

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JAIME VIANA DE SOUSA

**TOLERÂNCIA A FALHA EM REDES ÓPTICAS DE NOVA GERAÇÃO**

DM - 21 / 2006

UFPA / ITEC / PPGE  
Campus Universitário do Guamá  
Belém-Pará-Brasil  
2006

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

JAIME VIANA DE SOUSA

**TOLERÂNCIA A FALHA EM REDES ÓPTICAS DE NOVA GERAÇÃO**

ORIENTADA POR: PROF. DR. ANTÔNIO JORGE GOMES ABELÉM

Dissertação submetida à  
Banca Examinadora do Programa de  
Pós-Graduação em Engenharia  
Elétrica da UFPA como requisito para  
a obtenção do Grau de Mestre em  
Engenharia Elétrica com ênfase em  
Computação Aplicada

UFPA / ITEC / PPGEE  
Campus Universitário do Guamá  
Belém-Pará-Brasil  
2006

S725t Sousa, Jaime Viana de  
Tolerância a Falhas em Redes Ópticas de Nova Geração /  
Autor, Jaime Viana de Sousa; Orientador, Antônio Jorge  
Gomes Abelém – Belém: [s.n.], 2006.

Dissertação (Mestrado) – Universidade Federal do Pará,  
Instituto de Tecnologia, Programa de Pós-Graduação em  
Engenharia Elétrica, Belem, 2006.

1. Comunicações ópticas. 2. Cabos de telecomunicação. 3.  
Telecomunicações – tráfego. I. Tolerância a falha em redes  
ópticas de nova geração.

CDD – 21. ed. 621.3827

UNIVERSIDADE FEDERAL DO PARÁ  
INSTITUTO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

**TOLERÂNCIA EM REDES ÓPTICAS DE NOVA GERAÇÃO**

AUTOR : JAIME VIANA DE SOUSA

DISSERTAÇÃO SUBMETIDA À AVALIAÇÃO DA BANCA EXAMINADORA APROVADA PELO COLEGIADO DO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA DA UNIVERSIDADE FEDERAL DO PARÁ E JULGADA ADEQUADA PARA OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA COM ÊNFASE EM COMPUTAÇÃO APLICADA.

APROVADA EM \_\_\_\_/\_\_\_\_/\_\_\_\_

BANCA EXAMINADORA:

---

Prof. Dr. Antônio Jorge Gomes Abelem  
(ORIENTADOR - UFPA)

---

Prof. Dr. João Crisóstomo Weyl Albuquerque Costa  
(EXAMINADOR - UFPA)

---

Prof. Dr. Roberto Betini  
(EXAMINADOR - UFPA)

VISTO:

---

Prof. Dr. Evaldo Gonçalves Pelaes  
(COORDENADOR DO PPGEE /ITEC/UFPA)

## AGRADECIMENTOS

Quero agradecer:

ao nosso senhor Jesus Cristo mestre de todos os mestres, filho daquele que me deu o dom da vida e força para superar os obstáculos mais difíceis;

ao professor Antônio Jorge G. Abelém, por entender na qualidade de orientador a minha condição de aprendiz, vendo, revendo, orientando e dando a correta condução em cada página deste trabalho;

a minha esposa Lucilene, pela paciência nos momentos difíceis e compreensão nas muitas horas em que me fiz ausente do nosso lar;

as minhas filhas Natália e Letícia, por representarem o meu elo com a eternidade e a motivação de querer sempre mais, para ter à ofertá-las;

ao PPGEE e ao departamento de computação da UFPA, pela qualidade dos serviços prestados;

ao GERCOM, por ter dado todo apoio e suporte necessário para o desenvolvimento deste trabalho, destaco a colaboração do colega Rafael Esteves por não negar esforços e conhecimentos nas várias dúvidas que tive no manuseio do NS e o apoio do colega Alan Tamer em todos os momentos desta compensadora jornada;

a todos os colegas do BCC da CESUPA de 2002, destacando os colegas Orlando Ohashi, Mariana Bechara e ao apoio recebido pelas Professoras Lêda Mara e Cássia Kahwage;

ao apoio recebido pelos colegas de trabalho Pedro Diniz, Fernando Rodrigues e Antônio Victor;

este trabalho sintetiza a soma dos esforços de todos aqueles que direta ou indiretamente estiveram ao meu lado e é para estas pessoas que eu externo o mais profundo agradecimento.

## SUMÁRIO

<b>1 Introdução</b> .....	12
1.1 Objetivos .....	14
1.2 Descrição do Trabalho .....	14
1.3 Organização do Trabalho .....	15
<b>2 Redes Ópticas</b> .....	17
2.1 Sistemas Ópticos .....	18
2.2 Transmissão Óptica.....	19
2.2.1 Fibra Óptica.....	19
2.2.2 WDM.....	22
2.2.3 Evolução dos Sistemas .....	23
2.3 Arquitetura das Redes .....	24
2.3.1 SDH/SONET .....	25
2.3.2 ATM.....	29
2.3.3 TCP/IP.....	31
2.4 Redes MPLS.....	33
2.4.1 GMPLS.....	35
2.5 Arquitetura de Redes de Nova Geração .....	36
2.6 Comutação Óptica .....	39
<b>3 Tolerância a Falhas em Redes Ópticas</b> .....	42
3.1 Técnicas de Detecção de Falhas.....	43
3.1.1 Detecção de Falhas no Transporte de Dados .....	43
3.1.2 Localização de Falhas .....	44
3.2 Técnicas de Proteção e Restauração.....	44
3.2.1 Técnicas de Proteção Linear .....	45
3.2.2 Técnicas de Proteção em Anel .....	46
3.2.3 Processamento de uma Comutação em Sistemas Lineares e Anel.....	47
3.2.4 Técnicas de Proteção em Malha.....	47
3.3 Trabalhos Correlatos .....	48
3.4 Modelo de referência adotado .....	49
3.5 Plano de Controle .....	51
3.5.1 Gerência de Recursos .....	52
3.5.2 Módulo de Conexão .....	53
3.5.3 Módulo de Proteção e Restauração .....	55
<b>4 Estudo de Caso</b> .....	57
4.1 Cenário de Testes Realizados na Rede <i>Testebed</i> .....	58

4.1.1	Resultados dos Testes.....	60
4.2	Cenário de Testes em Redes de Nova Geração Utilizando o NS.....	64
4.2.1	NS.....	65
4.2.2	Resultados das Simulações.....	69
4.3	Análise Comparativa.....	79
<b>5</b>	<b>Conclusões e Investigações Futuras.....</b>	<b>82</b>
5.1	Trabalhos Futuros.....	83
<b>6</b>	<b>Referências Bibliográficas .....</b>	<b>85</b>
<b>Anexo 1</b>	<b>.....</b>	<b>89</b>

## LISTA DE FIGURAS

Figura 2.1. Sistema de transmissão optica .....	19
Figura 2.2. Formato de uma fibra óptica.....	20
Figura 2.3. Propagação da luz no interior da sílica .....	20
Figura 2.4. Atenuação da luz através da fibra óptica de sílica [11].....	22
Figura 2.5. Evolução dos sistemas ópticos [6] .....	24
Figura 2.6. Multiplexação PDH. ....	25
Figura 2.7. Estrutura básica do sistema de multiplexação SDH/SONET [3].....	27
Figura 2.8. Estrutura do quadro STM .....	27
Figura 2.9. Camadas SDH/SONET.....	29
Figura 2.10. Formato da célula ATM.....	30
Figura 2.11. Arquitetura do protocolo ATM.....	31
Figura 2.12. Distribuição dos protocolos nas camadas .....	32
Figura 2.13. Comutação de pacotes baseada no endereço IP.....	33
Figura 2.14. Comutação de pacotes baseada no endereço MPLS .....	33
Figura 2.15. Formato do rótulo .....	34
Figura 2.16. Pilha de protocolos usados no GMPLS [24].....	35
Figura 2.17. Evolução da pilha de protocolo para redes de nova geração [16] .....	37
Figura 2.18.Arquitetura das redes de nova geração .....	38
Figura 2.19.Topologia física e virtual .....	39
Figura 2.20.Funcionamento básico de um comutador [6].....	39
Figura 2.21. (a) ADM derivando canal 2 do tronco A com 5 canais; (b) XC permutando canais 2 e 4 do tronco A com os mesmos canais do tronco B; (C) XC permutando os canais 2 e 4 do tronco A com os canais 3 e 5 do tronco B [6]. ....	41
Figura 3.1. Impacto causado pela interrupção de serviço de telecomunicações [27] .....	43
Figura 3.2. Tipo de proteção linear .....	46
Figura 3.3. Proteção em anel.....	47
Figura 3.4. Rede em malha.....	49
Figura 3.5. Modelo de sobreposição (“overlay”) [20]. ....	50
Figura 3.6. Modelo de pares (“peer”) [20]. ....	51
Figura 3.7. Plano de controle .....	52

Figura 3.8. Diagrama do plano de controle.....	52
Figura 3.9. Exemplo de LT .....	54
Figura 3.10. Diagrama de estados .....	55
Figura 4.1. Backbone óptico de longa distância [35].....	58
Figura 4.2. DA-3200 data network analyzer [29].....	58
Figura 4.3. Topologia utilizada nas simulações .....	59
Figura 4.4. Topologia utilizada na simulação SDH/SONET .....	60
Figura 4.5. Rompimento da fibra entre os pontos 19 e 20 .....	61
Figura 4.6. Recuperação do tráfego pela rota reserva.....	63
Figura 4.7. Throughput total corrente .....	64
Figura 4.7- Diagrama básico de um nó OWNS[43].....	66
Figura 4.8 - Diagrama básico de um nó MNS [42].....	67
Figura 4.7. Estrutura do nó LOCSnode.....	68
Figura 4.8. LSP Principal entre Belém e Fortaleza.....	69
Figura 4.9. Momento da Interrupção no Link Entre Belém e Santa Inês.....	70
Figura 4.10. Comutação para o LSP Reserva.....	71
Figura 4.10. Vazão no esquema de proteção LSP 1:1.....	73
Figura 4.11. Vazão no esquema de proteção LSP 1+1.....	74
Figura 4.12. Falha em dois LSP's simultaneamente.....	75
Figura 4.13. Vazão quando falham dois LSP's simultaneamente .....	76
Figura 4.14. Processamento do esquema de proteção de enlace.....	77
Figura 4.15. Vazão resultante quando adotado o esquema de proteção de enlace.....	78
Figura 4.16. Impacto causado pela interrupção de serviço de telecomunicações [27] .....	80

**LISTA DE TABELAS**

Tabela 2.1. Níveis hierárquicos PDH.....	26
Tabela 2.3. Níveis hierárquicos SDH/SONET.....	28
Tabela 2.4. Comparação entre os paradigmas de comutação óptica.....	41
Tabela 4.1. Dados gerados pelo instrumental após a ocorrência do evento.....	62
Tabela 4.2. Número de pacotes perdidos na técnica de proteção 1: 1.....	72
Tabela 4.3. Número de pacotes perdidos na técnica de proteção 1+1 .....	74
Tabela 4.4. Número de pacotes perdidos quando falham dois LSP's simultaneamente.....	76
Tabela 4.5. Número de pacotes perdidos com esquema de proteção de enlace.....	78

## RESUMO

Disponibilidade é uma considerável preocupação para projetistas de redes devido à crescente importância das informações que nelas trafegam, motivando as prestadoras de serviços de telecomunicações a melhorarem a capacidade e a qualidade de seus backbones. As redes ópticas de nova geração, baseadas em WDM (*Wavelength Division Multiplexing*) geralmente utilizam plano de controle baseado na tecnologia GMPLS (*Generalized Multiprotocol Label Switching*), em função desta oferecer uma melhor adequação entre o protocolo IP e a camada óptica. Este trabalho realiza uma análise comparativa, entre os mecanismos utilizados pelas redes ópticas tradicionais e as ditas de nova geração. Propõe a adoção de diferentes mecanismos de tolerância a falhas em função do tipo de tráfego. Realiza testes em redes reais baseadas na plataforma SDH/SONET e simulações em computador dos principais mecanismos oferecidos pelo modelo multicamadas IP-GMPLS/WDM para promover proteção e restauração de conectividade em redes ópticas de nova geração, objetivando referendar nossa proposta.

Palavras Chaves: Redes ópticas, GMPLS, Disponibilidade.

**ABSTRACT**

*Availability is of considerable concern for network designers due to the increasing importance of the information that pass through them, motivating the providers of telecommunications services to improve the capacity and the quality of their backbones. Optical networks that use WDM ("Wavelength Division Multiplexing") usually present control plane based in GMPLS (Generalized Multiprotocol Label Switching) architecture, because it provides one better adequation between IP protocol and the optical layer. This work makes a comparative study, between the mechanisms used for the traditional optical networks and the said ones of next generation. It considers the adoption of different mechanisms of fault tolerance in function of the traffic model, through simulations, In the networks implemented by SDH/SONET architecture and simulation in computer of the main mechanisms offered for the multilayer model IP-GMPLS/WDM to provide protection and restoration of connectivity in next-generation optical networks, being objectified to authenticate our proposal.*

*Key Words: Optical Networks, GMPLS, Availability.*

## 1 - Introdução

Fornecer infra-estrutura de telecomunicações com qualidade é uma das maiores preocupações das operadoras que trabalham nesse segmento. Dentre os vários parâmetros que definem essa qualificação está a disponibilidade. Para prestar serviços disponíveis torna-se necessário desenvolver uma política de tolerância à falhas.

Com a abertura do mercado das telecomunicações no Brasil, ocasionada pela privatização das empresas prestadoras de serviços, ocorrida na segunda metade da década de 1990, o que se pôde observar foi uma corrida das empresas que já estavam presentes no território nacional e outras que tentavam se instalar, implantando seus próprios *backbones*, outras substituindo seus antigos troncos de microondas em radio visibilidade, tropo-difusão e satélite por anéis ópticos [1][2].

Apesar de permanecerem sendo a última palavra em termos de velocidade e capacidade de transmissão, as fibras ópticas tiveram seus estudos amplamente divulgados, assim como, sua implantação definitiva na década de 1970, quando muitas concessionárias de serviços de telecomunicações decidiram começar a instalar exclusivamente serviços digitais, visando implementar as redes digitais de serviços integrados (RDSI), para oferecer uma variedade maior de serviços [2].

O rápido desenvolvimento dos sistemas digitais em nível internacional teve como resultado uma série de padrões hierárquicos para transporte de dados, que empregavam a Hierarquia Digital Plessiócrona (PDH) , porém, três padrões passaram a ter uso geral: O padrão "norte-americano", usado nos EUA e Canadá com velocidade primária de 1.544 Kbps denominado T1; padrão "europeu" usado nos países europeus e no Brasil com velocidades primárias de 2.048 Kbps denominado E1 e por ultimo o padrão "japonês" que foi desenvolvido nos moldes do padrão americano para velocidades inferiores a até 6.312Kbps, diferenciando para valores superiores [1].

A introdução das Hierarquias Digitais SDH (*Synchronous Digital Hirarchy*) e SONET (*Synchronous Optical Network*) trouxeram grandes benefícios no sentido de melhorar as possibilidades de gerências das redes, graças ao seu cabeçalho expandido e pelo fato de possuir uma técnica mais versátil de multiplexação [3].

Em relação à tolerância a falhas, a tecnologia SDH/SONET é caracterizada por possuir um sistema de supervisão de grande capacidade, canal reserva dedicado, comutação automática e rápida restauração de vias [3].

Apesar das inúmeras vantagens apresentadas pela tecnologia SDH/SONET, o perfil do tráfego das operadoras mudou bastante na última década. Houve aumento considerável no tráfego de dados, superando o tráfego de voz tradicional, impulsionado pelas novas aplicações multimídia, como vídeo sob demanda, vídeo conferência, ensino a distância, voz sobre IP, entre outros. A maioria dessas aplicações são realizadas via *Internet*, utilizando a pilha do protocolo TCP/IP, o que obrigou as operadoras a realizar o encapsulamento de pacotes IP em quadros SDH/SONET ou células ATM (*Asynchronous Transfer Mode*). Este empilhamento de camadas provoca redução na eficiência e aumento dos custos de gerenciamento [4].

Pesquisas recentes apontam como uma das soluções para a questão do aumento de banda e diminuição nos custos de gerência e operação dessas redes a redução das camadas intermediárias entre a camada IP e a camada óptica [4]. Isto é possível com a utilização de roteadores IP sintonizáveis com interfaces ópticas WDM (*wavelength division multiplexing*) (IP/WDM).

O WDM é uma técnica de multiplexação baseada nos conceitos de multiplexação por divisão de frequência (FDM). Sendo que esse divide o espectro de frequência luminosa em múltiplos canais ópticos para transportá-los em uma única fibra [5].

Entretanto existe a necessidade de possuir uma camada intermediária entre a camada IP e a WDM que desempenhe algumas funções como: otimização do roteamento, monitoramento, detecção e correção de falhas. Estas funções são perfeitamente implementadas pelo protocolo MPLS (*multi protocol label switching*) e seus aperfeiçoamentos [4].

Outro aprimoramento ainda em estudo é a eliminação dos componentes que realizam conversão de sinais ópticos para elétricos e em seguida para óptico novamente (OEO), para componentes puramente ópticos, ou seja, não necessitam fazer conversão OEO e são capazes de encaminhar as informações no domínio óptico, por isso são chamados (OOO)[6].

As redes formadas por equipamentos puramente ópticos e que utilizam o IP-MPLS sobre WDM serão denominadas neste trabalho de "redes ópticas de nova geração" [7][8] e são objetos de estudos acadêmicos, que visam uma implementação efetiva desta tecnologia.

Estas redes de nova geração possuem um nível de complexidade menor do que as SDH e ATM, assim como um custo operacional bem mais reduzido, principalmente no que diz respeito à tolerância a falha, pois não necessitam de um canal adicional de proteção para restauração de via e sim criando rotas alternativas com o auxílio do IP e do MPLS, o que permite otimizar a exploração da capacidade total de transmissão de uma fibra óptica, aproveitando a infra-estrutura já existente

através do uso efetivo das fibras que são utilizadas apenas como reservas na tecnologia SDH/SONET.

## 1.1 OBJETIVOS

Este trabalho realiza uma análise comparativa dos mecanismos de recuperação de falhas em redes SDH/SONET e redes ópticas de nova geração baseadas na arquitetura IP-GMPLS/WDM, objetivando mostrar as vantagens e desvantagens da adoção dessa tecnologia nos *backbones* nacionais, em substituição aos atuais que utilizam as arquiteturas SONET/SDH. Baseado nesta análise apresenta-se uma proposta para adoção de diferentes mecanismos de tolerância a falhas em função do tipo de tráfego.

Para validar essa proposta realizaram-se testes em uma plataforma real SDH/SONET de uma operadora de telecomunicações nacional. Em seguida executaram-se simulações do mesmo *backbone*, utilizando a arquitetura IP-GMPLS/WDM das redes de nova geração, sendo primeiramente analisado o comportamento das redes SONET/SDH em seguida a criação de caminhos alternativos fim a fim utilizando GMPLS e finalmente a utilização de comutação de lâmbdas na multiplexação WDM.

Com isto pretende-se aproveitar as atuais fibras ópticas já lançadas e utilizadas apenas para servirem de contingência em caso de falhas nas fibras principais evitando-se desta forma um investimento maior em infra-estrutura por parte das prestadoras de serviços, que poderão aumentar sensivelmente a capacidade de transmissão de seus *backbones*.

## 1.2 DESCRIÇÃO DO TRABALHO

Para alcançar os objetivos citados anteriormente, este trabalho faz um breve relato histórico sobre comunicações ópticas, aborda o contexto atual destas e revê questões importantes relacionadas à recuperação de falhas em redes ópticas baseadas na arquitetura IP-GMPLS/WDM; investiga a constituição de uma rede de nova geração proposta por Xin et al. [7] e, baseado nesta, analisa, através de simulações, as principais medidas de proteção adotadas em redes com planos de controles baseados na arquitetura IP-GMPLS/WDM em caso de falhas em um de seus enlaces ou nós.

O desenvolvimento deste trabalho começou com a realização de um estudo sobre a arquitetura SDH/SONET, objetivando adquirir tanto embasamento teórico sobre o tema como conhecimentos sobre o panorama atual das comunicações ópticas no Brasil neste segmento,

buscando identificar as características que mais necessitam de melhoria na questão da tolerância a falhas em redes ópticas de alta capacidade. Tal estudo produziu uma monografia [45].

Para propor melhorias na questão de tolerância a falhas no contexto citado anteriormente, foi necessário desenvolver também estudos aprofundados sobre redes ópticas de nova geração utilizando IP-GMPLS no seu plano de controle e WDM no plano de transporte de dados.

Por falta de um *testbed* para realizar os experimentos práticos em *backbone* de redes ópticas de nova geração, tornou-se necessário escolher uma ferramenta de simulação que permitisse analisar as novas tecnologias investigadas neste trabalho. Optou-se por adotar o NS (*Network Simulator*) por este possuir dois módulos adicionais o OWNS (*Optical WDM Network Simulator*) e o MNS (*MPLS Network Simulator*), como estes dois módulos não conversavam entre si, foram encontradas várias dificuldades em implementar na prática as propostas feitas neste trabalho, sendo portanto necessário integrar as funcionalidades do OWNS com as do MNS originando um novo nó chamado *LOCSnode* (*Labeled Optical Circuit Switching*). Este estudo gerou a publicação de um artigo em congresso nacional [36].

Para avaliar a nossa proposta, procurou-se mostrar primeiramente o desempenho dos sistemas existentes na atualidade baseados em SONET/SDH, através da simulação de falhas num cenário real. Em seguida, analisou-se através de simulações o comportamento de um *backbone* óptico com proteção a falhas baseado em comutação de lâmbdas na camada de transporte de dados (WDM) e finalmente investigou-se o desempenho do tratamento a falhas dado na camada do plano de controle baseado no IP-GMPLS, sendo gerada uma nova publicação em congresso nacional [37].

### 1.3 ORGANIZAÇÃO DO TRABALHO

Alem do capítulo introdutório, este trabalho possui mais quatro capítulos, que abordaram a evolução das tecnologias de transmissões ópticas voltadas à questão da tolerância a falhas, dando especial ênfase às redes de nova geração, com plano de controle baseado em GMPLS.

O segundo capítulo fará uma introdução ao estudo de redes ópticas, abordando primeiramente os componentes de sistemas ópticos, a propagação da luz, mostrando a constituição física de uma fibra, assim como as formas de comutação dando uma noção das arquiteturas de redes ópticas ATM, IP-MPLS e as tecnologias SDH/SONET. Será mostrado também as redes de nova geração onde serão abordados os principais modelos em estudo, os componentes puramente ópticos a arquitetura IP-MPLS sobre WDM e finalmente mostrado o GMPLS [10].

O terceiro capítulo deste trabalho abordará o tratamento que é dado a falhas nas atuais redes ópticas de grande capacidade, que utilizam a tecnologia SDH/SONET, assim como os avanços ocorridos nesta área até as redes de nova geração com planos de controles baseados em IP-GMPLS proposta por Xin et al. [7][8]. Serão também mostrados os principais trabalhos relacionados, objetivando verificar o estado atual e as principais contribuições já apresentadas ao tema.

A descrição da avaliação prática de nossa proposta é feita no quarto capítulo através de um estudo de casos, sendo primeiramente mostrado o cenário, as ferramentas usadas e os testes desenvolvidos na rede *testbed*. Em seguida serão apresentados os resultados do mesmo cenário agora implementado em redes de nova geração simulados no NS. Detalhes de implementação do nó proposto, denominado de "*LOCSnode*", também são apresentados. Conclui-se o capítulo com a análise comparativa das duas simulações.

Finalmente o quinto capítulo apresentará as conclusões gerais deste trabalho e fará também sugestões para possíveis trabalhos futuros.

## 2 – REDES ÓPTICAS

As comunicações "ópticas" não constituem um privilégio dos dias atuais. Desde os primeiros séculos, o homem soube aproveitar as fontes luminosas para fins de comunicações a distância[2]. "A primeira análise teórica completa sobre propagação eletromagnética em cilindros dielétricos, que correspondem a estrutura básica das futuras fibras ópticas é datada de 1910, feita pelos Alemães Hondros e Debies" [2].

A primeira transmissão em fibra de vidro foi feita em 1930, pelo alemão Lamb [11], no entanto a aplicação prática só ocorreu em 1951 com a invenção do *Fiberscope*, que permitiu a transmissão de imagens através de um feixe flexível de fibras de vidro[2]. As fontes de luz na época garantiam transmissões a distâncias muito reduzidas, somente com a invenção do raio laser, ocorrida em 1958 e sua capacidade luminosa elevada, permitiu-se conceber sistemas de comunicação ópticos a longo alcance e grande valor de banda passante [2].

O ano de 1966 é marcado pela introdução do dispositivo de recepção, através da criação do fotodiodo de avalanche (APD) de germânio em alta velocidade, neste mesmo ano foi publicado na Inglaterra um estudo sobre a propagação da fibra de vidro em transmissão a longa distância por Kao e Hockman [13], percebendo-se desta forma o grande potencial de transmissão em sistemas de telecomunicações.

As primeiras utilizações da fibra óptica no contexto comercial ocorreram na década de 1970. Em 1977 transmitiu-se voz em um link de 9Km, com dois repetidores unindo duas centrais telefônicas no Estado da Califórnia, EUA.

A capacidade total de transmissão de uma fibra óptica é de aproximadamente 50 Tbps [2][6], porém, existem vários obstáculos que impedem a exploração desta capacidade, dentre elas a mais significativa é a dificuldade de processamento do sinal óptico pelos diversos equipamento das pontas. Para que o sinal óptico seja processado é necessário convertê-lo para elétrico em seguida para óptico novamente, os equipamentos que realizam esta conversão, são chamados de "Ópticos Elétrico Ópticos (OEO)" ou "Opacos". A velocidade máxima conseguida em sistemas que utilizam equipamentos OEO é de 40Gbps.

Tal limitação motivou o desenvolvimento de pesquisas para implementação de equipamentos que não necessitem realizar a conversão do sinal óptico para elétrico, estes

equipamentos são chamados de equipamentos puramente ópticos ou "Ópticos Ópticos Ópticos (OOO)" ou "Transparentes". Estudos realizados pela *Lucent* no ano de 2002 em transmissão puramente óptica conseguiram obter uma velocidade em laboratório de 2.56Tbps [6], mais recentemente uma nova geração de amplificadores puramente ópticos estão sendo desenvolvidos pela UNICAMP: o FOPA (*Fiber Optic Parametric Amplifier*) que pretende aumentar em um número significativo de vezes a capacidade de transmissão de telefonia, dados e imagem via fibra óptica [45].

## 2.1 - SISTEMAS ÓPTICOS

Basicamente um sistema de comunicação por fibra óptica possui três partes fundamentais: transmissor óptico, o receptor óptico e a fibra óptica que corresponde ao meio.

O transmissor óptico é composto basicamente por um dispositivo emissor de luz e um *driver*, sendo que o dispositivo emissor de luz possui como função transformar a energia elétrica em energia luminosa, os dois dispositivos comumente usados são os Diodos Emissores de Luz (LED) e os Diodos a Laser (DL), sendo que o diodo a laser possui uma capacidade de transmissão superior, devido a sua maior potência luminosa, diretividade e consequentemente maior alcance. O *driver* possui a finalidade de regular a potência luminosa do emissor e a polarização do feixe luminoso.

O receptor óptico é composto por um foto detetor que tem a finalidade de transformar os pulsos ópticos recebidos em pulsos elétricos. A convenção usada para a transformação óptica em elétrica é: ausência de luz que corresponde a ausência de pulso elétrico ou seja nível lógico "0" e a presença de luz que corresponde a presença de pulso nível lógico "1". Os foto detetores trabalham sobre uma faixa larga de frequências, possibilitando que haja uma boa resposta para um grande conjunto de comprimentos de onda, os principais tipos de foto detetores são os diodos PIN e os Diodos de Avalanche APD (*Avalanche Photo diodes*), maiores detalhes sobre estes dois tipos de foto detetores podem ser obtidos em [2] [14].

A Fibra óptica, por sua vez, corresponde ao meio onde os sinais luminosos, injetados pelo emissor de luz, são guiados e transmitidos até o receptor [2]. A seção 2.2 deste capítulo abordará mais detalhadamente este assunto.

Com os links podendo ser expandidos por milhares de quilômetros, tornou-se factível acrescentar ADMs (*add-drop multiplexers*), para permitir adicionar e retirar informações em vários pontos ao longo do link óptico. A nova fase do ADM chama-se WADM (*Wavelength ADM*), que consiste na fixação de um comprimento de onda no canal que se deseja inserir ou retirar.

Outros componentes do sistema óptico que também devem ser citados são os amplificadores, que possuem como finalidade regenerar o sinal óptico ao longo do meio de transmissão, o modulador que possui a finalidade de codificar o sinal luminoso na transmissão e o demodulador cuja função é decodificar o sinal na recepção. A Figura 2.1 ilustra um sistema básico de transmissão óptica.

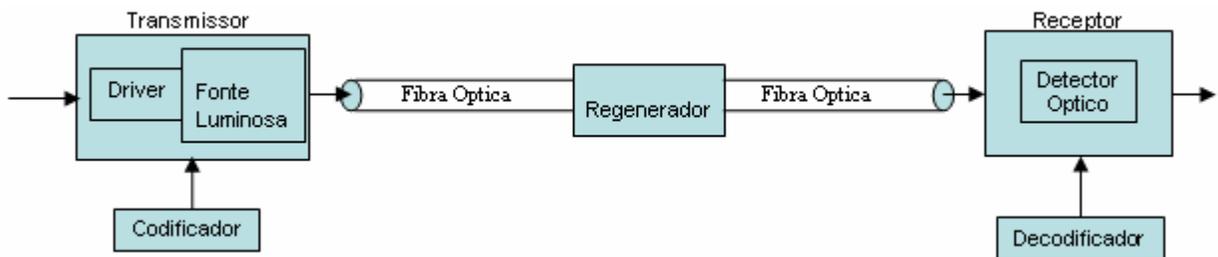


Figura 2.1. Sistema de comunicação por fibra óptica

## 2.2 TRANSMISSÃO ÓPTICA

A eficácia da transmissão de sinais luminosos entre dois pontos torna-se limitada devido a contribuição de vários fatores, dentre eles a necessidade de existir sempre uma visada direta desobstruída e a forte degradação da potência, que cai proporcional ao inverso do quadrado da distância entre estes dois pontos, tornando necessário canalizar esta energia de forma concentrada e diretiva, para aumentar o alcance e podendo ser flexionada para resolver a questão da visada direta.

### 2.2.1 Fibra Óptica

Uma fibra óptica funciona como um guia de onda luminosa, de forma cilíndrica como mostrado na Figura 2.2, composta por um núcleo fabricado com material de alto grau de transparência e flexibilidade, geralmente sílica. Este núcleo é revestido por uma camada

de sílica com menor índice de refração chamado de "casca". O ângulo formado por um raio luminoso que incide na região que separa o núcleo da casca é chamado: "ângulo crítico" [2]. Quando o raio incidente ultrapassa o valor deste ângulo, haverá a reflexão interna total da energia do raio, podendo este raio se propagar por longas distâncias sem sofrer muitas perdas [6].

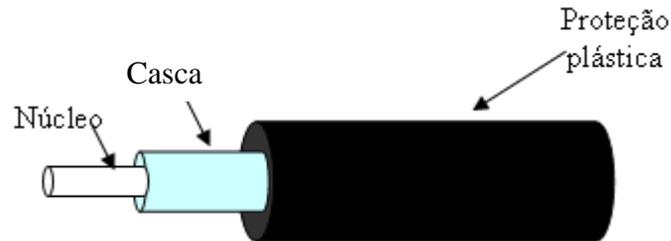


Figura 2.2. Formato de uma fibra óptica

A Figura 2.3(a) ilustra a propagação da luz no interior de uma fibra de sílica, colidindo com o ar em diferentes ângulos, em seguida a Figura 2.3(b) mostra o mesmo feixe incidindo com na casca em ângulos com valor acima do ângulo crítico em dois modos diferentes.

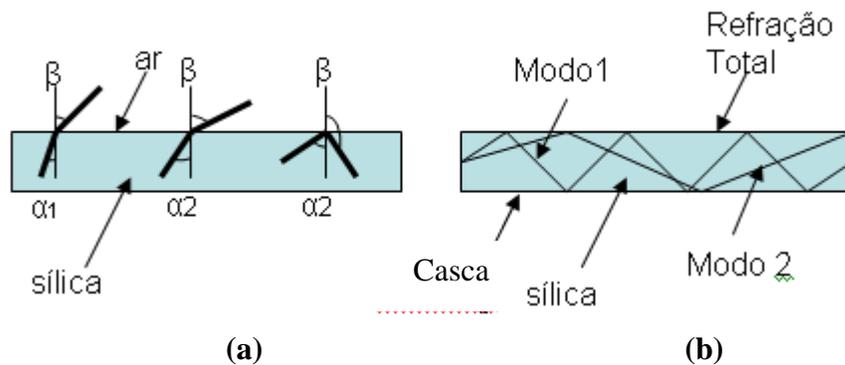


Figura 2.3. Propagação da luz no interior da sílica

### **2.2.1.1 Fibra Óptica Multimodal**

Analisando a Figura 2.3(b) verificam-se dois feixes com ângulo superior ao ângulo crítico incidindo na casca fazendo reflexões sucessivas, cada um com um "modo de propagação correspondente" [2]. Uma fibra com essa propriedade é chamada de "Fibra Multimodal" [2].

Uma fibra multimodal possui o núcleo com diâmetro de 50 a 85  $\mu\text{m}$  e diâmetro de casca de 125  $\mu\text{m}$ , permitindo que a luz se propague no interior desta fibra por diversos caminhos, estas fibras atualmente servem principalmente para redes de acesso ligando computadores individuais [6] e dependendo do índice de refração entre o núcleo e a casca podem ser classificadas em dois tipos: fibras ópticas multimodais com índice degrau e fibras ópticas multimodais com índice gradual.

A fibra óptica multimodal índice degrau dentre os outros tipos de fibras é a que possui o núcleo com maior diâmetro, fabricação mais simplificada, fácil operação, possuindo uma capacidade de transmissão bastante limitada. Já a fibra multimodal de índice gradual, possui uma complexidade de fabricação superior e dimensões moderadas em relação a degrau, isto implica numa conectividade mais complexa, porém, uma capacidade de transmissão maior [2].

### **2.2.1.2 Dispersão**

A dispersão pode ser definida de uma maneira geral como um alargamento do pulso óptico [6]. Dependendo do tipo de fibra a dispersão pode se apresentar em três formas, são elas: Dispersão Modal ou Intermodal, Dispersão Cromática e Dispersão de Modo de Polarização.

A dispersão intermodal é causada pelo espalhamento gradativo do pulso dos vários modos que se propagam no interior de uma fibra, devido as várias reflexões sucessivas ao longo de um determinado percurso. Este tipo de dispersão é a principal limitadora do uso da fibra multimodal, pois à medida que se aumenta a dispersão, torna-se mais difícil distinguir um pulso do outro, diminuindo a velocidade de transmissão e o alcance do feixe, este tipo de dispersão é combatida com o uso de fibras monomodais que serão abordadas ainda neste capítulo;

As diferentes velocidades de propagação da luz na fibra causam as dispersões cromáticas, que podem ser diminuídas com o uso de um tipo de laser chamado SLM (*Single Logitudinal Mode*), onde a energia transmitida está concentrada num só comprimento de onda [6], outra forma de combater a dispersão cromática é o uso de fibras ópticas que operam na faixa de 1550 nm, como por exemplo, (*Dispersion Shift Fiber*) DSF e a (*Dispersion Compensated Fiber*) DCF [2][6];

A dispersão de modo de polarização (PMD- *Polarization Mode Dispersion*), é causada pelas imperfeições no formato cilíndrico da fibra e outros pontos de estresse devido ao seu manuseio inadequado, causando uma distribuição inadequada da luz em diferentes pontos da casca que causam um desvio na polarização original, uma vez que esta foi transmitida pela sua fonte numa polarização definida. Como são formados vários modos de polarização aleatórios este efeito é considerado um efeito randômico e pode ser combatido com a diminuição da potência de transmissão óptica, que para grandes distâncias pode ser conseguido com a diminuição do diâmetro do núcleo da fibra. [2] [6].

### **2.2.1.3 Fibra Óptica Monomodal**

Observou-se que ao reduzir o diâmetro de uma fibra para aproximadamente 10 $\mu$ m, a luz poderia se propagar em linha reta, paralelamente ao eixo da fibra, combatendo desta forma a dispersão intermodal, dando um maior alcance e aumentando a velocidade de transmissão até dezenas de Tbps. Fibras com estas características são chamadas de “Fibras Monomodais”.

A Figura 2.4 mostra a relação entre a atenuação de uma fibra óptica em dB/Km e o comprimento de onda em microns. Observando-se a curva é notado que a atenuação mínima de 0,2 dB/Km, é obtida para valores de 1.3 e aproximadamente 1.55 micrômetros, portanto, é preferível usar transmissores que trabalhem com este comprimento de onda, para diminuir o número de repetidores.

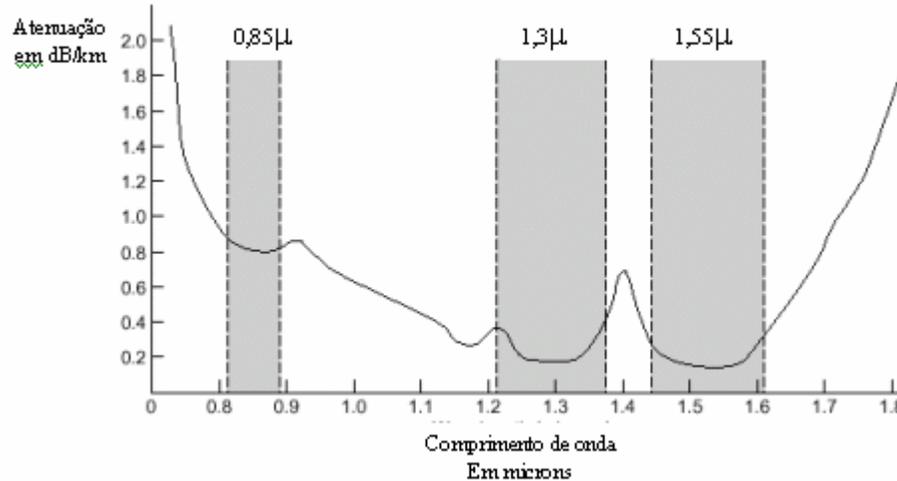


Figura 2.4. Atenuação da luz através da fibra óptica de sílica [11]

### 2.2.2 WDM

O desenvolvimento de sistemas multiplexadores WDM aumentou a capacidade e a possibilidade de transmissão bidirecional simultânea em fibras ópticas, este utiliza a técnica de multiplexação por divisão de frequência (FDM) aplicada aos sistemas operando nas frequências ópticas [11].

Na multiplexação WDM cada canal corresponde a transmissão de um sinal por um laser dedicado em um determinado comprimento lambda ( $\lambda$ ). Os diversos sinais são combinados para propagação na mesma fibra. No destino, os sinais em diferentes lambdas são novamente separados e destinados aos seus respectivos detectores ópticos, a Figura 2.5 (d) permite visualizar melhor este processo.

Os primeiros sistemas WDM multiplexavam apenas dois canais, nas regiões de 1310nm e 1550nm e possuíam um valor de espaçamento entre canais superior a 20nm. Com a implantação do CWDM (*Coarse WDM*), possibilitou-se multiplexar feixes com 4, 8, 16 canais com espaçamentos que variam de 3,2 até 1,6nm trabalhando na faixa de 1550nm, porém a modalidade mais importante do WDM é o DWDM (*dense WDM*), onde o espaço entre os canais possui um valor inferior a 1nm, tipicamente 0.8nm mas já existem sistemas operando com espaçamento de até 0.2nm.

### 2.2.3 Evolução dos Sistemas

A Figura 2.5 mostra a evolução dos sistemas ópticos desde sua introdução até os dias de hoje [8]. Os primeiros sistemas eram constituídos apenas de um canal ponto a ponto e as distâncias eram relativamente curtas, pois estes usavam fibras multimodais, com fontes luminosas utilizando LEDs, o que forçava a utilização de regeneradores ao longo do feixe distanciados de no máximo 2Km como mostrado na Figura 2.5 (a) .

Com a utilização de fontes luminosas a laser SLM as distâncias entre regeneradores foram aumentadas devido a sua alta diretividade para aproximadamente 40 Km [2], já com o advento da utilização das fibras monomodais em conjunto com fontes a laser MLM estas distâncias foram otimizadas para aproximadamente 100Km [2].

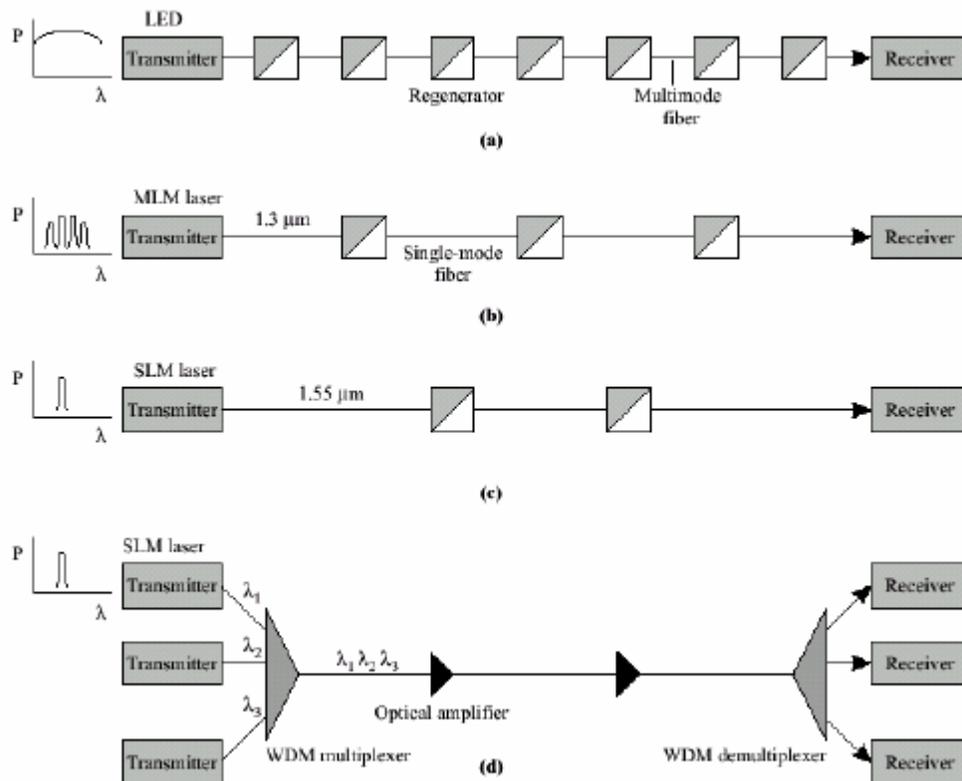


Figura 2.5. Evolução dos sistemas ópticos: (a) sistema usando LEDs sobre fibra multimodal; (b) uso de lasers MLM com fibra monomodal para evitar dispersão intermodal; (c) uso de lasers SLM para evitar dispersão cromática; (d) Sistema atual com multiploscomprimentos de onda e amplificadores ópticos em lugar de regeneradores. [6]

A descoberta dos amplificadores puramente ópticos utilizando érbio dopado EDFA foi o maior marco nas pesquisas para a extensão dos links de fibra na década de 1990 [5], permitindo um grande avanço no alcance das fibras para dimensões continentais, sem a necessidade de converter o sinal de óptico para elétrico, para realizar a amplificação. Foram desenvolvidos multiplexadores WDM, que também tratam os sinais no domínio óptico, permitindo desta forma um sensível aumento na capacidade de transmissão dos dados.

## **2.3 ARQUITETURA DAS REDES**

As fibras ópticas, possuem uma capacidade muito grande de transmissão de dados, o que incentivou as prestadoras de serviços em infra estrutura de telecomunicações a implantarem esta tecnologia em seus *backbones*. A grande questão é, sobre quais tecnologias empregar para explorar de forma mais otimizada possível a capacidade de transmissão de uma fibra óptica e como estas vão interagir entre si.

As principais arquiteturas tecnológicas utilizadas pelas redes ópticas atualmente são: SDH/SONET, ATM, IP-MPLS. Estas arquiteturas serão descritas de forma resumida nesta seção.

### **2.3.1 SDH/SONET**

A Hierarquia Digital Síncrona (SDH) é uma arquitetura desenvolvida pela ITU (*International Telecommunication Union*), já as Redes Ópticas Síncronas (SONET) foram desenvolvidas pela ANSI (*American National Standards*). Estas arquiteturas são baseados em níveis hierárquicos, sendo projetados para trabalharem com enlaces digitais em alta velocidade, que operam sobre a camada óptica.

As arquiteturas SDH/SONET foram desenvolvidas na década de 1980, em substituição as redes PDH ou hierarquia digital plessiócronicas, que foram desenvolvidas na década de 1960 e eram assíncronas, dentre as principais características das redes PDH pode-se citar: O primeiro nível (E1 ou T1) é tratado sob a forma de octetos, os níveis superiores são tratados sob a forma de bits, a duração dos quadros não é uniforme, o alinhamento de quadros é obtido mediante um sinal de alinhamento de quadro e baixa capacidade dos canais de serviço [3]. A Figura 2.6 mostra a estrutura básica da multiplexação PDH.

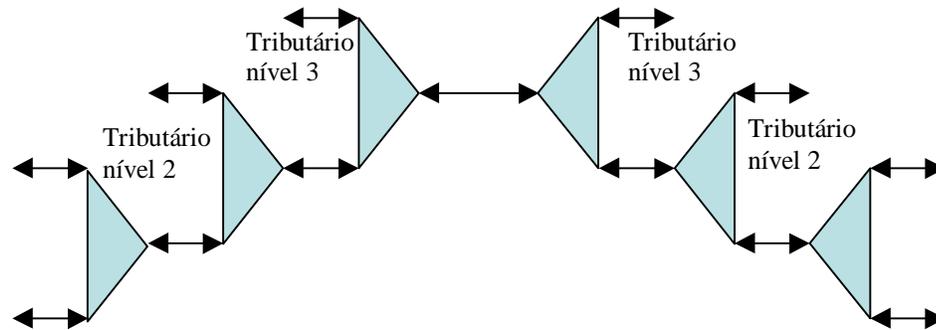


Figura 2.6. Multiplexação PDH.

A Tabela 2.1 mostra as velocidades de transmissão dos diversos níveis hierárquicos denominados de tributários, que no padrão europeu são representados pela sigla E1, E2, etc.. e no padrão americano possuem as siglas T1, T2, etc...

Tabela 2.1. Níveis hierárquicos PDH

Nível	EUA	Europa
T0/E0	64 Kbps	64 Kbps
T1/E1	1.544 Mbps	2.048 Kbps
T2/E2	6.312 Mbps	8.448 Kbps
T3/E3	44.736 Mbps	34.368 Kbps
T4/E4	139.264 Mbps	139.264 Kbps

As redes PDH possuíam inúmeras desvantagens dentre elas pode-se citar: a padronização parcial, dificuldade de inserção e derivação de tributários, além de possuir pouca capacidade de gerenciamento de redes, o que levou operadoras e fabricante a procurarem novos padrões.

As redes SDH/SONET possuem as seguintes características: tratamento em nível de byte, duração do quadro uniforme (125ms), ou seja, o quadro repete-se 8000 vezes por segundo, grande capacidade de supervisão, utilização de ponteiros para identificar os quadros dos tributários e para adaptação de velocidade (justificação) e canais de serviços.

A característica mais importante das redes SDH/SONET é o fato destas serem síncronas e os sistemas síncronos podem ser encarados como o último estágio na hierarquia dos sistemas de transmissão, pois possibilitam a inserção e extração enlaces sem que seja

necessária a demultiplexação. Numa rede em perfeito sincronismo entre todos os enlaces, é possível saber exatamente a que enlace pertence determinado bit, assim como saber onde começa e onde termina o enlace [1].

A Figura 2.7 mostra a estrutura básica para multiplexação SDH/SONET, os bytes vindos dos sinais de tributários são empacotados dentro de um contêiner específico, padronizado pelo Comitê Consultivo Internacional de Telefonia e Telegrafia (CCITT), a cada contêiner são associados bytes que funcionam como rótulos, chamados de POH (*Path Overhead*), cuja função é fazer o gerenciamento de todo o caminho percorrido pelo contêiner, assim como o controle do conteúdo. O conjunto formado pelo contêiner e seu POH é chamado de “contêiner virtual”, que uma vez montado é colocado na área útil do quadro STM-N, chamada de *payload área* [1].

Cada contêiner virtual é associado a um ponteiro cuja finalidade é delimitá-lo este sendo em seguida multiplexado, formando um grupo de unidades tributárias. Esses grupos são reunidos em um grupo de contêineres virtuais, que possui também um rótulo POH. Vários destes grandes contêineres são multiplexados dentro de um grande grupo chamado de grupo de unidades administrativas. Para indicar a posição dos contêineres dentro desse grupo, cada um deles é associado a um ponteiro de unidade administrativa.

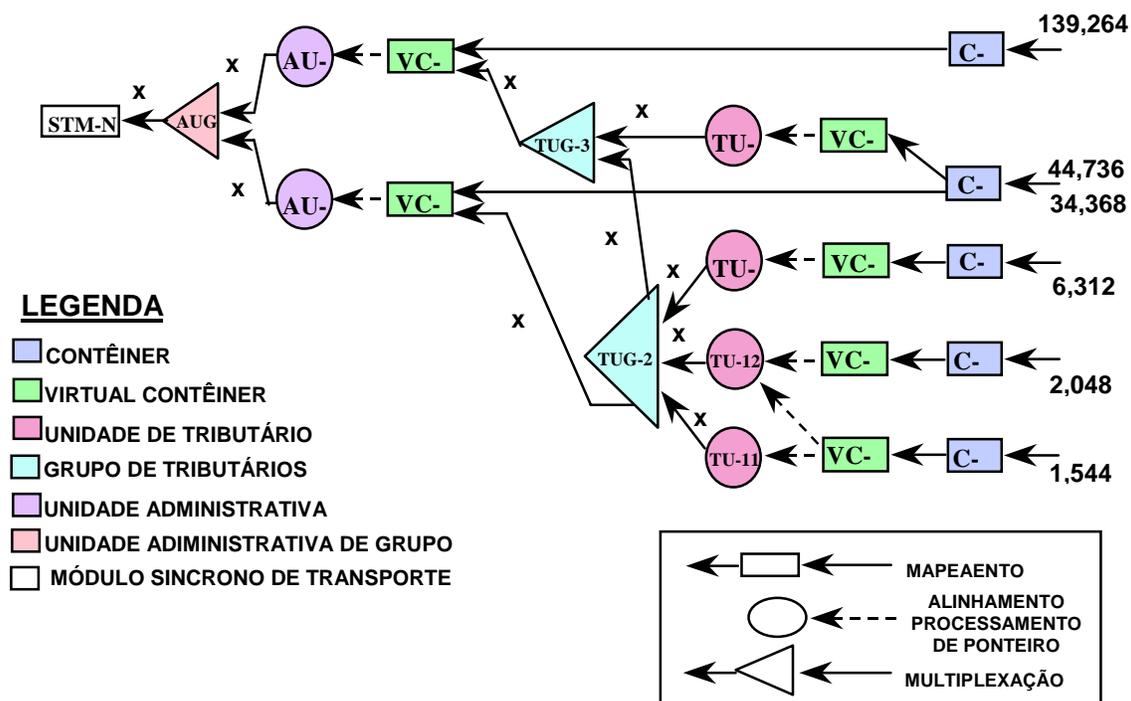


Figura 2.7. Estrutura básica do sistema de multiplexação SDH/SONET [3].

Finalmente, vários grupos de unidades administrativas são intercalados dentro do *payload* do STM-M. Um rótulo de quadro chamado de SOH (*Section Overhead*) é associado ao *payload* e é dividido em duas partes o cabeçalho de seção regeneradora (RSOH) e o cabeçalho de seção multiplex (MSOH). A Figura 2.8 mostra a estrutura de quadro STM.

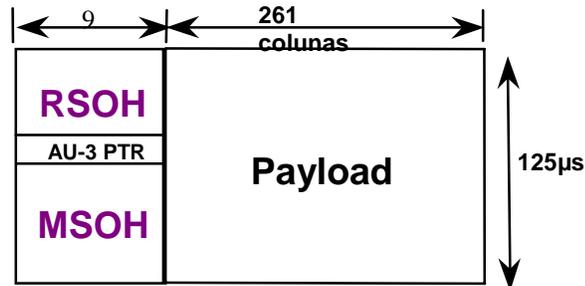


Figura 2.8. Estrutura do quadro STM

A taxa de transmissão básica SDH/SONET é de 155,52 Mbps, que é chamada de STM-1 (*Synchronous Transport Mode-1*) e corresponde ao primeiro nível na hierarquia, a Tabela 2.2 mostra os níveis hierárquicos padronizados SDH/SONET, onde se pode observar que os níveis superiores são múltiplos inteiros da taxa básica.

Tabela 2.2. Níveis hierárquicos SDH/SONET

SONET	SDH	Taxa Mbps
STS-1		51,84
STS-3	STM- 1	155,52
STS-12	STM- 4	622,08
STS-24		1244,16
STS-48	STM- 16	2488,32
STS-192	STM- 64	9953,28

A arquitetura SDH/SONET é composta por quatro subcamadas que serão descritas a seguir:

Camada física: é responsável pela transmissão de bits na fibra incluindo especificações sobre o tipo de fibra óptica utilizada, detalhe sobre potência mínima

necessária, dispersão do sinal transmitido, sensibilidade dos receptores e conversão eletro-óptica dos sinais;

Seção de regeneração: responsável pela criação dos quadros SDH, embaralhamento, controle de erros e é finalizada em cada seção regeneradora da rede;

Seção de Multiplexação: esta camada é responsável por multiplexar várias conexões da camada de caminho em um único enlace entre dois nós. Esta camada é finalizada em cada multiplexador terminal de linha (TM), os nós intermediários são equipados com multiplexadores de inserção/derivação (ADM) ao longo de uma rota de conexão SDH/SONET. A camada de multiplexação é também responsável por realizar certos tipos de comutações de proteção para restaurar serviços em caso de falha nos enlaces;

Camada de caminho é responsável pelo transporte de dados fim-a-fim da sinalização apropriada processada apenas nos terminais [1].

A Figura 2.9 mostra o diagrama das camadas SDH/SONET, maiores detalhes podem ser conseguidos em [1][2][5].



Figura 2.9. Camadas SDH/SONET

### 2.3.2 ATM

O modo assíncrono de transmissão (ATM) é a tecnologia de comutação e transporte das redes digitais de serviços integrados de faixa larga (RDSI-FL), possuindo acesso em alta velocidade para usuários domésticos e comerciais na faixa de 155Mbps a 622Mbps [18].

Esta tecnologia tenta eliminar as limitações das redes síncronas dentre elas: a complexidade de gerência de mapeamento e alocações de canais na hierarquia, o não aproveitamento da banda restante para serviços cujos tráfegos possuem taxas contínuas e inferiores a banda alocada por cada *time slot*, assim como a disponibilidade de bandas por longos tempos muitas vezes sem uso.

A banda passante no ATM é dividida em segmentos fixos de informações chamados de células, que possuem o seu formato ilustrado na Figura 2.10, onde os campos VCI (*Virtual Channel Identifier*) e VPI (*Virtual Path Identifier*), são responsáveis pela comutação das células, através dos comutadores de ATM; o PT (*Payload Type*) indica qual é o tipo de célula; O campo CLP (*Cell Loss Priority*) indica a prioridade da célula para descarte em caso de algum congestionamento em algum nó do meio; o campo HEC (*Header Error Check*) permite a camada física verificar a integridade do cabeçalho, através da verificação de erros na transmissão e o campo GFC (*Generic Flow Control*) serve para dar informações gerais sobre a célula como, por exemplo, se ele está em manutenção ou operação.

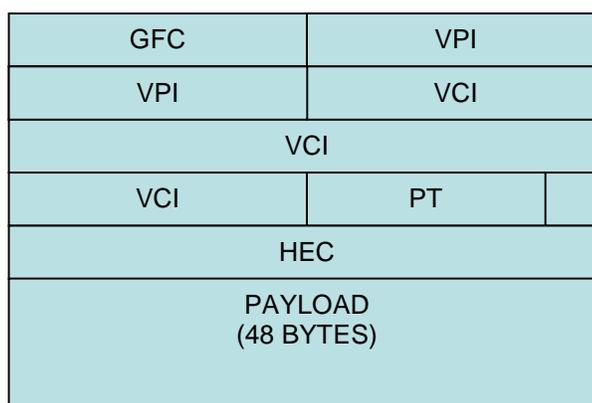


Figura 2.10. Formato da célula ATM.

As células são transmitidas através de conexões com circuitos virtuais que podem ser circuitos virtuais permanentes (CVP) ou circuitos virtuais comutados (CVC) [18]. O fato de poder-se alocar dinamicamente uma determinada quantidade de banda passante é de grande valia para a transmissão de dados cujo tráfego pode ser de rajada, pois não precisa desperdiçar banda nos longos períodos de latência da fonte geradora [19].

A tecnologia ATM é organizada em quatro camadas que são mostradas na Figura 2.11, este modelo utiliza planos distintos a fim de separar funções de usuários, de gerenciamento e controle. O plano de gerenciamento é responsável pela manutenção da rede e execução de funções operacionais, gerenciando os demais planos e a si próprio, o plano de usuário seria responsável pelo transporte de informações do usuário [19].

O plano de usuário é dividido em camadas inferiores e superiores. As camadas superiores são definidas pelas recomendações para RDSI-FL e as camadas inferiores serão descritas abaixo:

A camada física realiza a delimitação de células, controle de erros e acesso ao meio de transmissão;

A camada ATM realiza multiplexação e demultiplexação das células para compartilhamento do meio por canais lógicos, roteamento das células para seu destino, geração e retirada dos cabeçalhos das células e controle de fluxo de transmissão;

A camada de adaptação ATM ou AAL(*ATM Adaption Layer*) interage com as camadas superiores (IP ou aplicações nativas de ATM), existe apenas nos sistemas terminais e possui várias versões diferentes dentre elas: AAL1 para serviços de taxa de bits constantes, AAL2 para serviços de taxa de bits variáveis, AAL3/AAL4 é usado para transporte de dados, encapsulamento das camadas superiores, segmentação e remontagem em segmentos ATM de 48 bytes e AAL5 que é a AAL de baixo custo usado para transporte de datagramas IP [18].

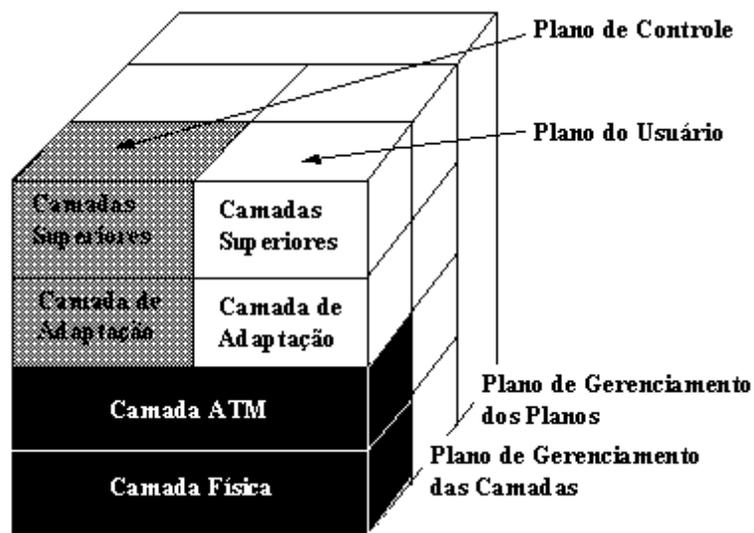


Figura 2.11. Arquitetura do protocolo ATM.

O modelo ATM não necessita de um módulo de gerenciamento centralizado, pois as conexões são feitas por meio de protocolos, usualmente os sistemas de gerenciamento só existirão para prover facilidades centralizadas de monitoração, faturamento, contabilidade e autenticação [14].

A complexidade e os altos custos tornam o ATM um protocolo caro e lento para ser implementado. Soluções mais baratas estão sendo implementadas como o MPLS, que reduz os custos e facilita a integração com a arquitetura IP.

### **2.3.3 TCP/IP**

A arquitetura TCP/IP é a mais utilizada no mundo das interconexões de redes a longa distância [14] sendo o protocolo de redes usado na Internet e nas *Intranets* e basicamente está dividido em quatro camadas mostradas na Figura 2.12, e descrito resumidamente a seguir.

Camada de Aplicação - cuida, das diversas aplicações que usam a rede, assim como padroniza as apresentações de dados e gerência os diálogos existentes entre as diversas aplicações; Camada de Transporte - esta camada é a responsável pelo transporte fim-a-fim dos dados, podendo estes serem confiáveis ou não; Internet - encaminha os datagramas entre as diversas redes; Interface de redes - esta última camada é a que cuida da transferência de pacotes, provendo assim uma comunicação muitas vezes confiável ponto a ponto. Trata do transporte em nível de bits, gerenciando assim as características físicas da rede, uma abordagem mais detalhada de todas as camadas desta arquitetura pode ser conseguida em [11][18].

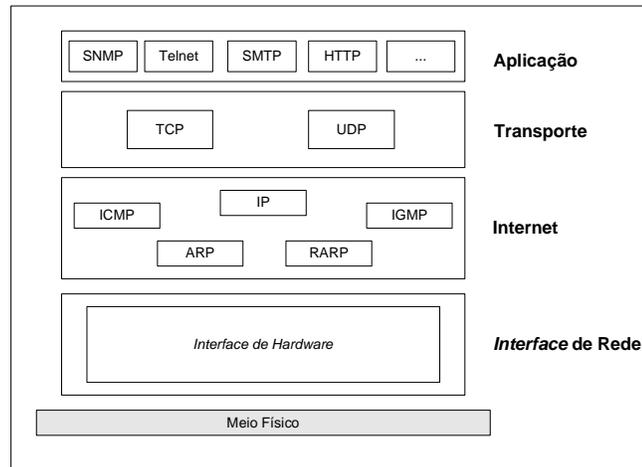


Figura 2.12. Distribuição dos protocolos nas camadas

O Protocolo TCP/IP não oferece qualidade de serviços (QoS) e nem promove engenharia de tráfego que são definidos como:

O QoS consiste em organizar a maneira como o tráfego flui numa rede, buscando evitar congestionamentos gerados pela utilização desigual de recursos desta. O TCP/IP confia nas mensagens dos roteadores para identificar falhas nos enlaces, porém estes são geralmente lentos para responder;

A engenharia de tráfego realiza o mapeamento dos fluxos de tráfego na infraestrutura física de transporte de modo a atender a critérios definidos pela operação de redes [20], a figura 2.13 ilustra o processamento do tráfego em uma rede de comutação de pacotes utilizando o protocolo TCP/IP.

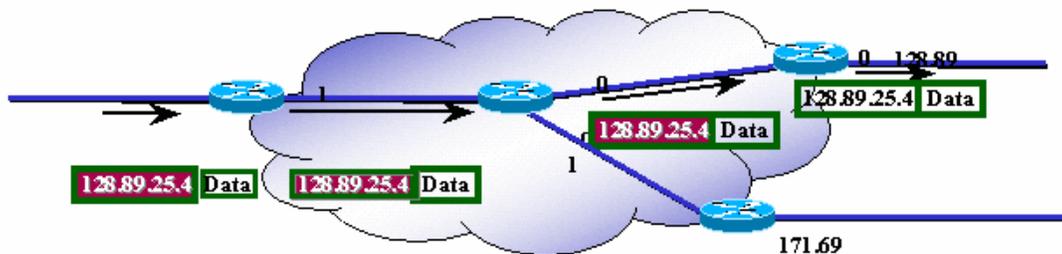


Figura 2.13. Comutação de pacotes baseada no endereçamento IP

## 2.4 MPLS

O MPLS é um conjunto de protocolos desenvolvidos para trabalhar em redes de comutação de pacotes, baseados em comutação de rótulos, esta tecnologia uma vez associada ao TCP/IP melhora o desempenho de suas redes, suportando novas aplicações, implementando QoS e promovendo engenharia de tráfego. A figura 2.14 ilustra uma rede utilizando MPLS, em seguida é dada a definição básica de cada um de seus componentes.

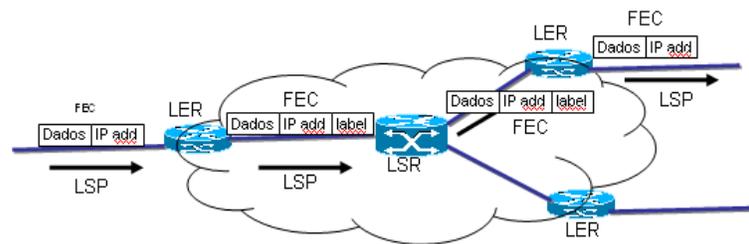


Figura 2.14. Comutação de pacotes baseada no endereço MPLS

*LSR (Label Switching Router)*: são equipamentos de comutação situados no interior das redes, que estão habilitados a comutar pacotes baseados em rótulos;

*LER (Label Edge Router)*: são equipamentos de comutação localizados na periferia da rede MPLS, que interfaceiam com outras redes e são responsáveis pela atribuição e retirada dos rótulos;

*LSP (Label Switch Path)*: é o caminho formado pela seqüência ordenada e unidirecional de LSRs, sendo que o primeiro é chamado de LSR de ingresso e o último de LSR de egresso. Os LSPs são criados através de mapeamento de informação da camada de rede em caminhos comutados da camada de enlace que são realizados através do protocolo *LDP (Label Distribution Protocol)*;

*FEC (Forwarder Equivalency class)*: é um conjunto de pacotes encaminhados da mesma maneira, cada LSP é associado a uma FEC;

*LIB (Label Information Base)*: é a tabela que contém a relação de rótulos e as interfaces que estes estão associados;

*Label*: é um identificador de tamanho fixo de 20 bits, posicionado entre o cabeçalho da camada 2 e o cabeçalho da camada 3, possuindo o formato ilustrado na figura 2.15

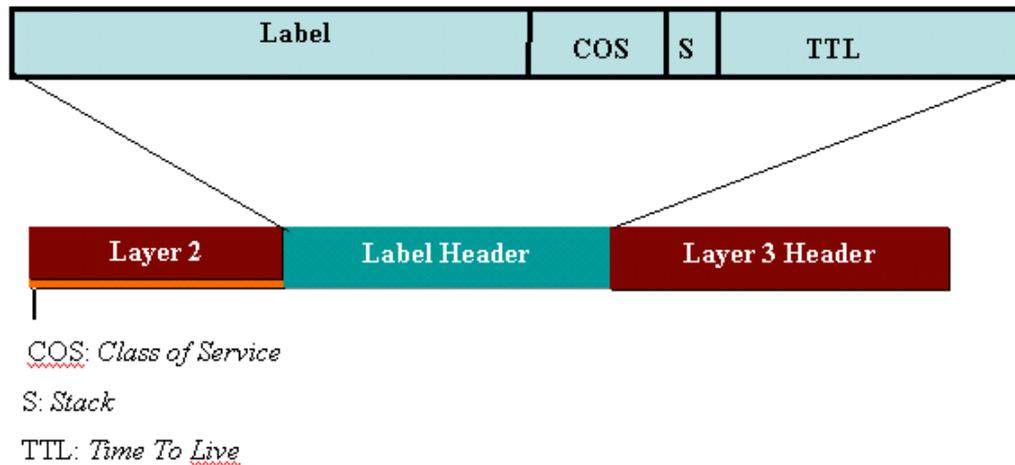


Figura 2.15. Formato do rótulo

O funcionamento do MPLS consiste na entrada de um pacote IP na rede MPLS, o LER de ingresso verifica se este pacote pertence a uma FEC, em caso afirmativo o pacote recebe um *label* que é encaminhado através do LSP associado a FEC, cada LSR busca em sua LIB a entrada correspondente ao *label*, ocorrendo a troca do *label* de entrada pelo *label* de saída associada a FEC do pacote, sendo este pacote encaminhado pela interface indicada na LIB, quando o pacote chega ao LER de egresso o *label* é removido e o pacote IP volta a ser roteado de forma convencional.

Pacotes pertencentes a um LSP podem ser chaveados rapidamente para outro LSP se houver uma falha na rede, garantindo assim uma rápida restauração do serviço. Por isso o MPLS pode ser usado para prover restauração rápida em uma rede IP em caso de falha, o que não é possível através de mecanismos de IP por si só [14].

Dois protocolos de sinalização estão disponíveis para configurar LSPs em uma rede o RSPV (*Resource Reservation Protocol*) e o CR-LDP (*Label Distribution Protocol With Constrained Routing*)[20].

### 2.4.1 GMPLS

O GMPLS é uma extensão do MPLS, que visa otimizar o seu plano de controle podendo utilizar para constituir seus rótulos: divisão de tempo, comprimento de onda e comprimento de espaço, além de permitir o estabelecimento de rotas bidirecionais, o que não é possível com o MPLS. Este trabalho enfatizará o uso do MPLS/GMPLS que utiliza comprimento de onda óptica ( $\lambda$ ) como rótulo. A Figura 2.16 mostra a pilha de protocolos usados no GMPLS:

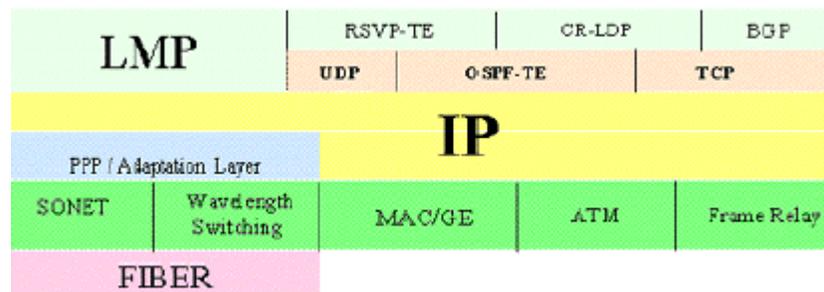


Figura 2.16. Pilha de protocolos usados no GMPLS [24].

São três os principais grupos de protocolos utilizados no GMPLS: o protocolo de roteamento, sinalização e gerenciamento de link.

O protocolo de roteamento é usado para descobrir a topologia da rede automaticamente assim como informar os recursos disponíveis. As principais ênfases do protocolo de roteamento são: informar o tipo de proteção do link, implementar links derivados para prover escalabilidade, aceitar e informar os links com endereço IP e link ID e criar rotas ópticas reservas para diferentes rotas ópticas principais. Os principais protocolos utilizados no protocolo de roteamento são OSPF-TE (*Open Shortest Path First-Traffic Engineer*) e IS-IS-TE (*Intermediate System-to-Intermediate system*) [18].

O protocolo de sinalização é o responsável em prover engenharia de tráfego nos LSPs suas principais funções são: Estabelecimento de LSPs bidirecionais, gera sinalização para estabelecimento do LSP reserva, envia atribuições via o rótulo sugerido, realiza o suporte ao chaveamento do respectivos comprimentos de onda. Os principais protocolos são o RSVP-TE (*Resource Reservation Protocol - Traffic Engineer*) e CR-LDP (*Constraint-Based-Label Distribution Protocol*)[5].

O Protocolo gerenciador de enlaces que atualmente está padronizado é o LMP [6] sendo este responsável pela criação de links virtuais entre dois nós distintos no plano de dados e gerência destes links no plano de controle, verificando a qualidade das conectividades físicas entre nós vizinhos, identificação das propriedades dos nós adjacentes e isolamento de falhas simples ou múltiplas no domínio óptico.

O estabelecimento de um LSP no GMPLS é similar a forma utilizada nas redes MPLS já descrito anteriormente. O grande desafio das redes GMPLS é proporcionar uma restauração de vias com uma performance igual ou melhor que as redes SDH/SONET, no MPLS esta restauração é feita através da pré alocação de um LSP, que serve de reserva para o LSP principal. Uma vez detectada uma falha, o nó de origem utiliza seu mecanismo de roteamento, descartando o LSP principal e roteando seu tráfego para o LSP reserva. Uma outra forma de restauração oferecida pelo MPLS é a alocação de subcaminhos, onde é alocado apenas um link entre dois nós, estas formas de comutação serão mais bem detalhadas no Capítulo 3.

#### 2.4.2 Arquitetura de Redes de Nova Geração

Como visto nas seções anteriores, a tecnologia mais promissora para acomodar o crescimento explosivo de tráfego na Internet e de redes LANs, MANs e WANs é o WDM. Uma fibra óptica possui uma banda teórica de aproximadamente 50 Tbps, usando o WDM esta banda pode ser dividida em múltiplas sub-bandas ou vários canais ópticos.

Atualmente, a maioria das arquiteturas das redes que utilizam o protocolo TCP/IP de longa distância, encapsulam pacotes IP em células ATM transportando pacotes IP em quadros SDH/SONET. Esta superposição de protocolos implica na redução da eficiência além de aumentar custos de gerenciamento e manutenção [15].

Gradativamente as redes ATM foram substituídas pelas redes IP e parcialmente pelas redes SDH/SONET, enquanto os roteadores IP se tornam cada vez mais capazes de prover interfaceamento direto com equipamentos SDH/SONET. O MPLS ajudou a enriquecer as funcionalidades do IP, acrescentando vários recursos de QoS, engenharia de tráfego e simplificando o envio de pacotes. O acréscimo de velocidade nos roteadores IP e

o aumento de capacidade habilitam estes a trabalharem em *backbones* IP de alta performance, usando diretamente canais ópticos como link entre dois roteadores.

A Figura 2.17 ilustra evolução da pilha de protocolos para a arquitetura de redes de nova geração.

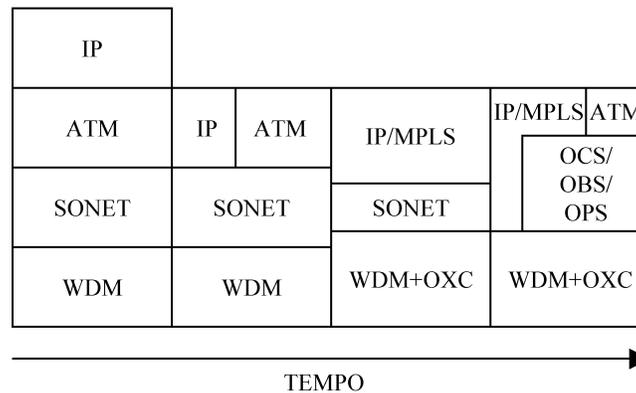


Figura 2.17. Evolução da pilha de protocolo para redes de nova geração [16]

A Figura 2.18 ilustra a arquitetura em camadas para redes de nova geração publicada pela ITU-T, esta arquitetura é dividida em duas hierarquias básicas: a superior que é denominada de hierarquia de transporte digital (Och), que trata do roteamento fim-a-fim dos caminhos ópticos e a inferior ou hierarquia de transporte óptica, que representa as seções de um caminho óptico dentro de uma rede totalmente óptica [21][22].

A hierarquia de transportes digitais está dividida em três sub camadas que serão descritas a seguir:

OCPU (*Optical Channel Payload Unit*): provê suporte para os sinais provenientes dos clientes ex: pacotes IP, células ATM e pacotes *ethernets*.

OCDU (*Optical Channel Data Unit*): responsável em prover a independência da conexão de cada cliente, assim como proteção e monitoração.

OCTU (*Optical Channel Transport Unit*): Provê correção de erros, monitora e protege a seção de multiplexação.

A hierarquia de transporte óptica também é dividida em três camadas são elas:

OCL (*Optical Chanel Layer*): Provê canais ópticos fim a fim entre dois nós suportando clientes com diferentes *payloads*.

OMS (*Óptica Multiplex Section*): Multiplexa os vários canais ópticos em uma única composição para ser transmitido numa única fibra utilizando o WDM, na recepção é feito o trabalho inverso.

OTS (*Optical Transmission Section*): Realiza a transmissão do sinal óptico no tipo específico de fibra.

Uma descrição mais detalhada desta arquitetura pode ser conseguida em [5].

Hierarquia Digital de Transportes	OCPU	IP/GMPLS
	OCDU	
	OCTU	
Hierarquia Óptica Digital	OCL	WDM
	OMS	
	OTS	

Figura 2.18.Arquitetura das redes de nova geração

O modelo atual de redes ópticas para interconexão de redes IP apresenta o ATM ou o SDH/SONET em sua camada óptica. Estas tecnologias apresentam um comportamento pouco dinâmico, pois seu ambiente operacional, baseado em banda fixa é geralmente estabelecido manualmente, e, portanto, não é o mais apto para a dinâmica de conexão e desconexão de canais ópticos.

Os fatores que mais contribuem para o baixo desempenho destas tecnologias são: o processamento eletrônico de pacotes, que insere um atraso a cada nó da rede e o uso ineficiente dos recursos de rede que acarreta indisponibilidade de recursos. O modelo multicamada apresentado na Figura 2.19 é apontado como uma alternativa para atender as dificuldades citadas anteriormente neste parágrafo, uma vez que este utiliza o IP-GMPLS sobre WDM.

Neste novo paradigma de redes ópticas a camada óptica utiliza a topologia física da rede para estabelecer estes caminhos. Este procedimento se baseia, principalmente, na disponibilidade de lambdas nas fibras. O estabelecimento destes caminhos da camada óptica gera uma topologia virtual para a camada IP-GMPLS como mostrado na Figura 2.19. Esta camada, por sua vez utiliza a topologia virtual para estabelecer suas conexões, os

LSPs, que nem sempre correspondem aos mesmos caminhos estabelecidos fisicamente pelo WDM, porém seus destinos são os mesmos [38].

Com a multiplexação de vários canais em uma única fibra-óptica, a ocorrência de uma falha é cada vez mais significativa para a rede, pois a interrupção de uma fibra pode ocasionar falha em diversos serviços oferecidos nos diversos canais que trafegam nesta única fibra. Neste contexto, a sobrevivência a falhas em redes ópticas é questão essencial no projeto e operação destas redes.

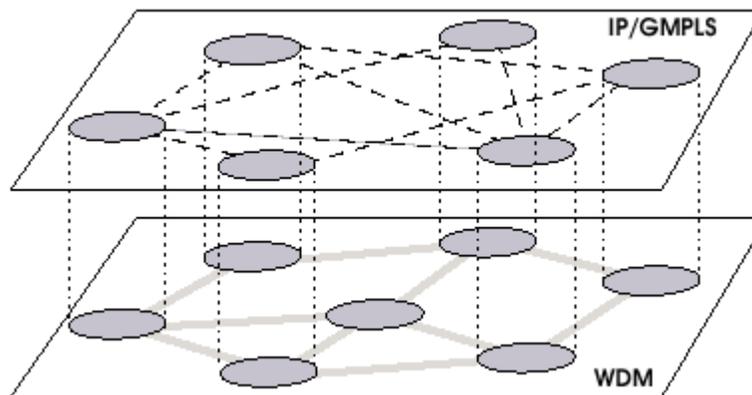


Figura 2.19. Topologia física e virtual [38]

## 2 Comutação Óptica

A função principal de um comutador óptico é fornecer facilidades de comutação para movimentar os dados recebidos por uma porta de entrada através de uma matriz de comutação, para uma ou mais portas de saída. Movimentando assim os dados de um enlace óptico a outro até que eles alcancem seu destino [6]. A Figura 2.20 ilustra o funcionamento básico de um comutador.

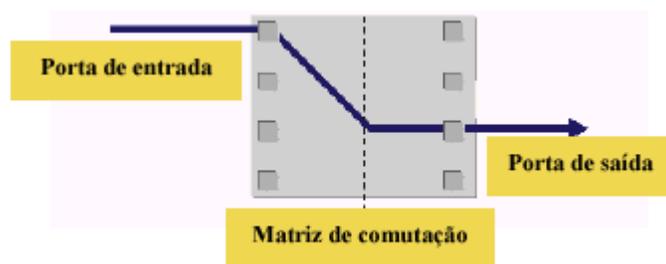


Figura 2.20. Funcionamento básico de um comutador [6].

Os comutadores SDH/SONET, ATM, FDDI e *Ethernet* usados nas redes ópticas atuais, são comutadores eletrônicos com portas de entrada e saída ópticas (OEO). Entretanto a capacidade de comutação eletrônica é da ordem de gigabits por segundo (GBPS), não acompanhando desta forma a transmissão óptica que é da ordem de terabits por segundo (TBPS). Para solucionar este problema é necessário o uso de comutação puramente óptica (OOO), onde tanto as portas de entrada e saída como a matriz de comutação são ópticas, as principais vantagens e desvantagens desta tecnologia são abordadas em [5] e [6].

As redes puramente ópticas baseiam-se em três tipos de comutações com características idênticas as usadas nas redes opacas: a comutação de lâmbdas, a comutação de pacotes ópticos e a comutação de rajadas ópticas.

A comutação de lâmbdas estabelece uma conexão entre dois pontos distintos por um relativo período de tempo, possuindo três fases distintas: o estabelecimento do circuito, transmissão de dados e a liberação do circuito [6]. Este tipo de comutação mantém disponibilizada a conexão entre os dois pontos independente da existência ou não de tráfego. A Figura 2.21 ilustra alguns dispositivos típicos usados neste tipo de comutação, que serão também usados no estudo de caso do Capítulo 4, os ADMs (*Add-Drop Multiplexors*) e os XCs (*Crossconnects*). Um ADM permite a derivação de um tronco multiplexado para uma outra rota, o XC permite roteamento geral de canais entre múltiplos enlaces estes são usados em redes SDH/SONET onde os canais são de capacidade configurável, já o OADM (*Óptical ADM*) e o OXC (*Optical XC*), são usados em canais WDM, onde um canal corresponde a um lambda [6].

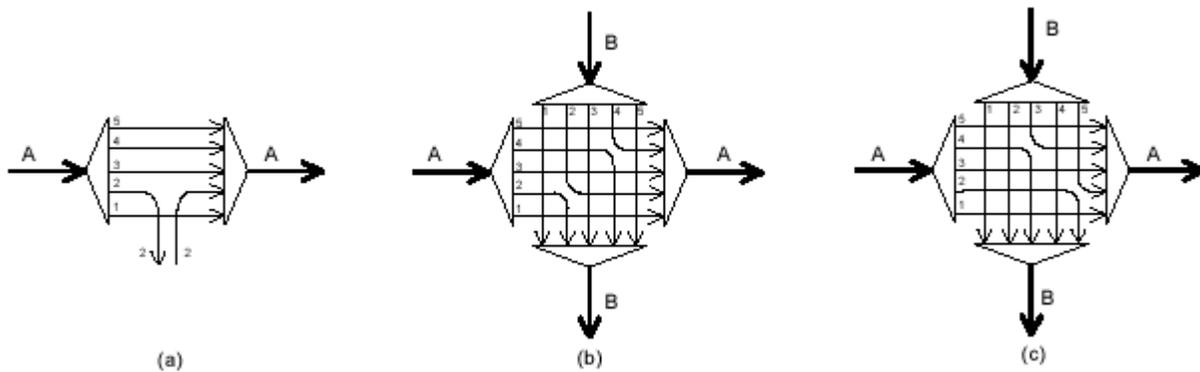


Figura 2.21. (a) um ADM derivando o canal 2 do tronco A com 5 canais; (b) um XC permutando os canais 2 e 4 do tronco A com os mesmos dois canais do tronco B; (c) um XC permutando os canais 2 e 4 do tronco A com os canais 3 e 5 do tronco B [6].

Na comutação de pacotes os dados são transmitidos em blocos de informação com tamanho fixo ou variável chamados de “pacotes” [6], que possuem uma sobrecarga de informação chamadas de cabeçalho cuja finalidade é distinguir um pacote do outro, endereçá-los e fazer verificação de erros. Existem dois tipos de redes de pacote: as orientadas a conexão que funcionam de forma idêntica ao serviço postal e seus pacotes são chamados de datagrama, redes de pacotes não orientadas a conexão são colocados na rede com informação suficiente em seus cabeçalhos para chegarem ao seu destinatário independente destes estarem conectados ou não no mesmo momento em que é enviado, maiores detalhes podem ser encontradas em [5] [6].

A comutação de rajada possui uma granularidade intermediária entre a comutação de circuito e a de pacotes, onde uma rajada é constituída por uma seqüência de pacotes com uma capacidade que varia entre dezenas de quilobytes até centenas de megabytes, na comutação por rajadas o pacote de controle é transmitido antes da rajada, com a finalidade de configurar cada nó ao longo do caminho em que se deseja transmitir o fluxo em rajada, criando assim um caminho virtual. Uma vez concluída a transmissão este caminho será desfeito, e, se por ventura a mensagem não puder ser atendida em algum nó intermediário ao longo do caminho, a rajada de dados será sumariamente descartada. A tabela 2.3 resume as principais características dos três paradigmas.

Tabela 2.3 - Comparação entre os paradigmas de comutação óptica

<b>Paradigma De Comutação Óptica</b>	<b>Utilização Da Banda</b>	<b>Latência</b>	<b>Dificuldade de Implementação</b>	<b>Adaptabilidade</b>
<b>LAMBDA</b>	Baixa	Alta	Baixa	Baixa
<b>RAJADA</b>	Alta	Baixa	Média	Alta
<b>PACOTES</b>	Alta	Baixa	Alta	Alta

### 3 – Tolerância a Falhas em Redes Ópticas

As quatro causas mais comuns de falhas nos sistemas de transmissões ópticos são: erro de roteamento, interrupção de linhas, degradação de desempenho e falhas de hardware. Que são definidas como [1] [5].

A interrupção de linha é causada por um enlace danificado ou uma fibra óptica quebrada, que pode ser ocasionado por uma escavação que interrompe o cabo acidentalmente, subsistência e tremores de terra [27].

Degradação de desempenho corresponde a uma alta taxa de erros causada por acúmulo de *jitter*, baixa potência de recepção, reflexões ópticas devidas as conexões ruins ou a cabos e conectores.

Falhas de *hardware* de elementos de rede, embora os atuais elementos de redes sejam altamente confiáveis é provável a ocorrência de falhas nos complexos dispositivos eletrônicos ao longo de sua vida operacional.

Erro de roteamento corresponde ao roteamento incorreto de caminho dentro de um ADM ou SDXC, problema este que pode ser causado por erro de operação ao ser ajustados caminhos na rede, usando múltiplos sistemas de gerenciamento de configuração, ou resultante de *bug* no *software* de gerenciamento de configuração.

A Figura 3.1 ilustra o impacto causado pela interrupção dos serviços de telecomunicações em relação ao tempo em que estes ficam indisponíveis. Nos primeiros 50 milissegundos, correspondente ao tempo médio de comutação de uma chave comutadora SDH/SONET, OXC ou PXC, a única consequência causada é no alinhamento de quadros, ocorrendo perda de pacotes.

Quando a interrupção atinge 200 milissegundos a qualidade do sinal de voz é comprometido devido a redução gradativa da banda de voz, as sinalizações dos links e LSP's começam a ser interrompidas, iniciando o processo de roteamento dos serviços. Ao final de 2 segundos caem totalmente as chamadas de voz, por serem circuitos dedicados. Em 10 segundos caem os circuitos comutados, linhas privadas, os pacotes X-25 são descartados e começam os primeiros *time-outs* nas sessões de dados.

No final de 5 minutos os circuitos X-25 são desconectados e todas as sessões de dados entram em time-out, até 30 minutos ocorrerá congestionamento da rede e um pequeno impacto social. Apartir de 30 minutos ocorrerá um grande impacto social.

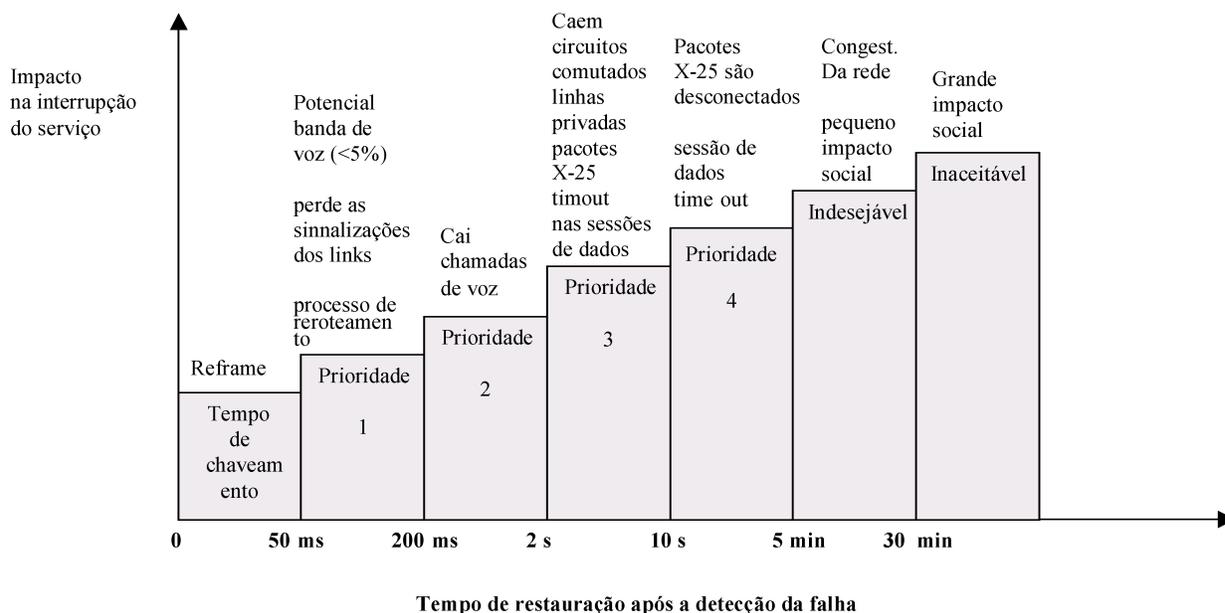


Figura 3.1. Impacto causado pela interrupção de serviço de telecomunicações [27]

### 3.1 Técnicas de Detecção de Falhas

Um dos mais importantes aspectos dos sistemas de telecomunicações ópticos é a sua capacidade de detectar e localizar problemas, assim como descobrir sua causa. As plataformas SDH/SONET incluem mecanismos de detecção e classificação quase imediata de problemas isto é; feito monitorando a integridade do sinal entre os pontos, analisando cada camada da Figura 2.9.

A seguir serão abordadas as várias causas de falhas no transporte de dados num sistema óptico, localização dos problemas, qualidade do sinal e finalmente serão vistos métodos e terminologias para caracterização de cada problema.

### 3.1.1 Detecção de Falhas no Transporte de Dados

Para detectar problemas de transporte de dados num sistema óptico é necessário criar um sistema de supervisão no qual serão levados em consideração os seguintes parâmetros: Supervisão de continuidade do sinal, supervisão de conectividade, supervisão da qualidade do sinal e monitoração de alinhamento.

Supervisão de continuidade do sinal: a supervisão da continuidade do sinal consiste em verificar se o sinal transmitido é recebido com sucesso. A falta de continuidade na camada óptica ou elétrica causa a condição LOS (*Loss of Signal*), tendo como causa a falha no transmissor, ruptura na fibra, falha no WDM, etc...[27]. A perda de supervisão pode ser descoberta usando o alarme AIS (*Alarm Indication Signal*) [27].

Supervisão de conectividade: esta modalidade de supervisão trata de problemas relacionados a má conexão entre dois pontos distintos ocasionando perdas, em fuga de sinal luminoso. Para determinar esta anormalidade é usado o identificador de traços de fuga, sendo detalhado pelo TCM (*Tandem Connection Monitoring*)[27].

Supervisão da qualidade do sinal: a supervisão da qualidade do sinal verifica se o sinal recebido contem erros ou distorções do sinal transmitido, para isto são inseridas técnicas de supervisão como bit de paridade, CRC, FEC etc...

Monitoração de Alinhamento: Quando um sinal TDM é recebido é importante ser verificado o início e o fim de cada quadro assim como seu alinhamento. Quando os sinais são multiplexados juntos na plataforma SDH/SONET os ponteiros precisam ser monitorados os principais alarmes causados por monitoração de alinhamento de quadros são: Alinhamento de quadro e perda de quadro LOF (*Loss of Frame*), Perda de pacotes, Processamento de ponteiros e Perda de ponteiros LOP (*Loss of Pointer*).

### 3.1.2 Localização de Falhas

Uma vez detectado o problema, sua exata localização deve ser identificada para propósitos de pesquisas e reparo. Os mecanismos utilizados para este objetivo são o AIS (*Alarm Indication Signal*) e o RDI (*Remote Detect Indicate*).

O AIS é um alarme de manutenção gerado em uma instância do sistema e propagado para instâncias superiores, conforme seu grau de severidade [1]. O próximo ponto da rede que recebe este AIS retornará para o gerador um RDI, indicando que em sua ponta remota existe um defeito, facilitando assim a localização deste, um estudo mais detalhado destas técnicas podem ser obtidas em [1][27].

## 3.2 Técnicas de Proteção e Restauração

A idéia geral que existe por traz das técnicas de proteção e restauração é a utilização de recursos redundantes como reserva para serem habilitadas no momento em que o circuito primário ou principal em uso falhar. O termo proteção é usado para denotar o paradigma pelo qual um recurso reserva é preparado para restaurar o serviço principal atingido pela falha. Já o termo restauração é usado para denotar o paradigma pelo qual os recursos reservas não ficam dedicados a um determinado circuito primário, porém com uma grande disponibilidade para substituir o circuito principal na hora em que este apresentar qualquer irregularidade.

Os parâmetros básicos que definem a qualidade dos mecanismos de proteção e restauração dos circuitos são: Confiabilidade, Robustez, Largura de banda eficiente, Tempo de regeneração e Interoperabilidade. Um estudo mais detalhado sobre estas características pode ser obtido em [27].

Os mecanismos de proteção e restauração em redes ópticas apresentam-se em três técnicas distintas são elas: Proteção Linear, Proteção Baseada em Anel e Proteção em Malha ou *Mesh*.

### 3.2.1 Técnicas de Proteção Linear

A Proteção Linear é o mais rápido e eficaz dos mecanismos de proteção, podendo apresentar-se de duas formas, a primeira é a proteção 1+1 como mostrado na Figura 3.2(a),

onde, para cada circuito principal existe um circuito reserva escravizado, para quando falhar o principal o reserva assumir o tráfego automaticamente, num tempo máximo de 50ms.

A segunda forma de proteção linear é a conhecida como "Proteção Linear 1:N", onde 1 corresponde ao link de proteção ou reserva utilizado, já o N corresponde ao número de circuitos primários existentes, que são comutados para o circuito reserva seguindo uma ordem de prioridade no caso de mais de um circuito principal falhar.

A terceira forma de proteção linear ilustrada na Figura 3.2(b) é chamada "Proteção Linear M:N" onde M é o número de circuitos reservas e N são os circuitos principais, sendo que cada M e N possuem um número de identificação ou ID que permite estabelecer uma ordem de prioridade de comutação dos circuitos N para o circuito M, no caso de  $M < N$ .

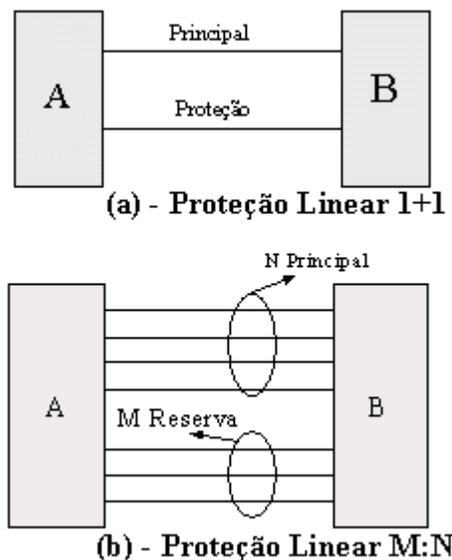


Figura 3.2. Tipo de proteção linear

As principais vantagens dos mecanismos de proteção linear são a alta disponibilidade dos circuitos reserva e o baixo tempo restauração dos serviços.

### 3.2.2 Técnicas de Proteção em Anel

A proteção em anel possui capacidade própria para realizar a proteção das vias de transporte, com a utilização de ADM (Add Drop Multiplexer), possibilitando inclusive o tráfego de IP diretamente sobre o sistema.

Existe uma tendência muito grande de se utilizar largamente este mecanismo, por ser o mesmo utilizado nas redes SDH/SONET com SNCP(*Subnetwork Connection Protection*). A recepção dos sinais ópticos principal e de proteção fica disponível o tempo todo. Ocorrendo uma interrupção no tráfego principal este é automaticamente comutado para a via de proteção. O tempo de comutação é menor que 50 ms [2], possibilitando assim um desempenho melhor que o sistema de proteção linear, por possuir um número maior de vias de proteção, a Figura 3.3 permite visualizar a estrutura básica deste mecanismo[28].

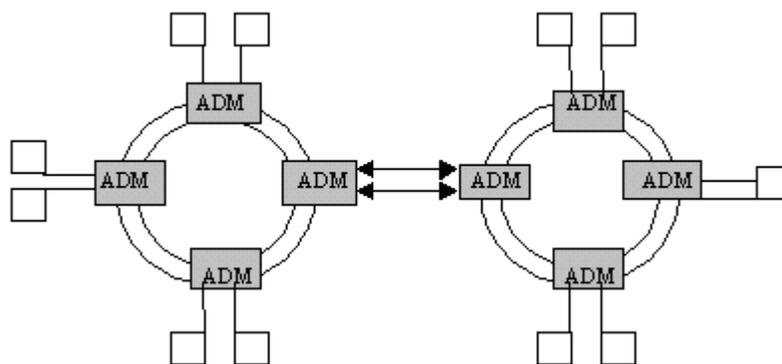


Figura 3.3. Proteção em anel

Para a escolha do tipo de configuração em anel, deve-se considerar a facilidade de planejamento, reconfiguração e principalmente da topologia do tráfego a transportar. A eficiência no reuso de frequência depende também do mesmo fator, um estudo detalhado sobre as redes em anel pode ser obtido em [1][27].

### 3.2.3 Processamento de uma Comutação em Sistemas Lineares e Anel

A chave automática de comutação pode ser acionada devido a detecção de uma falha de sinal, ou comando externo enviado pelo módulo central de gerenciamento. O tempo de comutação é de aproximadamente 50ms, após a comutação um indicativo de PSE (*Protection Switch Event*) deve ser reportado ao módulo central de gerenciamento.

O restabelecimento da comutação é feito logo após a resolução do problema na seção defeituosa, para poder permitir que outros canais principais possam fazer uso do canal reserva. Geralmente, no caso do restabelecimento da comutação, é incrementado um período chamado WTR(*Wait-to-Restore*) aproximadamente de 5 a 10 minutos

(programável) para evitar comutações em tempos muito reduzido e o conseqüente desgaste da chave.

#### 3.2.4 Técnicas de Proteção em Malha

Com a expansão das redes SDH/SONET, a combinação de chaves digitais síncronas "*cross connects*" (OXC e PXC) de alta velocidade e interconecção óptica passaram a formar o núcleo das redes.

As chaves "*cross connects*" são conectadas em uma malha para prover diversidade de rota. O arranjo mais simples é o de três chaves conectadas. Se o enlace direto de uma chave para outra falhar, a rota alternativa através da terceira chave ainda estará disponível e mudanças de roteamento do agregado serão possíveis em milissegundos. Esta topologia será melhor detalhada ainda neste capítulo na Seção 3.4.

### 3.3 Trabalhos Correlatos

Devido a grande importância dada a tolerância a falhas em redes ópticas de nova geração os estudos voltados a este assunto estão sendo muito investigados pela comunidade científica, uma vez que já começam a ser encontrados vários artigos e dissertações que discutem o assunto. Esta seção apresenta alguns trabalhos relacionados ao tema abordado nesta dissertação.

Bicudo em [38] propõe um novo um mecanismo de sobrevivência que visa oferecer uma maior flexibilidade a rede no atendimento aos requisitos de sobrevivência e, conseqüentemente, tornando-a mais adaptada às necessidades do usuário. A probabilidade de bloqueio e a disponibilidade de conexões são utilizadas como métrica de desempenho da rede. O mecanismo proposto adiciona a configuração da rede um parâmetro chamado fator de relaxação de restrições SRLG (*Shared Risk Link Group*). Através do ajuste dessa variável é possível controlar o compromisso entre o ganho da probabilidade de bloqueio e a perda de disponibilidade. Os resultados da conectividade da rede mostram que o custo de uma rede mais conexas, associado à instalação de enlaces ópticos, é recompensado pelos ganhos tanto na probabilidade de bloqueio quanto na disponibilidade. Nas simulações de reversibilidade, os resultados mostram que os mecanismos não reversíveis, ao contrário do

que se previa, podem resultar em melhor disponibilidade, dependendo somente do tempo de comutação entre os canais ópticos, primário e de proteção, que constituem uma conexão óptica.

Em [25] é apresentado um ambiente de desenvolvimento de agentes inteligentes baseados em Redes Neurais Artificiais aplicados a gerência pró-ativa de redes IP, MPLS e GMPLS, denominado RENATA 2, objetivando prever situações problemáticas em enlaces que utilizam o protocolo GMPLS, devido a ausência de mecanismos de re-roteamento rápido destinados a falhas em *links* ópticos neste protocolo, aproximando com isto a forma de restauração de falhas 1:N da forma 1+1, proporcionando desta forma redução dos custos e aumento na confiabilidade.

O artigo [39] explica que pode ser muito benéfico explorar a funcionalidade dos mecanismos de recuperação em redes que utilizam IP-GMPLS sobre WDM, para otimizar significativamente a eficácia de custos da recuperação de falhas em ambas as camadas, cruciais para alcançar as exigências elevadas das disponibilidades de serviços críticos. Diversos estudos de caso práticos ilustram este artigo e destacam as oportunidades e os desafios a serem enfrentados.

Outro trabalho correlato que merece destaque é o artigo [41], que apresenta uma heurística para projeto de redes ópticas, buscando encontrar uma topologia virtual baseada em anéis disjuntos com o objetivo de minimizar o congestionamento, levando em consideração sua sobrevivência a falhas. É apresentada e comparada com estratégias convencionais e os resultados mostraram que a estratégia proposta consegue obter melhores valores de congestionamento, reduz o esforço computacional e garante alternativas para o roteamento em caso de falhas.

Nossa proposta se diferencia das demais apresentadas aqui, por apresentar uma análise comparativa aprofundada dos mecanismos de tolerância a falhas, entre as redes SDH/SONET e as redes de nova geração com plano de controle baseados em IP-GMPLS/WDM. A partir desta análise apresentamos também uma proposta de adoção de diferentes mecanismos de tolerância a falhas em função do tipo de tráfego utilizado.

Outro diferenciador de nosso trabalho foi realizar duas experiências distintas, sendo a primeira utilizando uma rede *testbed* toda implementada na arquitetura

SDH/SONET, abrangente em todo território brasileiro e explorado por uma empresa prestadora de serviços de telecomunicações. A segunda experiência simula a mesma planta utilizada na experiência anterior no *software* NS toda implementada em redes de nova geração com plano de controle baseado em IP-GMPLS/WDM.

### 3.4 Modelo de referência adotado

Esta dissertação abordará a topologia em malha em maiores detalhes, assim como a comutação de lambdas para o estudo de redes de alta velocidade usando IP-GMPLS, como mostrado na Figura 3.4.

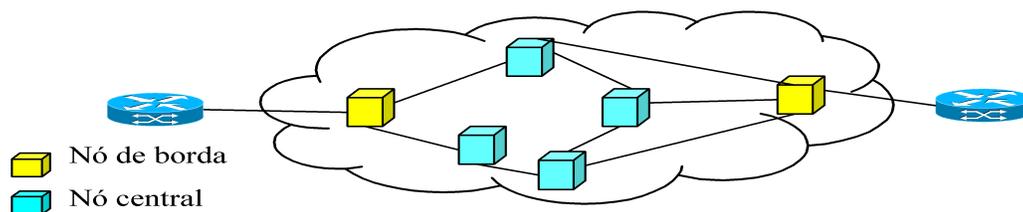


Figura 3.4. Rede em malha

Uma rede óptica em malha é formada por um conjunto de nós conectados entre si. Estes nós são divididos em dois grupos principais que são os nós "centrais" que se localizam no interior das redes e os nós "borda" que ficam localizados nas extremidades e servem como interface com outras redes ou roteadores de clientes que suportam IP-MPLS em muitos casos [5]. Dependendo do modelo de serviço adotado, cliente-servidor ou integrado [5], a interação entre o plano de controle das redes IP e das redes ópticas poderá ser, respectivamente, menos ou mais estreita [5][8][7][20][27]. Existem dois modelos básicos considerados: o modelo de pares (*peer*) e o sobreposto (*overlay*).

No modelo sobreposto, o domínio IP age como um cliente do domínio óptico e as redes ópticas fornecem "conexões" para o domínio IP. O roteamento IP-GMPLS, a topologia de distribuição e os protocolos de sinalização IP são independentes dos esquemas de roteamento, topologia de distribuição e sinalização na camada óptica (ver Figura 3.5). Na verdade, este modelo é conceitualmente similar ao IP sobre ATM clássico, só que

aplicado diretamente sobre inter-redes ópticas. Este modelo pode ser fornecido estaticamente usando um sistema de gerenciamento de rede ou pode ser fornecido dinamicamente.

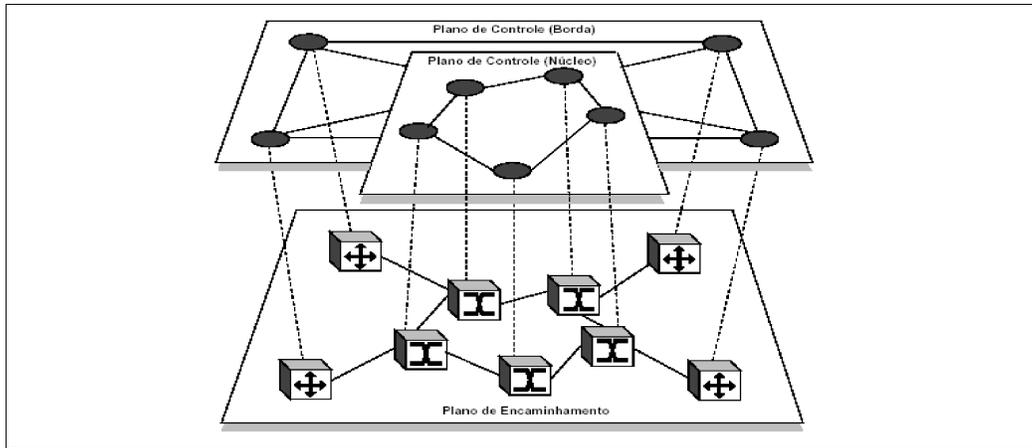


Figura 3.5. Modelo de sobreposição (“overlay”) [20].

No modelo de pares (Figura 3.6), os dois domínios são integrados para serem gerenciados de forma unificada. Os roteadores IP e os comutadores ópticos agem como pares de modo que apenas uma instância de protocolo de roteamento e um plano de controle existam para os dois domínios. Quando existe apenas um domínio administrativo envolvido, um único protocolo intra-domínio (“*Interior Gateway Protocol-IGP*”), como OSPF ou IS-IS, com as extensões apropriadas, pode ser usado para trocar informações topológicas. Quando diversos ASs estão envolvidos, protocolos de roteamento e sinalização inter-domínio são necessários. Supõe-se, logicamente, que no modelo de pares os comutadores ópticos e os roteadores possuam um esquema de endereçamento comum (e.g. endereços IP).

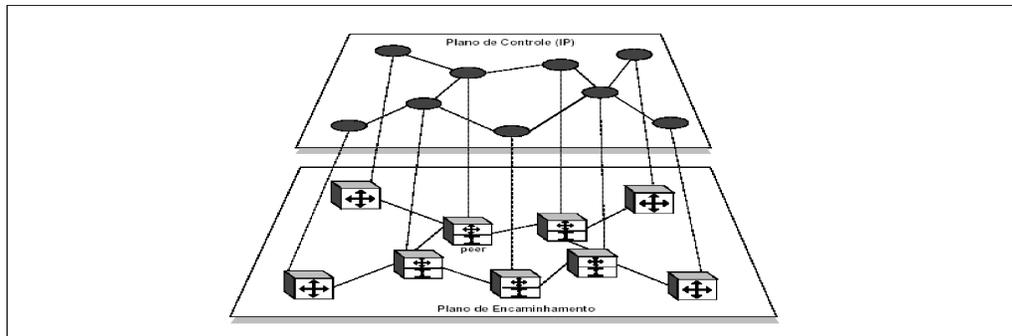


Figura 3.6. Modelo de pares (“peer”) [20].

Existe ainda o modelo aumentado, que nada mais é do que um meio termo entre os dois modelos anteriores. Nele existem instâncias separadas de protocolos de roteamento sendo executadas nos domínios ópticos e IP. Contudo, neste caso, informações de rotas são trocadas entre as duas instâncias através de um protocolo padrão. Por exemplo, os endereços IP poderiam ser atribuídos aos dispositivos ópticos, bem como transportados pelos protocolos de roteamento óptico para permitir que informações de alcançabilidade fossem compartilhadas.

De uma forma geral, o que se pode observar a partir dos modelos de interação propostos é que o modelo de pares é a melhor alternativa para o futuro, oferecendo escalabilidade e fácil interoperabilidade. Contudo, ele atualmente ainda é inviável. Para este início de transição o modelo viável é o de sobreposição, enquanto o modelo aumentado atenderia a uma etapa intermediária, antes de ser possível implementar o modelo de pares. É interessante observar que o plano de controle do GMPLS suporta o modelo de sobreposição, o modelo de pares, assim como o modelo aumentado. Na verdade, o GMPLS é apropriado, tanto para controlar cada camada independentemente em futuro próximo como oferece uma solução elegante que facilitará o desenvolvimento de futuros modelos. Neste trabalho, como estamos considerando o uso de redes de nova geração puramente ópticas, adotaremos o modelo de pares, onde a integração entre o plano de controle IP e óptico é mais estreita.

### 3.5 Plano de Controle

Como ilustrado na Figura 3.7, conceitualmente cada nó é formado por duas unidades distintas: o plano de controle e o plano de dados. O plano de controle é um conjunto de *softwares* e *hardwares* usados para controlar operações vitais das redes como alocação de banda, descoberta de rotas e tolerância a falhas [5]. O plano de dados é a unidade que cuida do transporte dos dados sendo constituído basicamente pelas chaves comutadoras e pelo dispositivo multiplexador WDM.

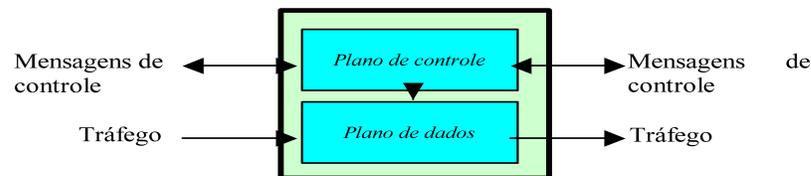


Figura 3.7. Plano de controle

A troca de sinalização entre dois nós vizinhos é feita através da troca de mensagem de controle entre estes através de um canal dedicado e fora da banda de transmissão de dados, possuindo um comprimento de onda pré-configurado para transmitir dados de forma confiável usando, por exemplo, o TCP. Este canal é normalmente chamado "canal de controle" [7].

A Figura 3.8 mostra o diagrama básico de um plano de controle sugerido por Xin al [7], que utiliza os recursos do MPLS/GMPLS e seus módulos serão descritos a seguir. O módulo principal realiza o processo de inicialização e interação entre os três outros elementos que constituem o nó.

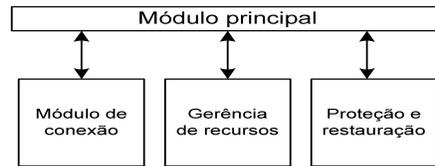


Figura 3.8. Diagrama do plano de controle.

### 3.5.1 Gerência de Recursos

O módulo de gerência de recursos – RMM (*Resource Management Module*) possui a finalidade de descobrir e manter rotas assim como dar suporte à QoS e RWA (*Routing Wavelength Assignment*). As informações necessárias são obtidas a partir de duas tabelas: a TCM (*Topology Connectivity Matrix*), que enumera todos os nós da rede e suas respectivas disposições e a LRT (*Local Resource Table*) que possui informações do nó local como: a identificação ID do mesmo, suas respectivas portas e o rótulo( $\lambda$ ) atribuído a cada porta.

Caso ocorra uma falha em um enlace ou nó, este poderá ser recuperado utilizando um dos seguintes mecanismos: Proteção de LSP (*1+1 LSP Protection, 1:1 LSP Protection*), Proteção de enlace (*1+1 Link Protection, 1:1 Link Protection, 1:N Link Protection*), Restauração de LSP (*End-to-end LSP Restoration with Re-provisioning*), Otimizado (*Enhanced*) e Tráfego Extra (*Extra Traffic*) [30][31][32].

O mecanismo de proteção de LSP 1+1 faz uso de um LSP redundante por onde trafega uma cópia do fluxo de dados do LSP principal. Na ocorrência de uma falha o LSP redundante assume o papel de principal. Na abordagem proteção de LSP 1:1 cria-se um caminho dedicado alternativo, simultaneamente ao estabelecimento do LSP principal, por onde os dados serão enviados se o LSP principal estiver inoperante.

No mecanismo de enlace 1+1 um enlace auxiliar recebe uma cópia dos dados que trafegam no enlace que está sendo protegido e o nó de saída decide de qual deve receber o tráfego. Na técnica de proteção de enlace 1:1, um enlace alternativo previamente estabelecido é utilizado em caso de falhas. Na proteção de enlace 1:N existe 1 enlace de reserva compartilhado entre N enlaces ativos.

O mecanismo Otimizado (*Enhanced*)[7] define que outros mecanismos, como anéis de proteção, devem ser utilizados para assegurar um grau de confiabilidade mais elevado do que um esquema 1+1. No mecanismo de Tráfego Extra [7], um LSP pode ser estabelecido a partir de recursos que estão protegendo outros tráfegos, sendo que na ocorrência de falhas este LSP pode sofrer preempção. No esquema de restauração de LSP, uma nova rota é calculada somente após a ocorrência da falha sem nenhuma garantia acerca da existência de recursos para o estabelecimento dessa nova rota.

### 3.5.2 Módulo de Conexão

A principal função do módulo de conexão – CM (*Connection Module*) é realizar a manutenção e gerar sinalização entre os nós. Cada nó possui uma tabela de enlaces – LT (*Link Table*), que é mantida pelo módulo de conexão para monitorar todos os enlaces ópticos (origem, destino e passagem) sobre o OXC. A Figura 3.9 mostra uma LT. A identificação do link é feita por um número único na rede o link ID, que identifica o nó de origem, nó de destino e número de seqüência. O número de seqüência identifica o nó dentro de um enlace, caso este seja um nó de passagem. Os atributos de status indicam o estado do enlace (criação, reserva, ativo ou deletado). O QoS *Type* indica o tipo de tratamento a falha utilizado. O input, output port ID representa o ID entrante e saínte do link no OXC. O lambda ID indica qual o comprimento de onda designado para label GMPLS no respectivo enlace.

Link ID			Status	QoS Type	Input Port ID	Output Port ID	λ ID
ORG Nó ID	DEST Nó ID	SEQ NUM					

Figura 3.9. Exemplo de LT

A sinalização de um enlace óptico é desenvolvida através do modelo salto a salto. Quando o módulo principal do plano de controle de um determinado nó de borda recebe uma solicitação de um cliente, esta solicitação é transferida para o módulo de proteção e restauração, onde os atributos de tratamento a falhas são extraídos do solicitante, o módulo de proteção e restauração solicita ao módulo de gerência de recursos que

implemente o tipo de tratamento a falhas solicitado para implementar RWA, sendo criada para cada enlace conectado a este nó, uma mensagem de solicitação de conexão, que é incluída numa tabela LT. A lista de enlaces principais e reservas são também incluídas na mensagem. Esta mensagem é processada salto a salto até chegar no nó de borda a que se destina, o qual envia então um ACK de retorno para o nó de origem. Caso ocorra um problema no enlace entre origem e destino, será enviado um NAK para o nó de origem.

Para cada salto, o canal óptico de controle pode operar em duas fases: a primeira é a de reserva/liberação de recursos e a segunda é a de transferência de estado. Na reserva de recursos o canal de controle reserva o comprimento de onda luminosa, disponibilizando o enlace no momento necessário, adotando o seguinte procedimento: determina a porta de entrada e saída através de mensagem de controle do nó e verifica se o tratamento de falhas é baseado em proteção de LSP, proteção de enlace ou restauração de LSP, para realizar as adaptações necessárias. Caso o comprimento de onda esteja reservado, compara-se a lista de enlaces ou LSPs que estão em tráfego através das mensagens de controle com os comprimentos de onda reservados para uma possível falha, se esta lista conflitar, adiciona-se a lista o comprimento de onda designado.

O processo de transferência de estado é invocado quando o módulo de conexão recebe um ACK ou NAK de um enlace em que possui um nó interrompido. A Figura 3.10 mostra um diagrama contendo as transferências de estados em um enlace óptico. Após a sucessão dos recursos de reserva, o CM aloca uma LT e determina todos os atributos na entrada com os atributos destinados a criação. Quando um módulo de conexão recebe um ACK confirmando que um enlace em que houve queda normalizou, o estado do atributo é colocado para ativo ou reservado dependendo de qual é o enlace principal. A proteção do enlace em reserva de estado é ativa quando o módulo de proteção e restauração detecta uma falha no enlace principal e invoca o processo de proteção. Quando o CM recebe um NAK de um enlace com um nó interrompido durante o processo de inicialização, ou se houver solicitação de um aborto de mensagem após o enlace ser estabelecido, o recurso irá se atualizar e a entrada associada na LT irá ser apagada.

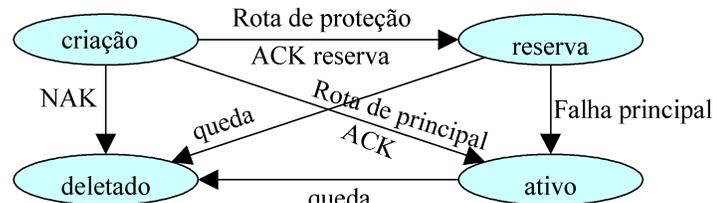


Figura 3.10. Diagrama de estados

### 3.5.3 Módulo de Proteção e Restauração

O módulo de proteção e restauração – PRM (*Protection and Restoration Module*) é responsável por iniciar e coordenar a proteção de um enlace óptico, realizando detecção e notificação de falhas, restaurando o enlace, selecionando e atuando no local onde ocorreu a interrupção, para prover rápida recuperação entre dois pontos mesmo sem localizar o enlace ou nó defeituoso.

Quando o enlace de um determinado cliente é interrompido, esta falha é percebida pelo módulo principal e é transferido para o módulo de proteção, então este chama o módulo de recursos através do protocolo RWA, com os parâmetros de QoS extraídos do cliente. Para cada enlace, uma mensagem de solicitação de conexão é criada e o módulo de conexão é invocado pelas sinalizações do módulo de proteção. Se o cliente solicitar proteção, a sinalização de dados e proteção do enlace será invocada em paralelo pelo módulo de proteção que trabalha sempre com reconhecimento de ACK ou NAK, que são gerados pelo plano de controle de dois nós distintos. Apenas se ambos os sinais de dados e proteção nos enlaces tiverem iniciados com o módulo de controle enviando um ACK para o cliente. De outra forma quando um dos dois enlaces falha na inicialização, o módulo de controle envia um NAK para o cliente. Se outro enlace estiver sendo iniciado, este será usado para substituir o que falhou.

O módulo de proteção e restauração é também responsável pela detecção de falhas, proteção e restauração que são feitas pela detecção de alguma anormalidade prejudicial. No plano de controle o mecanismo de descoberta de falha no nó vizinho é usado para detectar falha de um enlace via troca periódica de ACK, NAK. Uma falha no nó pode ser dividida entre falha no XC ou no plano de controle. Uma falha no XC pode ser detectada pelo plano

de controle diretamente através do mecanismo de hardware. Uma falha no plano de controle pode ser detectada indiretamente através do mecanismo de detecção de falha dos nós vizinhos. Se um plano de controle falha, todos os vizinhos não receberão a mensagem de sinalização do nó interrompido. Como resultado, todos os planos de controle vizinhos irradiam uma mensagem informando a nova topologia para o restante da rede. Depois de conhecida a nova topologia, todos os planos de controle passarão a trabalhar sem contar com aquele que se encontra defeituoso.

Depois de sanada a falha o plano de controle irá enviar uma mensagem para cada enlace afetado pela transmissão chamada de FIS (*failure indication signal*) em direção ao nó de origem. Esta notificação é enviada salto a salto rumo ao nó de origem. Uma vez que o plano de controle de origem recebe o FIS, este checará os atributos de tolerância à falha, fazendo todas as adequações.

#### 4- Estudo de Caso

Objetivando validar a análise comparativa e consolidar a proposta feita por este trabalho, foram realizados dois tipos de testes distintos: no primeiro teste foram provocadas situações de falhas utilizando um *testbed* real todo implementado em redes SDH/SONET, que é parte integrante de um *backbone* óptico utilizado por uma operadora de telecomunicações com abrangência em todo território nacional. O segundo tipo de teste consistiu na simulação de várias situações de falhas neste mesmo *backbone* implementado no *software* NS-2 [15], onde foram estudadas e desenvolvidas novas funcionalidades para analisar os impactos promovidos pelos mecanismos de proteção e restauração de falhas utilizando o protocolo IP-GMPLS sobre redes WDM, pois trata-se de uma proposta acadêmica ainda não explorada na prática.

A Figura 4.1 ilustra o *backbone* real citado no parágrafo anterior, este *backbone* a grosso modo é constituído por 64 nós, distribuídos entre repetidores e estações terminais. Sendo que os repetidores possuem a função de amplificar o sinal óptico ao longo de todo o percurso exigido por um enlace da origem até seu destino, já as estações terminais possuem a finalidade de multiplexar, demultiplexar e processar os sinais ópticos.

Estes nós estão interligados entre si por fibras ópticas monomodo com capacidade teórica de transmissão de até 50Tbps, sendo a ocupação de sua banda determinada pelos multiplexadores SDH/SONET existentes nas estações terminais. Estas fibras estão distribuídas ao longo do território brasileiro através de ferrovias, rodovias, cabos submarinos e cabos aéreos utilizando linhas de distribuição de energia onde são abrigados no cabo de aterramento, por esta razão são identificados pela sigla OPGW ("*Optical Ground Wire*").

Para realização dos testes de tolerância a falhas nos dois contextos que pretendemos avaliar, foram escolhidas os seguintes mecanismos de proteção a falhas já descritas no Capítulo 3, que são: Proteção de LSP (*1+1 LSP Protection*, *1:1 LSP Protection*), Proteção de enlace (*1:1 Link Protection*) e Restauração de LSP (*End-to-end LSP Restoration with*

*Re-provisioning*). Esses esquemas foram escolhidos por apresentarem os resultados mais representativos.



Figura 4.1. Backbone óptico de longa distância [35]

#### 4.1 Cenário de Testes Realizados na Rede *Testebed*

Para realização do primeiro conjunto de testes foi necessário utilizar um roteador de borda "Cisco 1700", com porta serial WAN obedecendo ao padrão V-35 estabelecida pela ITU-T e velocidade de 2048Kbps, conectado a um analisador e monitor de redes WAN.

Para analisar o impacto causado no rompimento de uma fibra óptica em um sistema redundante que utiliza proteção em anel na plataforma SDH/SONET, utilizou-se o analisador e monitor de redes WAN "*DA-3200 Data Network Analyzer*" fabricado pela "*Acterna*" [29].



Figura 4.2. DA-3200 Data network analyzer [29]

As principais características deste instrumento são: rápida identificação de problemas numa rede WAN, trabalha com protocolos PPP, HDLC, Frame Relay, PRI; faz análise de tunelamento, trabalha com multi interfaces físicas, realiza análise completa nos sete níveis da arquitetura OSI, geração de tráfego Frame Relay, análise em tempo real e captura eventos ocorridos para posterior análise, geração de históricos e relatório de análise de tráfego. Maiores detalhes sobre este instrumentos podem ser obtidos em [29].

A Figura 4.3, ilustra o mesmo *backbone* exposto na Figura 4.1 porém esse é apresentado através do visualizador *Network Animator* (NAM), que acompanha o pacote do NS, para facilitar a ilustração do comportamento do *backbone* durante os testes. Todos os nós desta rede foram configurados para nós centrais (*core*) e numerados de 0 a 24, foram escolhidos apenas os 25 nós mais significativos dentre os 64 que totalizam a rede, facilitando desta forma a compreensão do estudo e posteriormente as simulações no NS.

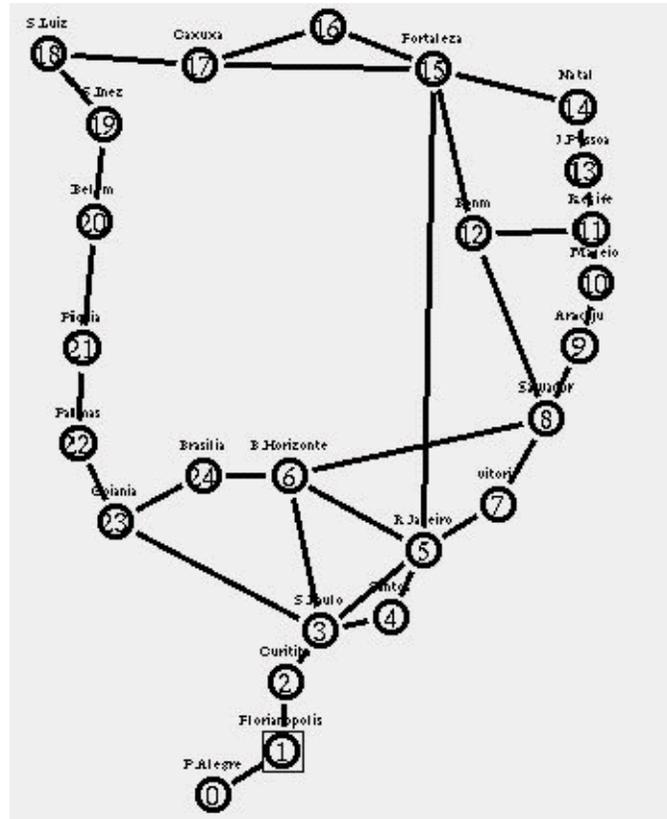


Figura 4.3. Topologia utilizada nas simulações

#### 4.1.1 Resultados dos Testes

A primeira bateria de testes realizada, consistiu em inserir o analisador de WAN entre o roteador de borda e um tributário de um multiplexador SDH com velocidade de 2048Kbps, como ilustra a Figura 4.4.



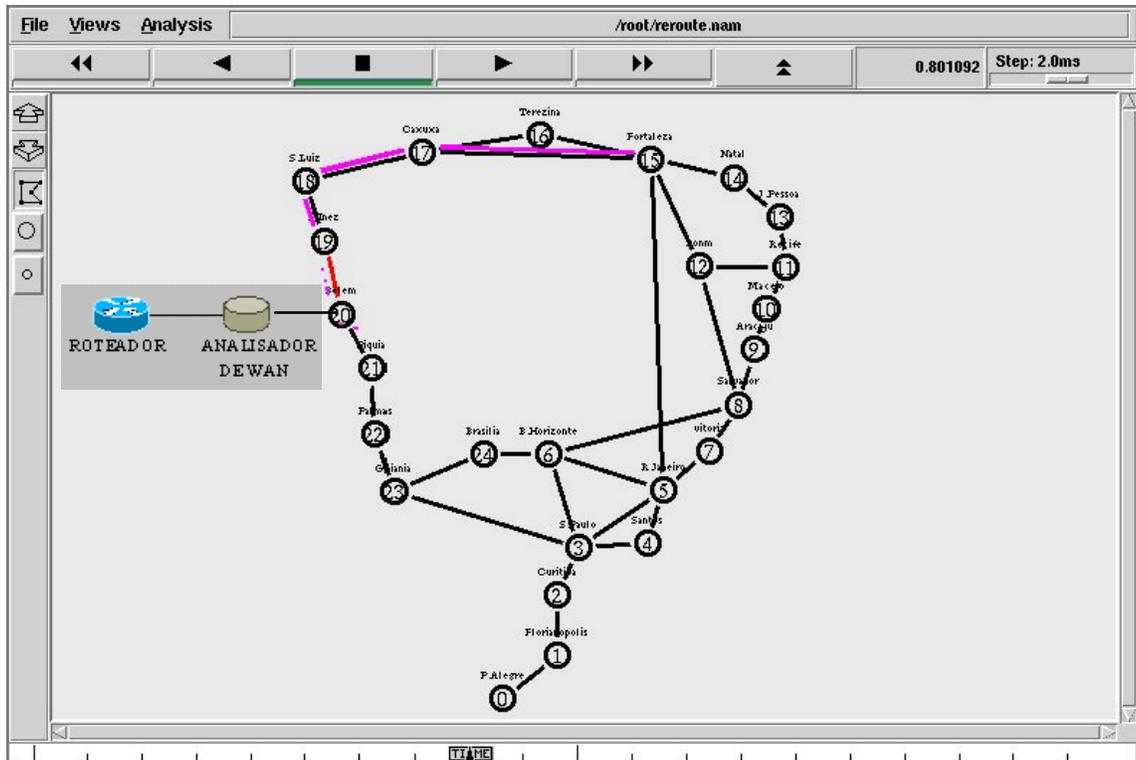


Figura 4.5. Rompimento da fibra entre os pontos 19 e 20

O tráfego gerado para realização deste teste consiste no envio, através do comando "ping", de 1000 pacotes ICMP de 18024 bytes, sendo enviados em quadros de 2048Kbps dos quais 64Kbps são dedicados para supervisão do quadro ex: FCS (*Frame Check Character*), Alinhamento de quadro, CRC4 etc... Os 1984Kbps restantes são dedicados ao transporte efetivo de dados. Buscou-se desta forma definir métricas para analisar os diversos testes realizados em redes SDH/SONET e de nova geração.

O primeiro parâmetro calculado foi a "Vazão", que corresponde a Fração de tempo em que o canal transmite de forma bem sucedida seus dados [44]. Este valor tem que ser o mais alto possível, definido matematicamente. Pela razão entre o total de bits transmitidos e o tempo em que estes bits permanecem bloqueados com absoluta interrupção do meio de transmissão, multiplicado pela velocidade da transmissão dos dados:

$$V_z = \left(\frac{T_{btx}}{T_{bl}}\right) \times \frac{8}{V}$$

Onde:  $V_z$  = Vazão (Adimensional)

$T_{btx}$  = Total de Bytes Transmitidos (bytes)

$T_{bl}$  = Tempo de Bloqueio (S)

$V$  = Velocidade (Bps)

O segundo parâmetro calculado através de nossos testes foi a "Probabilidade de Bloqueio", que corresponde a probabilidade de um pedido de conexão não ser atendido por falta de recursos da rede, este parâmetro pode ser utilizado para medir a eficiência de utilização da rede [38]. O valor deste parâmetro tem que ser o menor possível. A fórmula que define a probabilidade de bloqueio para esse caso é:

$$P_b = \left(\frac{T_{pd}}{T_{pe}}\right) \times 100$$

Onde:  $P_b$  = Probabilidade de Bloqueio (adimensional)

$T_{pd}$  = Total de Pacotes Descartados

$T_{pe}$  = Total de Pacotes Enviados

Tabela 4.1. Dados gerados pelo instrumental após a ocorrência do evento

Tempo Total	2s
Tempo de Interrupção	2s
Tempo de Bloqueio	50ms
Total de pacotes enviados	148
Total de pacotes descartados	4
Total de pacotes recebidos	144
Vazão	208,4025
Probabilidade de Bloqueio	0,015367475

A Tabela 4.1 ilustra primeiramente as características gerais do teste realizado pelo instrumento durante 353 segundos que correspondeu ao tempo total de testes, porém foram considerados apenas os dois segundos sobre o tempo total, para efeito de padronização dos cálculos de vazão e probabilidade de bloqueio. Observou-se uma perda muito pequena de pacotes, apenas 4 do número total transmitido, o que garante uma vazão relativamente alta, assim como uma probabilidade de bloqueio muito baixa, mostrando uma eficácia muito grande dos sistemas SDH/SONET no tratamento de tolerância a falhas.

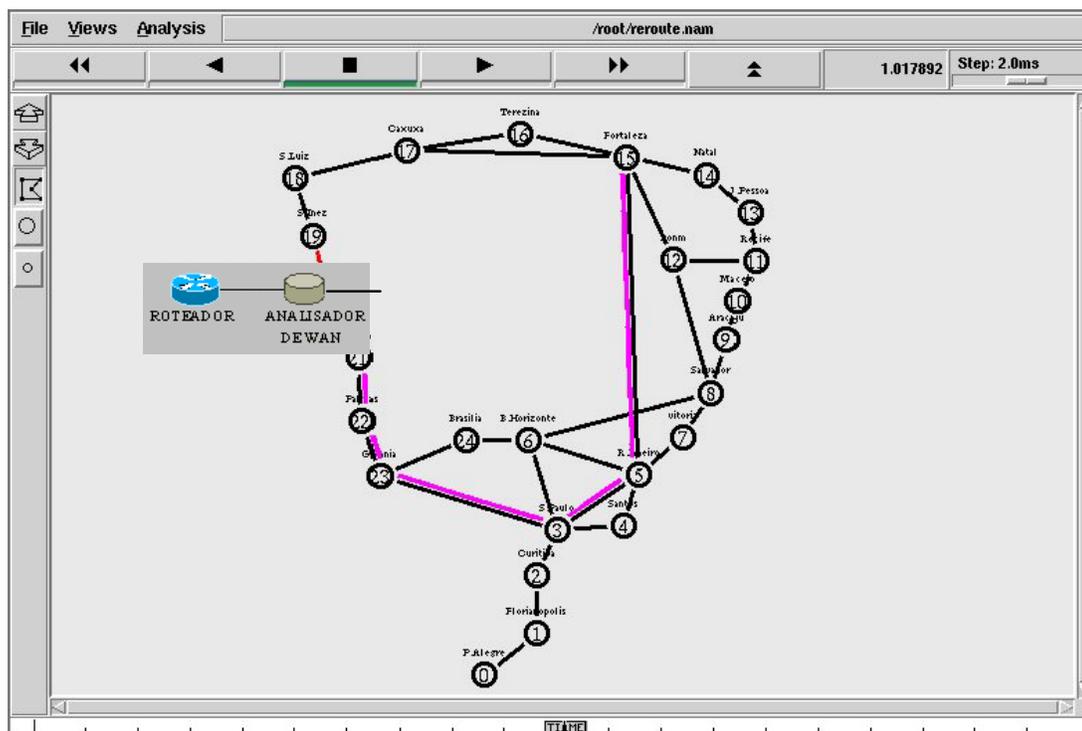


Figura 4.6. Recuperação do tráfego pela rota reserva

A Figura 4.7 ilustra a curva correspondente ao impacto causado na vazão ocasionado pela interrupção nos dados efetivamente transmitidos, no tempo real da falha. Observando o gráfico nota-se que em determinado momento ele começa a decrescer, isto acontece no momento exato da interrupção da transmissão, permanecendo em queda até o momento da comutação da chave que corresponde a tarja vertical, voltando a crescer o tráfego até a condição normal, após a comutação da chave.

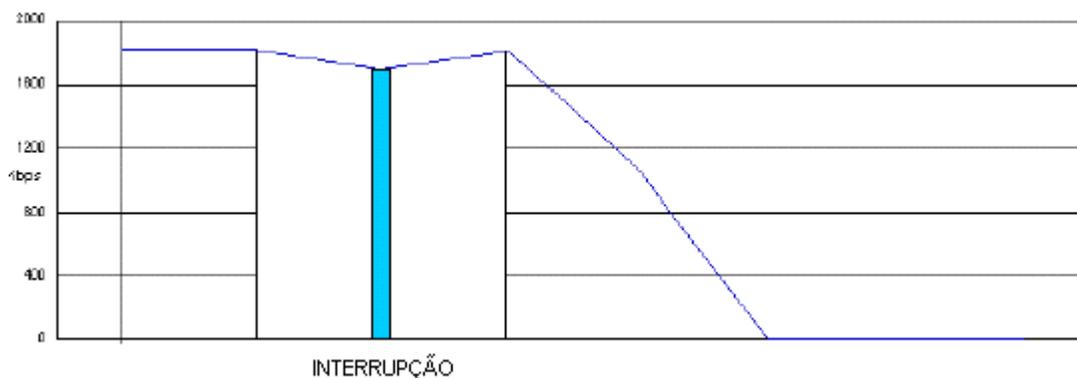


Figura 4.7. *Throughput* total corrente

O analisador de dados não detalha precisamente o tempo de interrupção, para podermos expor melhor os resultados obtidos, porém, maiores detalhes sobre este teste podem ser obtidos no Anexo 1, que corresponde ao relatório detalhado gerado pelo instrumento, para poder validar melhor este teste.

Observou-se que os excelentes resultados de tolerância a falhas obtidos pelos sistemas SDH/SONET são alcançados graças a manutenção de um enlace reserva dedicado, que fica ocioso durante grande parte do tempo, sendo acionado apenas para atendimento de falhas o que representa um desperdício muito grande de recursos, outra desvantagem é a necessidade do uso de uma supervisão centralizada para monitoração e controle de tráfego, no caso de falhas, o que aumenta a complexidade do sistema, ocasionando também uma considerável taxa de *overhead* nos enlaces.

#### 4.1 Cenário de Testes em Redes de Nova Geração Utilizando o NS

Para que fossem realizados os testes de tolerância a falhas em redes ópticas de nova geração e devido a carência de uma rede *testbed* utilizando esta tecnologia, tornou-se necessário realizarmos um estudo aprofundado do *software* NS, utilizando suas funcionalidades e acrescentando outras, para simular a mesma rede tratada nos testes anteriores porém implementada com a nova tecnologia.

Foram simulados enlaces ópticos com capacidade de 10Gb possuindo retardos calculados para os valores reais de cada link. O tipo de tráfego usado foi o CBR (“*Constant Bit Rate*”). A origem e o destino de cada tráfego será definido de acordo com a necessidade de cada simulação.

Conforme apresentado no Capítulo 3, o esquema de proteção de LSP 1+1 faz uso de um LSP auxiliar que recebe uma cópia dos dados do LSP principal. Na proteção de LSP 1:1 o caminho alternativo não recebe uma cópia dos dados, mas é ativado na ocorrência de falhas, deixando seus recursos disponíveis para criação de outros enlaces e novos tráfegos no caso de não existência de falhas. Na técnica de proteção de enlace 1:1, um enlace alternativo previamente estabelecido é utilizado em caso de falha num link do LSP principal. No esquema de restauração de LSP, uma nova rota é calculada somente após a ocorrência da falha.

#### 4.1.1 NS

O NS, atualmente disponível na versão 2.29, é uma ferramenta desenvolvida em C++ e *Object Oriented Tool Command Language* (OTcl), cuja principal função é oferecer suporte à simulação de redes locais e remotas, além de um grande número de tecnologias distintas de redes, com ou sem fio, em diferentes cenários.

Trata-se de um programa livre, ou seja, o seu código-fonte é aberto. Com isso, qualquer desenvolvedor pode interagir implementando melhorias, além de poder ser adquirido gratuitamente na Internet.

Outro ponto positivo do NS é a sua interação com o *Network Animator* (NAM), que é uma ferramenta simples e bastante funcional para animação gráfica de transmissão de dados, que permite visualizar graficamente as simulações feitas no NS.

A versão do NS utilizada neste trabalho foi a 2.16, pois a mesma apresenta melhor compatibilidade com as extensões do NS que simulam redes ópticas WDM baseadas em comutação de lambdas, o OWNS (*Optical WDM Network Simulator*) [33], e redes MPLS, o MNS (*MPLS Network Simulator*) [34], que são fundamentais no contexto deste trabalho, a seguir serão descritos mais detalhadamente o OWNS e o MNS.

#### 4.1.2 OWNS

O OWNS é uma ferramenta que tem o objetivo de estudar redes ópticas WDM com ênfase na camada de rede, é uma extensão do NS que foi desenvolvida utilizando o NS-2 como base, baseia-se no paradigma de comutação de circuitos e Permite a adição de novas

funcionalidades como algoritmos de roteamento e algoritmos de atribuição de comprimentos de onda (*wavelength assignment*). A Figura 4.7 ilustra a organização e a interação entre os componentes internos de um nó básico OWNS.

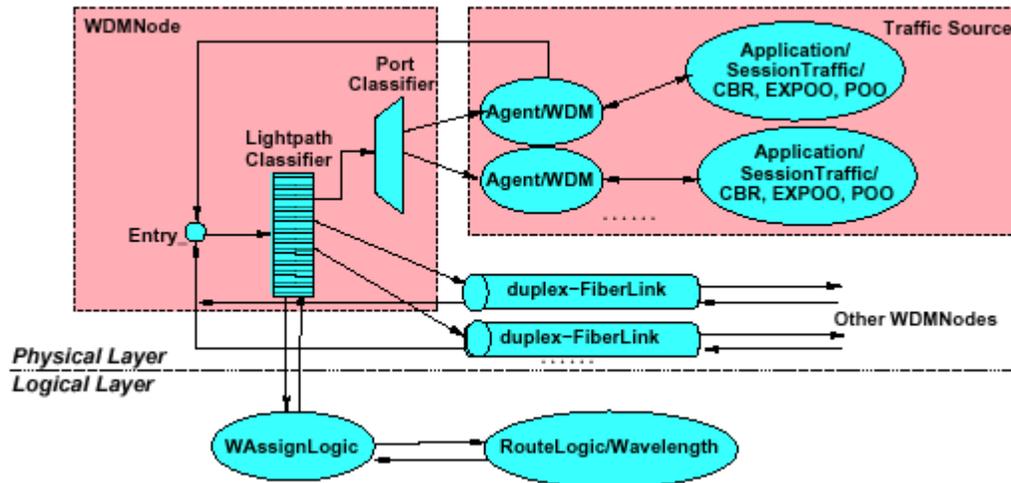


Figura 4.7- Diagrama básico de um nó OWNS[43]

O sinal que entra no nó OWNS através de fibras ópticas bidirecionais, provenientes do plano de dados de um outro nó, possui seu feixe óptico dividido em vários comprimentos de ondas distintos ( $\lambda$ ) através do classificador de caminhos ópticos (*Lightpath Classifier*), que obedece a formação de um caminho virtual feito pelo módulo de comprimento de onda (*Wassign Logic*) que está ligado ao módulo de roteamento (*Route Logic / Wavelength*), que possui a função de computar as diversas rotas necessárias para estabelecerem os diversos caminhos ópticos.

Ao sair do classificador óptico, o sinal é enviado à um segundo classificador denominado classificador de porta (*Port Classifier*), que possui como finalidade definir o agente responsável em tratar a informação recebida do usuário final.

#### 4.1.3 MNS

O MNS é uma ferramenta que permite estudar redes, suportando simulações do protocolo MPLS, sendo desenvolvido para rodar no NS-2, a Figura 4.8 ilustra a arquitetura interna de um nó MNS.

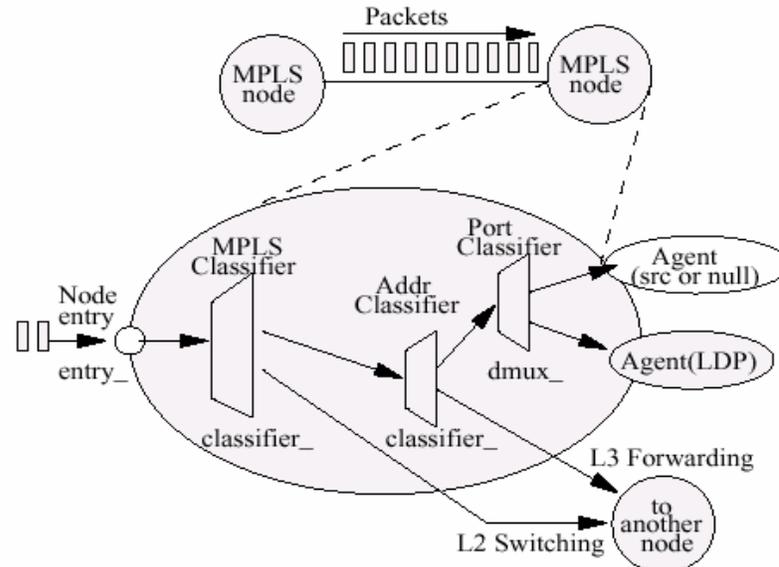


Figura 4.8 - Diagrama básico de um nó MNS [42]

sinal óptico de entrada no nó MNS proveniente de um plano de controle localizado em outro nó, primeiramente é classificado de acordo com seu rótulo correspondente através do classificador MPLS onde são separados os dados que foram destinados ao nó local e os que possuem os rótulos endereçados para outros nós, Um segundo classificador (*Addr Classifier*), realiza a mesma separação dos dados recebidos utilizando como elemento diferenciador o endereço IP, finalmente o sinal é demultiplexado e enviado para os respectivos agentes.

#### 4.2.1.3 *LOCSnode*

Para realizar as simulações desejadas, verificou-se a necessidade de promover a integração dos módulos OWNS e MNS, desenvolvidos separadamente e sem interação entre suas funcionalidades, para tornar possível a simulação de redes ópticas WDM com plano de controle baseado em GMPLS. Adicionando assim novas extensões ao simulador ou mesmo acrescentando novas características aos módulos já existentes, é necessário ter um bom conhecimento da hierarquia de classes do NS e saber onde cada parte do código está situada dentro da árvore de diretórios do simulador [34].

A primeira etapa dessa integração foi a criação de uma nova estrutura de nó do NS que possui as funcionalidades de um nó MPLS em conjunto com as de um nó WDM. As estruturas de nó existentes nos módulos MNS e OWNS permitiram essa nova implementação.

Esse novo nó criado no desenvolvimento deste trabalho denomina-se *LOCNode* (*Labeled Optical Circuit Switching*), pois baseia-se no paradigma de comutação de circuitos com plano de controle baseado em GMPLS. O *LOCNode* herda as capacidades de atribuição e distribuição de rótulos através do protocolo LDP (*Label Distribution Protocol*), suporta mecanismos de engenharia de tráfego, incluindo os mecanismos de proteção e restauração abordados neste trabalho e permite a criação de caminhos de luz (*lightpaths*) associando o estabelecimento dos mesmos com o evento da criação de um LSP (*Label Switched Path*). O *LOCNode* interage com os enlaces ópticos nativos do OWNS. A Figura 4.7 ilustra a estrutura desse novo nó.

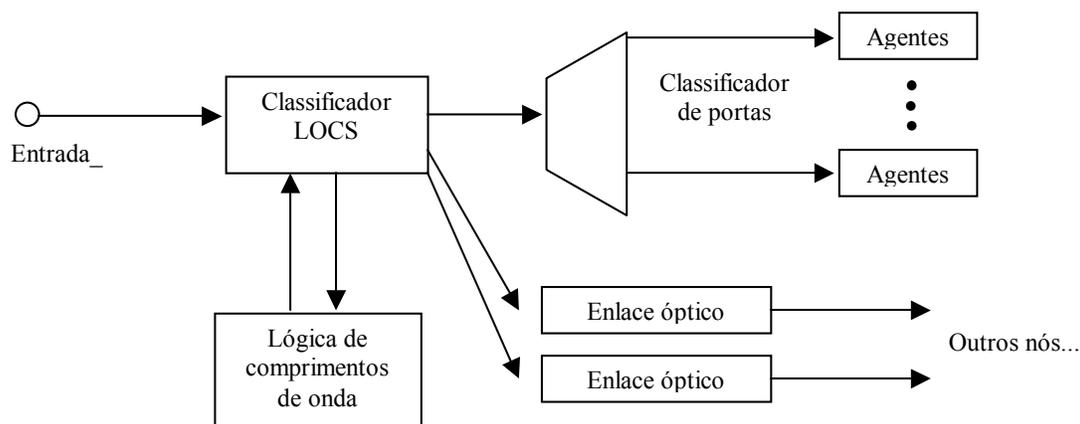


Figura 4.7. Estrutura do nó *LOCNode*

O classificador LOCS é a união dos classificadores do nó MPLS e do nó WDM pertencentes ao MNS e ao OWNS respectivamente. O classificador é responsável por encaminhar a informação para o objeto de simulação apropriado. A partir desse novo classificador constrói-se uma estrutura que guarda as informações dos comprimentos de onda alocados em cada enlace com base nos LSPs estabelecidos. Se o próximo salto do pacote for o próprio nó, ele é repassado para o classificador de portas que define qual agente será responsável por tratar a informação recebida. Caso contrário, o pacote é repassado para o próximo nó através do enlace óptico.



Partiu-se para a realização das simulações com o objetivo de comparar os mecanismos de proteção e restauração do GMPLS escolhidos no trabalho, investigando os impactos promovidos pelos mesmos no comportamento da rede.

Uma vez estabelecidas as mesmas métricas usadas nos testes em redes SDH/SONET para análise da eficiência e eficácia das redes de nova geração, simularam-se falhas no enlace entre os nós 20 e 19 da topologia descrita anteriormente. Estas ocorrem no instante 0,8s da simulação e o enlace retorna à condição inicial no instante 1,3s. As simulações possuem um tempo total de 2,0 segundos, sendo enviados pacotes com 4.371 bytes cada um, a Figura 4.9 ilustra a interrupção ocorrida.

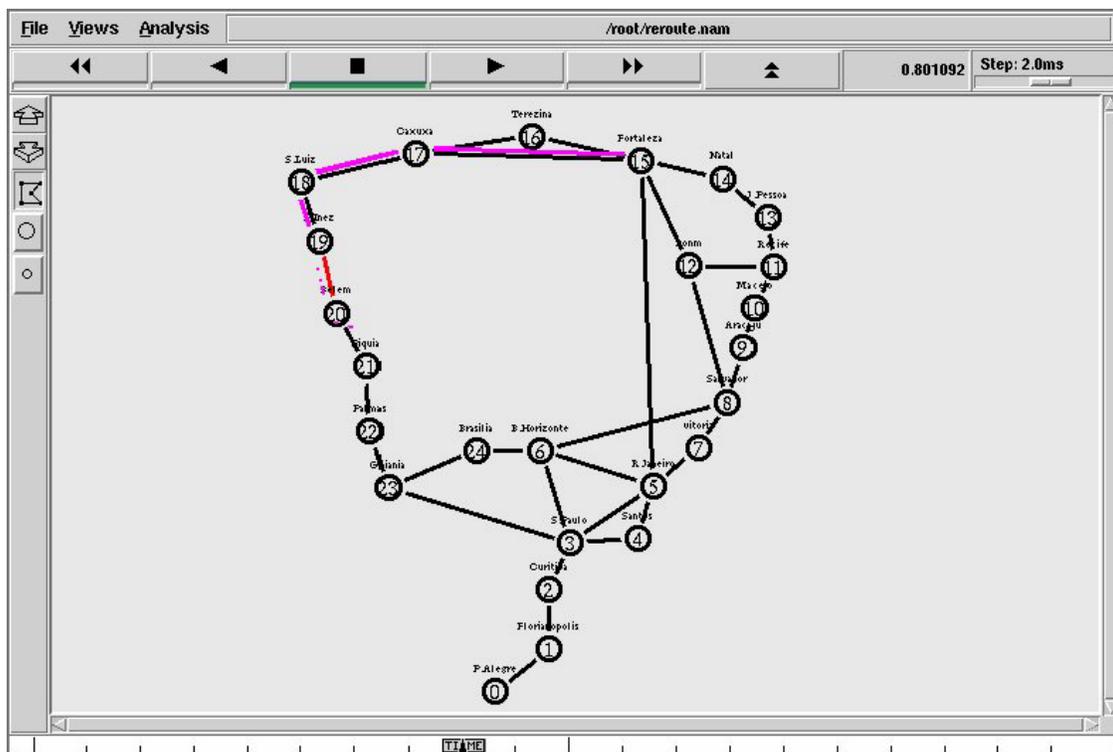


Figura 4.9. Momento da interrupção no link entre Belém e Santa Inês

A Figura 4.10 ilustra o chaveamento do LSP principal para o reserva, no momento em que ocorre a interrupção do link óptico pertencente ao enlace principal. Serão analisadas aqui três formas de proteção distintas em redes de nova geração, a primeira utilizará técnica de proteção 1:1, que consiste na comutação do LSP principal para um LSP



Tabela 4.2. Número de pacotes perdidos na técnica de proteção 1: 1

Tempo Total	2s
Tempo De Interrupção	495ms
Tempo De Bloqueio	120ms
Total de pacotes enviados	937
Total de pacotes descartados	22
Total de pacotes recebidos	915
Vazão	136,53
Probabilidade de Bloqueio	2,34

O impacto da interrupção ocasionada no LSP e a comutação para o LSP reserva, na vazão dos dados transmitidos, utilizando o mecanismo de proteção 1:1 é mostrado na Figura 4.10. Fazendo-se uma breve análise nesta figura, observa-se que o tráfego efetivo de dados é iniciado no tempo de 420 milissegundos, este é o tempo que o protocolo GMPLS leva para mapear toda a rede e criar o LSP principal que tráfegará com os dados, deixando também armazenado em seu buffer os dados das rotas alternativas para que na ocorrência de alguma falha no LSP principal, possa criar um LSP reserva.

Aos 900 milissegundos os dados são interrompidos em virtude de uma falha simulada no LSP principal ocasionando uma queda brusca dos dados, retornando tráfego de dados 120 milissegundos após a interrupção utilizando o enlace reserva. No instante 1425 milissegundos o defeito no LSP principal é sanado e o tráfego retorna as condições originais.

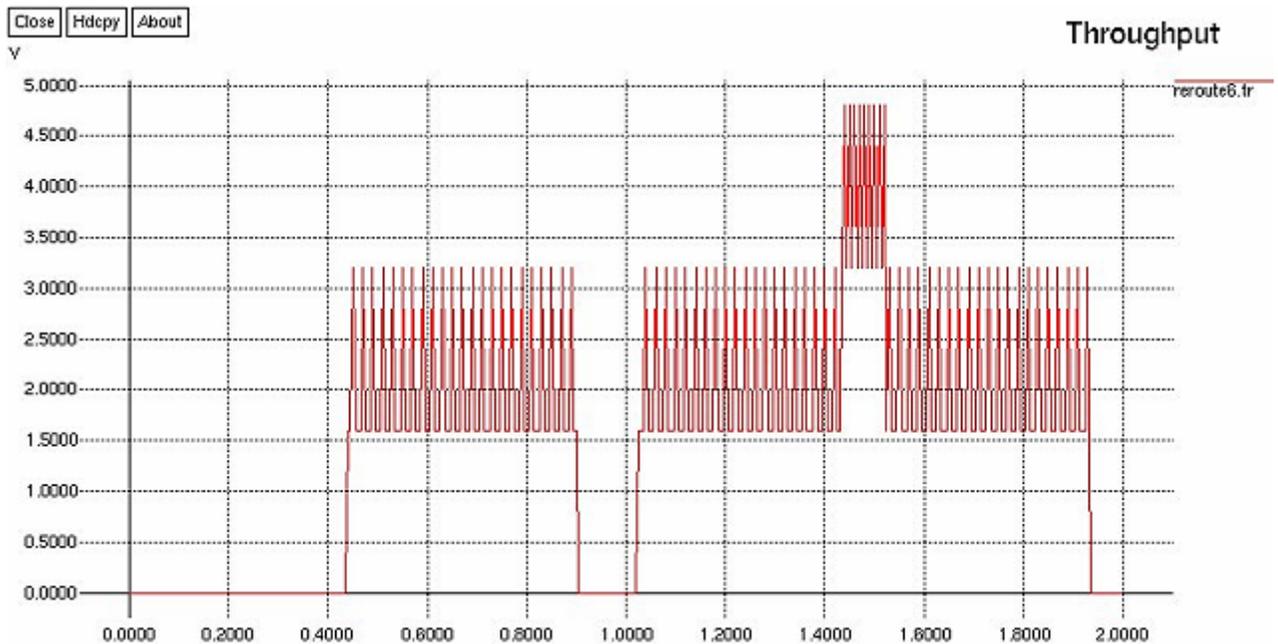


Figura 4.10. Vazão no esquema de proteção LSP 1:1

Simulou-se uma segunda falha no mesmo link que une o ponto 19 ao 20 mostrado no exemplo anterior, porém, com transmissão simultânea no LSP principal e no reserva mostrado na simulação anterior, que corresponde ao esquema de proteção de enlace 1+1.

A Tabela 4.3 ilustra um resultado bem otimista em relação aos testes anteriores, tendo em vista que a vazão tende a infinito e a probabilidade de bloqueio é zero, quanto as perdas de pacotes transmitidos. Este mecanismo de proteção pode ser considerado o mecanismo ideal pois elas inexistem, porém, a desvantagem deste mecanismo é a alocação constante de um LSP reserva, o que acarreta perda de banda no enlace em que este LSP for criado.

Tabela 4.3. Número de pacotes perdidos na técnica de proteção 1+1

Tempo Total	2s
Tempo De Interrupção	515
Tempo De Bloqueio	0
Total de pacotes enviados	937
Total de pacotes descartados	0
Total de pacotes recebidos	937
Vazão	$+\infty$
Probabilidade de Bloqueio	0

A Figura 4.11 ilustra o impacto sofrido na vazão dos dados transmitidos com a implementação da técnica de proteção LSP 1+1, nota-se que não existe interrupção nos dados transmitidos, pois uma vez que o LSP principal é interrompido os dados continuam chegando ao seu destino continuamente pelo LSP reserva.

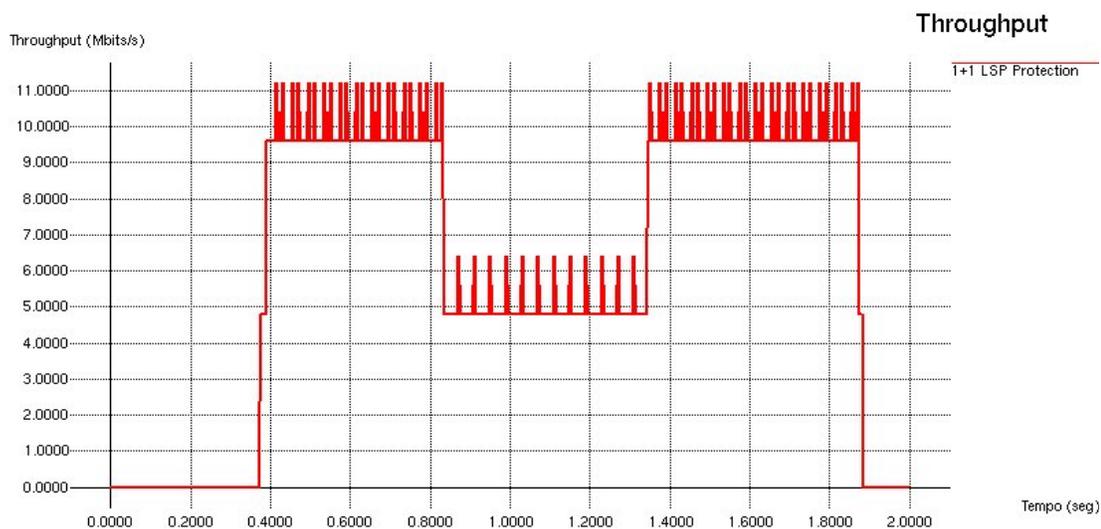


Figura 4.11. Vazão no esquema de proteção LSP 1+1

A terceira simulação realizada consistiu numa nova interrupção do link principal que une os pontos 19 e 20 e ao tentar-se uma comutação para o LSP reserva, o link que une os pontos 5 ao 15 do LSP reserva é interrompido, o que forçou a criação de um terceiro LSP reserva para garantir o tráfego como ilustra a Figura 4.12.

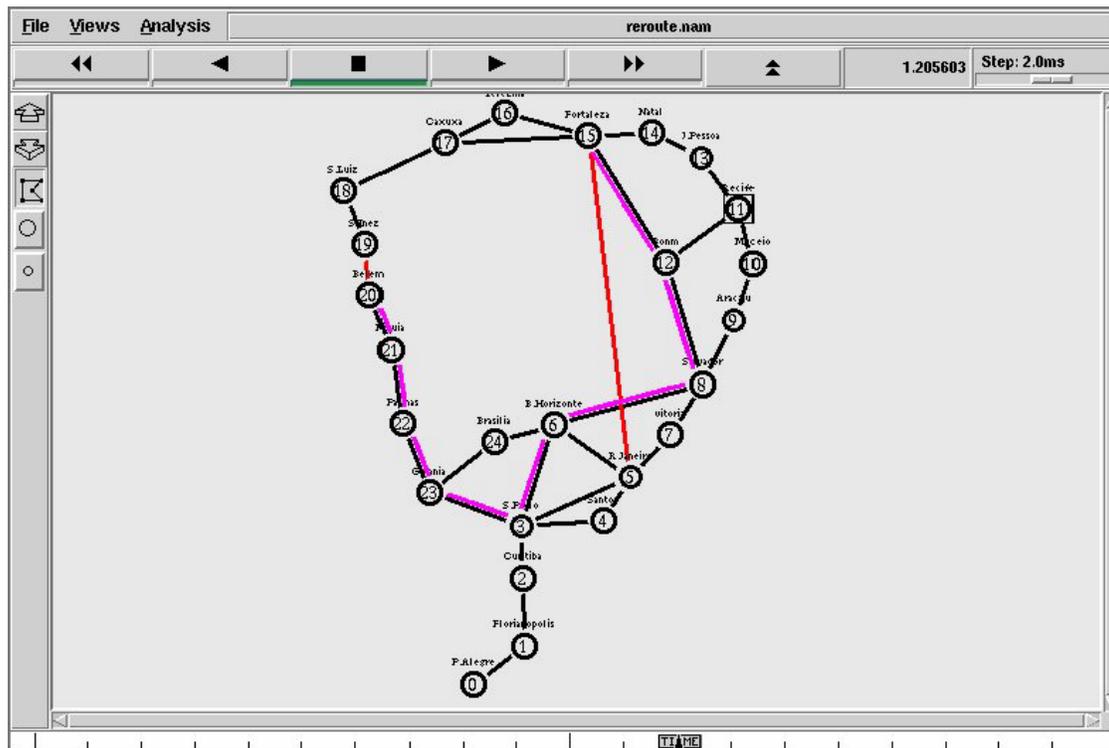


Figura 4.12. Falha em dois LSP's simultaneamente

A Tabela 4.4 mostra os resultados colhidos com este novo teste, já era esperado um aumento substancial na probabilidade de bloqueio assim como uma diminuição na vazão dos dados transmitidos em virtude do alto tempo levado para a configuração de um segundo LSP reserva, porém, é mostrada neste teste uma das maiores vantagens do protocolo GMPLS quando usado para tratamento de falhas em redes WAN's em relação a arquitetura SDH/SONET, que é a diversidade de rotas que podem ser configuradas no caso de várias interrupções sucessivas.

Tabela 4.4. Número de pacotes perdidos quando falham dois LSP's simultaneamente.

Tempo Total	2s
Tempo De Interrupção	615ms
Tempo De Bloqueio	239ms
Total de pacotes enviados	937
Total de pacotes descartados	37
Total de pacotes recebidos	900
Vazão	68,5523
Probabilidade de Bloqueio	3,948772679

A Figura 4.13, ilustra o comportamento da vazão quando são interrompidos dois LSP's, o principal e o outro reserva, sendo necessário a criação de um terceiro.

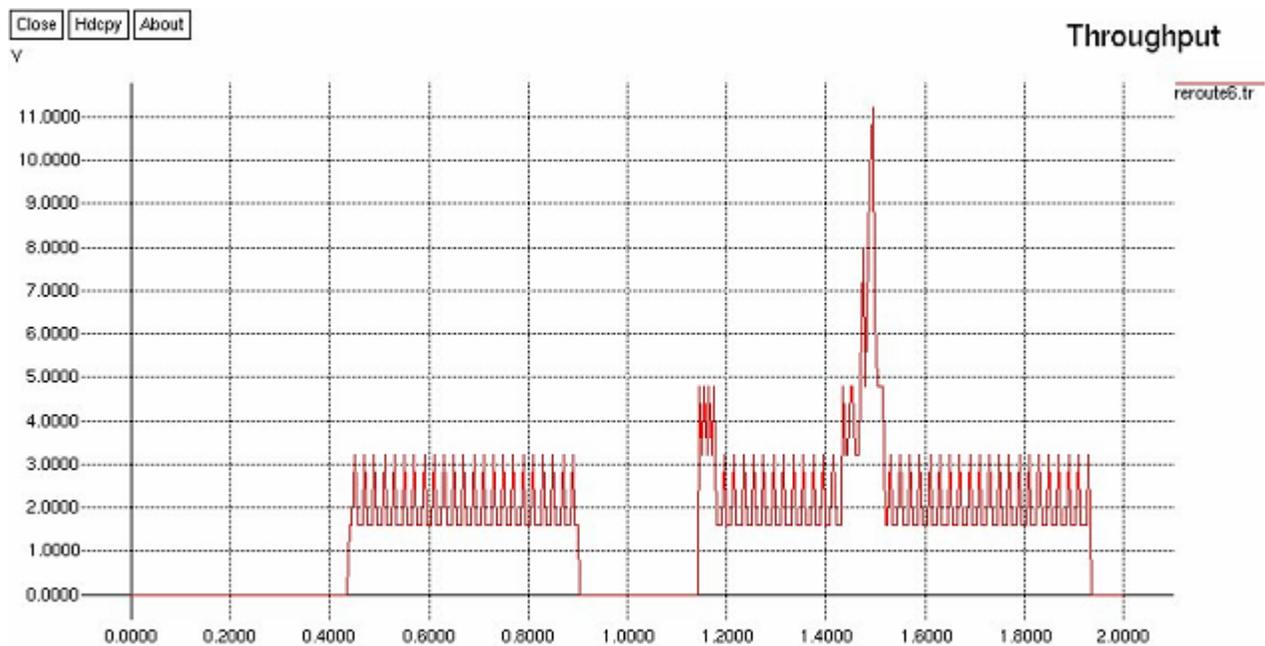


Figura 4.13. Vazão quando falham dois LSP's simultaneamente

A Última simulação escolhida para compor os testes desta dissertação consiste em provocar uma interrupção no link que une os pontos 17 e 15 com o objetivo de demonstrar



Tabela 4.5. Número de pacotes perdidos com esquema de proteção de enlace

Tempo Total	2s
Tempo De Interrupção	557ms
Tempo De Bloqueio	70ms
Total de pacotes enviados	937
Total de pacotes descartados	21
Total de pacotes recebidos	916
Vazão	234,05
Probabilidade de Bloqueio	2,24

A Figura 4.15 ilustra o comportamento da vazão do tráfego quando o esquema de proteção de enlace é adotado.

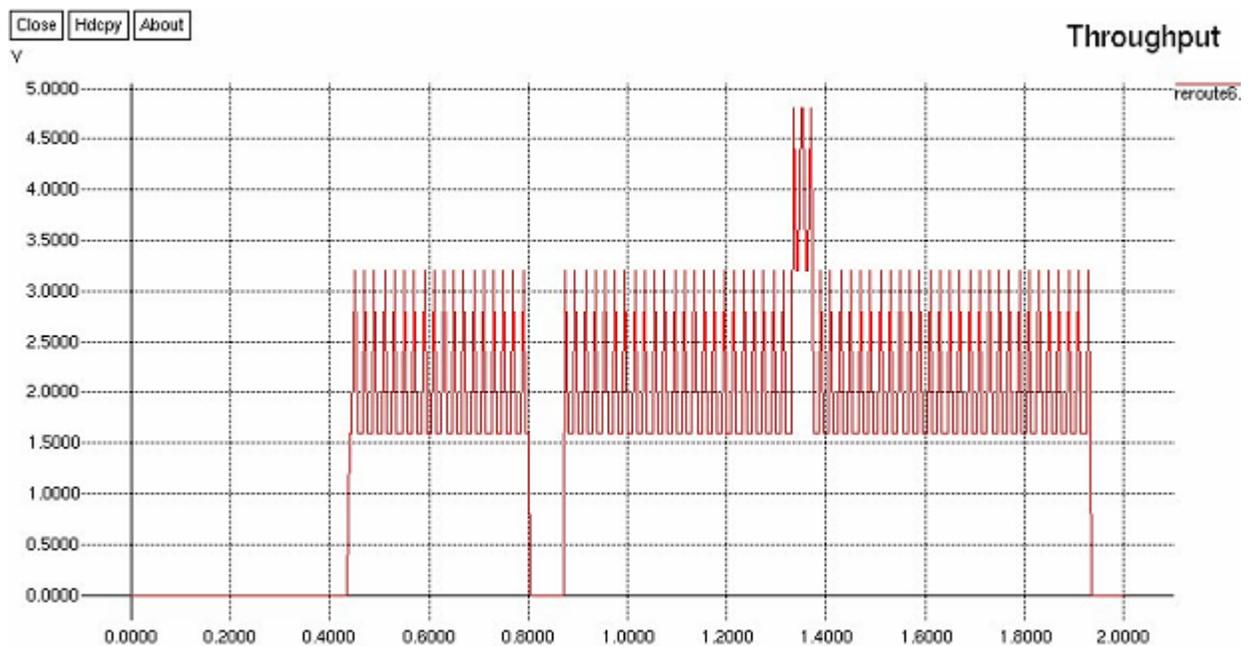


Figura 4.15. Vazão resultante quando adotado o esquema de proteção de enlace

### 4.3 ANÁLISE COMPARATIVA

Do estudo comparativo realizado pôde-se concluir que para promover proteção e restauração de conectividade em redes ópticas, as técnicas apresentadas podem trabalhar com granularidade de caminhos ou enlaces. Na plataforma SDH/SONET o tráfego é reroteado entre os nós das extremidades do caminho onde houve a falha. Já nas redes ópticas de nova geração, com plano de controle baseado em IP-GMPLS/WDM o tráfego é reroteado entre os nós do enlace onde a falha ocorreu.

Deve-se observar, contudo, que em função das características do protocolo IP, as opções baseadas em recuperação dinâmica e no compartilhamento dos enlaces reservas, tendem a ser as mais promissoras do que aquelas que utilizam caminhos reservas dedicados, como SDH/SONET.

Observou-se no estudo de caso que pacotes pertencentes a um LSP principal podem ser rapidamente comutados para outro LSP reserva sem necessitar de um canal dedicado, caso seja detectada alguma falha no LSP principal o que representa uma grande vantagem desta tecnologia em relação as existentes hoje SDH/SONET que necessitam de um canal reserva exclusivo.

Outra vantagem observada foi a simplicidade de implementação desta tecnologia, pois trata-se de uma arquitetura que não necessita de camadas intermediária, possuindo pouco *overhead* de controle e alta capacidade de tráfego, caso sejam implementados equipamentos puramente ópticos sem conversão para dados eletrônicos.

Uma terceira vantagem notada corresponde a diversidade de enlaces alternativos que podem ser criados, uma vez ocorrido problema em outro enlace reserva, no momento em que o enlace principal é interrompido, sem que para isto seja necessário manter enlaces dedicados para reserva, como na plataforma SDH/SONET.

Fazendo uma análise em termos de custos, observa-se que a implementação de redes ópticas de nova geração, pode reaproveitar todas as fibras reservas de um anel óptico SDH/SONET, que ficam sem tráfego, quando a fibra que abriga o enlace principal está em funcionamento. Isto aumentaria consideravelmente o tráfego sem a necessidade de acréscimo ou lançamento de fibras adicionais, realizando incrementos apenas nos seus nós, o que representa uma grande vantagem econômica para a operadora.

A desvantagem desta nova abordagem é o tempo de restabelecimento de uma via, pois existe um retardo na troca de sinalização e criação de um LSP reserva o que não acontece na utilização de comutadores SDH/SONET que já possuem uma rota alternativa configurada e pronta para assumir imediatamente em menos de 50 milissegundos, como observado nos testes práticos e nas simulações.

Analisando-se a Figura 4.16, que corresponde a uma cópia da Figura 3.1 e baseado nos resultados obtidos, é possível recomendar que o mecanismo de proteção de LSP 1+1 seja utilizado para aplicações em tempo real e missões críticas que não toleram perdas e são altamente sensíveis ao atraso e a variação deste (*jitter*), como por exemplo, sistemas de controle de tráfego aéreo. As técnicas de proteção de LSP 1:1 e proteção de enlace 1:1 são indicadas em casos onde se necessita de uma rápida recuperação. No entanto, pequenas perdas são toleradas, como em sistemas de comunicação multimídia, sendo que a proteção de enlace 1:1 apresenta um desempenho bem melhor.

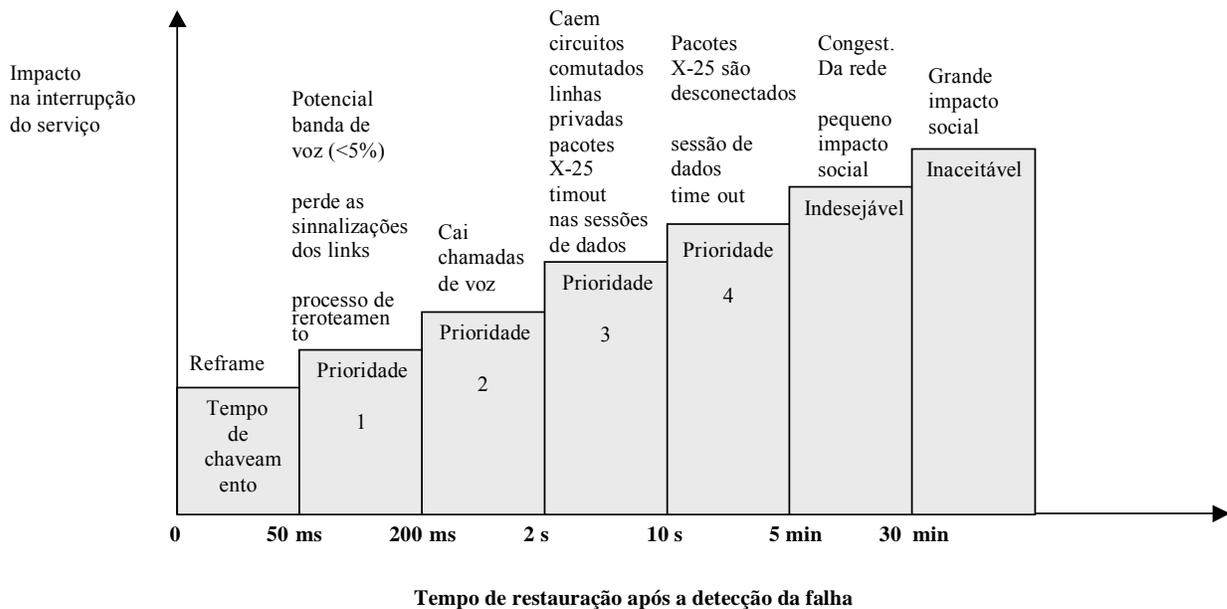


Figura 4.16. Impacto causado pela interrupção de serviço de telecomunicações [27]

As propostas de adoção de políticas específicas de tolerância a falhas em redes ópticas de nova geração com planos de controles utilizando IP-GMPLS/WDM, apresentam uma perfeita adequação ao atual cenário em que se encontram os *backbones* no Brasil, pois

suas extensões são muito vastas e em sua grande parte atendidas por fibra óptica. Em caso de implementação desta tecnologia não necessitaria do lançamento de novas fibras, sendo necessário apenas trocar os nós, havendo desta forma um grande incremento de banda óptica e diversidade de rotas alternativas, com grande economia para as operadoras, pois aproveitaria as fibras principais e reservas já lançadas.

## 5 - CONCLUSÕES E INVESTIGAÇÕES FUTURAS

O objetivo desta dissertação foi realizar uma análise comparativa dos mecanismos de recuperação de falhas em redes SDH/SONET existentes hoje nos *backbones* nacionais e redes ópticas de nova geração, baseadas na arquitetura IP-GMPLS/WDM, propondo, desta forma, a adoção de diferentes mecanismos para tratamento de falhas em redes de nova geração em função do tipo de aplicação utilizada.

Mostrou-se primeiramente um resumo teórico sobre os sistemas ópticos onde foram abordados os princípios de transmissão óptica, as características básicas de uma fibra, mostrando também a evolução dos sistemas, onde ressaltou a tecnologia WDM. Foram expostas as principais arquiteturas das redes ópticas: SDH/SONET, ATM, Redes IP, Redes MPLS e GMPLS, dando desta forma o embasamento teórico necessário para o desenvolvimento de um nó óptico que tenha no seu plano de controle o protocolo IP integrado ao GMPLS, trabalhando sobre um plano de dados baseado em WDM, para compor as redes ópticas de nova geração.

Sobre tolerância a falhas em redes ópticas, foram mostradas as principais técnicas de detecção de falhas e os principais tipos de técnicas de proteção e restauração em redes SDH/SONET e redes ópticas de nova geração, com planos de controles baseados em IP-GMPLS e plano de dados baseados em WDM. Foram investigadas as pesquisas mais recentes cujos temas são correlatos, objetivando mostrar o estado atual da arte para que, desta forma, permitisse elaborar um modelo de referência para ser estudado neste trabalho.

Uma vez concluído que o melhor interfaceamento entre a camada IP e a camada WDM para implementação de engenharia de tráfego em redes ópticas transparentes é o protocolo GMPLS, adotou-se o nó que trabalha com IP-GMPLS sobre WDM, para compor o modelo de referência a ser adotado na rede WAN implementada em redes de nova geração que foi utilizada efetivamente em todos os testes que utilizarão esta tecnologia.

Para poder realizar comparações entre diferentes tecnologias de tolerância a falhas em redes ópticas tornou-se necessário o aproveitamento de uma rede real explorada por uma operadora de telecomunicações para realização de testes na plataforma SDH/SONET. Esta mesma rede foi simulada utilizando o *software* NS, para a realização dos testes em redes de nova geração.

O *software* NS possui dois sub módulos de simulação desenvolvidos de forma distinta, para simulação de redes utilizando MPLS no seu plano de controle o MNS, o segundo módulo simula redes ópticas utilizando WDM no seu plano de dados o OWNS. Depois de exaustivos testes concluiu-se que estes dois módulos não se comunicavam entre si. Isto serviu de motivação para criar um novo nó chamado *LOCSnode* que herda as características do MNS no seu plano de controle e do OWNS no plano de dados, obtendo desta forma o nó ideal para nossos experimentos.

Uma vez realizadas todas as experiências práticas num *backbone* óptico implementado na plataforma SDH/SONET e este mesmo *backbone* implementado em redes de nova geração simulados no NS, permitiu-nos concluir as inúmeras vantagens da implementação dos diversos mecanismos de proteção a falhas desta nova tecnologia, nos *backbones* ópticos aqui no Brasil.

Apartir da análise comparativa entre as duas tecnologias estudadas identificou-se que as redes ópticas de nova geração possuem baixo custo de implementação, por aproveitar as fibras já lançadas e utilizadas como reserva na plataforma SDH/SONET; possuem fácil implementação desta tecnologia por apresentarem uma arquitetura simples com poucas camadas, ficando a camada de controle IP-GMPLS interagindo direto com a camada de transporte de dados WDM sem camadas intermediária; finalmente por tratar-se de redes em malhas utilizando GMPLS nos planos de controles dos nós e estes adotando os protocolos LMP, OSPF ou IS-IS, existirá uma diversidade maior de rotas alternativa, caso o enlace principal venha a ter problemas.

Tendo em vista as inúmeras vantagens citadas neste trabalho através de testes em situações reais e simuladas, deixa-se como contribuição a sugestão para adoção dos vários mecanismos de tolerância a falhas em redes ópticas de nova geração em substituição as redes SDH/SONET nos *backbones* brasileiros. Como contribuição acadêmica queremos ressaltar o desenvolvimento do nó *LOCSnode* para simulação de redes de nova geração com plano de controle baseado em IP-GMPLS/WDM, sendo uma ferramenta de extrema valia para simulação de redes *backbone* utilizando o NS.

## 5.1 TRABALHOS FUTUROS

Entre os possíveis trabalhos futuros, podemos sugerir a implementação de mecanismos de engenharia de tráfego para a geração de caminhos alternativos, priorizando os tráfegos essenciais, para restauração deste num espaço de tempo menor pelo GMPLS, aproximando, desta forma, o tempo de comutação de um LSP principal para um reserva do tempo de comutação entre enlaces na plataforma SDH/SONET.

A importância crescente dos dados que trafegam nos *backbones* das prestadoras de serviços de telecomunicações atuais, assim como as grandes vantagens das redes ópticas de nova geração, tem tornado cada vez mais viável a adoção desta tecnologia. Com o considerável retardo de comutação entre LSP's no protocolo GMPLS, torna-se imprescindível o desenvolvimento de mais estudos baseado em técnicas de inteligência artificial e redes neurais objetivando prover mecanismos de predição de falhas em redes de nova geração, baseados na aprendizagem do tráfego em pontos vulneráveis das redes.

Podemos sugerir a implementação de uma interface gráfica mais amigável no ambiente de desenvolvimento do NS, pois esta ferramenta é muito rica e poderia ser muito melhor aproveitada. Como se trata de um *software* de domínio livre, seria bastante válido o desenvolvimento de uma interface mais amigável. Outro incremento que poderia ser dado ao NS, seria a compatibilidade com outros sistemas operacionais além do *Linux*, pois existe uma tendência muito grande para o desenvolvimento de softwares multiplataforma e isto ajudaria muito mais na difusão desta ferramenta bastante útil para realização de trabalhos acadêmicos.

Ainda sobre o NS, vale sugerir o acréscimo de recursos de simulação para redes SDH/SONET, foram feitas várias pesquisas e não foram encontrados tais recursos, para comparar os dados obtidos na rede *testbed*, com simulações a serem realizadas na plataforma SDH/SONET.

**6 - REFERÊNCIAS BIBLIOGRÁFICAS**

- [1] MARTINAZZO, I.; BIHARI, A. " Hierarquia Digital Síncrona (SDH) " , edição 3 , EMBRATEL, 1996.
- [2] GIOZZA, W.; FERREIRA, E.; CONFORT, H. Waldman, "Fibras Ópticas Tecnologia e Projeto de sistemas". Rio de Janeiro: EMBRATEL, São Paulo: Makron, McGraw-Hill, 1991.
- [3] MARCONI, Communications Limited; "Curso Básico de SDH", (2000).
- [4] [http://www.gta.ufrj.br/~fagundes/IP\\_WDM](http://www.gta.ufrj.br/~fagundes/IP_WDM). Acessado em Fevereiro de 2004.
- [5] BLACK, Uyles, "Optical Networks Third Generation Transport Systems", Prentice Hall PTR, 2002.
- [6] ABELÉM, Antônio J.; STANTON, Michael A. "Inter-redes IP baseadas em Redes Ópticas", 2002.
- [7] XIN, Chunsheng; YE, Y. Wang; DIXIT, S. "On IP-Centric Optical Control Plane", Em: IEEE Communication Magazine, Editado por IEEE, 2001.
- [8] BO, Wen; Bhide, N. M.; SHENAI R. K.; SIVALINGAM K. M. " Optical Wavelength Division Multiplexing (WDM) Network Simulator (Owns): Architecture and Performance Studies", School of Electrical Engineering & Computer Science, Washington State University, Pullman, WA 99164, 2001.
- [9] HO, Pin-Han; MOUFTAH, H. "A Framework for Service-Guaranteed Shared Protection in WDM Mesh Network", Em: IEEE Communication Magazine, Editado por IEEE, 2002.
- [10] "Generalized Multiprotocol Label Switching (GMPLS)" The International Engineering Consortium, <http://www.iec.org>. Acessado em Julho de 2004.
- [11] TANENBAUM Andrew S. "Redes de Computadores", 3ª Edição, Editora Campus, 2000

- [12] <http://proenca.uel.br/curso-redes-graduacao/2000/trab-01/equipe-04/sdh.html>. Acessado em outubro de 2004.
- [13] YASUHARU, Suematsu; Iga, K. "Introduction to Optical Fiber Communications" John Wiley & Sons, 1982.
- [14] KAO, K. C.; HOCKHAM G. A. "Dielectric surface waveguides for optical frequencies". IEEE Communications Surveys & Tutorials, vol. 113, pp. 1151–1158, 1966.
- [15] AGOSTINHO, L. S. Filho; "Projeto de Redes Translúcidas de Longa Distância", Dissertação de mestrado : UNICAMP, Campinas - SP
- [16] BETINI, R.Cezar; REZENDE, S. M.; CAMIÑA, N. K. " IP/WDM – A união de tecnologias Robustas na Era da Convergência": PUC PR, 2004.
- [17] LEE, Youngseok; MUKHERJEE, B. "Traffic Engineering in Next-Generation Optical Networks", IEEE Communications Surveys & Tutorials, 2004.
- [18] KUROSE, James, K. W. Ross, "Redes de Computadores e a Internet uma nova abordagem" 2ª Edição, 2004.
- [19] <http://penta.ufrgs.br/rc952/trab2/atm1.html>. Acessado em setembro de 2004.
- [20] ELERI, Cardozo, MAGALHÃES, M. F. "Introdução a Comutação IP por Rótulos Através de MPLS". Apostila do Curso IA-003, Interconexão de Redes de Computadores. 2003.
- [21] ITU-T, Recommendation G.709, "Interface for the Optical Transport Networks", 2001.
- [22] ITU-T, Recommendation G.872, "Architecture of Optical Transport Networks", 2000.
- [23] <http://www.cyclades.com.br/pressroom/index.php?id=1058547600>. Acessado em janeiro de 2005.
- [24] COSORTIUM, The internet engineering, "Generalized Multiprotocol Label Switching (GMPLS)", <http://www.iec.org>. Acessado em março de 2005.

- [25] CARLOS, H. R. Gonsalves, "Utilizando Redes Neurais Artificiais para Predição de falhas em *Links* de redes ópticas", Universidade Federal do Ceará, dissertação de mestrado em Ciências da Computação, 2003.
- [26] MILTON, Gilmour, "Testes de Redes SDH", Hewlett-Packard Company – Divisão de Testes de Redes de Comunicações, David A. Lord, 1997.
- [27] BERNSTEIN, Greg; RAJAGOPALAN, B.; SAHAN, D. "Optical Network Control", Addison-Wesley, 2004.
- [28] <http://www.poncedaher.com.br/papers/dwdm/dwdm04.htm>. Acessado em Julho de 2004.
- [29] [http://www.jdsu.com/brazil/technical\\_resources/product\\_documents/datasheet/da320Otun\\_dsdat\\_tm\\_ae\\_1005.pdf](http://www.jdsu.com/brazil/technical_resources/product_documents/datasheet/da320Otun_dsdat_tm_ae_1005.pdf). Acessado em Janeiro de 2006.
- [30] LANG, J. ; RAJAGOPALAN, P. "Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification". *Internet Draft*, 2005.
- [31] MANNIE, E. "Generalized Multi-Protocol Label Switching (GMPLS) Architecture". *Internet Draft*, draft-ietf-ccamp-gmpls-architecture-07.txt. Maio, 2003.
- [32] NS. Network Simulator. Sitio do simulador. Url: <http://www.isi.edu/nsnam>. Acessado em: outubro, 2004.
- [33] AHN, Gaiel; CHUN, Woojik. "Design and Implementation of MPLS Network Simulator". Url: <http://flower.ce.cnu.ac.kr/~fog1/mns/>. Acessado em: outubro 2004.
- [34] ABELÉM, A. "Implementação de um Agente para Realizar Mapeamento entre Serviços Integrados e Serviços Diferenciados". Monografia, Departamento de Informática, PUC-Rio, Fevereiro, 2001.
- [35] <http://ntspo903/crtxbhe/RedeÓpticaLongaDistância/Rede%20Óptica%20Longa%20Distância.htm>. Acessado em Março de 2004.
- [36] ESTEVES, R.; VIANA, J.; ABELÉM, A.; COSTA, J. C.; STANTON, M. "A Model of GMPLS Signaling for Optical Burst Switched Networks: Description and Analysis" (Short-paper). In: Anais do 23o Simpósio Brasileiro de Redes de Computadores (SBRC2005), pp. 67-122, Fortaleza, CE, Brasil. Maio, 2005.
- [37] VIANA, J.; ESTEVES, R; ABELÉM, A; COSTA, J. C.; STANTON, M. "Análise de Mecanismos de Recuperação de Falhas em Redes Ópticas de Nova Geração com Plano de Controle Baseado no GMPLS". In: IV Workshop em Desempenho de

Sistemas Computacionais e de Comunicação-WPERFORMANCE (inserido no SBC2005), São Leopoldo, RS, Brasil. Julho, 2005.

- [38] BICUDO, Marco D. "Sobrevivência em Redes Ópticas Transparentes", Dissertação de Mestrado - Universidade Federal do Rio de Janeiro, COPPE, Rio de Janeiro, 2005.
- [39] PUYPE, Bart; VASSEUR, J.; GROEBBENS, A.; PICKAVET, M. e DEMEESTER, P. "*Benefits of GMPLS for Multilayer Recovery*", IEEE Communications Magazine, Vol. 43, No. 7, pp. 51-59, Julho 2005.
- [40] KARTOLOPOULOS, S. V.; "*Fault Detection in DWDM - Toward Higher Signal Quality & System Reliability*". New York: IEEE Press, 2001.
- [41] BUENO, L.; ALMEIDA, T. R.; SEGATTO E. V.; OLIVEIRA, E. "Uma Heurística para Projeto de Topologias Virtuais de Redes Ópticas Tolerantes a Falhas". Anais do 23o Simpósio Brasileiro de Redes de Computadores (SBRC2005), pp. 67-122, Fortaleza, CE, Brasil. Maio, 2005.
- [42] [http://www.irisa.fr/prive/bcousin/Articles/boudania\\_mplssimulator.pdf](http://www.irisa.fr/prive/bcousin/Articles/boudania_mplssimulator.pdf). Acessado em maio de 2006.
- [43] <http://dawn.cs.umbc.edu/Papers/2001/ONM01b.pdf>. Acessado em maio de 2006;
- [44] BIANCHI, G. "Performance analysis of the IEEE 802.11 Distributed Coordination Function". IEEE Journal on Selected Areas in Communications, VOL 18, N0 3 , pag.535-547, Março 2002;
- [45] [http://www.tidia.fapesp.br/portal/Midia/clipping-2003/inovacao\\_unicamp](http://www.tidia.fapesp.br/portal/Midia/clipping-2003/inovacao_unicamp). Acessado em maio de 2006.

# **ANEXO 1 - Resultados dos Testes nas rede Testbed Gerados pelo analisador de WAN DA-3200 WAN Traffic Report**



Prepared for: DISSERTA

Prepared by: Rocha/Jaime - EBT BLM

Test Start Time: 01/16/06 18:43:51

Test End Time: 01/16/06 18:49:44

**Physical Results for Data**

**Data Setup**

Access Mode	Data Monitor
Interface	V.35

**Data Status**

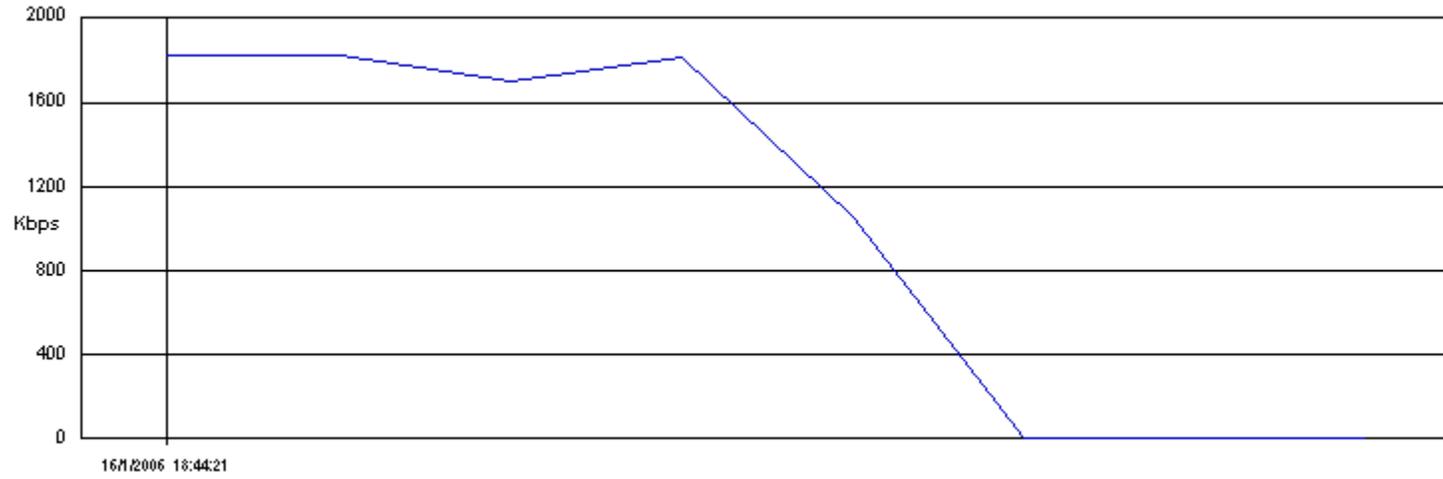
	From DTE	From DCE
Clock Present	␣	␣
Clock Loss	..	..
RTS RLS	␣	␣
DTR DSR	␣	␣
LL CTS	..	␣
RL TM	..	..

**Data Results**

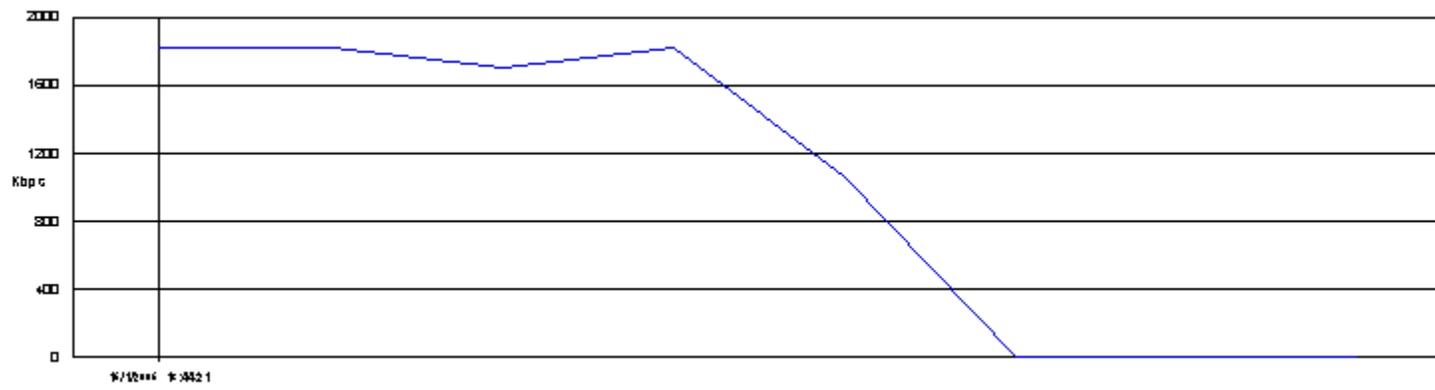
Elapsed Seconds	353	353	seconds
Clock Losses	0	0	count
TT	2047985		Hz
RT	2047985		Hz
ST	2047985		Hz
RT-ST Timing Slip	0		Hz

### Total Throughput Trend

#### From DTE



#### From DCE



**Total Link Statistics**

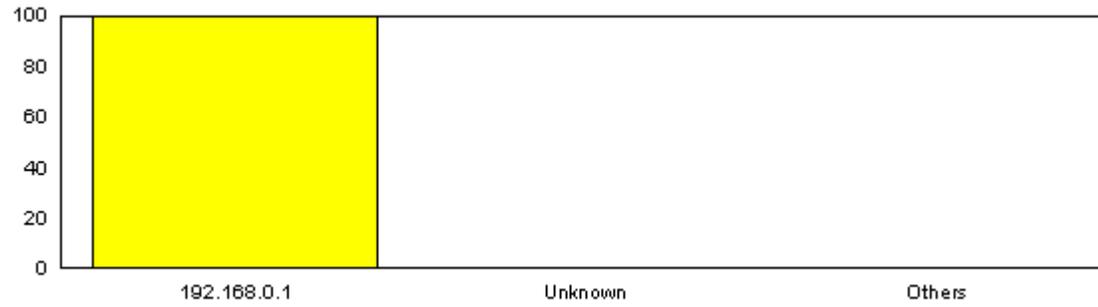
	From DTE	From DCE
Total Frames	26,029	26,030
Frame length(4-63)	36	39
Frame length(64-127)	0	0
Frame length(128-255)	0	0
Frame length(256-1023)	2,005	2,005
Frame length( > 1024)	23,988	23,986
Bad FCS	0	3
Aborted Frames	0	1
Undecodable Frames	0	0

**Conversations**

IP Address #1	IP Address #2	Application	Bytes		Packets	
			1 -> 2	2 -> 1	1 -> 2	2 -> 1
Totals			36,668,916	36,666,508	26,029	26,030
192.168.0.1	192.168.0.1	ICMP Reserved (ICMP Type 171, Code 205)	33,655,164	33,651,882	23,988	23,985
192.168.0.1	192.168.0.1	Echo Request (ICMP Type 8, Code 0)	1,506,000	1,506,000	1,000	1,000
192.168.0.1	192.168.0.1	Echo Reply (ICMP Type 0, Code 0)	1,504,494	1,504,494	999	999
Unknown	Unknown	Unknown	3,196	4,070	41	45
192.168.0.1	192.168.0.1	Fragment Reassembly Time Exceeded (ICMP Type 11, Code 1)	62	62	1	1

### IP Top Talkers

#### From DTE

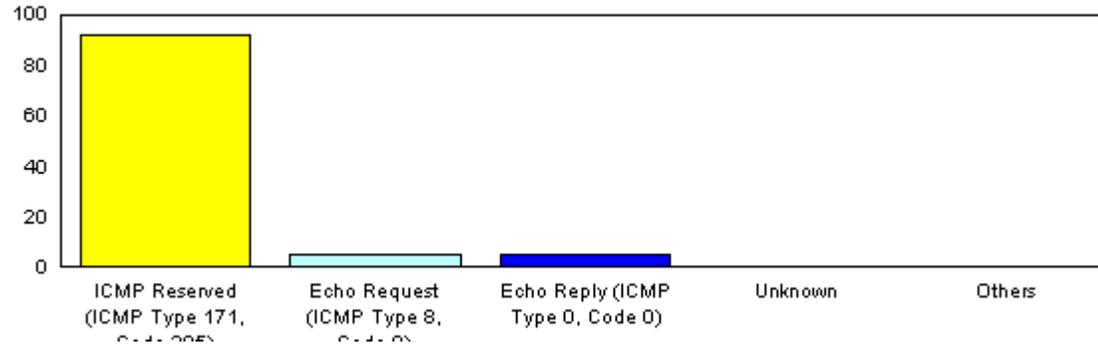


#### From DCE

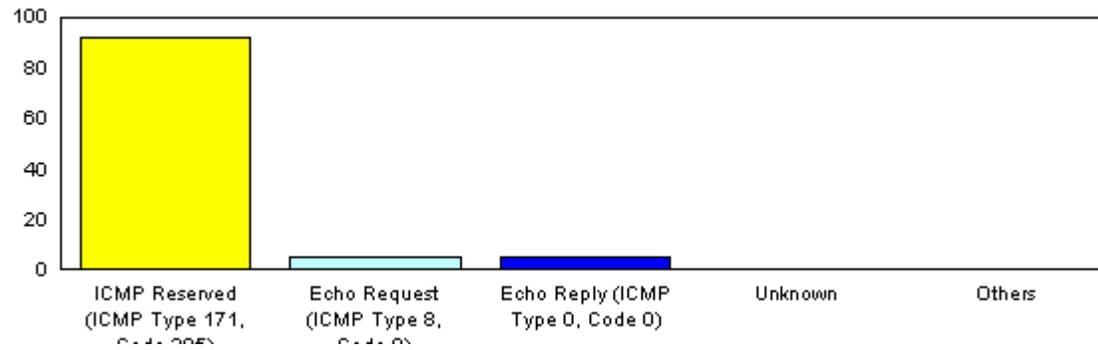


## Applications

### From DTE



### From DCE



### Top Protocols

#### From DTE



#### From DCE

