signals through metropolitan networks engineered for 10 Gbps signals”- Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference 5-10 March 2006 Page(s):3 pp.

[BOLLOBAS, 1998] BOLLOBÁS, B. “Modern Graph Theory”, Springer-Verlag, 1998.

[BORELLA, 1997] Michael S. Borella, Jason P. Jue, Dhritiman Banerjee, Byrav, Ramamurthy, Biswanath Mukherjee, “Optical Components for WDM Lightwave Networks” - Proceedings Of The IEEE, Vol. 85, No. 8, August 1997

[CARISMA, 2006] http://carisma.ccaba.upc.es

[CAVENDISH, 2000] Dirceu Cavendish, “Evolution of optical transport technologies: From SONET/SDH to WDM” - IEEE Communications Magazine, no. 6, June 2000 pp. 164-172

[CHALASANI, 2003] , Chalasani S.; Rajaravivarma, V.; “Survivability in optical networks” System Theory, 2003. Proceedings of the 35th Southeastern Symposium on 16-18 March 2003 Page(s):6 - 10

[CHLAMTAC, 1990] I. Chlamtac, A. Ganz and G. Karmi, “Lightnet: lightpath based solutions for wide bandwidth WANs” in INFOCOM’90, Vol. 3, Page(s): 1014{1021, 1990.

[CHOI, 2000] J. S. Choi, N. Golmie, F. Lapeyrere, F. Mouveaux, and D. Su, “A functional classification of routing and wavelength assignment schemes in DWDM networks: Static case,” in Proc. VII Int. Conf. on Optical Communication and Networks, Jan. 2000.

[CINCOTTI, 2006] Cincotti, G.; Moreolo, M.S.; Manzacca, G.; Wang, X.; Wada, N.; Kitayama, K.-I.; “Multi-dimensional optical code processing in MPLS photonic routers” Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference- 5-10 March 2006

[COMELLAS, 2003] Comellas, J.; Martinez, R.; Prat, J.; Sales, V.; Junyent, G.; “Integrated IP/WDM routing in GMPLS-based optical networks”, IEEE Network, Volume: 17 Issue: 2, Mar/Apr 2003, pp. 22-27

[CORNE, D, 1999] Corne, D., Sinclair, M.C. & Smith, G.D., “Evolutionary Telecommunications: Past, Present and Future” - Proc. GECCO’99 Workshop on Evolutionary Telecommunications: Past, Present and Future, Orlando, Florida, USA, July 1999, p.208

[CORREIA, 2002] Correia, Davi; "Algoritmos Genéticos e Elementos Finitos na Síntese de Dispositivos Fotônicos"- Dissertação de Mestrado - DMO/FEEC/UNICAMP – 2002.

[CRISPIM, 2006] Crispim, H. A. F. (2006). "Implementação de um sistema de controle centralizado para uma rede óptica transparente". Tese de Doutorado em Engenharia Elétrica, Publicação PPGENE.TD-011/06, Dep.de Engenharia Elétrica, Universidade de Brasília, Brasília: DF, 196p.

[DAVIK , 2004] Fredrik Davik, Mete Yilmaz, Stein Gjessing, Necdet Uzun, "IEEE 802.17 Resilient Packet Ring Tutorial" - IEEE Communications Magazine • March 2004

[DEB, 2001] K. Deb, "Multi-Objective Optimization using Evolutionary Algorithms" - John Wiley & Sons, Inc., New York, 2001.

[DE JONG , 1975] K.A. De Jong. "An analysis of the behavior of a class of genetic adaptive systems". PhD thesis, University of Michigan, 1975.

[DIJKSTRA, 1959] Dijkstra, E.W, "A note on Two Problems in Conexion with Graphs", Numerische Math - 1959)

[DONGYUN , 2000] Dongyun Zhou; Subramaniam, S.; "Survivability in optical networks" Network, IEEE Volume 14, Issue 6, Nov.-Dec. 2000 Page(s):16 - 23

[DOSHI, 1999] B. T. Doshi, et. al., "Optical Network Design and Restoration", Bell Labs Tech. Journal, Vol. 4, No. 1, Jan-Mar, 1999, pp.58-84

[DRAKE, 2005] J. Drake "Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)" – IETF-July 2005

[DROZDEK, 2002] Drozdek, Adam; "Estrutura de dados e Algoritmos em C++" – Ed. Pioneira Thomson Learning – São Paulo, 2002

[EHRHARDT, 2006] Ehrhardt, A, "Next Generation Optical Networks: an Operator's Point of View". International Conference on Transparent Optical Networks, ICTON 2006 Volume: 1Date: June 2006 Page(s): 93-97

[ELANTI, 2005] M. Elanti, S. Gorshe, L. Raman, and W. Grover, "Next Generation Transport Networks – Data,Management, and Control Plane Technologies", Springer, 2005.

[EL-SAYED, 2002] Mohamed El-Sayed, Jeffrey Jaffe, "A View of Telecommunications Network Evolution" IEEE Communications Magazine • December 2002.

[ELSENPETER, 2002]. Elsenpeter, Robert and Velte, Toby "Optical Networking: A beginner's guide".McGraw-Hill/Osborne - 2002.

[ESQUIVIAS, 2006] Ignacio Esquivias, et.al. "Manual LCO –Conceptos Fundamentales de Comunicaciones Ópticas" – Departamento de Tecnología Fotónica - Universidad Politecnica de Madrid (UPM) – Setembro 2006.

[FABREGAS, 2006] Josep M. Fabrega, Carlos Bock and Josep Prat, "Ultra-Dense WDM PON based on Homodyne Detection and Local Oscillator Reuse for Upstream Transmission" - 32nd European Conference on Optical Communication 2006 Proceedings –Cannes 2006.

[FOGEL, 1998] Fogel, D.B. "Evolutionary Computation. The Fossil Record" -. IEEE Press 1998

[FONSECA, 1998] P. F. Fonseca. "Pan-european multi-wavelength transport network network design, architecture, survivability and sdh networking". In DRCN'98, page P3, 1998.

[GEN 2000] M. Gen and R. Cheng. “Genetic Algorithms and Engineering Optimization”. Wiley, New York, 2000.

[GERSTEL,2003] Gerstel, O.; Ramaswami, R.; “Optical layer survivability: a post-bubble perspective” Communications Magazine, IEEE Volume 41, Issue 9, Sept. 2003 Page(s):51 - 53

[GILARDI, 2002] Guido Gilardi, Achille Pattavina, Giacomo Verticale “A Proposal for an Ethernet-over-WDM Wide Area Multiplexing Architecture”, IEEE explore, 2002

[GLOVER, 1990] Glover, F. “Tabu search - part I e II” ORSA Journal on Computing 1989 e 1990

[GNAUCK, 2006] Gnauck A.H., Winzer P.J., et. al.,“12.3 Tb/s C-Band DQPSK Transmission at 3.2 b/s/Hz Spectral Efficincy” - 32nd European Conference on Optical Communication 2006 Proceedings – Post deadline papers – Cannes 2006.

[GODSIL, 2001] GODSIL, C. R.,Gordon. “Algebraic Graph Theory”. Springer, 2001.

[GOLDBARG, 2000] Goldbarg, Marco Cesar, “Otimização Combinatória e Programação Linear: Modelos e Algoritmos” – Ed. Elsevier – 7ª Reimpressão – Rio de Janeiro - 2000

[GOLDBERG, 1989] Goldberg D.E. “Genetic Algorithms in Search, Optimization and Machine Learning” -. Addison-Wesley, 1989

[GONG , 2003] Yongtao Gong; Peiyuan Lee; Wanyi Gu; “A novel adaptive RWA algorithm in wavelength-routed network” - Global Telecommunications Conference, 2003. GLOBECOM ‘03. IEEE - Volume 5, 2003 Page(s):2580 - 2584 vol.5

[GORSHE, 2005] Steve Gorshe “A Tutorial on SONET/SDH Automatic Protection Switching (APS) Technology White Paper - - PMC-Sierra, Inc - February, 2005

[GORSHE_1, 2005] Steve Gorshe “Resilient Packet Ring (RPR) Technology” -White Paper - PMC-Sierra, Inc - May 2005

[GORSHE_2, 2005] Steve Gorshe “Generic Framing Procedure (GFP)” - White Paper - PMC-Sierra, Inc - April 2005

[GROSSMAN, 1999] D. Grossman, “Multiprotocol Encapsulation over AAL5”, RFC 2684, september 1999, ftp://ftp.upc.es/pub/doc/rfc/26xx/2684.

[HARTMANIS, 1965] Juris Hartmanis and Richard E. Stearns. “On the computational complexity of algorithms”. Trans. American Mathematical Society, 117:285--306, Maio 1965.

[HELD, 2005] HELD, G. Ethernet Networks: ”Design, Implementation, Organization and Management”. Wiley: Fouth Edition., 2005.

[HERNANDEZ, 2002] Enrique Hernandez-Valencia, Michael Scholten and Zhenyu Zhu, “The Generic Framing Procedure (GFP): An Overview”- - IEEE Communications Magazine • May 2002

[HO, 2004] Pin-Han Ho; Mouftah, H.T.; “Shared protection in mesh WDM networks” Communications Magazine, IEEE Volume 42, Issue 1, Jan 2004 Page(s):70 - 76

[HO, 2004] P. –H. Ho and H. T. Mouftah, “Reconfiguration of Spare Capacity for MPLS-based Recovery in the Internet Backbone Networks”, IEEE/ACM Transaction on Networking, Vol. 12, No. 1, Feb. 2004.

[IEEE 802.17-2004]. IEEE Standard 802.17-2004, Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specification - 2004

[IGLESIAS, 2004] J. L. Iglesias "Carrier Optical Broadband Services and Networks Evolution", http://www.rediris.es/rediris/boletin/66-67/ponencia5.pdf, 2004

[ITU-T G.707, 2003] ITU-T Recommendation G.707 "Network node interface for the Synchronous Digital Hierarchy (SDH)" - 2003.

[ITU-T G.7043/Y.1343, 2004] ITU-T Recommendation G.7043/Y.1343 "Virtual concatenation of Plesiochronous Digital Hierarchy (PDH) signals" - 2004.

[ITU-T G.7042, 2004] ITU-T Recommendation G.7042 "Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated signals" - 2004.

[ITU-T- G.7041, 2001] ITU-T Recommendation G.7041/Y.1303 "Generic Framing Procedure"-2001.

[ITU-T G.709, 2001] ITU-T Recommendation G.709 – "Interfaces for the optical transport network (OTN)" - 2001

[ITU-T-G.872, 2001] ITU-T Recommendation G.872, "Architecture of Optical Transport Networks (OTN)", Noviembre 2001.

[ITU-T-G.841, 1996] ITU-T Rec. G.841, "Types and Characteristics of SDH Network Protection Architectures," - 1996.

[ITU-T G.841, 1998] ITU-T Recommendation G.841, "Types and Characteristics of SDH Network Protection Architectures", October 1998.

[JAEGER, 2006] Jaeger, M."Network Architectures for Future Optical Networks" International Conference on Transparent Optical Networks, ICTON 2006 Volume: 1Date: June 2006 - Page(s): 147-150

[JAJSZCZYK, 2005] Andrzej Jajszczyk, "Automatically Switched Optical Networks: Benefits and Requirements" - IEEE Optical Communications • February 2005

[JOHANSSON, 1998] S. Johansson et al., "A Cost-Effective Approach to Introduce an Optical WDM Network in the Metropolitan Environment," IEEE JSAC, vol. 16, no. 7, Sept. 1998, pp. 1109–22

[JUNYENT, 2004] G. Junyent. "Experimental demonstration of two new GMPLS lightpath setup protocols for soft-permanent connections over Metro-DWDM DPRing implemented on EMPIRICO ASON testbed". A: Proceedings of the IEEE Global Telecommunications Conference 2004, Vol. 3. ieee, 2004, p. 1798-1802.

[JUNYENT, 2006] Apostila da Materia de Doutorado "Optical Networks" – Departament de Teoria del Senyal i Comunicacions – Doctorat – Universitat Politecnica de Catalunya – UPC (2006) – junyent@tsc.upc.edu.

[KARCIUS, 2004] Karcius Day Rosário Assis, "Suporte ao tráfego de internet pela rede óptica "planejamento e projeto" Tese de Doutorado.-UNICAMP-Campinas, SP, 2004. (Mitchell, 1993) Mitchell, M. "An Introduction to Genetic Algorithms" - MIT Press 1993

[KDEVELOP, 2006] http://www.kdevelop.org.

[KIRKPATRICK, 1983] Kirkpatrick, S; Gelatt, C.D. Jr.; Vecchi, M. P. "Optimization by simulated annealing". Science v220 May 1983 pp 671-680

[KODIALAM, 2001] Kodialam, M. e Lakshman, T.."Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks". Proc. IEEE INFOCOM.- 2001

[KOMPELLA, 2005] K. Kompella, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)" RFC 4203 - IETF - October 2005

[KOMPELLA2, 2005] K. Kompella, "Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)" RFC 4205 - IETF - October 2005

[KRISHNASWAMY, 2001] Krishnaswamy, R.M.; Sivarajan, K.N.; "Algorithms for routing and wavelength assignment based on solutions of LP-relaxations" - Communications Letters, IEEE - Volume 5, Issue 10, Oct. 2001 Page(s):435 – 437

[LANG, 2005] J. Lang, "Link Management Protocol (LMP)" RFC – IETF - October 2005

[LANGNER, 1998] Paul Langner, "SDL Data Link Specification" Lucent Technologies - September 28, 1998

[LARKIN, 2002] Nic Larkin, "ASON and GMPLS - The Battle Of The Optical Control Plane- An overview of the ongoing work of the IETF and ITU to standardize optical control plane protocols" Paper Data Connection http://www.dataconnection.com/ - August 2002

[LE , 2005] Vinh Trong Le, et.al. "A Hybrid Algorithm for Dynamic Lightpath Protection in Survivable WDM Optical Networks" Proceedings of the 8th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'05) – 2005.

[LEE, 1999] S. W. Lee and C. S. Wu, "K-Best paths algorithm for Highly Reliable Communication Networks", IEICE Trans. Communications Vol.E82-B, No.4, pp586-590, 1999

[LEE, 2004] Lee, D.; Libman, L.; Orda, A.;"Path protection and blocking probability minimization in optical networks" INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies Volume 1, 7-11 March 2004 Page(s):

[LEI, 2003] Lei Lei, Jijun Zhao, Yuefeng Ji; "Analysis and Comparison of Recovery Schemas for GMPLS Controlled Intelligent Optical Networks"—Proceedings of ICCT 2003.

[LI, 2005] Ming-Jun Li; Soulliere, M.J.; Tebben, D.J.; Nederlof, L.; Vaughn, M.D.; Wagner, R.E.; "Transparent optical protection ring architectures and applications" Lightwave Technology, Journal of Volume 23, Issue 10, Oct. 2005 Page(s):3388 – 3403

[LIU, 2005] Yu Liu. David Tipper. Peerapon Siripongwutikorn "Approximating optimal spare capacity allocation by successive survivable routing - IEEE/ACM Transactions on Networking (TON)" Volume 13 , Issue 1 (February 2005) Pages: 198 - 211

[MANCHESTER1, 1999] Manchester, J.; Bonenfant, P.; Newton, C.; "The evolution of transport network survivability" Communications Magazine, IEEE - Volume 37, Issue 8, Aug. 1999 Page(s):44 – 51

[MANCHESTER2, 2004] Manchester, J.; Saha, D.; Tripathi, S.K.; "Guest editorial - Proteção, restoration, and disaster recovery" Network, IEEE - Volume 18, Issue 2, Mar-Apr 2004 Page(s):3 - 4

[MANN, 1995] Mann, J.W.; Rayward-Smith, V.J.; Smith, G.D.- "Telecommunication traffic routing: A case study in the use of genetic algorithms" – Proc. ADT 95 – London, April, 1995.

[MANNIE, 2002] Mannie, E; et.al. Recovery (Protection and Restoration) terminology for GMPLS. IETF draft, draft-ietf-ccamp-gmpls-recovery-terminology-01, Nov. 2002, Work in progress.

[MANNIE2, 2002] Mannie, E; et.al. Generalized Multiprotocol Label Switching (GMPLS) architecture. IETF draft, draft-ietf-ccamp-gmpls-architecture-02, March. 2002, Work in progress.

[MANNIE, 2004] E. Mannie et al, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture" Request for Comments 3945 Standards Track – IETF - October 2004.

[METZ, 2000] Metz, Cris "IP over Optical: From Packets to Photons" – IEEE Internet Computing, November-December 2000

[MICHALEWICZ, 1996] Michalewicz, Z; "Genetic Algorithms + Data Structures = Evolution Programs" - Springer, 3rd edition, 1996.

[MICHALEWICZ, 2000] Z. Michalewicz and D.B. Fogel. "How To Solve It: Modern Heuristics". Springer, 2000.

[MOHAN, 1999] G. Mohan, C.S. Ram Murthy, "Routing and Wavelength Assigment for establishing dependable connection in WDM networks". Technical Digest IEEE International Symposium on Fault-Tolerant Computing – June 1999.

[MOUFTAH, 2002] B. Zhou and H. T. Mouftah, "Adaptive Alternate Routing for Multi-fiber WDM Networks Using Approximate Congestion Information", International Conference on Communication (ICC2002), New York City, USA, April 28-May 2, 2002

[MUKHERJEE, 1997] B. Mukherjee, "Optical Communication Networks", McGraw-Hill, New York NY, 1997.

[MURTHY, 2002] Murthy, C Siva Ram; Moham Gurusamy, "WDM Optical Networks: Concepts, design, and algorithms" – Prentice Hall PTR - 2002

[NGO, 2004] S. H. Ngo, X. Jiang, S. Horiguchi and M. Guo, "Ant-Based Dynamic Routing and Wavelength Assignment in WDM Networks", LNCS 3207, pp. 829-838, 2004.

[NORTEL, 2001] Nortel Networks, "MPLS and ASTN: Extending multiprotocol label switching for automatically switched transport networking". White Paper. (2001).

[OIF, 2000] OIF2000.125.1 "User Network Interface (UNI) 1.0 Proposal" Optical Internetworking Forum, July 2000

[OPNEAR, 2007] http://opnear.utdallas.edu/projects/omega.html - Dr. Andrea Fumagalli - The University of Texas at Dallas, Dept. of Electrical Engineering, MS - EC 33, TX 75080-0688.

[OU, 2002] Ou, C., Zhang, H. e Bmukherjee. "Sub-Path Protection for Scalability and Fast Recovery in Optical WDM Mesh Network". Proc. OFC.- 2002

[PAPADIMITRIOU, 2001] D. Papadimitriou et al, "Inference of Shared Risk Link Groups," Internet Draft, Work in progress, draft-manyinference-srlg-01.txt, July 2001

[PAPADIMITRIOU, 2003] Papadimitriou, D.. "Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control".Editor - draft-ietf-ccamp-gmpls-sonet-sdh-08.txt – August - 2003.

[PAPADIMITRIOU, 2005] D. Papadimitriou, et.al, "Requirements for Generalized MPLS (GMPLS) Signaling Usage and Extensions for Automatically Switched Optical Network (ASON)" RFC 4139-IETF -July 2005

[PARADISI, 2001] A. Paradisi, J.B. Rosolem and S.M. Rossi, "Status of the Wavelength routing optical network test-bed", 2sd Technical report CPqD/Ericsson, August 2001.

[PARETA, 2002] S. Sánchez, X. Masip-Bruin, J. Solé-Pareta, J.Domingo-Pascual, "PONNI: A routing Information Exchange Protocol for ASON", Eurescom Summit, Heidelberg (Alemania), 21-24 Octubre 2002.

[PARETA, 2006]. Josep Solé-Pareta Catedra da Materia de Doutorado "Optical Networks" – Departament de Teoria del Senyal i Comunicacions – Doctorat – Universitat Politecnica de Catalunya – UPC (2006) – pareta@ac.upc.edu

[PASTOR1, 2004] Eduardo T.L. Pastor, HAF Crispim, H. Abdalla Jr, A.J.M. Soares, et. al "Otimização de Alocação de Rotas e Comprimentos de Onda em redes WDM", XXI Simpósio Brasileiro de Telecomunicações, SBrT04, Setembro de 2004, Belém – PA.

[PASTOR2, 2005] Eduardo T. López Pastor, Martins, A.J., Amvame-Nze, G., H. Abdalla Jr, et.al. "Redes Convergentes: Tecnologias e Protocolos". Projeto Anatel-UIT/UnB-Finatec. DF, Abril 2005.

[PASTOR3, 2005] Eduardo T.L. Pastor, HAF Crispim, H. Abdalla Jr, A.J.M. Soares, "Interface de Usuário para rede óptica IP/WDM em ambiente Web", XXII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES - SBrT'05, 04-08 DE SETEMBRO DE 2005, CAMPINAS, SP

[PAVANI, 2003] Pavani, Gustavo; "Roteamento e Alocação de Comprimentos de Onda com Restrições de Potência usando Algoritmos Genéticos" - Dissertação de mestrado DECOM/FEEC/UNICAMP - Orientador: Hélio Waldman. Data da defesa: 16/09/2003.

[PAXSON, 1995] V. Paxson and S. Floyd, "Wide-area Traffic: The Failure of Poisson Modeling," IEEE/ACM Transactions on Networking, pp.226-244, June 1995.

[PICKAVET, 2006] Pickavet, M.; Demeester, P.; Colle, D.; Staessens, D.; Puype, B.; Depre, L.; Lievens, I.; "Recovery in multilayer optical networks" Lightwave Technology, Journal of Volume 24, Issue 1, Jan. 2006 Page(s):122 - 134

[PRAT, 2003] Prat, J.; Comellas, J.; Martinez, R.; Sales, V.; Junyent, G.; Integrated IP/WDM routing in GMPLS-based optical networks, IEEE Network, Volume: 17 Issue: 2, Mar/Apr 2003, pp. 22-27

[PRATHOMBUTR, 2003] P. Prathombutr, J. Stach and E. K. Park – "An Algorithm for Traffic Grooming in WDM Optical Mesh Networks with Multiple Objectives" 0-7803-7945-4/03 © 2003 IEEE

[PROESTAKI, 1999] Proestaki, A. Sinclair, M.C. "Impact of topology on wavelength and switch_port requirements in all-optical hierarchical multi-ring networks" - Proc. IEEE Global Telecom Conf. GLOBECOM-1999 - Rio de Janeiro – Brazil. December, 1999.

[RAJAGOPALAN, 2000] Rajagopalan, B.; Pendarakis, D.; Saha, D.; Ramamoorthy, R.S.; Bala, K.;"IP over optical networks: architectural aspects" Communications Magazine, IEEEVolume 38, Issue 9, Sept. 2000 Page(s):94 - 102.

[RAMAMURTHY, 1998] Byrav Ramamurthy and Biswanath Mukherjee, "Wavelength Conversion in WDM Networking", IEEE Journal on SAC (1998) vol 16, No 7, pp 1061-1073.

[RAMAMURTHY y MUKHERJEE, 1999] Ramamurthy, S. e Mukherjee, B. (1999). "Survivable WDM Mesh Networks: Part I, Protection". ACM Sigcomm - 1999.

[RAMAMURTHY, 2003] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM Mesh Networks," IEEE/OSA J. Lightwave Tech., vol. 21, Apr. 2003, pp. 870–83.

[RAMASWAMI, 1995] Ramaswami, R.; Sivarajan, K.N; "Routing and wavelength assignment in all-optical networks" - Networking, IEEE/ACM Trans. on – Vol.3, Issue 5, Oct. 1995 Page(s):489 – 500

[RAMASWAMI,1997] Rajiv Ramaswami, Galen Sasaki, "Multiwavelength Optical Networks with limited wavelength conversion" - Proceedings of the IEEE INFOCOM, 1997.

[RAMASWAMI, 1998]. Ramaswami, R. and Sivarajan, K.N. “Optical Networks, A Pratical Perspective”. Academic Press, San Diego, CA. - 1998.

[RAMASWAMI, 2002] Ramaswami, R. and Sivarajan, K.N. “Optical Networks, A Pratical Perspective”. 2da. Ed. Academic Press, San Diego, CA. - 2002.

[RedIRIS, 2005] http://www.rediris.es/rediris/

[RENAUD, 1997] Monique Renaud, Francesco Masseti, “Network and System Concepts for Optical Packet Switching” - IEEE Communications Magazine - April, 1997.

[ROCHA, 2002] Rocha, M.L., Paradisi, A., et al, “Experimental characterization of optical nodes in a mesh network,” in Proceedings of X Simpósio Brasileiro de Microondas e Optoeletrônica, SBMO 2002.

[ROSEN, 2001] ROSEN E.; VISWANATHAN A.; CALLON R., “Multiprotocolol Label Switching Arquiteture”. Internet Engineering Task Force. IETF RFC 3031, Janeiro 2001. http://www.ietf.org.

[ROSSI, 2002] S. M. Rossi, A. Paradisi, et. al. “Optical WDM networks with distributed IP-centric control plane”, in Proceedings of X SBMO 2002, pp. 92–95.

[ROUSKAS, 2002] George N. Rouskas “Optical network Engineering” – Departament of Computer Science, North Caroline State University – Raleigh – 2002.

[ROUSKAS, 2001] George N. Rouskas, “Routing and Wavelength Assignment in Optical WDM Networks”- Department of Computer Science- North Carolina State University - Raleigh, USA, 2001

[SACHS, 2003] Sachs, A.C., *et. al*. “Experimental Investigation on Data and Control Planes of the OMEGA Test Bed”, Proceedings SBMO/lEEE MTT-S IMOC 2003

[SÁNCHEZ, 2003] Sánchez López, Sergio “Interconnection of IP/MPLS Networks Through ATM and Optical Backbones using PNNI Protocols” - Tesis de Doctorado – UPC – 2003

[SAHA, 2003] Saha, D.; Rajagopalan, B.; Bernstein, G.; “The optical network control plane: state of the standards and deployment” Communications Magazine, IEEE Volume 41, Issue 8, Aug. 2003 Page(s):S29 - S34

[SANO, 2006] Akihide Sano, Hiroji Masuda, et. al., “14-Tb/s (140 x 111-Gb/s PDM/WDM) CSRZ-DQPSK Transmission over 160 Km Using 7-THz Bandwidth Extended L-band EDFAs” – 32nd European Conference on Optical Communication 2006 Proceedings – Post deadline papers – Cannes 2006.

[SATO, 2002] Sato, Ken-ichi. “Photonic Network Technology Development”. Global Optical Communications. (2002).

[SATO2, 2002] K. Sato, N. Yamanaka, Y. Takigawa, M. Koga, S. Okamoto, K. Shiomoto, E. Oki, W. Imajuku, GMPLS-based photonic multilayer roteador (Hikari roteador) architecture: an overview of traffic engineering and signaling technology, IEEE Communications Magazine, Volume: 40 Issue: 3, Mar 2002, pp. 96-101.

[SCHULTZ, 2003] Stephan Schultz “Pocket Guide for Asynchronous Transfer Mode and ATM Testing” Publisher: Wandel & Goltermann GmbH & Co Elektronische Meûtechnik – Germany -2003

[SEBOS, 2001] P. Sebos, J. Yates, G. Hjalmtysson and A. Greenberg, “Auto-discovery of Shared Risk Link Groups,” Optical Fiber Commun. Conf., March 2001

[SHIMAMOTO, 1993] Shimamoto, N; Hiramatsu, A.; Yamasaki, K.- “A dynamic routing control based on a genetic algorithm” – Proc. IEEE Intl. Conf. on Neural Networks –ICNN - San Francisco – California – USA – March/April, 1993

[SIMPSON, 1999] W. Simpson, "PPP over SONET/SDH", RFC 2615, June 1999, ftp://ftp.upc.es/pub/doc/rfc/26xx/2615

[SINCLAIR, 1998] Sinclair, M.C.- "Minimum network wavelength requirement design using a genetic-algorithm/heuristic hybrid"- Electronics Letters v. 34, n 4 - February 1998.

[SINCLAIR2, 1998] Sinclair, M.C. - "Minimum cost routing and wavelength allocation using a genetic-algorithm/heuristic hybrid approach" – Proc. 6th IEE Conf. on Telecommunications, Edinburgh – UK -March/April, 1998

[SINCLAIR, 1993] Sinclair, M.C."The application of a genetic algorithm to trunk network routing table optimisation" - Proc. 10th UK Teletraffic Symposium, Martlesham Heath. UK, April 1993

[SINCLAIR, 1999] Sinclair, M.C "Evolutionary Telecommunications: A Summary" - Proc. GECCO'99 Workshop on Evolutionary Telecommunications: Past, Present and Future, Orlando, Florida, USA, July 1999, pp.209-212

[SINCLAIR2, 1999] Sinclair, M.C. "Optical Mesh Topology Design using Node-Pair Encoding Genetic Programming" - Proc. Genetic and Evolutionary Computation Conference (GECCO-99), Orlando, Florida, USA, July 1999, pp.1192-1197

[SINCLAIR3, 1993] Sinclair, M.C. "The application of a genetic algorithm to trunk network routing table optimization" – Proc 10th UK Teletraffic Symposium. Martlesham Heath. UK – April 1993

[SUBRAMANIAN, 1996] S. Subramanian, M. Azizoglu and A. Somani, "All-Optical Networks with sparse wavelength Conversion", IEEE Trans. On Networking, vol. 4, no 4, pp. 544-557, Aug. 1996.

[TAN, 1995] Tan, L.G. and Sinclair, M.C. "Wavelength assignment between the central nodes of the COST 239 European optical network"- Proc 11th UK Performance Engineering Workshop Liverpool – UK – Sep.1995

[THIAGARAJAN, 1999] Sashisekaran Thiagarajan, Arun K. Somani, "An Efficient Algorithm for Optimal Wavelength Converter Placement on Wavelength-Routed Networks with Arbitrary Topologies" - Proceeding of the IEEE INFOCOM, 1999, pp.916-923.

[THOMPSON, 1997] Thompson, K.; Miller, G.J.; Wilder, R.; "Wide-area Internet traffic patterns and characteristics" Network, IEEE Volume 11, Issue 6, Nov.-Dec. 1997 Page(s):10 – 23.

[TO, 1994] M. To and P. Neusy, "Unavailability Analysis of Long-Haul Networks," IEEE JSAC, vol. 12, Jan. 1994, pp. 100–109.

[TOMSU , 2002] Peter Tomsu e Christian Schmutzer, Next Generation Optical Networks – The Convergence of IP Intelligence and Optical Technologies, Prentice Hall, PTR, 2002.

[UFSC, 2005] http://www.inf.ufsc.br/grafos/temas/custo-minimo/dijkstra.html, 28/11/2005

[WALDMAN, 2004] H. Waldman; K. D. R. Assis, "Approaches to Maximize the Open Capacity of Optical Networks". ONDM'04, Ghent, Belgium; February, 2004.

[WANG, 2002] Jian Wang; Sahasrabuddhe, L.; Mukherjee, B.; "Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signaling" - IEEE Communications Magazine , Volume: 40 Issue: 11 , Nov 2002

[XIN, 2002] Yufeng Xing. "Topology Design of Large-Scale Optical Networks" A dissertation submitted Degree of Doctor of Philosophy. North Carolina State University, 2002

[XU, 2001] Lisong Xu, Harry G. Perros, and George Rouskas, “Techniques for Optical Packet Switching and Optical Burst Switching” - IEEE Communications Magazine • January 2001.

[XU, 2006] Lei Xu; Ting Wang; Chowdhury, A.; Jianjun Yu; Gee-kung Chang; “Spectral efficient transmission of 40 Gbps per channel over 50 GHz spaced DWDM systems using optical carrier suppression, separation and optical duobinary modulation”- Optical Fiber Communication Conference, 2006 and the 2006 National Fiber Optic Engineers Conference - 5-10 March 2006 Page(s):10 pp.

[YAMANAKA, 2003] Yamanaka, N.; “Photonic MPLS network architecture based on Hikari-router” Design of Reliable Communication Networks, 2003. (DRCN 2003). Proceedings. Fourth International Workshop on 19-22 Oct. 2003 Page(s):152 - 157

[YE, 2000] Yinghua Ye; Dixit, S.; Ali, M.; “On joint protection/restoration in IP-centric DWDM based optical transport networks” Communications Magazine, IEEE Volume 38, Issue 6, June 2000 Page(s):174 - 183

[YUAN, 2004] S. Yuan and J. P. Jue, “Dynamic Lightpath Protection in WDM Mesh Networks under Wavelength Continuity Constraint,” IEEE Globecom, pp. 2019-2003, 2004.

[ZHANG, 2003] Zhang, J.. “Service Provision to Provide Per-Connetion-Based Availability Guarantee in WDM Mesh Network”. Proc. OFC. - 2003

[ZHANG2, 2003] J. Zhang et al., “On The Study Of Routing And Wavelength-Assignment Approaches for Survivable Wavelength-routed WDM Mesh Networks,” SPIE Optical Networks Magazine, Nov./Dec., 2003.

[ZHANG, 2004] Jing Zhang; Mukheriee, B.; “A review of fault management in WDM mesh networks: basic concepts and research challenges” Network, IEEE – Vol. 18, Issue 2, Apr 2004 Page(s):41 - 48

[ZHANG, 2004] Zhang, J. e Mukherjee, B.. « A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges ». IEEE Network – 2004.

[ZHENG, 2003] Zheng, Q. e Mohan, G.. « Protection Approaches for Dynamic Traffic in IP/MPLSover-WDM Networks. IEEE Communications Magazine »- 2003.

[ZHENG, 2004] Jun Zheng, Hussein T. Mouftah; “Optical WDM Networks: Concepts and Design Principles” Ed. Wiley-IEEE – 312 pag. ISBN 0471671703 - 2004

[ZITZLER 1999] E. Zitzler and L. Thiele, “Multiobjective Evolutionary Algorithms: A Comparative Case Study and the Strength Pareto Approach” IEEE Transactions on Evolutionary Computation, 3(4), November 1999, pp. 257-271.

[ZHOU 1, 2002] Bin Zhou; Mouftah, H. T.,”Spare capacity planning using survivable alternate routing for long haul WDM networks” Computers and Communications, 2002. Proceedings. ISCC 2002.

[ZHOU 2, 2001] B. Zhou, and H. T. Mouftah, “Balance Alternate Routing for WDM networks”, IASTED International Conference Wireless and Optical Communication 2001, Banff, Canada, July 17-19, 2001.