UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

IMPLEMENTAÇÃO DE UM SISTEMA DE CONTROLE CENTRALIZADO PARA UMA REDE ÓPTICA TRANSPARENTE

HONÓRIO ASSIS FILHO CRISPIM

ORIENTADOR: HUMBERTO ABDALLA JÚNIOR

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA
PUBLICAÇÃO: PPGENE.TD – 011/06

BRASÍLIA-DF, AGOSTO DE 2006

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

IMPLEMENTAÇÃO DE UM SISTEMA DE CONTROLE CENTRALIZADO PARA UMA REDE ÓPTICA TRANSPARENTE

HONÓRIO ASSIS FILHO CRISPIM

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

APROVADA POR:

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

_____
Prof. Dr. Antonio José Martins Soares (UNICAMP)
(Examinador Interno)

_____
Prof. Dr Luiz Fernando Ramos Molinaro (USP)
(Examinador Interno)

_____
Prof. Dr. Felipe Rudge Barbosa (UNICAMP)
(Examinador Externo)

_____
Prof. Dr Li Weigang, Dr (ITA)
(Examinador Externo)

BRASÍLIA-DF, AGOSTO DE 2006

FICHA CATALOGRÁFICA

CRISPIM, HONÓRIO ASSIS FILHO

Implementação de um sistema de controle centralizado para uma rede óptica transparente [Distrito Federal] 2006.

xvii, 196p., 297 mm (ENE/FT/UnB, Doutor, Engenharia Elétrica, 2006). Dissertação de Doutorado – Universidade de Brasília. Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1.Redes WDM 2.Sistema de Controle

3.RWA 4.Auditoria

I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

CRISPIM, H. A. F. (2006). **Implementação de um sistema de controle centralizado para uma rede óptica transparente**. Dissertação de Doutorado em Engenharia Elétrica, Publicação PPGENE.TD-011/06, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília: DF, 196p.

CESSÃO DE DIREITOS

AUTOR: Honório Assis Filho Crispim.

TÍTULO: Implementação de um sistema de controle centralizado para uma rede óptica transparente.

GRAU: Doutor ANO: 2006

_____

Honório Assis Filho Crispim.

QS 05 Rua 860 Casa 18 – Bairro Águas Claras.

72030-150 Distrito Federal – Brasil.

AGRADECIMENTOS

Agradeço em primeiro lugar a DEUS que, simplesmente, me permitiu existir.

Externo o mais profundo agradecimento ao meu orientador Humberto Abdalla Júnior, por acreditar na minha pessoa e me permitir caminhar sem amarras, mas com uma forte supervisão.

Agradeço a minha família por estruturar um alicerce que me deixa extremamente seguro ao caminhar.

Agradeço ao Corpo de Bombeiros Militar do Distrito Federal por todo apoio e credibilidade dispensada durante a minha caminha profissional.

Agradeço ao CPqD e a todos os seus funcionários por me permitirem uma aproximação baseada na busca de um conhecimento diferenciado e pragmático.

Externo meu agradecimento ao CNPq que representa uma chama de esperança para aqueles que persistem em estudar, mesmo quando as condições financeiras apresentam-se desfavoráveis e uma ajuda externa torna-se vital.

Agradeço...

Adão Teixeira de Macedo	Pelas ajudas nas implementações do módulo de segurança e auditoria.
Adriana Mariano Rêgo	Por suas valiosas traduções do português para o inglês e pelas noites perdidas na produção de artigos urgentes.
Alberto Paradisi	Pelo apoio dado desde a primeira visita ao CPqD, bem como pela paciência com o lento processo de aprendizado na área.
Aliomar Mariano Rêgo	Pelas ajudas com os *softwares* livres de desenvolvimento e banco de dados.
Amilton Mariano Rêgo	Pelas contribuições na Casa Militar, que

	me permitiu estar na Universidade nos momentos oportunos.
Antônio Carlos Lopez Medeiros	Pela compreensão quanto à continuidade dos estudos no decorrer de sua gestão.
Antônio de Campos Sachs	Por todos os auxílios prestados tanto no campo do conhecimento da física, quanto da estrutura dos trabalhos acadêmicos.
Antônio José Martins Soares	Pela compreensão do difícil processo de adaptação junto ao paradigma do doutorado.
Cristiane Arakaki	Pela paciência tipicamente japonesa no trato dos desafios técnicos demandados por mim.
Daniela Fávaro Garrossini	Por suas inúmeras contribuições tanto na área de disign, quanto no relacionamento em equipe.
Edivan Morais de Medeiros	Pelas valiosas figuras produzidas no Microsoft Visio.
Eduardo Tommy Lopez Pastor	Por todas as contribuições realizadas e por todos os trabalhos que fizemos e publicamos juntos.
Fabrício Braz	Pelas contribuições na área de orientação a objetos e, acima de tudo, na humana.
Felipe Rudge Barbosa	Pela adoção espontânea de um aluno incipiente na complicada área fotônica.
Georges Amvame-Nze	Por todas as contribuições na área de redes e, principalmente, na área humana.
Jorge Cezar de Araújo Caldas	Por, desde o princípio, permitir que eu freqüentasse a Universidade de Brasília para realizar o doutorado.
Juliana Fernandes Camapum	Pelas contribuições realizadas e o tempo dispensado com a troca de idéias.
Li Weigang	Pelo apoio concedido em todos os

	momentos que nos comunicamos.
Luís Fernando Ramos Molinaro	Por, durante toda minha permanência na UnB, me permitir desfrutar do Núcleo de Multimídia e Internet.
Oficiais e praças da Casa Militar	Pela compreensão das ausências e o carinho dispensado nas horas difíceis.
Professores da Elétrica	Por me mostrarem como é fascinante o processo de ensino-aprendizado.
Sandro Marcelo Rossi	Por todo o apoio a mim prestado, inclusive nos momentos de suas folgas e férias.
Secretárias e agentes administrativos da FT /Departamento de Eletricidade	Pelo apoio prestado ao difícil processo administrativo de formar um doutor.

Quando ingressei no doutorado da Engenharia Elétrica da UnB eu tinha a crença de não ter muito conhecimento. Hoje, após anos de estudo e término do curso, tenho a certeza absoluta.

O autor.

Dedico à minha esposa Ariene e aos meus filhos Calvin e Stéfane.

RESUMO

IMPLEMENTAÇÃO DE UM SISTEMA DE CONTROLE CENTRALIZADO PARA UMA REDE ÓPTICA TRANSPARENTE

Antes mesmo de considerar inovação e expansão, maximizar o aproveitamento de infra-estruturas de redes já implantadas tem sido o norte das ações de empresas na área de telecomunicações; exemplos dessa assertiva podem ser citados como as estratégias tecnológicas WDM e DSL.

O estudo registrado nesse documento trata especificamente da implementação de um modelo centralizado de controle de uma rede óptica transparente que, entre outros aspectos, agrega valor no processo de gerência quando viabiliza ações simples e rápidas sobre uma rede com relativa complexidade. Desta forma, fica para o gerente da rede a tarefa de otimizar o uso dos recursos já instalados, o que se coaduna com as boas práticas no mercado.

O modelo proposto, implementado e testado foi dividido em três camadas típicas: gerência, controle e simulação dos elementos físicos.

A camada de gerência implementa um forte conceito de segurança e auditoria, que permite um completo monitoramento de todas as ações sobre a rede. Esta camada foi desenvolvida no modelo Web, o que lhe conferiu simplicidade na interface e permitiu ao gerente alta mobilidade.

No sistema de controle usou-se o algoritmo de Dijkstra para o cálculo do melhor caminho, mas possibilitou-se a criação de rotas explícitas (criadas sob o controle exclusivo do gerente). Para a alocação do comprimento de onda associado à rota utilizou-se o algoritmo First Fit, que apresentou uma facilidade no processo de saturação da rede quando submetida a mais de trinta requisições num cenário de rede em malha com cinco nós.

A camada física foi simulada no que diz respeito ao acionamento dos OXCs e operações básicas dos transponders e amplificadores. Nesta etapa foi usado XML como elemento básico para armazenamento e trâmite dos dados.

Todo o trabalho realizado revelou como resultado a necessidade da adoção de uma solução híbrida para modelos de redes ópticas estruturadas em camadas. Em síntese, evidenciou-se como boa prática buscar a centralização das demandas com vistas à obtenção de segurança e rastreabilidade, centralização parcial do sistema de controle para permitir a adoção de processamentos mais inteligentes das demandas por caminhos ópticos e distribuição do mecanismo de proteção das rotas, por exigirem alto desempenho.

ABSTRACT

IMPLEMENTATION OF A CENTRALIZED CONTROL SYSTEM FOR A TRANSPARENTE OPTICAL NETWORK

Before to consider innovation and expansion, maximize the utilization of the implanted structures has been the north of the actions of companies in the area of telecommunications; examples of this assertive can be cited as the technological strategies WDM and DSL.

The study registered in this document treats specifically of the implementation of a centralized control model of a transparent optical network which, among others aspects, add value in manager process when makes possible simple and fast actions by a relative complexity network. In spite of this, it is for the manager of the network the task to optimize the use of the already installed resources, which is similar to good practices in market.

The implemented and tested model proposed was divided in three typical layers: manager, control and simulation of physic elements.

The manager layer implements a strong security and auditorship concept, which permits a complete supervise of all network actions. This layer was developed in web model, that gives simplicity in the interface and permits high mobility to the manager.

In the control system was used a Dijkstra algorithms to calculate the best way, but made possible the creation of explicit routes (created by a exclusive manager control). To the allocation of the lambda associated to the route was used the First Fit algorithms, which presented easiness in network saturation process when submitted to more than thirty solicitations in a scenery with five nodes.

The physical layer was simulated in respect of OXCs switching and basics operations of transponders and amplifiers. In this phase was used XML as basic elements to store and data process.

All the work realized showed as result the necessity of adoption of a hybrid solution to optical networks models structured in layers. In synthesis, was proved as good practice search the demands centralization to obtain security and log, partial control system centralization to permits the adoption of more intelligent proceedings to the demand of the optical networks and distribution of routes protection mechanism, to need high performance.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS, NOMECLATURA E ABREVIAÇÕES

ATM	*Asynchronous Transfer Mode* (Modo de Transferência Assíncrono)
CSMA/CD	*Carrier Sense Multiple Access / Collision Detection* (Acesso Múltiplo de Sentido da Portadora com Detecção de Colisão)
DWDM	*Dense Wavelenght Division Multiplexing* (Multiplexação Densa Por Divisão do Comprimento de Onda)
GMPLS	*Generalised Multiprotocol Label Switching* (Protocolo de Chaveamento por Rótulos Generalisado)
IETF	*Intenernet Engineering Task Force* (Força Tarefa para Engenharia da Internet)
IP	*Internet Protocol* (Protocolo de Internet)
ITU-T	*International Telecommunication Union – Telecommunication* (União Internacional de Telecomunicações - Telecomunicações)
LSP	*Label Switched Path* (Caminho Chaveado por Rótulo)
MPLS	*Multiprotocol Label Switching* (Multiprotocolo de Chaveamento por Rótulo)
MPλS	*Multiprotocol Lambda Switching* (Multiprotocolo de Chaveamento por Lambda)
OADM	*Optical Add-Drop Multiplexer* (Multiplexador Óptico de Inserção-Derivação)
OSI	*Open Systems Interconnection* (Interconexão de Sistemas Abertos)
OTDM	*Optical Time Division Multiplexing* (Multiplexação por Divisão Óptica no Tempo)
OXC	*Optical Cross-Connect* (Comutador Óptico)
RWA	*Routing and Wavelength Assignment* (Roteamento e Designação de Comprimento de Onda)
SDH	*Synchronous Digital Hierarchy* (Hierarquia Digital Síncrona)
SONET	*Synchronous Optical Network* (Rede Óptica Síncrona)
SRLG	*Shared Risk Link Group* (Grupo de Arcos com Risco Compartilhado)
WDM	*Wavelength Division Multiplexing* (Multiplexação por Divisão do Comprimento de Onda)

1 INTRODUÇÃO

Este capítulo descreverá os aspectos estratégicos do trabalho de pesquisa e desenvolvimento realizado, bem como sua justificativa e contexto. Desta forma, será realizada uma descrição do assunto abordado, definido o problema e apontados os objetivos desse estudo.

1.1 DEFINIÇÃO DO PROBLEMA

Este trabalho tem como foco estudar a viabilidade da implementação de um sistema de controle centralizado para uma rede óptica transparente como solução alternativa ao uso dos sistemas distribuídos. Assim, estudou-se por intermédio da revisão bibliográfica a evolução das redes ópticas, os componentes lógicos e físicos das mesmas, bem como se dissecou uma implementação distribuída para melhor embasar o leitor com relação ao assunto em pauta.

De uma forma geral, se percebe a complexidade desse trabalho espalhada ao longo dos vários pontos do mesmo, tanto relativo à parte física quanto à lógica. Assim, esta redação adotou uma estrutura de informação do tipo progressiva e diferenciada para que o leitor possa entender com clareza os resultados finais de tal estudo.

Após a definição clara da viabilidade ou não da implementação de uma solução centralizada, se faz necessário o teste exaustivo da solução proposta a fim de corroborar a correlação existente entre os aspectos teóricos utilizados e o comportamento prático do sistema projetado e desenvolvido.

O sistema distribuído utilizado como referência foi desenvolvido pelo CPqD[1] para uma rede óptica metropolitana denominada OMEGA. Neste trabalho foram desenvolvidos o *software* de controle da referida rede e toda a montagem e caracterização do *hardware*.

---

1 O CPqD (*Fundação CPqD Centro de Pesquisa e Desenvolvimento em Telecomunicações)* é um dos mais conceituados pólos de tecnologia do mundo em telecomunicações e tecnologia da informação.. *Endereço: Rodovia Campinas - Mogi-Mirim, km 118,5CEP 13086-902 - Campinas, SP - Brasil.* Acessado em http://www.cpqd.com.br/ - 17/6/2005 10:04:37.

Além das questões que envolvem diretamente os equipamentos e *software* de uma rede óptica metropolitana, este trabalho aborda aspectos relativos ao contexto prático da utilização dos mesmos, que se coadunam com ações de inovação e melhorias das operadoras de telecomunicações.

O sistema de controle da rede óptica desenvolvida pelo CPqD é calcado basicamente numa visão distribuída. Assim, cada nó da rede pode ser considerado um agente de controle capaz de interferir diretamente na operação dos demais e vice-versa. Esta solução é considerada avançada para os padrões atuais, mas apresenta limitações como a utilização de elementos genéricos num sistema altamente especializado (ex: microcomputador convencional), e a não possibilidade de um controle *out-off-band* do referido sistema na versão implementada por esse centro de pesquisa.

Os trabalhos que envolvem a área de óptica possuem um fator limitante fortíssimo, que é o financeiro. Os componentes são naturalmente caros e exigem equipamentos igualmente onerosos para serem testados em todas as suas nuances operacionais (caracterização). Nesse contexto, lançando mão dos estudos já realizados e das respectivas caracterizações realizadas pelo CPqD, este trabalho adotou o princípio da simulação da camada física com o objetivo de minimizar os aspectos relativos a custo.

Desta forma, o foco da pesquisa reside no estudo da viabilidade ou não da implementação e uso de um sistema de controle e gerência centralizados para uma rede óptica metropolitana composta por equipamentos semelhantes à rede OMEGA.

Assim, após os argumentos apresentados, se faz a seguinte pergunta, que se constituirá no problema da pesquisa: Um sistema de controle e gerência centralizados conferirá mais segurança a rede óptica metropolitana e atenderá aos exigentes requisitos de funcionalidade e desempenho da mesma?

1.2 OBJETIVOS DO ESTUDO

1.2.1 Objetivo Geral

Diagnosticar a pertinência do uso de um sistema de controle e gerência centralizados numa rede óptica metropolitana como forma alternativa ao modelo distribuído.

1.2.2 Objetivos Específicos

— Apresentar de forma clara e precisa todo o sistema, até o nível de elementos de rede, que compõe a rede óptica metropolitana;

— Pesquisar sobre o impacto do modelo centralizado no desempenho do plano de controle;

— Propor um modelo de *software* que simule a rede tanto do ponto de vista físico, quanto lógico;

1.3 JUSTIFICATIVA

O desenvolvimento tecnológico avançado das redes de computadores tem exigido sistemas de telecomunicações com alta capacidade de taxas de transmissão para as diversas aplicações e sistemas de informação. Assim, as redes ópticas, em especial as WDM, tem se apresentado como a melhor e mais confiável alternativa tecnológica para a resolução de tal problema.

Neste contexto, se percebe a substituição gradativa dos cabos metálicos pelas fibras ópticas na infra-estrutura das redes de telecomunicações, notadamente no núcleo de tais sistemas. Desta forma, esta estratégica vem aumentando significativamente a capacidade e a confiabilidade dos sistemas de comunicação existentes.

A fibra óptica possui uma alta capacidade de transmissão de dados. Associada a esta característica, os meios ópticos podem transmitir, na mesma fibra, diferentes comprimentos de onda através de mecanismos de multiplexação (ex: multiplexação por divisão do comprimento de onda ou WDM - *Wavelength-Division Multiplexing*).

A tecnologia WDM, projetada para usar dois comprimentos de onda, passou, com o uso de amplificadores ópticos baseados em fibra óptica dopada com érbio - EDFA (*Erbium Doped Fiber Amplifier*), a permitir a existência de sistemas comerciais com suporte a até 40 canais (lambdas). Desta forma, convencionou-se que sistemas WDM com número de canais superior a 16 receberiam o nome de sistemas WDM Denso - DWDM (*Dense Wavelength-Division Multiplexing*).

As redes ópticas que usam WDM permitem o desenvolvimento de aplicações de alta performance, que dão suporte a sistemas corporativos e residenciais de multimídia, vídeo-conferência, ensino à distância, TV digital e outros. Além de tais vantagens, essa tecnologia maximiza o uso da infra-estrutura de fibras ópticas existentes, o que permite um significativo e rápido retorno econômico do investimento realizado.

As redes ópticas metropolitanas, também conhecidas como redes metro-acesso/metro-tronco, permitem a implantação de acessos em alta velocidade para instituições por meio de uma infra-estrutura própria e dedicada. Dentre as várias redes metro já implantadas no Brasil destacam-se as das seguintes cidades: Rio de Janeiro, São Paulo, Belo Horizonte, Curitiba e os projetos em andamento para Brasília.

De acordo com o exposto, torna-se mister desenvolver tecnologias de custo atraente para redes ópticas metropolitanas que representem flexibilidade das interfaces quanto aos serviços e protocolos envolvidos na solução. Desta forma, o trabalho em questão corrobora tal assertiva e busca apresentar uma implementação centralizada do sistema de controle e gerência de uma rede metro, de maneira a permitir uma robusta operacionalização da mesma, bem como permitir maior escalabilidade e flexibilidade na sua montagem.

1.4 ESTRUTURA DO TRABALHO

As redes ópticas envolvem soluções nas diversas camadas e apresentam um grau de complexidade acentuada. De uma forma geral, tem-se uma visão estratégica dessas camadas em três níveis em ordem crescente: o primeiro nível corresponde ao físico, o segundo ao de controle e o terceiro e último à gerência.

Considerando o modelo estratégico apresentado anteriormente, este trabalho será estruturado de forma a permitir ao leitor um entendimento intuitivo e prático tanto do problema em si, quanto de toda a solução proposta e testada para as respectivas camadas.

Do ponto de vista da organização do conhecimento, o estudo em questão está estruturado em duas fases. A primeira fase corresponde a exposição do embasamento teórico que permita ao leitor o entendimento claro do problema e das possíveis soluções, bem como apresenta a definição clara do trabalho a ser realizado. Assim, fazem parte da primeira etapa o Capítulo 1, 2, 3, 4, 5 e 6.

O capítulo 1 descreve o problema em si, aponta o objetivo principal e os específicos da pesquisa e apresenta a justificativa para o estudo proposto.

O capítulo 2 aponta as questões relativas ao histórico das redes ópticas através de uma rápida visão de uma rede metropolitana e das gerações que compõem uma rede óptica.

O capítulo 3 tem foco na camada física de uma rede óptica. Assim, são apresentados os elementos físicos da mesma.

O capítulo 4 apresenta e discute a camada de controle. Inicialmente, são mostrados os modelos preconizados tanto no mercado, quanto na área acadêmica. Neste capítulo também estão inseridas as apresentações dos protocolos MPLS, MPΛS, GMPLS, Ethernet e IP.

O capitulo 5 detalha os aspectos específicos da rede OMEGA, que serviu como modelo de uma implementação distribuída para este estudo.

Por último, o capítulo 6 descreve os princípios científicos que embasam o estudo apresentado. Assim, são explicitadas neste texto as questões relativas a delimitação do universo e do espaço amostral para a realização do estudo, bem como o porquê da utilização do conceito de simulação e as assertivas que embasarão tal simulação. Além destes tópicos são apresentados os aspectos computacionais relativos a implementação da solução.

A segunda etapa corresponde à apresentação dos resultados, a discussão dos mesmos e a conclusão. Esta etapa é composta dos Capítulos 7 e 8.

O capítulo 7 apresenta os resultados obtidos no estudo, bem como a discussão sobre os mesmos.

O capítulo 8 é dedicado à apresentação da conclusão e das recomendações para trabalhos futuros.

A estrutura deste estudo se apresenta como um modelo típico de um trabalho científico, que tem sua macro-organização baseada nos seguintes princípios: apresentação clara do problema a ser estudado, existência de uma forte revisão bibliográfica que fundamente o leitor e o conduza ao entendimento pleno do estudo, a definição de uma metodologia científica coerente com o trabalho proposto, a apresentação dos resultados obtidos e a discussão sobre os mesmos e, por último, a conclusão a que chegou a pesquisa e as repercussões da mesma sobre trabalhos futuros.

2 ARQUITETURA DE REDES ÓPTICAS

Este capítulo apresenta as três gerações de redes de tecnologia óptica: as redes ópticas de Primeira Geração, caracterizadas pela substituição dos meios de transmissão de redes metálicas por fibras ópticas; as de Segunda Geração, que dispõem as fibras em arranjos específicos para sua funcionalidade; e as de Terceira Geração, as quais utilizam roteamento de comprimento de onda.

A divisão desse tópico em gerações é meramente didática e tem o objetivo básico de evidenciar características julgadas marcantes no processo de apresentação cronológica da evolução da tecnologia fotônica. Assim, se deve entender que em outras abordagens literárias essa estratificação não seja a mesma em função de aspectos físicos que permeiam as tecnologias e, consequentemente, não permitem uma divisão tão cartesiana da evolução das mesmas em simples camadas.

2.1 HISTÓRICO

Transmissão em fibras ópticas tem se constituído numa peça chave para o crescimento da largura de banda nas redes de telecomunicações. Fibras ópticas em comparação com cabos metálicos, além de disponibilizarem uma banda muito maior, também oferecem inúmeras outras vantagens como: baixa taxa de erros para maiores velocidades; alta resistência física e flexibilidade; imunidade a ruído e interferência eletromagnética; além de segurança e privacidade. Como conseqüência dessas vantagens, elas estão sendo o meio preferido para a transmissão de dados em qualquer sistema com taxas de transmissão da ordem dos Gbps e sobre distâncias maiores que 1 Km. Além disso, são utilizadas para interconexões a pequenas distâncias dentro de redes de computadores.

As redes baseadas em fibra começaram a ser implementadas no começo da década de 80 e, atualmente, são largamente usadas em muitas redes de telecomunicações. No final dessa década e início dos anos 90 começou-se a planejar arquiteturas de redes inovadoras, além da simples transmissão ponto-a-ponto. A maior parte dos esforços concentrou-se em redes WDM e similares (OTDM), o que continua até hoje.

Ao se incorporar algumas das funções de comutação, roteamento e processamento na parte óptica da rede, as quais eram desempenhadas apenas por equipamentos eletrônicos, muitas vantagens foram sendo adquiridas, tais como: maior capacidade de transmissão, decorrente da conseqüente diminuição na sobrecarga de processamento eletrônico, assim como transparência na rede.

No final da década de 90, o desenvolvimento de sistemas WDM de alta capacidade operando com 8, 16 e 32 comprimentos de onda, cada qual transportando informações a 2.5 Gbps e, posteriormente, 10 Gbps, tornou redes ópticas transparentes uma realidade prática. Pesquisas laboratoriais recentes estão testando taxas de 40 Gbps por canal e que atingem a ordem dos Tbps de capacidade total por fibra.

2.2 REDES ÓPTICAS DE PRIMEIRA GERAÇÃO

Com a fibra óptica como meio de transmissão de alta velocidade, agregado a um desenvolvimento da tecnologia fotônica de um modo geral, os sistemas de comunicações começaram a dispor da fibra como meio de transporte em substituição ao par trançado. Essa revolução fez surgir diversos padrões de transmissão como o *Synchronous Optical Network* (SONET) nos Estados Unidos e *Synchronous Digital Hierarchy* (SDH) na Europa. Além disso, fomentou o desenvolvimento de redes metropolitanas como a FDDI (*Fiber Distributed Data Interface*), que é uma das representantes mais conhecidas, e redes responsáveis pelo interligamento de computadores de grande porte, como por exemplo a ESCON (*Enterprise Serial Connection*).

Entretanto, visto que, nessas redes, apenas os enlaces de transmissão passaram a pertencer ao domínio óptico, todas as tarefas de comutação, processamento e roteamento continuavam a ser desempenhadas no domínio eletrônico. Estes tipos de redes são classificados como Redes Ópticas de Primeira Geração. Atualmente, essas redes estão largamente implementadas nas infra-estruturas públicas de telecomunicações, na interconexão de computadores, bem como em redes locais e metropolitanas.

2.3 REDES ÓPTICAS DE SEGUNDA GERAÇÃO

O desenvolvimento de dispositivos estáticos e passivos, com capacidade de dividir e combinar sinais ópticos, realizando conectividade entre transmissores e receptores ópticos no domínio fotônico, impulsionaram a Segunda Geração de redes ópticas. A essas redes ópticas, que estabeleceram tais conectividades sem dispor de mecanismos de roteamento da luz de acordo com o seu comprimento de onda, designou-se de redes ópticas de Segunda Geração.

Redes baseadas nessa arquitetura, para que consigam estabelecer conectividade óptica total entre todos os seus integrantes, necessitam, ao receber o sinal de um determinado nó, transmiti-lo a todos os outros nós que a integram. Além disso, para que a detecção de um sinal seja possível, a presença na recepção de algum mecanismo capaz de sintonizar um canal (comprimento de onda) específico e rejeitar os vizinhos torna-se imprescindível. Devido a essas características mencionadas acima, as redes ópticas de Segunda Geração também são comumente referidas como redes *Broadcast and Select*.

Por não utilizarem nenhuma função de roteamento, é indispensável que essas redes também disponham de um compartilhamento do meio para o estabelecimento das conexões [SOMANI, 2006]. Dessa forma, faz-se necessário à utilização de topologias físicas adequadas, capazes de permitir a distribuição dos sinais luminosos em todos os comprimentos de onda para todos os nós da rede. As duas topologias mais populares para essas arquiteturas de rede são a estrela (Figura 2.1) e o barramento (Figura 2.2), ambas as quais fazem uso de acopladores ópticos[2].

[2] Acopladores Ópticos são dispositivos ópticos passivos e recíprocos, capazes de combinar e dividir a potência do sinal sem qualquer seletividade de comprimento de onda.

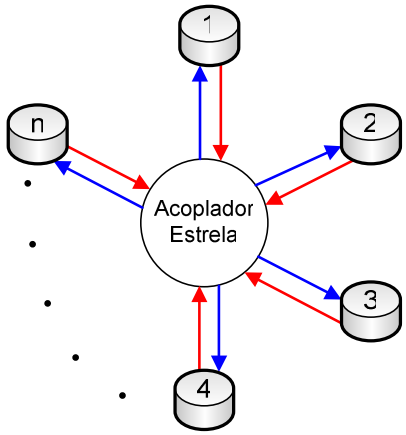

Figura 2.1 - Rede óptica com topologia estrela.

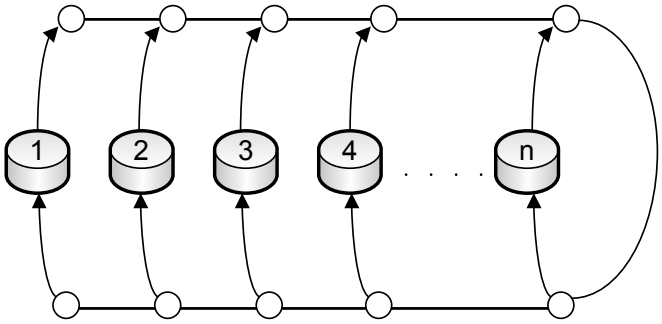

Figura 2.2 - Rede óptica com topologia em barramento.

Cada um dos nós da figura acima (mostrados como círculos) podem ser construídos utilizando um ou mais acopladores direcionais 2x2. Estes são dispositivos de quatro portas (quadripolo) tal que, a potência óptica proveniente de uma determinada fonte, ao entrar no acoplador mediante uma das portas de entrada, é dividida linearmente e combinada com uma parcela do sinal provinda da outra entrada, gerando assim parcelas de ambas as entradas nas saídas do acoplador, conforme mostrado na Figura 2.3, onde as portas 1 e 2 são as entradas e 1´ e 2´ as saída.

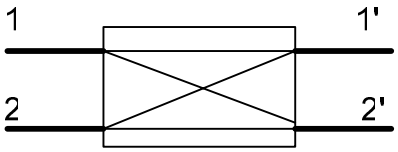

Figura 2.3 - Acoplador Óptico 2x2

Na topologia de barramento da Figura 2.2, os nós transmitem ao barramento através dos acopladores superiores (observe que apenas uma das portas de saída é utilizada), e recebem através dos inferiores (neste caso, uma das portas de entrada é a inutilizada), necessitando assim de 2-n acopladores, sendo n o número de nós da rede. Um fato interessante nesse tipo de topologia é que não é vantajoso se fazer uma repartição igualitária das potências, pois a maior parte desta deve permanecer no barramento para poder alimentar os outros nós.

Em nível de funcionalidade, as duas topologias são idênticas, pois ambas são redes *broadcast* com a potencialidade de suportar conexões unidirecionais ponto-a-ponto entre os n nós da rede. Entretanto, as redes em estrela apresentam-se mais eficientes quando comparadas às em barramento no que diz respeito à conservação e distribuição da potência do sinal. O acoplador em estrela, conforme explicado anteriormente, combina os sinais provenientes dos transmissores (Tx) de todas as estações e os distribui para todos os receptores (Rx) das outras estações (incluindo o da própria transmissora), permitindo assim conectividade óptica entre todos os pares Tx e Rx presentes nas estações. Contudo, um nó cliente só poderá receber informações de um outro nó cliente qualquer (estabelecendo assim uma conectividade lógica com ele), caso o Rx presente em sua estação de acesso à rede selecione (sintonize) o comprimento de onda responsável por transportar a informação destinada para ele e descarte todos os outros.

Neste contexto se deve diferenciar a topologia física das topologias lógica e virtual, esta última também conhecida como topologia de caminhos físicos [GRENN Jr., 1993].

A topologia física de uma rede é a responsável pela interligação física dos nós da mesma, ou seja, refere-se à presença e à disposição dos componentes da rede óptica, tais como as fibras, acopladores ópticos e outros. Sobre a topologia física, pode-se sobrepor uma topologia de caminhos físicos particulares, sendo esta entendida pelo grafo que descreve a trajetória da informação por todos os nós intermediários entre o nó origem e o nó destino, para cada par origem-destino. Desta forma, pode-se definir a topologia lógica como sendo a representação que descreve a cada instante as conexões ativas na rede, sem que se preocupe com a forma de disposição dos seus elementos nem com a trajetória seguida pela informação.

As figuras a seguir (Figura 2.4 e Figura 2.5) procuram mostrar a distinção entre as topologias física e virtual de uma rede óptica. A topologia física é composta pelo acoplador óptico em estrela, pelos três nós da rede e pelos três pares de fibras interconectando os nós ao acoplador. A topologia virtual, que pode ser entendida como a configuração de rede vista pela camada cliente da parte fotônica, é composta por caminhos físicos representados por um ramo direcionado para cada par de nós em que o transmissor da origem do ramo e o receptor do destino do ramo estejam sintonizados no mesmo comprimento de onda. Portanto, devido à forma como os lasers e filtros estão sintonizados na Figura 2.4, a topologia virtual resultou num grafo com disposição em anel, conforme mostra a Figura 2.5.

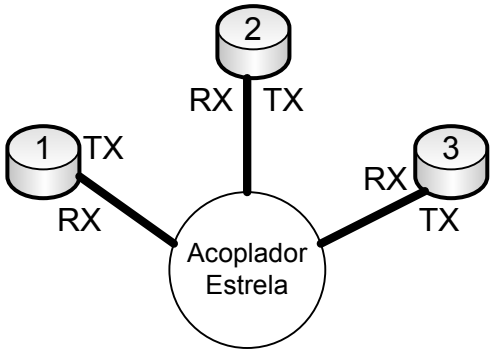

Figura 2.4 - Topologia física da rede

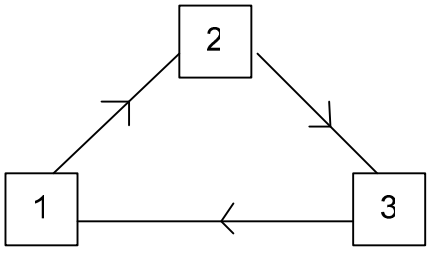

Figura 2.5 - Topologia virtual da rede

Os argumentos apresentados acima mostram claramente que a utilização de uma topologia física do tipo *broadcast and select* implica uma conectividade física total entre todos os nós da rede, não significando, contudo, que esta mesma conectividade (total) se transporte obrigatoriamente para a topologia de caminhos físicos. Fatores como a restrição no número de pares Tx/Rx presentes nas estações de acesso à rede, a qual acarreta a necessidade de sintonizar um conjunto restrito de canal por vez, associado com as

limitações de agilidade na mudança de sintonia dos componentes são os principais impossibilitadores dessa transferência.

Visto que numa rede *broadcast and select* qualquer sinal transmitido por um nó é difundido para todos os outros nós da rede e que cada nó necessita selecionar o sinal desejado entre todos os transmitidos, caso alguns deles estejam utilizando transmissores e/ou receptores sintonizáveis, haverá a necessidade de informá-los em qual comprimento de onda se deve transmitir/receber a informação para que suas conexões possam ser estabelecidas com sucesso. Assim, se dois desses nós transmitirem simultaneamente no mesmo comprimento de onda, seus sinais irão colidir e ambos serão perdidos.

Uma outra possibilidade a analisar é a de dois ou mais nós transmitirem simultaneamente em comprimentos de onda diferentes, porém para um mesmo destino. Caso o nó destino possua apenas um único receptor sintonizável, ele só será capaz de selecionar um dos canais, sem que consiga, portanto, receber as informações provenientes dos outros nós. Nesse caso, é dito que houve uma contenção.

Para se resolver questões como contenções e colisões na rede, responsáveis por um empobrecimento da capacidade de transmissão de informações entre os nós, deve-se empregar alguns mecanismos para coordenar as transmissões e recepções dos vários nós da rede. Esses mecanismos são designados de Protocolo de Controle de Acesso ao Meio (MAC - *Media-Acess Control Protocol*).

2.4 REDES ÓPTICAS DE TERCEIRA GERAÇÃO

Nas redes ópticas de Primeira Geração, pelo fato de terem tido apenas a substituição dos meios de transmissão existentes por fibras ópticas, toda a função de processamento e roteamento do sinal continuava a ser desempenhada exclusivamente em domínios eletrônicos. Desta forma, acabaram fazendo com que os equipamentos eletrônicos precisassem tratar não apenas as informações destinadas para si, mas também as que necessitavam ser processadas e encaminhadas a outros nós da rede. Se estas últimas informações pudessem ser roteadas nos domínios ópticos, a sobrecarga nos dispositivos eletrônicos seria significativamente reduzida.

Com as redes de Segunda Geração, algumas vantagens tornaram-se imediatamente perceptíveis: transparência fornecida à camada cliente nas redes *single-hop*; possibilidade de as redes que se utilizavam de Tx e/ou Rx sintonizáveis rearranjarem sua topologia virtual sem precisarem alterar sua topologia física; possibilidade de se fornecer serviços de transmissão de pacotes ópticos, caso a sintonia fosse suficientemente rápida e bem coordenada, entre outras. Porém, a forma como os caminhos físicos eram estabelecidos acarretava um espalhamento da potência óptica entre todos os receptores, o qual impossibilitava a reutilização espacial dos comprimentos de onda, por conseguinte produzindo uma não escalabilidade da rede.

Uma arquitetura muito mais flexível e prática é conseguida quando são introduzidas funções de roteamento na camada óptica da rede, fazendo com que os nós sejam capazes de reconhecer comprimentos de onda e roteá-los individualmente de uma porta de entrada para uma das diferentes portas de saída. A esses tipos de redes com roteamento por comprimento de onda, que possuem inúmeros benefícios e peculiaridades chamam de redes ópticas de Terceira Geração [BLACK, 2002].

Considere uma rede óptica com roteamento por comprimento de onda, cuja topologia física esteja representada pela Figura 2.6. Os nós ópticos, aqui designados roteadores de comprimento de onda por possuírem a habilidade de rotear o sinal óptico de acordo com o seu comprimento de onda, são interconectados por fibras ópticas, nas quais são transmitidos os sinais WDM.

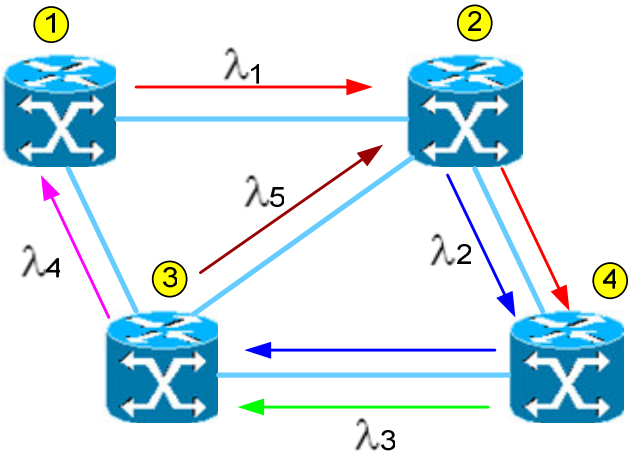

Figura 2.6 - Topologia de uma rede WDM com 5 comprimentos de onda

Devido à inserção da função de roteamento nos nós, essa rede deixará de espalhar o sinal óptico e passará a canalizá-lo através de vias específicas (caminhos), passando então a prover às camadas superiores o que chamamos de caminhos ópticos, a fim de que sejam atendidas as requisições de conexões entre seus usuários. Os caminhos ópticos serão gerados mediante a alocação de um comprimento de onda em cada enlace do seu percurso. Logo, terão a flexibilidade de serem roteados de diversas formas na rede. Além disso, poderão compartilhar um mesmo enlace com diversos outros caminhos ópticos, desde que, obviamente, não ocorra que dois desses caminhos utilizem o mesmo comprimento de onda em um mesmo enlace.

A topologia virtual das redes de Terceira Geração será formada por ramos interligando os nós que, na topologia física, possuem um caminho óptico estabelecido entre eles. Da forma como está representada a Figura 2.6, sua topologia virtual conteria um ramo ligando 1 a 3 e outro 3 a 4.

As redes com roteamento por comprimento de onda permitem que um mesmo comprimento de onda seja reusado em diversos caminhos ópticos presentes simultaneamente na rede (desde que nenhum destes compartilhem um mesmo enlace). Pode-se perceber, portanto, que a substituição das redes de Segunda Geração pelas de Terceira faz com que a forma como as conexões são criadas deixem de ser função apenas da coordenação entre os lasers dos transmissores e receptores e passem a ser função também dos nós ópticos da rede, acarretando assim um tratamento adicional do sinal a nível fotônico. Assim, essas possibilidades causaram uma redução substancial nos investimentos em equipamentos das camadas superiores, tais como SONET, SDH, ATM, entre outros.

Resumidamente, uma das grandes vantagens do roteamento de comprimento de onda é a possibilidade de reutilizá-los livremente no espaço, a menos que a condição de ausência de colisão nos enlaces não seja devidamente obedecida. Como conseqüência imediata, tem-se a obtenção de um enorme aumento na capacidade da rede, uma vez que o número de caminhos ópticos possíveis de serem providos passa a ser muito maior que o número de comprimentos de onda disponíveis, contribuindo dessa forma para tornar as redes que dispõem de roteamento em nível fotônico bastante escaláveis.

As redes de Terceira Geração também apresentam as seguintes características:

— Transparência: a transparência nessas redes está associada ao fato de os caminhos ópticos poderem transportar dados em uma variedade de taxas, protocolos e formatos. Essa flexibilidade será a responsável por possibilitar que alguns caminhos ópticos transportem tráfego SONET ou SDH, enquanto outros transportem células ATM ou pacotes IP, e assim por diante, tornando a camada óptica capaz de suportar várias camadas superiores operando ao mesmo tempo.

— Confiabilidade: com a presença de roteamento na camada óptica, esta poderá ser configurada tal que, na ocorrência de falhas, consiga re-rotear automaticamente seus caminhos ópticos por rotas alternativas. Além disso, muitos de seus componentes, tais como multiplexadores e demultiplexadores, são passivos e, por isso, menos susceptíveis a falhas.

— Comutação por circuito: conforme já mencionado acima, as redes de Terceira Geração têm a função de prover caminhos ópticos para o atendimento das requisições das camadas superiores. Dependendo da forma como for a demanda por caminhos ópticos, estes podem ser ora ativados ou desativados da rede.

Esse é um procedimento análogo à ativação/desativação de circuitos numa rede comutada por circuitos, exceto que a periodicidade de tal ação deverá ser muito menor no caso da rede fotônica do que, por exemplo, no caso da rede telefônica. Vale ressaltar que comutação de pacotes não será realizada na camada óptica dessas redes, sendo, portanto, uma tarefa deixada para as camadas superiores, tais como a ATM ou IP.

Dado o aumento da demanda por largura de banda, as operadoras tiveram que adotar várias estratégias para incrementar a capacidade dos seus enlaces. Uma das abordagens que se mostra mais promissora para o aprimoramento nas capacidades dos enlaces é a multiplexação por comprimento de onda, conhecida pela sigla WDM (*Wavelenght Division Multiplexing*). Como o nome da solução denota, essa consiste em multiplexar, em uma mesma fibra, vários comprimentos de ondas, permitindo a utilização de uma significativa porção da banda disponível na fibra que não era anteriormente aproveitada.

O roteamento desses sinais pode ser realizado pelo comprimento de onda, determinando o caminho de comunicação, através da sua atuação como uma espécie de assinatura do endereço de origem, destino ou rota. Estes e outros processos acontecem na camada física óptica que será abordada neste capítulo.

2.5 REDES WDM

O WDM é uma técnica de multiplexação eficiente que oferece maior capacidade ao criar múltiplas fibras virtuais (vários comprimentos de onda em uma mesma fibra), sem muita mudança na infra-estrutura da rede existente. Assim, em uma rede de comunicação óptica com WDM, a capacidade de transmissão sobre fibra é incrementada permitindo capacidades de 2,5, 10 e até 40 Gbps por canal, e da ordem dos Terabits por segundo (Tbps) por fibra.

A primeira evolução apresenta topologias PP (ponto-a-ponto), caracterizadas por velocidades de canal ultra-altas, além de confiabilidade e proteção. O uso de amplificadores ópticos permite a transmissão de sinais ópticos acima de vários kilometros sem qualquer conversão eletro/óptica. Sistemas baseados em WDM podem também incorporar multiplexadores add/drop ópticos (OADM), que fazem a seleção dos comprimentos de onda a serem inseridos ou retirados do anel. A Figura 2.7 ilustra esta primeira evolução [SATO, 2002].

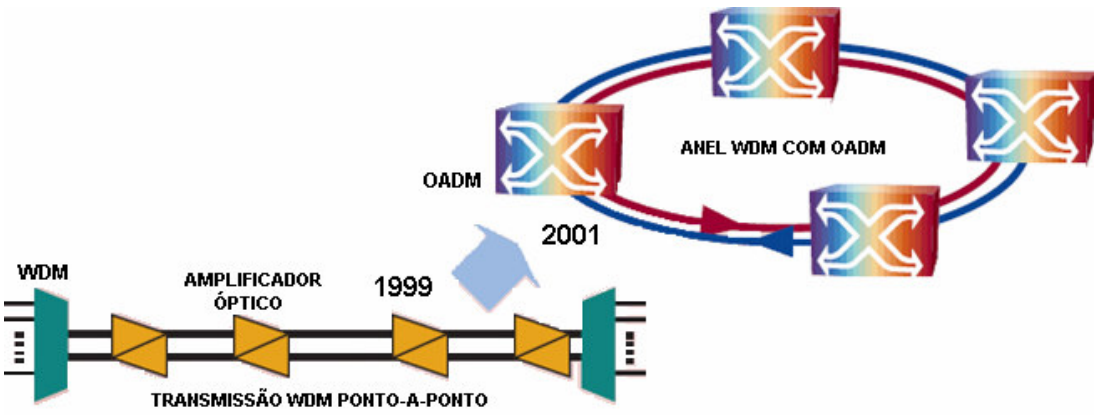

Figura 2.7 - Primeira evolução das redes ópticas WDM

Configurações em anel podem ser desenvolvidas com um ou mais nós OADMs, disponíveis em algumas redes metropolitanas.

O rápido desenvolvimento da tecnologia óptica permitiu a evolução desde os sistemas de transmissão WDM ponto-a-ponto até uma rede *backbone* todo-óptica, que possa maximizar o aproveitamento da largura de banda disponível na fibra. Esta rede consiste de *Optical cross-connects* (OXCs) em uma topologia arbitrária, e sua principal função é prover interconexão para sub-redes cliente [ROUSKAS, 2002].

Assim, no próximo salto evolutivo, os elementos de rede introduzidos foram os OXC (*Optical Cross-Connects*), ou chaves ópticas, e os roteadores MPLS fotônicos (PXC – *Photonics Cross Connects*), fundamentais na arquitetura de uma rede totalmente óptica. Estes avanços são apresentados na Figura 2.8.

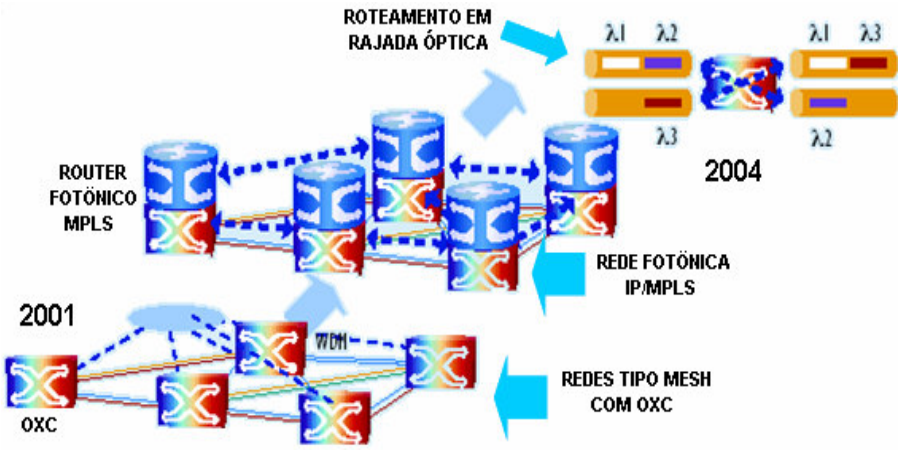

Figura 2.8 - Segunda evolução das redes de ópticas WDM

2.5.1 Arquitetura de rede óptica com roteamento de comprimento de onda

A infra-estrutura de rede completamente óptica é construída sobre a base do roteamento de comprimento de onda (*wavelength routing*). A Figura 2.9 mostra uma rede deste tipo. Nela, OXCs conectados por enlaces de fibra formam uma topologia em malha arbitrária. Os serviços para as sub-redes cliente estão na forma de conexões lógicas implementadas usando o conceito de *lightpaths*. A informação que é transmitida em um *lightpath* não experimenta qualquer conversão de formas eletrônicas na rede óptica. Assim, não existe processamento no sinal de dados que é transportado no *backbone*.

O comutador OXC deve ser precedido por um demultiplexador de comprimento de onda e seguido por um multiplexador. Configurando adequadamente os OXCs do caminho físico, conexões lógicas (*lightpaths*) podem ser estabelecidas entre um par de sub-redes cliente.

Cada OXC tem associado uma unidade de controle eletrônica. A unidade de controle é responsável pelas funções de controle e gerência relativas ao estabelecimento e eliminação de um caminho óptico e demais comandos de configuração. A unidade de controle também se comunica com as unidades de controle dos nós adjacentes ou com as interfaces das sub-redes clientes, quando o OXC é um comutador de borda (*edge*). Esta unidade faz parte do Plano de Controle, que será abordado no Capitulo 4 deste trabalho.

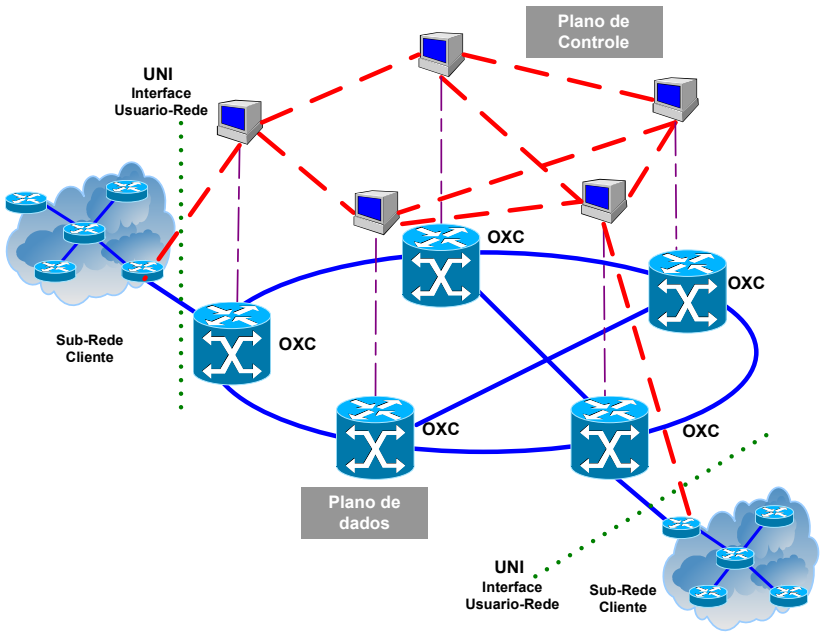

Figura 2.9 - Arquitetura de rede óptica

Um OXC também pode ser equipado com conversores que permitem comutar a informação em um comprimento de onda na entrada de uma fibra para algum outro comprimento na saída de uma dada fibra. Estes equipamentos são conhecidos como *transponders*.

Assim, o principal mecanismo de transporte é o comprimento de onda, conhecido como *lightpath* (caminho óptico entre um nó origem e um destino), que corresponde a um canal de comunicação óptico estabelecido sobre a rede de OXCs, o qual pode abranger um certo número de enlaces de fibra (saltos). Desta forma, se conclui que um *lightpath* é uma

conexão óptica estabelecida fim-a-fim entre duas sub-redes cliente conectadas ao *backbone* óptico, que pode estar em duas situações: com conversão de comprimentos de onda nos vários nós ou sem conversão do comprimento de onda.

Se não existir conversão de comprimento de onda, um *ligthpath* é associado com o mesmo comprimento de onda em cada salto. Observa-se aqui que aparece uma restrição para a criação de caminhos na dependência da continuidade do comprimento de onda ao longo de todo o percurso do sinal. Contudo, usando conversores, diferentes comprimentos de onda em cada salto podem ser usados para criar um *lightpath*.

Por outro lado, usando conversores, diferentes comprimentos de onda em cada salto podem ser usados para criar um *ligthpath*, mas isso sempre tem um impacto de custo na rede óptica.

3 ELEMENTOS DE REDE DA CAMADA ÓPTICA

Os elementos da rede óptica estudada correspondem aos OXCs, amplificadores, *transponders* e as fibras. Desta forma, será apresentado abaixo cada um destes elementos bem como discutido o conceito de escalabilidade de rede.

3.1 COMUTADORES ÓPTICOS OXC

Os comutadores ópticos OXC (*optical cross-connect*) são a opção para a comutação dos comprimentos de onda (canais), já que evitam o processamento eletrônico, que produz um aumento na latência da transmissão. Um OXC é um elemento de comutação que estabelece caminhos roteados para os canais ópticos mediante a conexão local de uma porta de entrada (fibra) a uma porta de saída (fibra), no mesmo comprimento de onda, sem fazer qualquer tipo de conversão óptico-elétrico. Desta forma, se percebe que o OXC é um elemento híbrido que usa multiplexores/demultiplexores e comutadores ópticos.

Um OXC provê multiplexação e demultiplexação usando geralmente filtros baseados em tecnologia de filme de múltiplas camadas, que são componentes encontrados no mercado (por exemplo, JDS Uniphase ou E-TEC). A estrutura interna dos filtros segue o modelo Fabry-Perot Etalon, composta por cavidades e espelhos, atuando como um filtro passa-faixas. O comprimento da cavidade determina o centro do comprimento de onda do passa-faixas. Para conseguir filtragem bastante fina, capaz de separar canais muito próximos (100 GHz), os filtros são construídos com mais de 50 camadas. Essas camadas são constituídas de filmes de SiO2 separados por filmes de TiO2. A espessura do SiO2 corresponde à metade do comprimento de onda central do filtro.

Os comutadores ou chaves ópticas são geralmente feitos usando guias de onda com tecnologia termo-óptico. Esta tecnologia é usada para fazer pequenos comutadores ópticos tipicamente na faixa de 1 x 1, 1 x 2 e 2 x 2. Esta é uma tecnologia planar, de maneira que maiores *switches* podem ser formados integrando componentes básicos 2 x 2 no mesmo *wafer*. O principio de operação se baseia em que, pelo aquecimento de um divisor passivo, o índice de refração pode ser mudado para alterar a direção do comprimento de onda entre uma saída ou outra. A Figura 3.1 apresenta a configuração da unidade de chaveamento da

chave termo-óptica 8 x 8. A Figura 3.2 mostra um arranjo local de uma chave termo-óptica 8 x 8.

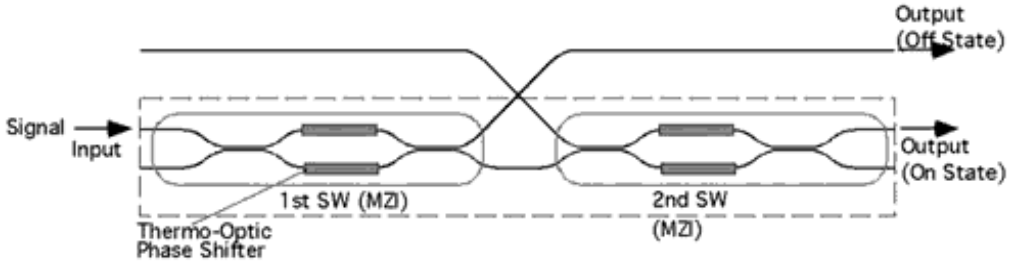

Figura 3.1 - Configuração da unidade de chaveamento da chave termo-óptica 8 x 8

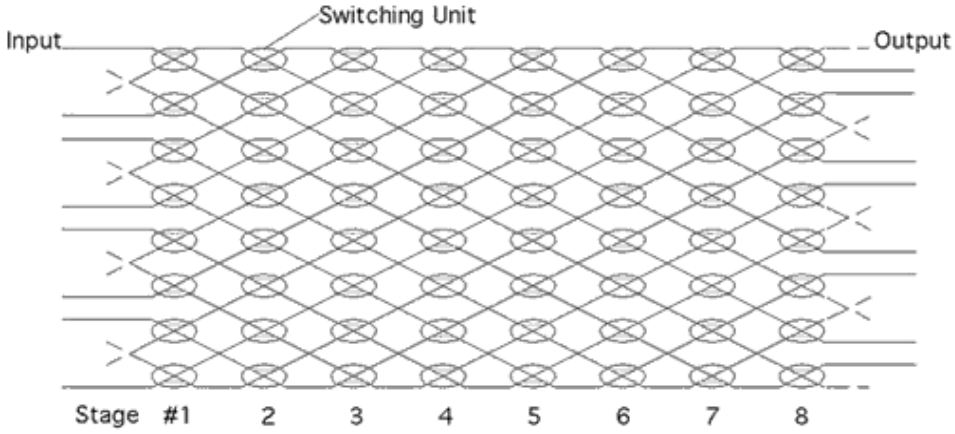

Figura 3.2 - Arranjo local de uma chave termo-óptica 8 x 8

3.2 AMPLIFICADORES ÓPTICOS

O advento dos amplificadores ópticos empregando fibras ópticas dopadas com elementos das terras-raras [DESURVIRE *at al*, 1987] [MEARS, 1987], fez com que sistemas com alta capacidade de transmissão de informações pudessem se tornar realidades comerciais [RAMASWANI, 1998].

No início, os sistemas ópticos utilizavam regeneradores eletrônicos que recuperavam, após uma determinada distância da fonte, a forma e a amplitude dos sinais transmitidos. O processo de funcionamento destes repetidores consistia em converter o sinal do domínio óptico para o eletrônico, onde ele era amplificado e reformatado, e do domínio eletrônico

para o óptico, onde o sinal eletrônico gerado após a recuperação do sinal óptico inicial modulava direta ou indiretamente a luz de um laser semicondutor de saída.

De uma maneira técnica, o repetidor era eficiente, pois conseguia recuperar satisfatoriamente o sinal e aumentar a distância dos enlaces ópticos. Contudo, a complexidade dos circuitos óptico-eletrônicos do repetidor, particularmente daqueles projetados para a recuperação de sinais ópticos modulados digitalmente em altas taxas, fazia que o custo final dos mesmos se tornasse proibitivo. Desta forma, o custo acabava inviabilizando a transmissão de mais de um canal óptico (comprimento de onda) por fibra.

Com a melhoria dos processos de fabricação da fibra, que minimizaram a sua dispersão intrínseca, e com o aparecimento dos amplificadores ópticos que usavam fibra dopada a érbio (*Erbium Doped Fiber Amplifier* – EDFA), a transmissão multicanal por uma única fibra óptica tornou-se técnica e economicamente viável. De posse de tais evoluções e com a baixa dispersão, o processamento do sinal ficou resumido à sua amplificação, que passou a ser realizada totalmente no domínio óptico.

Um EDFA tem a capacidade de realizar a amplificação simultânea de vários canais modulados ou chaveados com mínima interferência entre eles, em uma ampla banda de comprimentos de onda (cerca de 35 nm) na janela de 1.550 nm. Desta forma, na transmissão óptica multicanal, onde se adota a tecnologia WDM, cada canal pode ser amplificado com o mínimo de intermodulação, e utilizar, potencialmente, a ampla banda de transmissão da fibra óptica. Esta prática aumenta a capacidade efetiva de transmissão e diminui o custo por canal, em relação a sistemas com regeneradores. Na média, o limite de alcance de um enlace óptico que não utiliza amplificadores e opera com taxas de transmissão da ordem de Gbps é de, aproximadamente, 200 km [SUDO, 1997]. Desta forma, para redes ópticas de longo alcance, como, por exemplo, enlaces transoceânicos, torna-se imperativa a utilização de amplificadores ópticos.

O EDFA pertence a uma família de amplificadores obtidos a partir da dopagem de uma fibra óptica com elementos químicos pertencentes ao grupo das “terras-raras”. Dentre estes elementos se destaca o érbio em sua forma iônica (Er+3), sendo, atualmente, o mais utilizado nos amplificadores (1550 nm). Contudo, outros possíveis dopantes, como o praseodímio (usado para amplificação na faixa de 1300 nm), e o itérbio (usado como co-dopante junto com o érbio), também estão sendo utilizados [STERN, 1999] [SUDO, 1997].

A função de um amplificador óptico em um sistema pode ser subdividida em três tipos, de acordo com a sua localização física: o amplificador de potência, o amplificador de linha e o pré-amplificador. Contudo, todos devem apresentar o ganho e a figura de ruído condizente com cada aplicação.

O amplificador de potência, onde o ganho é um fator importante, é colocado próximo à saída do bloco transmissor de um sistema óptico e tem como função aumentar o nível de potência óptica de saída do transmissor. Assim, pode-se, dependendo do tamanho do enlace ou da acessibilidade da planta óptica, compensar antecipadamente as perdas ópticas e evitar a colocação de novos amplificadores ao longo do sistema.

Os amplificadores de linha, geralmente colocados em pontos estratégicos ao longo do enlace de transmissão, têm como função restaurar a amplitude do sinal óptico de forma a compensar a atenuação na fibra. Assim, deseja-se que estes amplificadores possuam ganho acentuado e baixa figura de ruído. Portanto, os amplificadores de linha são utilizados quando o comprimento do enlace é tal que o nível do sinal que chega ao receptor não é suficiente para a detecção com baixa taxa de erros, mesmo após a utilização de amplificadores de potência. Contudo, em determinados enlaces ópticos, a necessidade de um amplificador de linha pode ser substituída pela utilização dos chamados pré-amplificadores ópticos. Neste caso, o nível do sinal que chega ao receptor continua não sendo suficiente para a detecção com baixa taxa de erros. Porém, a colocação do amplificador na entrada do receptor óptico permite a recuperação do sinal a nível adequado à sensitividade do fotodetector, aumentando a sua relação sinal-ruído, com a vantagem extra de permitir fácil acesso ao amplificador, em caso de necessidade de manutenção. Portanto, observa-se que a utilização comercial do EDFA depende de sua função (ou posição) no enlace óptico.

Como o amplificador pode ser implementado em diferentes topologias, é possível que cada uma destas seja mais indicada para um tipo específico de aplicação (potência, linha ou pré-amplificação), para um tipo especifico de bombeio. Por meio da verificação de desempenho destas configurações de EDFA, que é consideravelmente facilitada pela utilização de simulações computacionais, pode-se determinar as condições de operação mais adequadas para cada função de amplificação, permitindo, inclusive, otimizações, antes que testes de campo sejam conduzidos [MILO, 2003].

3.3 TRANSPONDERS

Como relatado anteriormente, *transponders* são os adaptadores de comprimento de onda. Assim, os clientes podem ser sinais SDH com comprimento de onda qualquer (entre 1300 nm e 1600 nm), que passando pelo *transponder* têm o seu comprimento de onda convertido para um dos comprimentos de onda da rede. No caso da rede OMEGA, os comprimentos de onda correspondem à grade ITU com separação de 200GHz, e para ela foram escolhidos os valores ímpares de centena de Gigahertz conforme padronizado pela grade da Telcordia para sistemas WDM com 16 comprimentos de onda. Para a obtenção dos respectivos valores em nm se devem utilizar pelo menos 6 algarismos significativos para a velocidade da luz (exemplo, $c=2{,}99792458 \times 10^8$ m/s para compor a Tabela 3.1):

Tabela 3.1 - Grade ITU e correspondentes valores de Comprimento de Onda

192,3 THz	192,5 THz	192,7 THz	192,9 THz	193,1 THz	193,3 THz	193,5 THz	193,7 THz
1558,98 nm	1557,36 nm	1555,75 nm	1554,13 nm	1552,52 nm	1550,92 nm	1549,32 nm	1547,72 nm

Nesta rede, o sistema pode ser ampliado para comportar até 16 comprimentos de onda mantendo-se a mesma separação entre canais (200 GHz), sem sair da banda útil de ganho dos amplificadores que usam fibra dopada com érbio (banda C). Contudo, para aumentar a capacidade da rede para 32 comprimentos de onda por fibra é necessário reduzir a separação entre canais para 100GHz, o que envolverá o uso de equipamentos muito mais caros.

3.4 FIBRAS ÓPTICAS

As primeiras fibras ópticas foram produzidas na década de 1920 [KAPANY, 1959], baseadas no princípio de guia da luz por reflexão interna total. Porém, o desenvolvimento das fibras experimentou seu primeiro grande avanço nos anos 50, quando uma camada de revestimento (*cladding*) com índice de refração pouco inferior ao do núcleo da fibra passou a ser utilizada.

No final dos anos 60 as perdas proporcionadas por este meio ainda eram relativamente altas e atingiam os 1000 dB/km [KAPRON, 1970], sendo comparáveis às perdas dos cabos metálicos utilizados em redes de telecomunicações. No entanto, a partir dos anos 70, o avanço no processo de fabricação das fibras reduziu sua atenuação para cerca de 20 dB/km e, por volta de 1979, atingiu um valor de cerca de 0,25 dB/km, [PAYNE, 1974] [FRENCH, 1974], muito próximo ao limite mínimo teórico imposto pelo espalhamento Rayleigh [MIYA, 1979], para a região espectral de 1550 nm. Essa baixíssima atenuação, estendendo-se por uma largura de banda com cerca de 20 THz [RAMASWAMI, 1998], não se observa em outros materiais e fez com que as restrições impostas aos sistemas de transmissão por fibras ópticas passassem a ser determinadas por outros fenômenos, como dispersão e efeitos não-lineares.

As primeiras fibras a serem utilizadas em sistemas de telecomunicações foram as fibras ópticas multi-modo. Nestas, o campo eletromagnético se propaga com diferentes configurações (modos) [LEE, 1986], cada uma tendo sua própria velocidade efetiva de propagação. Devido a esta diferença de velocidades, torna-se relevante a dispersão intermodal e restringe-se o alcance desses sistemas a poucos quilômetros, antes que o sinal precise ser regenerado eletronicamente.

As fibras multi-modo ainda são utilizadas, sobretudo para conectar redes de computadores a baixos custos, porém tem limitações em alcance e taxa de transmissão, restritos a até alguns quilômetros e algumas centenas de Mbps [RAMASWAMI, 1998].

As fibras monomodo, que possuem apenas uma configuração de campo para cada polarização possível, começaram a ser utilizadas pelos sistemas de telecomunicações no início da década de 1980. Sendo a propagação em um único modo, não apresentam dispersão intermodal e sua capacidade sistêmica é tipicamente limitada pela dispersão cromática (ou intramodal) [GARRET, 1970], pelos efeitos não-lineares, e pelo ruído de amplificadores ópticos [RAMASWAMI, 1998], além da sensibilidade do receptor, a algumas dezenas de quilômetros e alguns Gbps.

As primeiras fibras monomodo, conhecidas como Fibras Padrão (STDF- *Standard Fiber*), e atualmente descritas pela recomendação G. 652 do ITU-T [ITU-T-1, 2000], possuíam dispersão nula na janela de 1300 nm e ainda eram limitadas pela atenuação desta

janela. Para aumentar a distância entre regeneradores, no final dos anos 80, houve uma migração para a janela de baixas perdas em 1550 nm.

Contudo, a crescente exigência pelo aumento da taxa de transmissão de bits fez com que a dispersão da terceira janela, cerca de 17 ps/(nm.km), começasse a comprometer o desempenho das Fibras Padrão. Apesar da introdução de fontes de largura espectral relativamente estreita, como os lasers DFB, a dispersão cromática da terceira janela motivou o desenvolvimento da Fibra de Dispersão Deslocada (DSF- *Dispersion Shifted Fiber*), que possui tanto dispersão nula, como atenuação mínima na terceira janela. Estas fibras são normatizadas pela recomendação G.653 do ITU-T [ITU-T-2, 2000].

Considerando que a geração dos sinais é feita eletrônicamente e que serão posteriormente convertidos para o domínio óptico, a taxa de transmissão está limitada a cerca de 40 Gb/s [HAYEE, 1999]. Através de técnicas de Multiplexação no Domínio do Tempo (TDM- *Time Domain Multiplexing*), tais taxas de transmissão de bits estão, admitindo-se que cada Hertz codifique 1 bps, muito aquém da largura de banda proporcionada pelas fibras. Então, para aproveitar os recursos oferecidos pelas fibras, é usada a Multiplexação por Divisão em Comprimentos de Onda (WDM). Este acontecimento, junto com o desenvolvimento dos Amplificadores de Fibra Dopados a Érbio (EDFA- *Erbium Doped Fiber Amplifiers*), fez com que as fibras ópticas conseguissem um grande desenvolvimento.

Os efeitos não-lineares desempenham um papel crucial na propagação de sinais por fibras ópticas, advindo da resposta não-linear da sílica (ou de qualquer material do qual a fibra seja constituída), a um campo eletromagnético externamente aplicado [ABBADE, 2001]. Fundamentalmente, a origem desta resposta não linear está relacionada ao movimento anarmônico dos elétrons ligados sob a influência do campo aplicado e é tanto mais relevante quanto maiores forem os níveis de potência utilizados ou quanto menor for o espaçamento, em freqüência, entre os canais.

Os efeitos não-lineares podem ser divididos em duas classes. Na primeira delas, temos aqueles efeitos que ocorrem devido à dependência existente entre o índice de refração e a potência óptica. Entre estes efeitos, pode-se citar a Automodulação de Fase (SPM- *Self Phase Modulation*), a Modulação Cruzada de Fase (XPM- *Cross Phase Modulation*), a Mistura de Quatro Ondas (FWM- *Four Wave Mixing*) e a Instabilidade Modulacional (MI-

Modulation Instability) [ABBADE, 2001]. Estão também nesta classe, os efeitos não-lineares de ordem superior, como o *Self-Steepening* e o Auto-Desvio de Freqüência, relevantes na propagação de pulsos de duração inferior a 1 ps.

A outra classe de efeitos não-lineares compreende os efeitos de espalhamento devidos à interação entre o campo eletromagnético e as vibrações moleculares do meio que constitui a fibra. Nessa classe, enquadram-se os fenômenos de Espalhamento Estimulado Brillouin (SBS- *Stimulated Brillouin Scattering*) e Espalhamento Estimulado Raman (SRS- *Stimulated Raman Scattering*) [ABBADE, 2001].

Além dos problemas inerentes à propagação dos sinais descritos acima, existem muitos outros que ainda precisam ser resolvidos, como o baixo aproveitamento espectral dos recursos da fibra [ITU-T-3, 1998], e a questão de conversão de comprimentos de onda [ASO *et al*, 2000] [TOMKOS, 1999].

3.5 ESCALABILIDADE E TOPOLOGIA DE REDES ÓPTICAS

A escalabilidade de uma rede pode ser definida com respeito à capacidade [GILLNER, 1996], [GILLNER, 1999], e ao tamanho da rede [K._Y, 2000].

A escalabilidade em termos de capacidade da rede inclui os parâmetros:

- Número de canais (comprimentos de onda);
- Taxa de bit por comprimentos de onda;
- Número de portas de entrada/saida por nó.

A escalabilidade em termos de tamanho da rede inclui os parâmetros:

- Número de nós;
- Separação de nós;

A capacidade de escalabilidade depende do tamanho da rede e o tamanho da escalabilidade depende da capacidade desta. Assim, uma rede operando com altas taxas de bits é menos escalável em tamanho que uma rede operando a baixas taxas. Também, uma rede com grande separação entre nós é menos escalável em capacidade que uma rede com menor separação.

De uma forma geral, a deterioração física tem maior impacto na escalabilidade da rede. A Tabela 3.2 apresenta cada parâmetro de escalabilidade e uma lista de defeitos físicos que impactam sobre o parâmetro.

Tabela 3.2 - Parâmetro de escalabilidade e defeitos físicos para cada parâmetro.

Parâmetro	**Defeitos físicos críticos**
Número de Comprimentos de onda	*Cross-talk* *Four wave mixing* *Raman Scattering* *Cross-phase modulation*
Taxa de bit por comprimento de onda	*Chromatic dispersion* *Polarization mode dispersion* *Amplified spontaneous emission*
Número de portas por nó	*Cross-talk*
Número de nós	*Cross-talk*
Separação de nós	*Amplified Spontaneous Emission*

Em redes transparentes DWDM o problema físico é mais crítico que em sistemas de transmissão ponto-a-ponto, por varias razões. Em primeiro lugar, os efeitos causados em detrimento das questões físicas nos pulsos ópticos (*broadening*, ruído, distorsão, desvanecimento etc.) são cumulativos. Considerando redes ópticas de longo alcance, os efeitos acumulativos podem ser muito nocivos para a performance do sistema. Em segundo lugar, quando a rede tem mecanismos de proteção, os pulsos enviados para o caminho *backup* podem ir através de um longo caminho quando comparado ao caminho primário, causando degradação extra. Por último, considerando que muitos sinais diferentes podem passar através de um segmento de rede, este segmento tem de ser configurado de forma mais rigorosa para os respectivos formatos de sinal.

A escolha da topologia tem um impacto forte na escalabilidade. Para um anel óptico, acumulação de *cross-talk* tem menos impacto que em uma rede em malha [GILLNER, 1999]. A pesquisa de correlação entre topologia e escalabilidade é a chave na escolha da melhor topologia de forma a reduzir o acúmulo de deterioração física.

Em uma rede em malha, *cross-talk* é o mais crítico das deteriorações físicas. *Cross-talk* é uma contaminação em uma porta de saída de fibra, que supostamente não existiria nessa porta. Em *cross-talk* entre bandas o canal é contaminado com luz a diferentes comprimentos de onda e depende principalmente da qualidade do mux e demux usado no nó. Esse fenômeno é, possivelmente, o mais crítico de eliminar sem impactar na capacidade da rede óptica.

4 CAMADA DE CONTROLE

Nos últimos anos, a noção de um plano de controle óptico tem passado de ser um mero conceito para um detalhado conjunto de protocolos minuciosamente especificados, padronizados e desenvolvidos.

O projeto de um plano de controle focado em IP, para redes ópticas, foi descrito primeiramente num *draft* do IETF em novembro de 1999, depois que vários fabricantes já tinham introduzido o conceito em seus produtos. Baseado na aplicação do modelo de controle MPLS em redes ópticas, primeiro veio a se denominar MPλS (*Multiprotocol Lambda Switching*). Contudo, dado que os mesmos conceitos podiam ser generalizados também ao controle de qualquer rede de comutação de circuitos, incluido interfaces TDM (*Time-Division Multiplex*), se denominou MPLS generalizado ou GMPLS.

Neste Capítulo serão abordadas as características e funcionalidades do plano de controle de uma rede óptica IP/WDM. Primeiramente serão revisadas as redes de comutação de pacotes e apresentada a evolução destas quando orientadas às redes de transporte óptico. Uma vez realizado esse passo, serão vistas as funções do plano de controle e mostradas as diferentes arquiteturas de redes IP/WDM, para terminar com uma descrição dos planos de controle MPλS (*Multiprotocol Lambda Switching*) e GMPLS (*Generalized Multiprotocol Lambda Switching*). Além disto, serão apresentadas as principais características da tecnologia Ethernet e do protocolo IP, que foram usados como suporte à implementação realizada neste estudo.

4.1 REDES DE COMUTAÇÃO A PACOTES

No caso das redes de dados baseados em pacotes são usadas técnicas de comutação com base em multiplexação estatística. Essa técnica permite economia da banda passante, quando comparada à técnica de comutação de circuitos, entre outras vantagens.

A rede comutada a pacotes foi projetada para transmitir dados. Cada pacote possui dados (*payload*) e um cabeçalho (*overhead*) de controle. Em uma rede de dados IP os pacotes são entregues ao primeiro nó da rede, que verificará as informações do cabeçalho e

os enviará para o próximo nó. Esse processo é repetido até cada pacote chegar ao seu destino. Uma conexão entre dois nós pode ser usada por vários pacotes de diferentes destinos e origens. Assim, um caminho não será exclusivo e pode ser compartilhado por outros usuários.

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

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

4.1.1 Evolução da rede de comutação a pacotes orientada ao transporte óptico

O desenvolvimento do *backbone* IP está focado principalmente nos mecanismos de encaminhamento. Nos primeiros estágios das redes IP, roteadores eram interconectados usando serviços *leased-line* para produzir configurações ponto-a-ponto, este serviço é conhecido como IP sobre SDH. Com a contínua expansão do tráfego foi necessário o aumento das capacidades do nó. Assim, foram desenvolvidos roteadores IP eletrônicos para roteamento na ordem de Terabits a fim de interconectar estes com enlaces WDM de grande capacidade. Esta técnica é conhecida como IP sobre SDH sobre WDM.

Paralelamente, a tecnologia ATM (*Asynchronous Transfer Mode*) é introduzida em redes IP de larga escala para permitir conexões de roteadores usando rotas e canais virtuais sobre redes tipo malha (IP sobre ATM). Isto habilita capacidade de comutação nos nós e promove as bases para a engenharia de tráfego e qualidade de serviço (QoS) na rede.

Contudo ainda sem total integração, pois as camadas IP e ATM são gerenciadas separadamente.

Como conseqüência, a arquitetura das redes de transporte óptico veio a ter quatro camadas: IP para o roteamento de aplicações e serviços, ATM (*Asynchronous Transfer Mode*) para a Engenharia de Tráfego e QoS, SONET/SDH para transporte e proteção de dados e DWDM (*Dense Wavelength Division Multiplexing*) para proporcionar altas capacidades de transporte (Figura 4.1). Um problema dessa arquitetura é a escalabilidade, que é pequena para volumes de tráfego muito grandes.

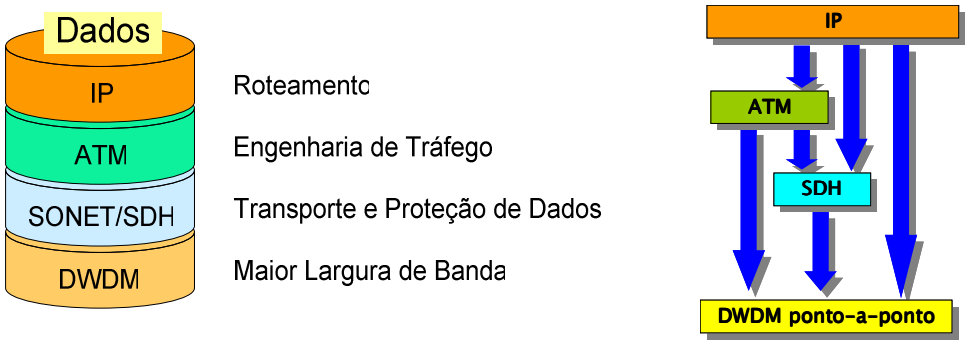

Figura 4.1 - Camadas da Rede de Transporte

Estas redes multicamadas foram projetadas, inicialmente, para comutação de circuito e orientadas à transmissão de voz, que constituia o tráfego dominante. Esta arquitetura funcionava bem para o transporte de voz TDM, mas não era ideal para a transmissão de dados, principalmente em termos de eficiência e custo. Cada camada não sabe muito bem o que se passa nas outras, sendo necessário o aumento do cabeçalho para um melhor controle, existindo ainda a possibilidade de duplicação de serviços.

Para alcançar maior eficiência e escalabilidade, a rede precisava reduzir o número de camadas. Embora o roteamento de nível 3 (IP) tenha sido bastante utilizado, os nós de comutação operam cada vez mais sobre uma comutação de nível 2, que se mostra mais eficiente. Para implementar gerência integrada de camada 2 (enlace) e camada 3 (rede) do modelo OSI, e assim integrar IP com ATM e outras tecnologias de camada de enlace, apareceu o MPLS (*Multiprotocol Label Switching*). MPLS é um modelo híbrido que explora as melhores propriedades do roteamento de pacotes e da comutação de circuitos. Essa técnica tem, entre outras possibilidades, a capacidade de criar circuitos virtuais para controlar o roteamento do tráfego, diminuindo o tempo de encaminhamento de pacotes e

evitando o processamento de nível 3, como atualização das tabelas de roteamento, cálculo de métricas e descobrimento de rede.

O MPLS permite incorporar as funções de comutação e engenharia de tráfego, suprimindo a necessidade de camadas intermediárias. Uma rede deste tipo é mostrada na Figura 4.2.

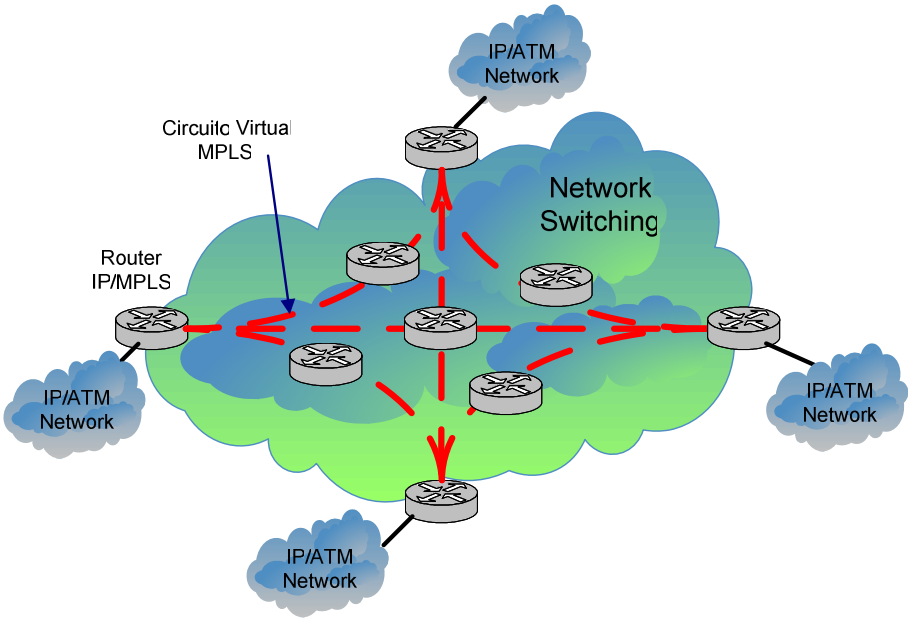

Figura 4.2 - Exemplo de uma rede de comutação IP/MPLS.

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

Para transporte de pacotes, o MPLS é baseado no paradigma de comutação de rótulos. Um rótulo é um identificador de tamanho fixo (20 bits) e que tem significado local. Um domínio MPLS é formado por roteadores de núcleo e roteadores de borda, que interligam subdomínios. Quando um pacote entra no domínio MPLS, a ele é atribuído um rótulo, que, na prática, permite o desacoplamento entre o roteamento e o encaminhamento. Assim, os roteadores só analisam os rótulos para poderem encaminhar o pacote [AWDUCHE, 2002].

O LER (*Label Edge Router*) e o LSR (*Label Switch Router*) são os roteadores de comutação de rótulos. O LER está situado na entrada e na saída do domínio MPLS. O LER da entrada tem a função de inserir rótulos nos pacotes, agrupá-los em uma FEC (*Fowarding Equivalence Class*), e encaminhá-los através de um LSP (*Label Switch Path*), com base no endereço IP destino do pacote. O pacote é logo encaminhado ao roteador adjacente seguinte, denominado LSR. O LER situado na saída do domínio é responsável por retirar o rótulo e entregar o pacote a sua rede destino.

Os LSR do núcleo MPLS têm a função de encaminhar os pacotes com base apenas no rótulo. Ao receber um pacote, cada LSR troca o rótulo por outro, passando o pacote para o próximo LSR e assim por diante até o LER de saída. Desse modo, cada pacote é encaminhado sem a necessidade de análise do cabeçalho IP [BLACK, 2002].

O LSP é o caminho dos pacotes na rede. A criação do LSP é feita usando os protocolos de roteamento e sinalização. Um LSP em MPLS é unidirecional, portanto, é preciso ter dois LSP para uma comunicação entre duas entidades. Estes elementos da rede MPLS são apresentados na Figura 4.3.

Uma FEC consiste em um conjunto de parâmetros (endereço IP fonte ou destino, número da porta fonte ou destino, etc.) que permitirão determinar um caminho para os pacotes. Os pacotes de uma mesma FEC serão encaminhados pelo mesmo caminho. Cada FEC é representada na entrada do domínio por um rótulo e cada LSP é associado a uma FEC. Ao receber um pacote, o LER verifica a qual FEC ele pertence e o encaminha através da LSP correspondente. Portanto, há uma associação pacote-rótulo-FEC-LSP [PASTOR, 2005].

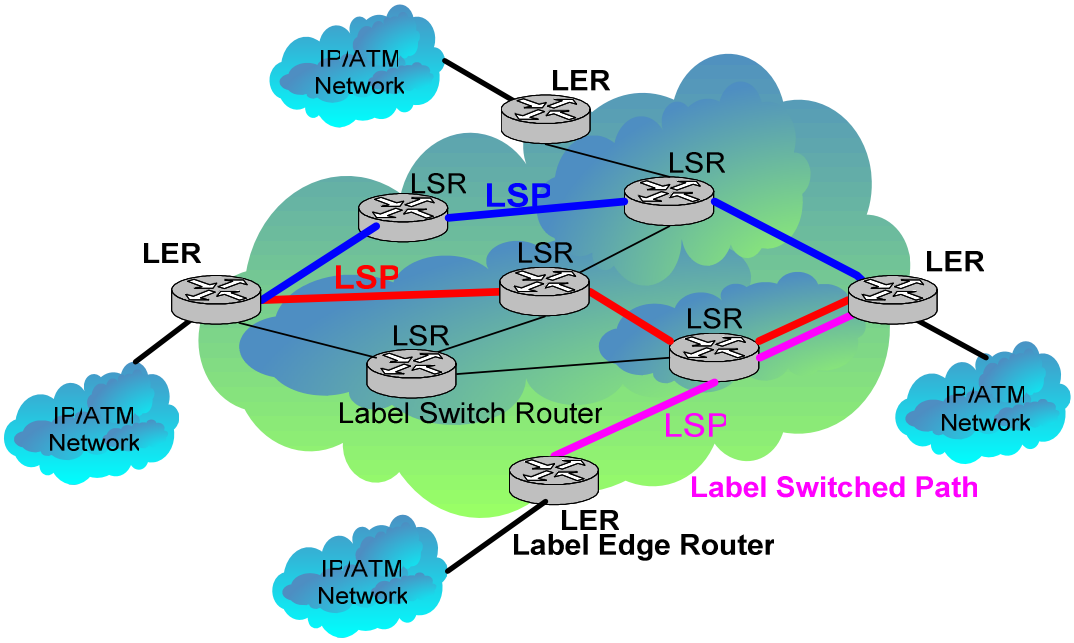

Figura 4.3 - Componentes LER, LSR e LSP de um domínio MPLS.

Para viabilizar a conjugação do MPLS e da tecnologia de transporte óptica, em uma única rede, são necessárias adaptações nos comutadores MPLS (LSR) e nos comutadores ópticos (OXC). Com o aumento das capacidades destes comutadores para o suporte às altas taxas de dados do transporte óptico é possivel eliminar as camadas SONET/SDH e ATM da arquitetura da rede de transporte. Para tornar isso possível, roteadores, OXCs e DWDMs devem implementar as funções necessárias das camadas a serem suprimidas, ver a Figura 4.4 [MURTHY, 2002].

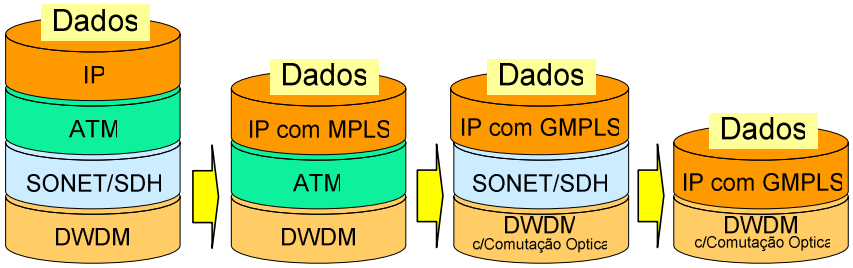

Figura 4.4 - Evolução da rede de transporte IP

Dessa forma, as redes tendem a convergir para o modelo de duas camadas com uma adaptação conveniente do IP para inclusão de QoS, características de engenharia de tráfego e mecanismos de proteção e restauração, através do plano de controle GMPLS.

A Figura 4.5 mostra um resumo da evolução e de como um núcleo de rede IP de longa escala pode ser desenvolvido com diferentes tecnologias [SATO, 2002].

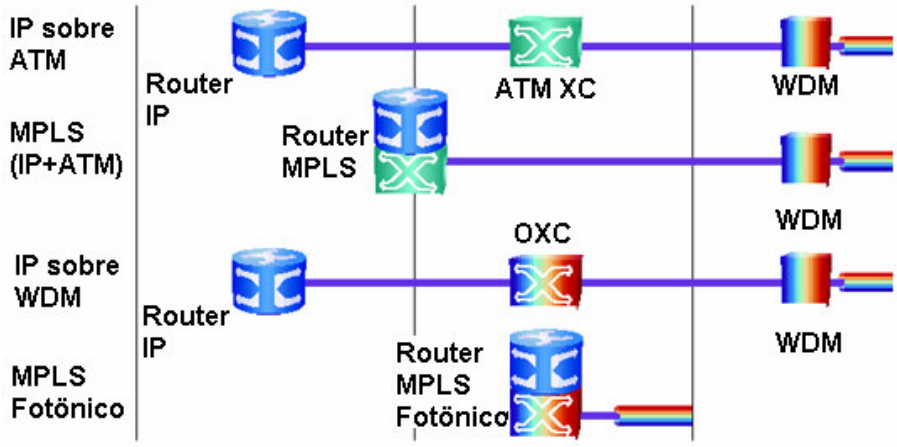

Figura 4.5 - Evolução das Configurações da Rede de Transporte baseadas em IP

4.2 PLANO DE CONTROLE DA REDE IP/WDM

Em redes MPλS e GMPLS, cada elemento de rede do plano de transporte pode ser controlado por um plano de controle seja este centralizado ou distribuído. Ambos os tipos de planos são apresentados na Figura 4.6 e Figura 4.7.

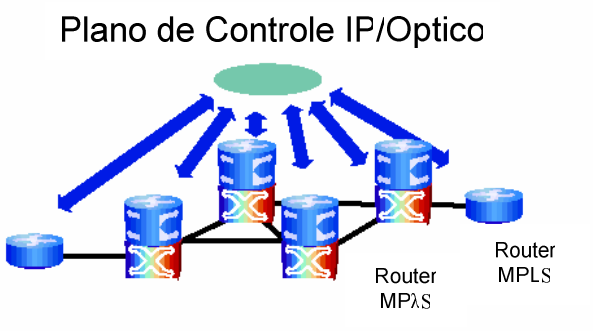

Figura 4.6 - Plano de Controle Centralizado

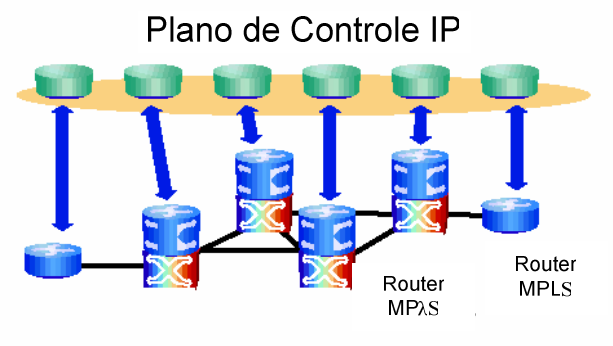

Figura 4.7 Plano de Controle Distribuído

4.2.1 Funções do plano de controle

As principais funções do plano de controle são:

— Descoberta do vizinho: função pela qual um elemento de rede informa automaticamente os detalhes de sua conectividade a todos seus vizinhos do plano de dados. Esta informação inclui a identidade dos vizinhos, a identidade das terminações do enlace, etc.

— Encaminhamento: o encaminhamento cobre dois aspectos:

1) Estabelecimento automático da topologia e a descoberta de recursos, que permite aos agentes de controle ter uma visão local da conectividade do plano de dados e a disponibilidade dos recursos na rede. Este procedimento implica num mecanismo para inundar a informação de conectividade do enlace para todos os agentes de controle da rede.

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

— Sinalização: Indica a sintaxe e a semântica da comunicação entre agentes de controle no estabelecimento e manutenção das conexões. Para tal, se faz uso de protocolos de comunicação. Tais protocolos, atualmente, tendem a ser abertos e padronizados.

— Gerência de recursos locais: encarregado da administração dos recursos localmente disponíveis e controlado por um agente específico, que também tendem a serem padronizadas por protocolos específicos (por exemplo, SNMP).

4.3 ARQUITETURA DE REDES IP/WDM

4.3.1 Tecnologias de comutação em redes IP sobre WDM

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

A Comutação de Circuitos Ópticos (OCS) é uma tecnologia já madura que usa *lighpaths* como circuitos ópticos. Para o transporte do tráfego IP são usadas as infra-estruturas ATM e SDH, para provisão de engenharia de tráfego e transporte com proteção respectivamente. Isto traz, de acordo com o texto apresentado, o incremento do número de camadas (IP/ATM/SDH/WDM) no *backbone* da rede de transporte, gerando cabeçalhos adicionais. Contudo, utilizando um circuito, antes da transmissão, é estabelecido um caminho roteado em comprimento de onda. Este caminho (*lighpath*) não faz uso de multiplexação estatística, tirando pouco proveito da capacidade que oferece a largura de banda, que tem capacidades fixas de 2,5Gb/s, 10Gb/s ou 40Gb/s (pouca granularidade).

Se o aprovisionamento de rotas requer intervenção manual do administrador da rede, a rede é dita "estática". Um avanço significativo é a automatização do processo de estabelecimento de rota. Processos de sinalização precisam ser introduzidos no domínio óptico para viabilizar estas redes, ditas "dinâmicas", e conhecidas também como ASTN (*Automatic Switched Transport Nework*) [NORTEL NETWORKS, 2001].

Com o passar do tempo, a comutação óptica de pacotes vai-se tornando uma realidade. A informação contida em cabeçalhos específicos (rótulos) pode ser usada para que se decida como o pacote será comutado em cada nó da rede. O comprimento do *payload* define a quantidade de dados que está sendo transmitida em cada pacote, o que resulta numa granularidade mais fina. Assim, a tecnologia WDM está evoluindo para tecnologias como OBS e OPS, as quais suportam diretamente IP sobre WDM. Ambas as tecnologias de comutação têm sido testadas como protótipos e estão em processo de otimização continua sendo ainda bastante custosa a sua implementação. Em compensação, estas redes utilizam eficientemente os recursos de largura de banda pelo uso da multiplexação estatística.

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

Em redes OPS, a entidade de comutação básica é o pacote. No momento, redes OPS suportam pacotes de tamanho fixo devido a problemas de sincronismo. Aqui, o cabeçalho e a carga útil são enviados juntos. Ao alcançar um nó, o cabeçalho é extraído e processado eletronicamente. A carga útil é opticamente retardada usando fibras de retardo (FDL), sendo logo comutada da porta de entrada para a porta de saída.

Usualmente comutação óptica de rajadas requer um mecanismo de gerência de recursos rápido para minimizar as colisões de rajadas em um nó, enquanto que a comutação de pacotes ópticos requer memória óptica. A memória óptica efetiva ainda não existe, e isto representa uma séria dificuldade para o desenvolvimento desta técnica.

4.3.2 Modelos de Interconexão de Redes

A rede óptica da Figura 4.8 consiste de múltiplas sub-redes interconectadas por enlaces ópticos numa topologia em malha (*mesh network*).

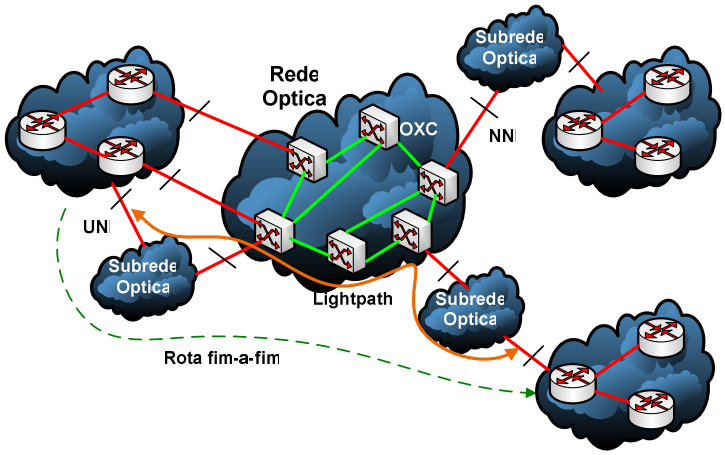

Figura 4.8 - Um modelo de IP sobre rede Óptica

A interação entre roteadores IP e o núcleo óptico é realizada sobre uma interface de roteamento bem definida e a sinalização é chamada de Interface Usuario-Rede (UNI – *User-Network Interface*). A interação entre sub-redes se dá sobre uma interface de roteamento bem definida e a sinalização é conhecida como Interface Rede-Rede (NNI – *Network-Network Interface*) [RAJAGOPALAN, 2000].

Os seguintes modelos de interconexão são possíveis para a arquitetura de rede IP sobre WDM:

4.3.2.1 Modelo *Peer*

Sob este modelo, as redes IP e as redes ópticas são tratadas juntas como uma única rede integrada, com gerência e engenharia de tráfego unificada. Os OXC são vistos como qualquer outro roteador pelo plano de controle.

Do ponto de vista de roteamento e sinalização não existe diferença entre as interfaces UNI, NNI ou qualquer outra interface roteador-roteador. Um único protocolo de roteamento é executado sobre ambos os domínios de redes (IP e Óptico).

A vantagem do modelo *Peer* é que permite interconexão das redes IP e Óptica sem arranjos. A desvantagem é que se faz necessária informação de roteamento específica para redes ópticas a ser conhecida pelos roteadores. A Figura 4.9 apresenta a arquitetura do modelo *Peer*.

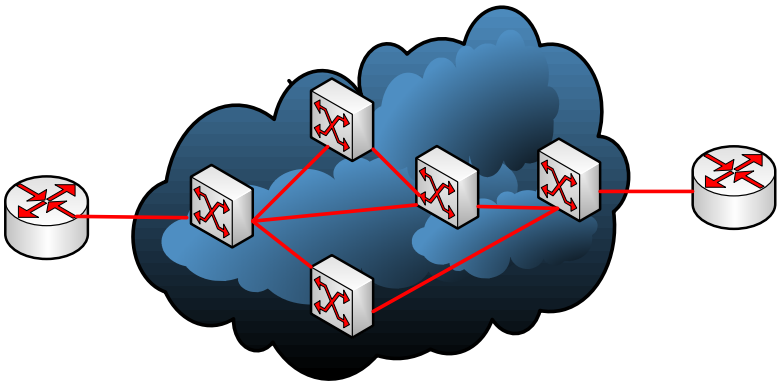

Figura 4.9 - Arquitetura do modelo Peer.

No modelo *Peer* com mecanismo de controle distribuído, OXCs e outros equipamentos são como roteadores IP virtuais; nele redes IP e ópticas usam protocolos de roteamento e sinalização comuns, tal como em GMPLS. Assim, roteadores IP e OXCs tem uma relação

"amistosa" em termos de plano de controle. Isto é mostrado na Figura 4.10; serviços além do IP, como SDH ou ATM, podem ser providos pela mesma plataforma.

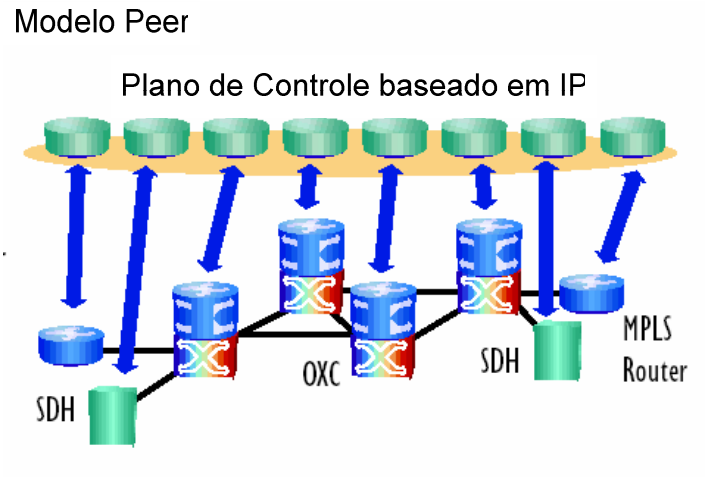

Figura 4.10 - Arquitetura do modelo Peer com controle distribuído

No modelo *Peer* cada nó mantém uma base de dados de informação de estado da rede (fluxo do tráfego, enlaces usados, disponibilidade de recursos ópticos, capacidade do caminho, etc). Dessa maneira, a rede pode auto adaptar-se dinamicamente às mudanças no tráfego.

4.3.2.2 Modelo *Overlay*

Sob este modelo, os protocolos de roteamento e sinalização das redes IP são independentes dos correspondentes protocolos em redes ópticas. Este modelo é conceitualmente similar ao modelo IP sobre ATM. A vantagem do modelo *Overlay* é sua relativamente não complicada implementação. Sua desvantagem é que esta requer a criação e gerência de adjacências de roteamento IP sobre a rede óptica. A Figura 4.11 apresenta a arquitetura do modelo *Overlay*.

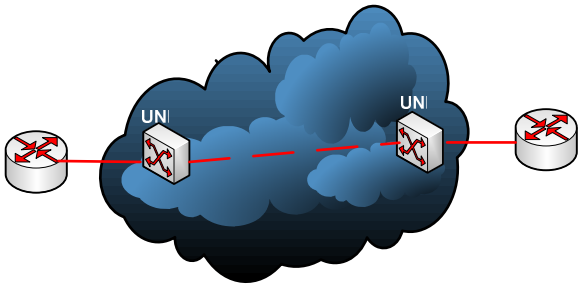

Figura 4.11 - Arquitetura do modelo Overlay.

No modelo *overlay*, enlaces provêm caminhos ópticos entre *routers* para a camada IP. A rede é administrada baseada no modelo cliente/servidor, onde a rede IP é o cliente da rede óptica. Informação de roteamento não é trocada entre as duas camadas; a topologia da camada óptica é invisível para a camada IP. O plano IP deve ter então capacidade de resolução de endereços, ou possuir uma base de dados dos caminhos ópticos. A Figura 4.12 mostra uma arquitetura centralizada para o modelo *overlay* (controle distribuído é também possível), que atende requisições de redes IP e de redes SDH.

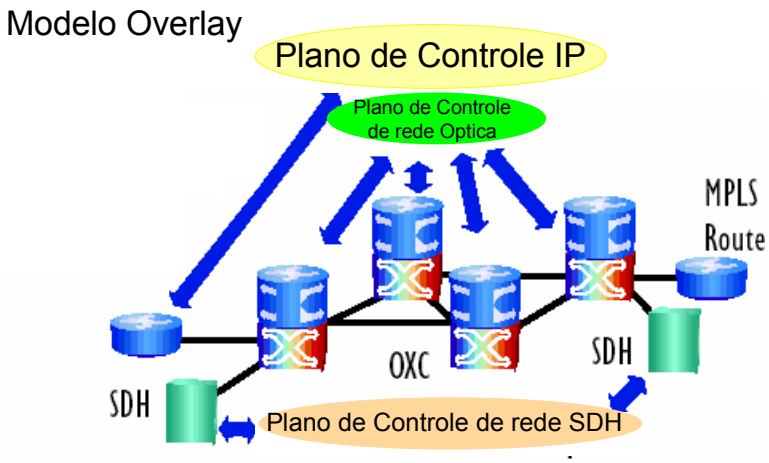

Figura 4.12 - Modelo Overlay com plano de controle centralizado

4.3.2.3 Modelo Interdomínio ou Híbrido

Sob este modelo existem instâncias de roteamento separadas nos dominios IP e Óptico. Embora cada camada tenha seu próprio plano de controle, a informação de uma instância de roteamento é repassada através da outra instância de roteamento. Por exemplo,

endereços IP serão transportados pelos protocolos de roteamento ópticos para permitir que a informação seja alcançada pelos clientes IP.

Este modelo combina o melhor dos modelos de interconexão *Peer* e *Overlay*. De uma forma geral, é mais simples de implementar que o modelo *Peer* e não requer a gerência de adjacências de roteamento sobre a rede óptica, como no modelo *Overlay*.

4.4 MPΛS (*MULTIPROTOCOL LAMBDA SWITCHING*)

MPλS é um protocolo para plano de controle centrado em IP. É uma extensão do MPLS direcionado para redes WDM, tornando os elementos da rede aptos a suportar altas taxas de dados. O MPλS fornece também uma estrutura orientada a conexão para protocolo IP, tornando mais fácil a incorporação de QoS na Internet.

MPλS descreve um plano de controle para comutadores ópticos que foi influenciado pelas técnicas desenvolvidas para a engenharia de tráfego no MPLS. A proposta usa a tecnologia OXC para administrar o aprovisionamento, em tempo real, dos canais ópticos. Além disto, permitir o uso de semântica uniforme para gestão de rede e operações de controle em redes híbridas, com elementos de rede OXCs e roteadores MPLS. Esse modelo proposto ajudará na gestão da largura de banda do canal óptico e o seu aprovisionamento dinâmico, assim como na sobrevivência da rede por meio de capacidades melhoradas de proteção e restauração [AWDUCHE, 2001].

Da mesma forma que o MPLS, MPλS se baseia apenas em rótulos para definir o próximo roteador. Então, não é necessário subir até a camada de rede para processar endereços IP. Esse rótulo funciona como um índice na tabela de roteamento. O comprimento de onda é usado como rótulo e é o identificador único. Isto possibilita a roteadores e *switches* realizar as funções necessárias de encaminhamento.

O plano de controle tem topologia fixa e é separado do plano de transporte de dados. O plano de controle para OXC usa protocolos IP estendidos para distribuir a informação de estado da rede de transporte óptica, incluída a informação de estado da topologia. Esta informação de estado é usada por um sistema de roteamento baseado em restrições

[KOMPELLA, 2000], para calcular os caminhos dos canais ópticos ponto a ponto. O plano de controle de OXC usa um protocolo de sinalização de MPLS para os canais ópticos ponto-a-ponto. Assim, pacotes IP podem ser diretamente transportados sobre redes WDM.

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

Posteriormente à junção entre o plano de controle MPLS com os comutadores OXC, que deu origem ao MPλS, desenvolveu-se o GMPLS como uma solução de convergência tecnológica de engenharia de tráfego e QoS para as redes de transporte.

4.5 GMPLS (GENERALIZED MULTIPROTOCOL LAMBDA SWITCHING)

GMPLS é um conjunto de protocolos estendidos de MPLS e MPλS em um plano de controle comum, tanto para redes ópticas como eletrônicas, que é necessário para possibilitar a próxima geração de redes IP sobre WDM [ROUSSEAU, 2003].

GMPLS estende MPLS e MPλS para incluir a comutação por divisão no tempo na rede de transporte, dando suporte a tecnologias como SONET/SDH que multiplexam no tempo; além de aprimorar o plano de controle para tecnologias de comutação de comprimentos de onda (lambdas), espacial (porta/fibra) e pacotes/células [MANNIE, 2003]. Assim, o GMPLS aparece como uma solução de convergência dentro da próxima geração das redes de transporte.

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

O principal foco do GMPLS é o plano de controle das diversas camadas de comutação, permitindo hierarquias para o transporte da informação. O plano de controle e o plano de

transporte de dados encontram-se, para esta arquitetura, desagregados fisicamente (Figura 4.13).

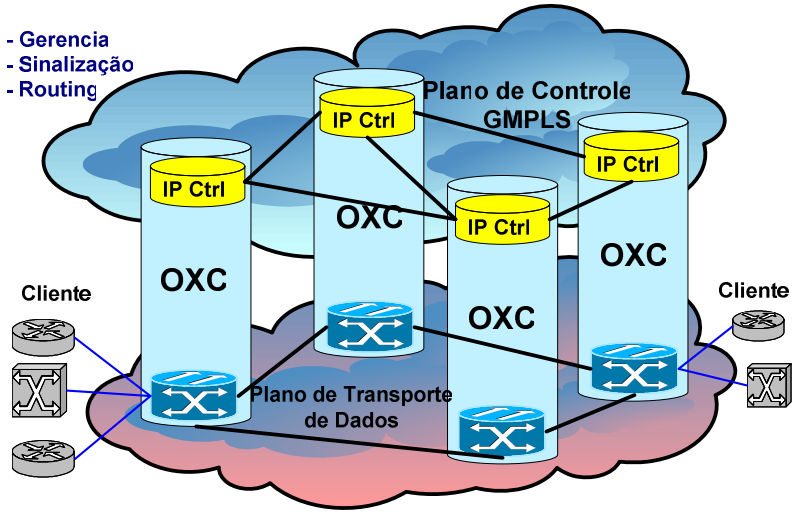

Figura 4.13 - Plano de controle e plano de transporte de dados

4.5.1 Protocolos do plano de controle GMPLS

O plano de controle GMPLS compõe-se de protocolos de sinalização e roteamento, usados no mundo IP, que têm sido modificados. Um novo protocolo é incorporado para a gerência de enlaces, o *Link Management Protocol* (LMP). Estes protocolos são apresentados na Figura 4.14.

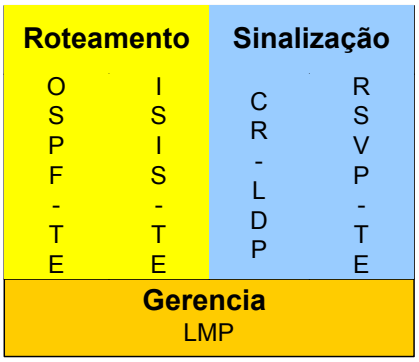

Figura 4.14 - Protocolos usados em GMPLS

Os protocolos de sinalização e roteamento requerem ao menos um canal de controle bidirecional para diagnosticar se dois LSR adjacentes estão conectados mediante enlaces unidirecionais. O LMP pode estabelecer, manter e gerenciar estes canais de controle. O conjunto de protocolos de GMPLS realizam as seguintes funções:

— Gerência do enlace: O LMP (*Link Management Protocol*) [LANG, 2003] é a especificação do IETF para verificação da conectividade do enlace, a gerência do canal de controle, a correlação das propriedades do enlace e o isolamento de falhas.

— Descoberta da topología: Os protocolos de encaminhamento de estado de enlace IP, OSPF (*Open Shortest Path First*) e IS-IS *(Intermediate System - Intermediate System*), têm-se estendido com caracteristicas adicionais (OSPF-TE e ISIS-TE) para a descoberta da topologia distribuída das redes ópticas [BANERJEE, 2001]. Definições para extensões específicas para as redes SONET/SDH também se vêm desenvolvendo na IETF [PAPADIMITRIOU, 2003].

— Aprovisionamento de conexão: Os protocolos de sinalização usados em MPLS, o RSVP-TE (*Resource Reservation Protocol* com extensões de Engenharia de Tráfego) e o CR–LDP (*Constraint Routed Label Distribution Protocol*), têm sido generalizados para aprovisionamento dos elementos de rede e enlaces nas redes ópticas [BANERJEE, 2001]. Além disto, se tem estendido estes protocolos para suportar as redes SONET/SDH [RAJAGOPALAN, 2000].

— Proteção e Restauração de conexão: Área relativamente nova no grupo de trabalho CCAMP[3], que especifica os protocolos GMPLS, RSVP-TE e CR-LDP baseados em mecanismos de sinalização de proteção e restauração [PAPADIMITRIOU, 2003].

4.6 ANÁLISE DE REDES ETHERNET E IP

A tecnologia Ethernet e o protocolo IP correspondem ao principal alicerce desse estudo no que diz respeito ao suporte a implementação. Assim, serão apresentadas as características básicas do protocolo de enlace, bem como uma correlação entre o protocolo IP e as tecnologias de transporte já apresentadas anteriormente.

[3] A pesquisa desenvolvida em GMPLS é feita pelo grupo de trabalho CCAMP (*Common Control and Management Plane*) da IETF.

4.6.1 Redes Ethernet

Atualmente, a maior parte do tráfego na Internet é originado e terminado em conexões Ethernet. Desde sua origem nos anos 70, concebido para redes LAN (*Local Area Network*), Ethernet tem evoluído junto com a grande demanda de alta velocidade que a Internet vem originando. Quando a fibra óptica foi introduzida, Ethernet foi-se adaptando para tirar vantagem da superior largura de banda e baixa taxa de erro que este meio oferece. O desenvolvimento da tecnologia Gigabit Ethernet tem estendido a original tecnologia LAN a distâncias que fazem da Ethernet atualmente também um padrão para MAN (*Metropolitan Area Network*) e WAN (*Wide Area Network*). Assim, o mesmo protocolo que transportava dados a 3 Mbps em 1973 pode agora transportar dados a 10 Gbps e taxas superiores.

A idéia original do protocolo Ethernet foi permitir dois ou mais *hosts* a usar o mesmo meio sem interferência entre seus sinais. Este problema de múltiplos usuários acessando a um mesmo meio compartilhado foi estudado no início dos anos 70 na University do Hawai. Um sistema chamado de Alohanet foi desenvolvido para permitir as várias estações terem um acesso estruturado para o compartilhamento de banda de radiofreqüência na atmosfera. Este trabalho estabeleceu as bases para o método de acesso da Ethernet conhecido como CSMA/CD [ABRAMSON, 1970].

De uma forma geral, o sucesso da tecnologia Ethernet é atribuído aos seguintes fatores:

— Simplicidade e fácil manutenção;

— Capacidade para incorporar novas tecnologias;

— Confiabilidade;

— Baixo custo de instalação e atualização.

Em 1985, o comitê de padrões da IEEE para redes locais e metropolitanas publicou um acervo de padrões para LANs. Esses documentos para esses padrões, conhecidos como *standards*, iniciam com o número 802. O *standard* para Ethernet é o 802.3. Para manter o *standard* compatível com a ISO (*International Standards Organization*) e o modelo OSI, a IEEE 802.3 orientou o *standard* para as necessidades da camada 1 e para a parte mais baixa da camada 2 do OSI. Como resultado, algumas pequenas modificações do original Ethernet foram feitos no 802.3.

Os 10Mbps de largura de banda Ethernet foram mais que suficientes para os lentos PCs dos anos 80. Contudo, no início dos anos 90 os PCs ficaram muito mais velozes, os arquivos aumentaram em tamanho, e gargalos no fluxo de dados começaram a acontecer. Dessa forma, tornou-se necessário um incremento na largura de banda. Em 1995, a IEEE anuncia um *standard* para 100 Mbps Ethernet, conhecido como fast Ethernet, que foi seguido pelos padrões para Gigabit Ethernet em 1998 e 1999.

Todos esses padrões são essencialmente compatíveis com o Ethernet original. Assim, um *frame* Ethernet pode sair desde uma placa NIC (*Network Interface Card*) coaxial a 10 Mbps num *desktop*, ser colocado dentro de um enlace de fibra 10 Gbps Ethernet, e finalizar numa outra placa de um PC com NIC a 100 Mbps. Em todo o percurso o *frame* Ethernet não muda por esta razão esta tecnologia é considerada muito escalável. A largura de banda da rede pode ser incrementada muitas vezes, porém a tecnologia Ethernet permanece a mesma.

Ethernet é uma família de tecnologias de rede que inclui o Ethernet legado, *Fast Ethernet e Gigabit Ethernet*. As taxas de transmissão em Ethernet podem ser de 10, 100, 1000 ou 10.000 Mbps. O formato de *frame* básico IEEE e as subcamadas para o modelo OSI camada 1 e 2 mantém consistência para todas as formas de Ethernet [CISCO$_a$, 2005].

A tecnologia Ethernet utiliza sinal de banda base, o qual imprime o uso toda a largura de banda do meio de transmissão. O sinal de dados é transmitido diretamente sobre o meio de transmissão.

Ethernet opera em duas camadas do modelo OSI. Estas são: a camada inferior da camada de enlace de dados, conhecida como a subcamada MAC, e a camada física.

Os dados que vão de uma estação Ethernet para outra freqüentemente passam por um repetidor. Todas as estações no mesmo domínio de colisão vêem passar o tráfego através de um repetidor (por exemplo, hub). De uma forma simples, um domínio de colisão é um recurso compartilhado onde os problemas originados numa parte de um domínio usualmente impactarão todo o domínio de colisão.

Um repetidor envia tráfego para todas as portas menos para a porta da qual a recebeu. Qualquer sinal detectado pelo repetidor será enviado. Contudo, se o sinal esta degradado, seja por atenuação ou ruído, o repetidor tentará reconstruir e regenerar o sinal antes de enviá-lo.

Para garantir a mínima largura de banda e a operabilidade, o padrão especifica o máximo número de estações por segmento, o máximo comprimento do segmento e o máximo número de repetidores entre estações. Estações separadas por *bridges*, *switches* ou *routers* estão em diferentes domínios de colisão.

A Figura 4.15 apresenta uma variedade de tecnologias LANs para a camada 1 e a subcamada 2 do modelo OSI. A camada 1 envolve sinais, *bit streams*, componentes que colocam sinais no meio de transmissão, assim como várias topologias. A camada 1 Ethernet constitui um ponto chave na comunicação entre dois dispositivos com várias funções e suas limitações, as quais são supridas pela camada 2.

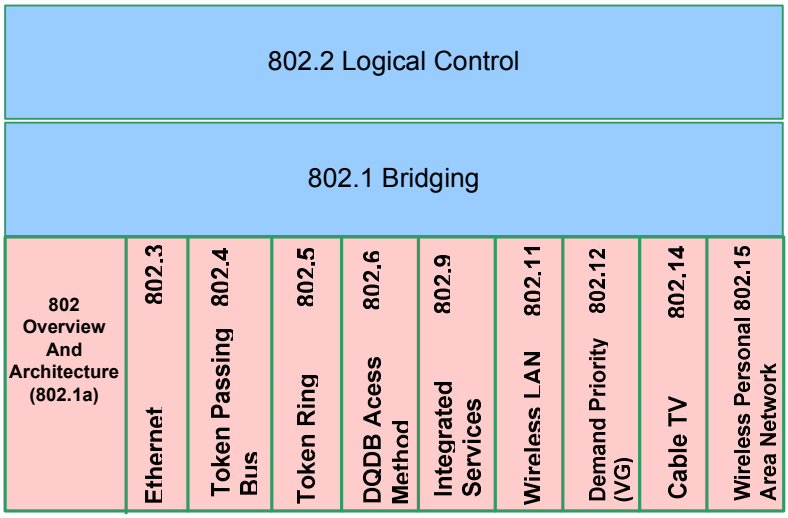

Figura 4.15- Tecnologias LANs para a camada 1 e a subcamada 2 do modelo OSI

A camada de enlace de dados contribui significativamente na compatibilidade tecnológica e na comunicação entre estações. A subcamada MAC se preocupa com os componentes físicos que serão usados para a comunicação da informação. A subcamada LLC (*Logical Link Control*) permanente relativamente independente do equipamento físico que será usado para o processo de comunicação.

Assim, para que a camada 1 possa se comunicar com as camadas superiores, a camada 2 usa a LLC. Como a camada 1 não pode identificar computadores, a camada 2 usa processos de endereçamento para tal. A camada 1 pode só descrever *stream* de *bits*, já a camada 2 usa *framing* para organizar ou agrupar os *bits* de informação. A camada 1 não é capaz de decifrar qual computador transmitirá dados binários entre um grupo onde vários estão tentando transmitir ao mesmo tempo. A camada 2 usa um sistema de controle de acesso ao meio chamado MAC (*Media Acesso Control*).

A Figura 4.16 apresenta a subcamada MAC, dentro do contexto do modelo OSI, para o padrão Ethernet.

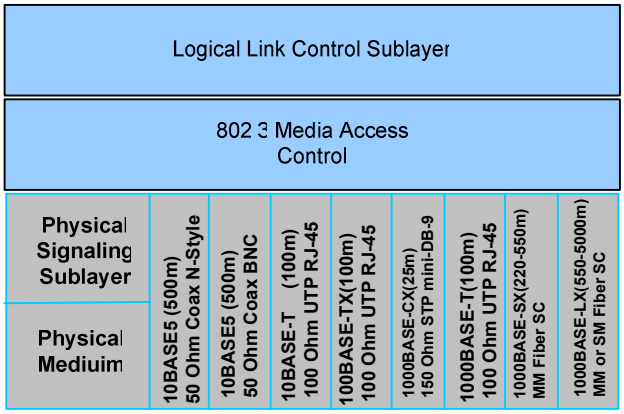

Figura 4.16 - Subcamada MAC – OSI

4.6.1.1 Endereços MAC usados por Redes Ethernet

Um sistema baseado em endereços é requerido para identificar computadores e interfaces, permitindo assim a entrega de *frames* na tecnologia Ethernet.

A tecnologia Ethernet usa endereços MAC que possuem 48 bits de comprimento e é expresso como 12 dígitos hexadecimais. Os primeiros 6 dígitos são administrados pela IEEE e identifica o fabricante ou vendedor. Esta parte do endereço é conhecida como OUI (*Organizational Unique Identifier*). Os últimos 6 dígitos hexadecimais representam o número da interface serial ou outro valor administrado pelo fabricante. A Figura 4.17 apresenta esta formatação. Os endereços MAC são armazenados em ROM (*Read Only Memory*) e são copiados em RAM (*Ramdom Acesso Memory*) quando a NIC é inicializada.

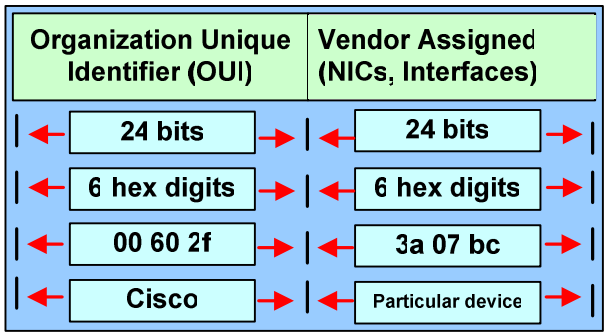

Figura 4.17 - Formato do endereço MAC

Um cabeçalho MAC é adicionado aos dados que vêm das camadas superiores no modelo OSI. O cabeçalho contém informação de controle para a camada de enlace de dados do sistema destino. Os dados, que vêm desde as camadas superiores, são encapsulados dentro de um frame de enlace de dados e logo enviados à rede para serem transmitidos.

A NIC receptora usa o endereço MAC para determinar se uma mensagem deve passar para as camadas superiores do modelo OSI. Quando um dispositivo envia dados numa rede Ethernet este pode usar um endereço de destino MAC para abrir um caminho de comunicação para outro dispositivo. O dispositivo fonte coloca no *header* o endereço MAC do dispositivo destino e envia dados através da rede. Na rede compartilhada, as NICs em cada dispositivo verificam se o endereço MAC destino corresponde ao seu respectivo NIC. Caso não seja, a NIC descarta o frame. Quando os dados alcançam o nó destino, a NIC faz uma cópia deste e passa o frame às camadas superiores. Assim, numa rede Ethernet, todos os nós devem examinar o cabeçalho MAC.

Todos os dispositivos conectados a uma rede LAN Ethernet têm interfaces com endereços MAC. Isto inclui estações, impressoras, roteadores, switches etc.

4.6.1.2 Frames Ethernet Camada 2 do modelo OSI

Codificar *bit streams* ou dados, no meio físico, representa uma grande complexidade tecnológica. Contudo, somente esta tarefa não é suficiente para fazer a comunicação acontecer. O mecanismo de *framing* provê informação essencial para a transmissão dos dados. Esta informação inclui:

— Quais computadores estão em comunicação com outros;

— Quando comunicações entre computadores individuais começaram e quando estas terminam;

— Que erros tem ocorrido entre os computadores que se comunicavam;

— Qual computador será o seguinte em se comunicar.

Framing é o processo de encapsulamento de camada 2. Um *frame* é a unidade de dados de protocolo (PDU) de Ethernet da camada 2. Os campos permitidos ou requeridos num Frame 802.3 Ethernet, e que são apresentados na Figura 4.18, são:

— *Preamble*

— Delimitador de Inicio de *Frame* (*Start Frame Delimiter*)

— Endereço Destino (*Destination Address*)

— Enedereço Origem (*Source Address*)

— Comprimento/Tipo (*Length/Type*)

— Dados e *Pad*

— *Frame Check Sequence* (FCS)

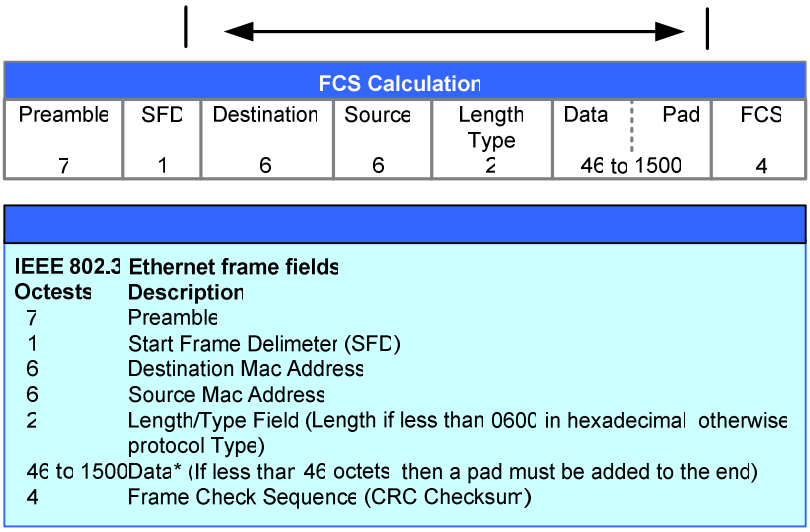

Figura 4.18 - Frame 802.3 Ethernet

Em 10 Mbps e versões anteriores da Ethernet, o *Preamble* provê informação de temporização que o nó receptor precisa para interpretar o sinal elétrico que está recebendo. O *Start Frame Delimiter* marca o fim da informação de temporização.

Vale ressaltar que 10 Mbps e versões anteriores de Ethernet são assíncronas. Isto é, elas devem usar informação de temporização do *preamble* para sincronizar o circuito receptor para a entrada de dados. 100 Mbps e implementações de alta velocidade de Ethernet são síncronas e não precisam da informação de temporização, porém por razões de compatibilidade o *Preamble* e o SFD estão presentes.

Os campos de endereços do *frame* Ethernet contem endereços fonte e destino de camada 2, ou endereços MAC. O campo de comprimento possui dois octetos, que indicam o número de octetos de dados da camada lógica (LLC). O campo de dados da camada lógica contém um conjunto de n octetos, de acordo com o máximo especificado na implementação de uma tecnologia particular.

Frames são usados para enviar os dados das camadas superiores e das aplicações de usuário desde uma fonte até um destino. O pacote de dados inclui a mensagem a ser enviada, mas *bytes* adicionais podem ser colocados para os *frames* ter um mínimo comprimento para atender a propósitos de temporização. *Bytes* LLC são também incluídos no campo de dados.

A subcamada LLC toma os dados do protocolo de rede, geralmente pacotes IP, e adiciona informação de controle para ajudar à entrega do pacote ao nó destino. A camada 2 comunica-se com as camadas superiores através da subcamada LLC.

Todos os *frames* são susceptíveis a erros. Assim, o campo *Frame Check Sequence* (FCS) de um *frame* Ethernet contém um número que é calculado pelo nó fonte baseado nos dados contidos no *frame.* No nó destino isto é recalculado e comparado para determinar se os dados recebidos estão completos e livres de erro. Se os dois números deste campo são diferentes, um erro é assumido, e o *frame* é descartado. Dado que a fonte não tem como detectar que o *frame* foi descartado, a retransmissão desse *frame* só é possível por iniciativa de protocolos orientados a conexão das camadas superiores, as quais cuidam do controle no fluxo de dados. Um protocolo deste tipo é o protocolo TCP, o qual espera por um *frame* de reconhecimento (ACK) a ser enviado pela estação destino dentro de certo tempo, sem o qual a retransmissão ocorre.

4.6.1.3 Protocolo MAC

O protocolo MAC determina qual computador, no contexto do meio compartilhado ou domínio de colisão, é permitido transmitir dados. MAC e LLC formam parte da versão IEEE da camada 2 do modelo OSI. Desta forma, MAC e LLC são subcamadas da camada 2.

O protocolo MAC pode se classificar em duas grandes categorias: como protocolos determinísticos e não-determinísticos. Exemplos de protocolos determinísticos incluem a Token Ring e FDDI. Numa rede Token Ring os *hosts* são colocados num anel e um *token* vai para cada *host* em seqüência ao redor do anel. Quando um *host* deseja transmitir, este segura o *token*, transmite os dados por um tempo limitado e então envia o *token* para o próximo *host* no anel. Token Ring é um contexto sem colisões dado que só um *host* pode transmitir por vez [CISCO$_b$, 2005].

O protocolo MAC não-determinístico usa uma aproximação "primeiro a enviar, primeiro a ser atendido", baseado num sistema chamado CSMA/CD (*Carrier Sense Multiple Acesso with Collision Detection*).

Como tecnologias de camada 1 podem-se citar: Token Ring, FDDI e Ethernet, com as topologias apresentadas na Figura 4.19 Todas usam LLC, *naming*, *framing* e MAC da camada 2. Assim temos que:

— Em Ethernet usa-se uma topologia lógica bus para controle do fluxo de informação numa topologia física de bus linear ou numa topologia estrela;
— Em Token Ring usa-se uma topologia lógica em anel (*ring*) para o controle do fluxo de informação e uma topologia física estrela;
— Em FDDI usa-se uma topologia lógica em anel (*ring*) para o controle do fluxo de informação e uma topologia física em duplo anel (*dual-ring*).

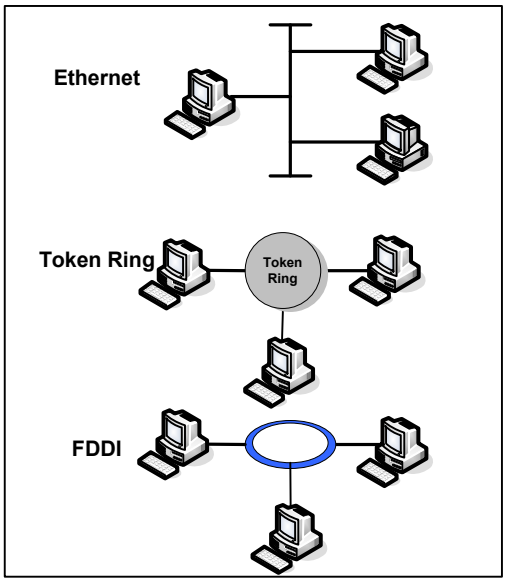

Figura 4.19 - Topologias físicas Ethernet, Token Ring e FDDI

4.6.1.4 Detecção de Colisão numa rede CSMA/CD

Como dito anteriormente, Ethernet é uma tecnologia *broadcast* num meio compartilhado. O método de acesso CSMA/CD usado realiza suas funções:

— Transmitindo e recebendo *frames* de dados;

— Decodificando frames de dados e verificando estes para validar endereços antes de serem passados para as camadas superiores do modelo OSI;

— Detectando erros dentro dos *frames* de dados ou na rede.

No método de acesso CSMA/CD, dispositivos da rede com dados a transmitir operam num modo "escuta antes de transmitir". Quando um nó deseja enviar dados, este deve primeiro verificar se o meio de transmissão esta ocupado. Se o nó escuta que a rede se encontra ocupada, esperará um tempo aleatório antes de tentar novamente. Se o nó determina que o meio de rede não está ocupado, então começará a transmitir e escutará no meio para se assegurar que outro nó não esta transmitindo ao mesmo tempo. Depois de completar a transmissão dos seus dados, o nó retornará ao modo de escuta. Isto é apresentado na Figura 4.20.

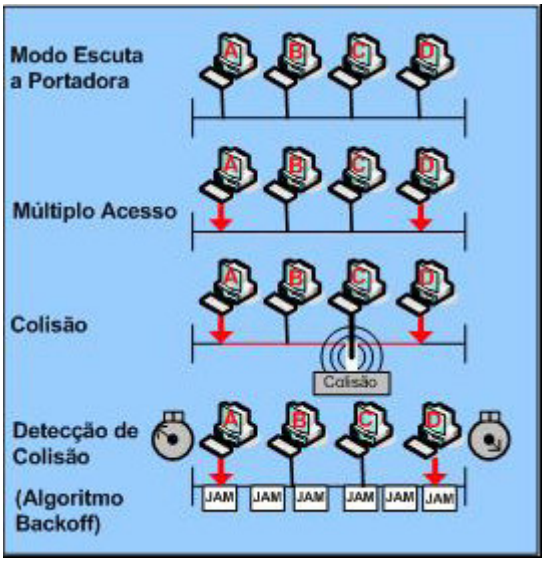

Figura 4.20 - Método de acesso CSMA/CD

Dispositivos de rede detectam que uma colisão aconteceu quando a amplitude do sinal no meio de transmissão está incrementada. Quando uma colisão acontece, cada nó que estava transmitindo continuará a transmitir por um curto tempo para se assegurar que todos os nós detectaram a colisão. Assim, quando todos os nós têm detectado a colisão, um algoritmo de concessão (*backoff algorithm*) é invocado e a transmissão é interrompida. Todos os nós da rede param por um período de tempo aleatório, determinado pelo algoritmo de *backoff*. Quando o período de espera termina, cada nó pode tentar o acesso ao meio de rede. Os dispositivos que estiveram envolvidos na colisão não terão prioridade na transmissão. Um fluxograma desta operação é mostrado na Figura 4.21.

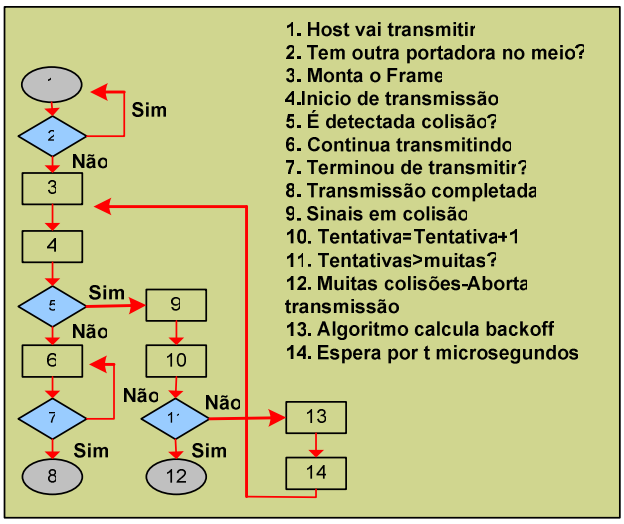

Figura 4.21 - Fluxograma da operação do CSMA/CD

Os sinais elétricos consomem um tempo ao viajar pelo cabo (*delay*). Assim, é possível por este atraso, que mais de uma estação inicie simultaneamente, ou em tempo muito próximo, a transmissão. Isto resultará numa colisão.

Se a estação conectada está operando em modo *full-duplex* então pode enviar e receber simultaneamente e colisões não devem acontecer. Contudo, em modo *half* duplex, assumindo que uma colisão não tenha ocorrido, a estação transmitira 64 *bits* de informação de sincronização de temporização que é conhecido como *Preamble*. A estação então transmitirá a seguinte informação:

— Informação de endereços MAC de fonte e destino;

— Outras informações no cabeçalho;

— *Payload* de dados;

— *Checksum* (FCS) usado para assegurar que a mensagem não foi corrompida ao longo do caminho.

A estação receptora do *frame* recalculará o FCS para determinar se a mensagem entrante é válida e então passará a mensagem para as camadas superiores da pilha de protocolos.

As versões de Ethernet de 10 Mbps e anteriores são assíncronas. Neste modo de transmissão cada estação receptora utilizará os 8 octetos de informação de temporização para sincronizar o circuito de recepção para a entrada dos dados e logo descarta estes octetos. Implementações Ethernet de 100 Mbps e de taxas superiores são síncronas. Isso significa que a informação de *Preamble* e *Start Frame Delimiter* (SFD) não são requeridas, mas por motivos de compatibilidade são ainda mantidas.

Para todas as taxas de transmissão de Ethernet o padrão descreve que uma transmissão não pode ser menor que um *slot time*. Um *slot time* para 10 e 100 Mbps Ethernet é 512 *bit-time*s, ou 64 octetos. Um *slot time* para 1000 Mbps Ethernet é 4096 *bit-times*, ou 512 octetos. *Slot time* é calculado assumindo o máximo comprimento do cabo numa autêntica arquitetura de rede.

O *slot time* calculado é justamente maior que o total teórico de tempo requerido para viajar entre os pontos mais distantes do domínio de colisão, colidir com outra transmissão no último instante possível, e então ter os fragmentos da colisão retornando à estação que enviou e ser detectada.

Em Ethernet a 10 Mbps um *bit* na camada MAC precisa 100 nanosegundos (ns) para transmitir. Em 100 Mbps o mesmo *bit* precisa 10 ns para transmitir, e a 1000 Mbps só toma 1 ns. Assim, grosso modo, 20,3 cm (8 polegadas) por nano segundo é frequentemente usado para calcular retardo de propagação num cabo UTP. Para 100 metros de UTP, isto significa que um sinal 10BASE-T tomaria aproximadamente 5 *bit-times* para viajar pelo comprimento do cabo.

Para a operação Ethernet CSMA/CD, a estação que transmite deve estar certa de uma colisão antes que esta tenha completado a transmissão de um *frame* de tamanho mínimo. A 100 Mbps a temporização do sistema é dificilmente hábil para 100 metros de cabo. A 1000 Mbps especiais ajustes são requeridos, pois um frame inteiro de tamanho mínimo seria transmitido antes que o primeiro bit alcançasse o final dos primeiros 100 metros de cabo UTP. Por esta razão *half duplex* não é permitida em 10 Gigabit Ethernet.

O mínimo espaçamento entre dois *frames* que não colidem é também chamado de espaçamento *interframe* (*interframe spacing*). O espaçamento *interframe* é requerido para assegurar que todas as estações tenham tempo para processar o frame prévio e preparar-se para o próximo frame.

Colisões podem ocorrer em vários pontos durante a transmissão. Uma colisão onde um sinal é detectado no circuito transmissor e receptor ao mesmo tempo é dita uma colisão local. A colisão que acontece antes que o mínimo numero de *bytes* possa ser transmitido é chamada de colisão remota. Uma colisão que sucede depois que os primeiros 64 *bytes* de dados foram enviados é considerada uma colisão atrasada. A NIC não retransmitira automaticamente para este tipo de colisão.

Colisões local e remota são consideradas como parte normal da operação Ethernet, colisões atrasadas são consideradas um erro. Erros em Ethernet resultam da detecção de tamanhos de *frames* que são maiores ou mais curtos que os padrões permitidos.

4.6.2 Gigabit Ethernet

Este padrão especifica meios de fibra e cobre para transmissão de dados. O *standard* 1000BASE-T, IEEE 802.3ab, usa cabo de cobre Categoria 5. O standard 1000BASE-X, IEEE 802.3z, especifica 1 Gbps *full duplex* sobre fibra óptica.

Os padrões 1000BASE-TX, 1000BASE-SX, e 1000BASE-LX usam o mesmo parâmetro de temporização, que é de 1 ns. O *frame* Gigabit Ethernet tem o mesmo formato usado por 10 e 100 Mbps Ethernet. Algumas implementações de Gigabit Ethernet podem usar diferentes processos para converter *frames* em *bits* no cabo.

As diferenças entre os padrões Ethernet, Fast Ethernet e Gigabit Ethernet ocorrem na camada física. Devido ao incremento de velocidade destes novos padrões, a curta duração do *bit times* precisa de especial consideração. Dado que os *bits* são introduzidos no meio por uma curta duração, a temporização é critica. Estas altas velocidades de transmissão requerem altas freqüências, que origina mais susceptibilidade ao ruído no meio de cobre.

A susceptibilidade ao ruído levou a Gigabit Ethernet a usar dois passos de codificação separados, pois a transmissão de dados é mais eficiente quando códigos são usados para representar o *stream* de *bits*. A codificação dos dados prove sincronização, eficiente uso da largura de banda, e melhora a relação sinal-ruido.

Na camada física o padrão de *bits* desde a camada MAC é convertido em símbolos, que podem também levar informação de controle. O *frame* é então codificado em símbolos de controle e símbolos de dados para incrementar seu *throughput* na rede.

Gigabit Ethernet baseado em fibra, ou 1000BASE-X, usa codificação 8B/10B, o qual é similar ao conceito 4B/5B. Este é seguido pela codificação de linha *nonreturn to zero* (NRZ), codificando o sinal de luz na fibra óptica. Este processo de codificação é possível, pois a fibra pode transportar sinais de grande largura de banda.

4.6.2.1 1000BASE-SX e LX

O padrão IEEE 802.3 recomendou que Gigabit Ethernet sobre fibra fosse à tecnologia preferida no *backbone*.

A temporização, o formato de *frame* e a transmissão são comuns a todas as versões de 1000 Mbps. Dois esquemas de codificação de sinal são definidas na camada física. O esquema 8B/10B é usado para fibra óptica e meio de cobre protegido, e modulação por amplitude de pulso 5 (PAM5) é usado para UTP.

Como dito anteriormente, 1000BASE-X usa codificação 8B/10B convertido para codificação de linha NRZ (non-return to zero). Codificação NRZ está baseada no nível de sinal encontrado na janela de temporização para determinar o valor binário para este período de *bit*. Muito diferente de outros esquemas de codificação, este sistema de codificação é tratado por nível em lugar de ser tratado por flanco (*edge*). Assim, a determinação de si um *bit* é 0 ou 1 é feito por nível do sinal.

Após a codificação, os sinais NRZ são, então, pulsados dentro da fibra usando fontes de luz de curto comprimento de onda (*short-wavelength*), ou longo comprimento de onda (*long-wavelength*). O primeiro usa fontes de luz laser ou LED na janela de 850 nm em fibra multimodo (1000BASE-SX). Esta é uma opção de baixo custo, mas para curtas distâncias. Para longo comprimento de onda é usado laser a 1310 nm em fibras monomodo ou multimodo (1000BASE-LX). Fontes Laser usadas com fibra monomodo podem alcançar distâncias acima de 5 Km. A luz é pulsada usando baixa e alta potência. Um "0" lógico é representado por baixa potência e um "1" lógico para alta potência.

O método MAC trata o *link* como ponto-a-ponto. Dado que fibras separadas são usadas para transmissão (Tx) e recepção (Rx) a conexão é inerentemente *full-duplex*. Assim, Gigabit Ethernet permite só um único repetidor entre duas estações.

Na arquitetura Gigabit Ethernet as limitações de distância de enlaces *full-duplex* estão limitadas só pelo meio, e não pelo retardo da viajem de ida e volta (*round-trip delay*). Assim, topologias estrela (*star*), e estrela estendida são permitidas.

4.6.2.2 10-Gigabit Ethernet

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

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

A camada física 10Gb Ethernet permite uma extensão em distância de 40Km sobre fibra monomodo e compatibilidade com redes SONET (*Synchronous Optical Network*) e redes SDH (*Synchronous Digital Hierarchy*). Operações a 40 km de distância habilitam a 10GbE para operar em redes MAN.

A compatibilidade com redes SONET/SDH operando acima de velocidades de OC-192 (9.584640 Gbps) fazem de 10GbE uma tecnologia WAN viável. Assim, 10GbE compete com ATM em algumas aplicações.

De uma forma geral, 10GbE comparado com outras variedades de Ethernet apresenta as seguintes características:

— O formato de *Frame* é o mesmo, isto permite interoperabilidade entre todos os tipos de Ethernet: legado, fast, gigabit, e 10 *gigabit*, sem *reframing* ou conversão de protocolo;

— O tempo de *bit* (*bit time*) é de 0.1 nanosegundos;

— Dado que só são usadas conexões de fibra, CSMA/CD não é necessário;

— As subcamadas IEEE 802.3 dentro das camadas 1 e 2 do modelo OSI são preservadas, com algumas adições para acomodar enlaces de fibra a 40 km e interoperabilidade com tecnologia SONET/SDH;

— Redes Ethernet flexíveis, eficientes, confiáveis e de relativamente baixo custo fim-a-fim tornam-se possível;

— TCP/IP pode rodar sobre LANs, MANs, e WANs com um método de enlace camada 2.

O padrão para CSMA/CD é IEEE 802.3. Um suplemento IEEE 802.3, denominado 802.3ae, delimita a família 10GbE. Uma variedade de implementações estão sendo consideradas para 10 GbE, incluindo:

— 10GBASE-SR – Projetado para curtas distâncias sobre fibra multimodo já instalada. Suporta um range entre 26 m a 82 m;

— 10GBASE-LX4 – Usa WDM (*wavelength division multiplexing*). Suporta 240 m a 300 m sobre fibra multimodo já instalada e 10 km sobre fibra monomodo;

— 10GBASE-LR e 10GBASE-ER – Suporta 10 km e 40 km sobre fibra monomodo;

— 10GBASE-W, projetado para trabalhar com equipamento baseado em módulos de transporte síncrono WAN SONET/SDH OC-192.

O IEEE 802.3ae Task force e o 10 Gigabit Ethernet Alliance (10 GEA) estão trabalhando para padronizar estas tecnologias emergentes. 10 Gbps Ethernet (IEEE 802.3ae) foi padronizada em Junho de 2002, sendo um protocolo *full-duplex* que só usa fibra óptica como meio de transmissão. A máxima distância de transmissão depende do tipo de fibra que é utilizado.

Quando usado fibra monomodo como meio de transmissão, a máxima distancia é 40 kilometros (25 milhas). Atualmente, na IEEE, tem-se sugerido a possibilidade de padrões para 40, 80, e 100 Gbps Ethernet.

A curta duração do tempo de *bit* pelo incremento na velocidade requer especial consideração. Para transmissões em 10 GbE, a duração de cada *bit* de dados é 0.1 nanosegundo. Isto significa que seriam 1.000 GbE *bits* de dados no mesmo tempo de *bit* que um *bit* de dados num *stream* de dados Ethernet a 10 Mbps. Por causa da curta duração do *bit* de dados de 10 GbE, frequentemente é difícil separar os *bit* de dados do ruído. Assim, transmissão de dados em 10 GbE baseia-se em exata temporização de *bit* para separar os dados dos efeitos do ruído na camada física. Este é o propósito da sincronização.

4.6.3 Futuro do padrão Ethernet

Ethernet tem seguido a evolução das seguintes tecnologias: legado —> Fast —> Gigabit —> MultiGigabit.

Ethernet é agora o padrão para conexões horizontal, vertical, e *inter-building*. Recentes versões desenvolvidas de Ethernet estão tornando difusa a distinção entre LANs, MANs, e WANs.

Propostas para outros esquemas de arbitragem Ethernet, além do CSMA/CD, têm sido apresentadas. Tal como UTP e fibra óptica com caminhos separados de Tx e Rx.

O futuro do meio de rede é triplo:

— Cobre (acima de 1000 Mbps, talvez mais)

— *Wireless* (aproximadamente 100 Mbps, talvez mais)

— Fibra Óptica (normalmente a 10.000 Mbps a mais)

Os meios baseados em cobre e *wireless* tem certas limitações físicas e práticas nos sinais de alta freqüência que podem ser transmitidos. Isto não é um fator limitante para fibras ópticas.

Tecnologias Ethernet de alta velocidade *full-duplex* que agora dominam o Mercado estão demonstrando ser suficiente no suporte a aplicações com QoS-intensivos.

4.7 IP – CERNE DA ARQUITETURA DE TRANSMISSÃO DE DADOS

Como apresentado anteriormente, o protocolo IP tende a ser um requisito a ser atendido com relação a qualquer uma das tecnologias das camadas de transmissão de dados. Considerando tal fato, será apresentada uma descrição focada em cada camada e sua respectiva inter-relação com o *Internet Protocol*.

4.7.1 IP over ATM

Muitos *carriers* têm *backbone* ATM, de fato 80% do tráfego da Internet vai sobre ATM. A tecnologia ATM prove integração de voz, imagem, vídeo e dados, assim como gerência de tráfego, sinalização e roteamento com qualidade de serviço.

ATM foi projetado para *carriers*, principalmente para favorecer o tráfego de voz, porém se introduz complexidade no sistema final, uma das razões pelo qual não pode alcançar os usuários finais.

O encapsulamento LLC (*Logical Link Control*) é necessario quando diferentes protocolos são transportados sobre o mesmo enlace (ATM VCC). O PDU LLC/SNAP (*Sub-Network Access Point*) é transportado no *payload* do PDU do protocolo AAL5

(ATM *Adaptation Layer* 5). Por sua vez o PDU LLC/SNAP encapsula os pacotes IP para seu posterior transporte no circuito virtual ATM.

A Figura 4.22 apresenta o caminho entre um usuário final e o servidor remoto para um usuário que acessa via modem com interface básica ISDN (I.430). No roteador é necessário implementar também uma interface ISDN para comunicação com o usuário. Para o acesso à rede ATM os pacotes IP são encapsulados em LLC/SNAP e logo adaptados com AAL5. Estabelecido o circuito virtual, a informação é transmitida usando-se enlaces SDH.

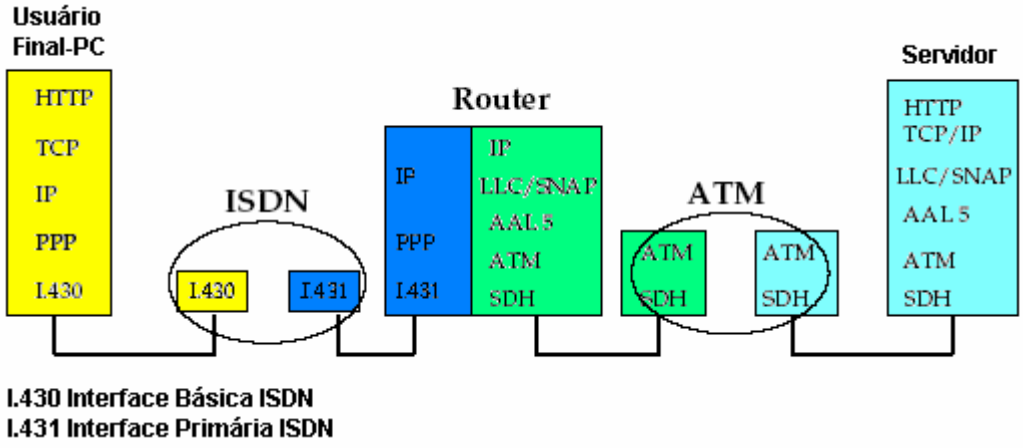

Figura 4.22 - Exemplo de uma rede IP/ATM usando encapsulamento LLC

4.7.1.1 Eliminando a camada ATM

Os provedores de serviço Internet (ISPs - *Internet Service Providers*) estão buscando transmitir IP diretamente sobre SDH. A razão principal dada pelos ISPs é que usando ATM para transportar IP é adicionado um *overhead* acima de 25%.

O *overhead* que o ATM adiciona inclui:

— Cabeçalho ATM (5 *bytes*);

— Trailer AAL5 (8 *bytes*);

— *Overhead* do encapsulamento LLC/SNAP (8 *bytes*); e

— PAD (ultimo segmento de alinhamento - 48 *bytes*).

Isto é especialmente significativo para pacotes pequenos. As estatísticas dizem que aproximadamente 50% de pacotes IP são de 40-44 *bytes* de comprimento [THOMPSON,

1997]. Para pacotes de 40-44 *bytes* requerem-se duas células ATM a serem transmitidas, mas a segunda célula vai quase vazia.

A Figura 4.23 apresenta a medida da distribuição do tamanho de pacotes num enlace doméstico. Pode-se ver que aproximadamente os 50% dos pacotes são pacotes muito curtos.

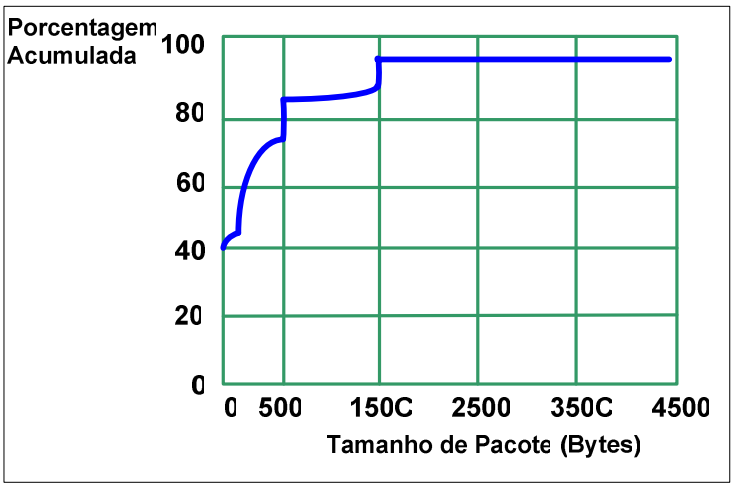

Figura 4.23 - Tamanho de pacotes num enlace doméstico [THOMPSON, 1997]

Retirando a camada ATM e redistribuindo suas funcionalidades nas outras camadas, quando possível, têm-se propostas de arquitetura baseadas em:

— IP/SDH;

— IP/WDM;

— Redes todo Ópticas (*Routing/Switching* Óptico): IP/ASON (*Internet Protocol/Automatically Switched Optical Networks*), IP/OPS (*Internet Protocol/Optical Packet Switching*).

A Figura 4.24 apresenta o resultado da retirada da camada ATM, bem como as propostas restantes.

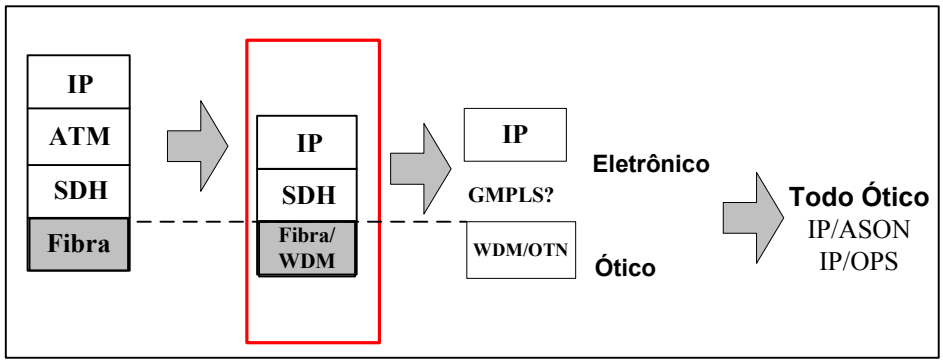

Figura 4.24 - Eliminação da camada ATM e propostas para IP diretamente sobre fibra

4.7.2 IP/SDH (ou SONET)

4.7.2.1 Encapsulamento

O encapsulamento SDH possui os níveis de *overhead* listados abaixo e diagramados na Figura 4.25:

1. SOH: *Section error monitoring* (F1 OAM);
2. LOH: *Line error monitoring* (F2 OAM);
3. POH: *Path error monitoring* (F3 OAM);

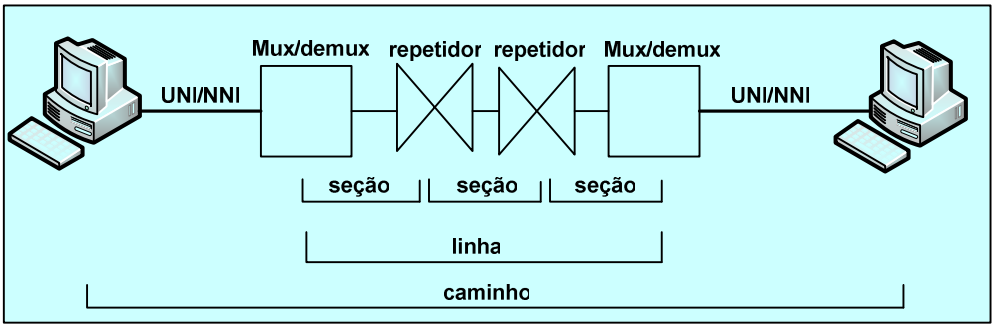

Figura 4.25 - Níveis de *overhead* em SDH/SONET

A malha STS-1, malha básica em SONET apresentada na Figura 4.26, é um conjunto bidimensional de 90 colunas por 9 filas de *bytes*. Assim,

- As primeiras 3 colunas (27 *bytes*) são o *overhead* de transporte;
- A velocidade é de 8000 malhas por segundo (uma a cada 125 microsegundos);
- 90 x 9 x 8 x 8000=90 x 9 x 64 kbps = 51,84 Mbps;

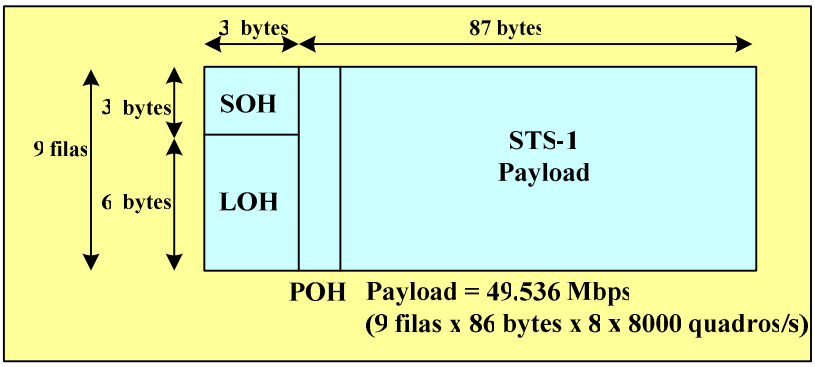

Figura 4.26 - Malha básica STS-1 (SONET)

SDH tem melhor escalabilidade que ATM em termos de taxa de transmissão. A tecnologia IP/ATM é limitado a um máximo de 622 Mbps. Já o IP/SDH pode escalar até 10 Gbps. Porém, um problema que se apresenta quando se deseja implementar IP/SDH são os processos de encapsulamento.

IP não provê sincronização de *bit* nem delineamento de pacote (demarcação de pacote). Em IP/LANs, sincronização de *bit* e delineamento de *frame* são provistos pela camada MAC. Já em IP/ATM, SDH prove sincronização de *byte*, ATM prove sincronização de célula e AAL5 delineamento de *frame*.

Em IP diretamente sobre SDH a tecnologia SDH também prove sincronização de bit, mas também é necessario prover delineamento de pacotes IP. Assim, IP/SDH requer um encapsulamento adicional para o delineamento de pacotes IP. IP/SDH usa um tipo de encapsulamento PPP HDLC (RFC 1662).

O PPP (*point-to-point protocol*) é um método padrão para transportar datagramas multi-protocolo multiplexados sobre um enlace ponto-a-ponto. Assim, esse protocolo prove:

— Encapsulamento de pacotes IP;
— Controle de erro (descartando *frames* corrompidos);
— Inicialização de enlace;

O HDLC provê:

— Reporte de Erros;

— Delineamento dos pacotes IP encapsulados em PPP (usando *byte stuffing*).

A Figura 4.27 apresenta um exemplo de uma rede IP/SDH fazendo uso de encapsulamento PPP-HDLC.

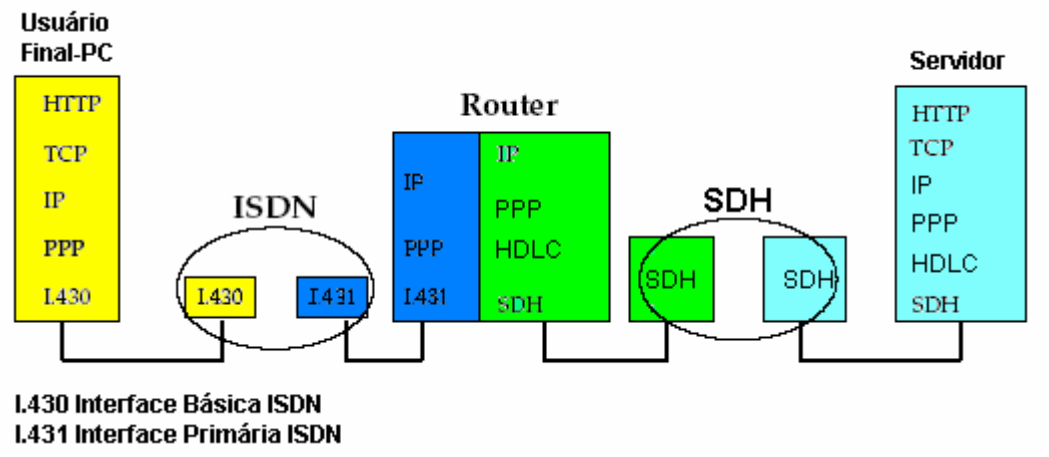

Figura 4.27 - Rede IP/SDH usando encapsulamento PPP-HDLC

A Figura 4.28 apresenta algumas configurações de redes IP sobre SDH, conhecidas também como PoS (*Packet over* SDH).

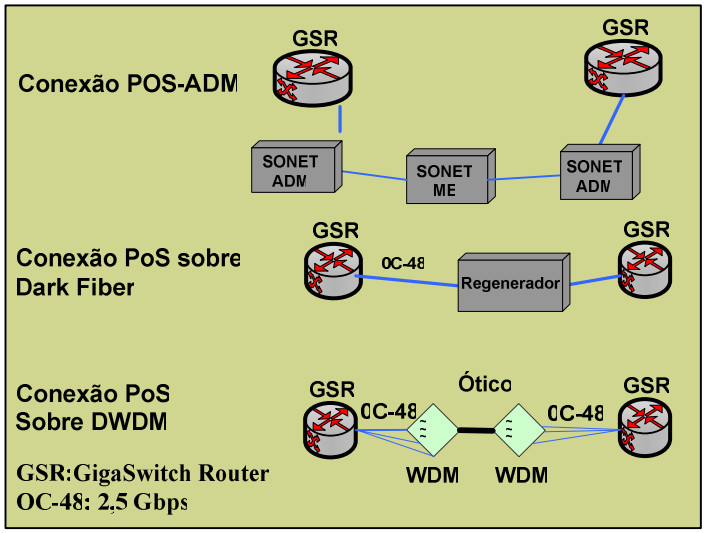

Figura 4.28 - Configurações de Rede IP sobre SDH

Desvantagens de IP sobre SDH:

— Escalabilidade até 2,4 Gbps (OC-48/STM-16);

— O mecanismo de delineamento baseado em HDLC não escala facilmente acima de 2.4 Gbps. No lado do transmissor cada saída de pacotes precisa ser monitorada e o s*tuffing* melhorado. O receptor precisa monitorar cada entrada de dados e fazer o *destuffing*;

— SDH é uma tecnologia *circuit switching*;

— Com o desenvolvimento da Internet e o incremento na transmissão de dados, a tecnologia mudou para serviços *packet switching*, o qual cria a necessidade de tecnologias de adaptação para o uso de SDH, o que significa, na prática, a introdução de maior *overhead* na rede.

4.7.3 IP/SDL

Alguns protocolos simples para escalar acima de 2,4 Gbps e evitar este problema em IP, que se apresenta em HDLC quando se deseja transmitir IP sobre SDH são requeridos. Um exemplo é o protocolo SDL (*Simplified Data Link*) projetado pela Lucent Technologies. Um *frame* SDL consiste de um indicador de comprimento de *payload* e dois CRC (*cyclic redundancy check*) um para o *header* e outro para o *payload*, em separado. Dessa maneira, espera-se evitar os problemas de *stuffing/destuffing*.

4.7.4 IP sobre ATM diretamente sobre fibra

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

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

— Técnica de transmissão mais simples;

— Overhead de camada física menor (aproximadamente 16 vezes menor);

— Não há um severo mecanismo de temporização a ser colocado na rede.

Vale ressaltar que esta proposta não está sendo endossada pela indústria.

A Tabela 4.1 apresenta uma porcentagem de *overhead* e capacidade de enlace para diferentes métodos de encapsulamento num enlace a 2,4 Gbps.

Tabela 4.1 - *Overhead* e capacidade de enlace

Encapsulamento/*Framing*	*Overhead*	Capacidade do Enlace (em Mbps)
IP/ATM/SDH	22%	1944
IP/ATM/Cell-based	19%	2011
IP/PPP/SDH	6%	2338
IP/SDL	3%	2411

4.7.5 IP/WDM

SDH não provê muita flexibilidade em termos de expansão de capacidade. Este é um dos motivos da migração das redes *backbone* IP para transporte óptico baseado em tecnologia WDM (*Wavelength Division Multiplexing*).

A instalação de mais fibra para suportar a demanda sem precedentes de maior capacidade seria muito caro. Incrementar a taxa de transmissão do sistema TDM não provê muita flexibilidade. A multiplexação por comprimento de onda parece ser o caminho mais adequado.

4.7.5.1 Benefícios

Permite incrementos flexíveis de capacidade tais como:

— Granularidade SDH: 51 Mbps, 155 Mbps, 466 Mbps, 622 Mbps, etc.

— Maximiza o reuso e minimiza o custo do ciclo de vida da fibra existente. Exemplo: WDM pode ser usado para prover quatro interfaces OC-12 (622 Mbps) IP/ATM/SDH num único par de fibra. Para alcançar o mesmo porte sem WDM seriam necessários quatro pares de fibra;

— Prove solução de transporte para sinais TDM de alta capacidade;

— Para routers Gibabit emergentes com interfaces de alta velocidade (por exemplo, OC -48), a existente infra-estrutura de transporte pode passar a ser um gargalo;

— WDM é uma solução com excelente custo - beneficio, pois toma vantagem da capacidade comercial da fibra;

— Sistemas WDM comerciais existentes oferecem 16-32 comprimentos de onda. Assim, assumindo OC-192 (10 Gbps) para cada comprimento de onda, podemos ter 160 Gbps e 320 Gbps;

— Uma fibra servindo como meio de transporte para um circuito OC-12 (622 Mbps) esta só usando um 0.4% e um 0.2% da capacidade da fibra para 16 e 32 comprimentos de onda respectivamente;

— Permite a coexistência de múltiplos tipos de interface na mesma fibra:

— IP/ATM/SDH;

— IP/PPP/HDLC/SDH.

5 IMPLEMENTAÇÃO PRÁTICA DE UMA REDE IP/WDM

Uma implementação prática de uma rede óptica sugere que cada nó possua: um dispositivo add/drop local, um módulo de comutadores ópticos, um módulo de controle, amplificadores ópticos e *transponders*. Além disso, cada nó deve ter portas com fibras de entrada e de saída para a comunicação com os nós adjacentes.

Os comutadores ópticos, compostos por oito ou mais entradas e saídas, são responsáveis pelo redirecionamento de um dos comprimentos de onda de uma das várias entradas para uma das várias saídas (nós adjacentes e o add/drop local). Os amplificadores ópticos permitem amplificar a potência do sinal que é transportado no comprimento de onda. O *transponder* permite adaptar o sinal entrante no *add-drop multiplexer* (ADM) para um determinado comprimento de onda usado na rede óptica e vice-versa.

O plano de controle dessa rede pode apresentar ou uma arquitetura centralizada ou uma arquitetura distribuída. No caso de uma arquitetura distribuída, por exemplo, um módulo de controle poderia ser implementado por um computador com várias placas FastEthernet (100 Mbps) em cada nó (cada placa conectada a um nó vizinho), e placas controladoras dos comutadores ópticos do plano físico. A rede deveria implementar, ainda, um esquema de proteção e restauração em casos de falhas na mesma. Um exemplo de rede óptica transparente é a rede OMEGA do CPqD, que é mostrada na Figura 5.1 [ROSSI, 2002].

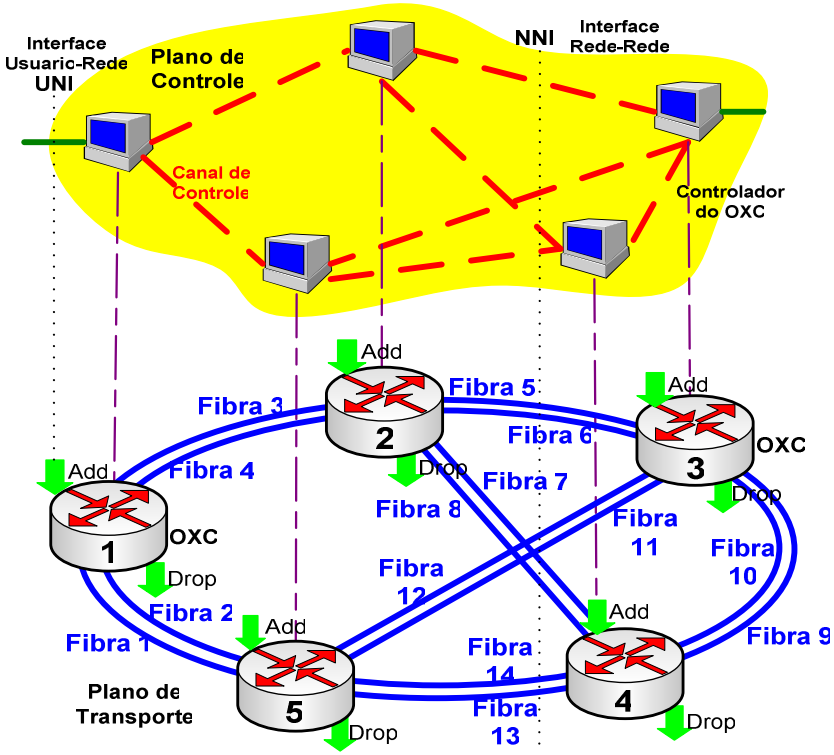

Figura 5.1 - Plano de Transporte e Plano de Controle da Rede OMEGA

5.1 REDE OMEGA MONTADA PARA TESTES

O objetivo da Rede OMEGA-WRON (*Optical Metro network for Emerging Gigabit Applications-Wavelength Routing Optical Network*)[4] é projetar, implementer e testar redes ópticas transparentes em malhas com um plano de controle distribuído, baseado em roteamento de comprimento de onda RWA (*Routing Wavelength Assignment*), algoritmo com um protocolo orientado a conexão e com caminhos bidirecionais [ROSSI, 2002].

Nessa rede, cada nó possui um dispositivo *add/drop* local; um módulo de comutadores ópticos; um módulo de controle; amplificadores ópticos e *transponders*. Para a comunicação de dados, cada nó implementa 4 portas, cada uma com fibras de entrada e de saída, sendo que três portas são conectadas com os nós adjacentes e uma é usada para add/drop.

[4] Todos os dados apresentados neste item foram obtidos através de publicações abertas.

Os comutadores ópticos, compostos por oito entradas e oito saídas, são responsáveis por redirecionar um dos oito comprimentos de onda desde uma porta de entrada para uma porta de saída. Nesta configuração, os nós OXC não provêem conversão de comprimento de onda.

5.1.1 Descrição do Plano de Transporte da Rede OMEGA

A rede óptica OMEGA é formada por cinco nós totalmente equivalentes funcionalmente com capacidade para se conectar com outros três nós da rede. Na versão usada na pesquisa realizada pelo CPqD nem todos os nós foram montados com sua capacidade total em função de questões econômicas.

Cada nó pode receber um comprimento de onda por uma porta e pode optar entre duas portas de saída para cada novo cliente. A Figura 5.2 mostra a topologia onde os nós possuem três portas se conectando a três nós adjacentes. Como cada porta tem duas fibras, sendo uma para entrada e outra para saída do sinal, o comprimento de onda poderá até mesmo retornar para o nó de origem, possibilitando assim a montagem de uma rede funcional em anel bidirecional.

Como relatado anteriormente, a topologia em anel é utilizada pelas redes SDH e pode ser especialmente útil se deseja-se comparar desempenho entre as duas tecnologias. Cada nó possui também uma porta bidirecional para entrada e saída dos clientes locais, capacitando a rede a permitir acesso a novos clientes a partir de qualquer um dos seus nós.

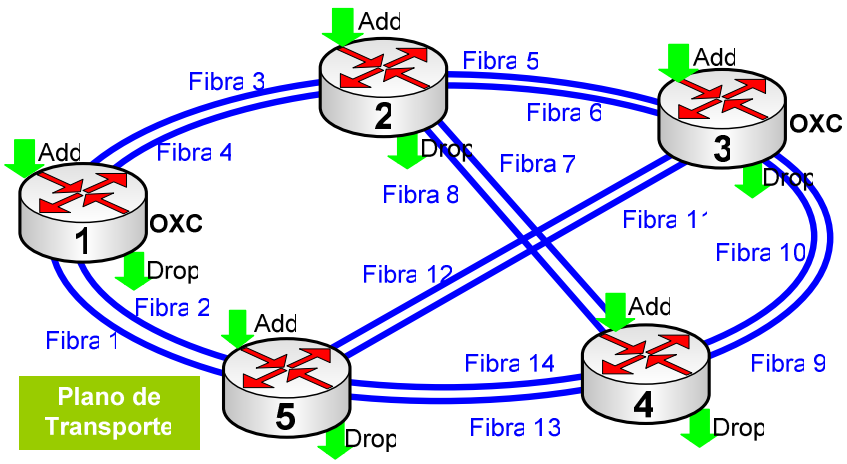

Figura 5.2 - Topologia da Rede OMEGA

Além do módulo de chaves ópticas, cada nó possui um módulo com *transponders*, que tem a função de adaptação dos comprimentos de onda dos clientes para os comprimentos de onda da rede, e um módulo de amplificação óptica necessário para manter o nível de potência compensando as perdas de inserção dos demais componentes.

A Figura 5.3 mostra a estrutura física de um destes nós, com o módulo de chaves ópticas no centro: o módulo de *transponders* está na parte inferior e o módulo de amplificadores ópticos na parte superior.

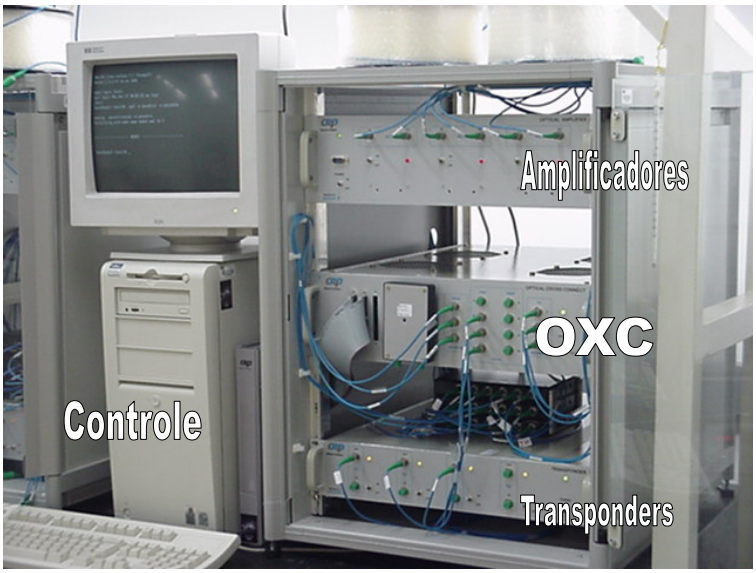

Figura 5.3 - Estrutura física de um nó da rede OMEGA

A Figura 5.4 representa esquematicamente os elementos de cada nó responsáveis pela conexão cruzada (OXC) e pelas operações de derivação e inserção (add/drop).

Na configuração implementada pelo CPqD, cada nó possui 4 chaves ópticas com oito entradas e oito saídas (8x8) ligadas de forma a emular 8 chaves de quatro entradas e quatro saídas. Esta estratégica exigiu a inibição de muitos estados possíveis para as chaves a fim de evitar que mesmos comprimentos de onda sejam inseridos na mesma fibra.

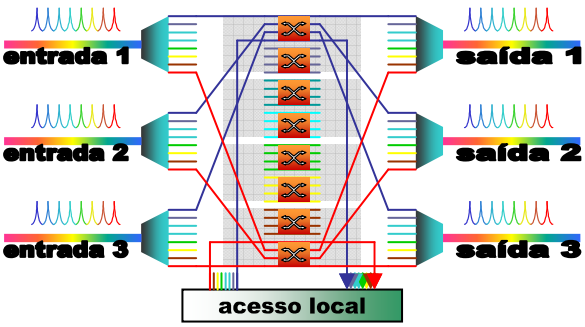

Figura 5.4 - Elementos de um nó e suas conexões

A Tabela 5.1 apresenta, de forma resumida, as características técnicas das chaves termo-ópticas 8 x 8 usadas na rede OMEGA.

Tabela 5.1 - Características típicas da chave termo-óptica 8 x 8 fabricada pela NEL.

Item	**Especificação**
Portas Entrada/Saída	8 × 8 (não-blocante)
Comprimento de onda de operação	Janela de 1.55 nm
Perda de inserção	<8dB
Uniformidade da perda	<2dB
Razão de extinção	>40dB
PDL	<0.5dB
Perda de retorno	>40dB
Velocidade de chaveamento	<3ms
Consumo de potência	<8W (Módulo PLC), 2.8W (circuito de controle)
Temperatura de operação	0 to 65℃
Controle de chaveamento	TTL (+5V)
Tensão de alimentação	+24V±5% / 0.85A (max)
Ventilação	Necessário ventilação forçada de ar (>1.5m/sec. recomendada)
Dimensões (W × D × H)	145 × 156 × 23 mm³

Nesta rede, a função de comutação possui três etapas que são:

1. Demultiplexação do sinal WDM separando os canais (os comprimentos de onda) entre si;
2. Cada comprimento de onda entra individualmente em uma das portas de uma chave óptica espacial que o direciona para uma das portas de saída;
3. Por último, os comprimentos de onda são direcionados para a mesma fibra de saída, porém agora multiplexados.

Cada *cross-connect* da rede OMEGA foi projetado para usar três muxs (1 x 8), e três demuxs (8 x 1) com espaçamento de canal de 200 GHz baseado na grade ITU-T, na faixa desde 1547.72 a 1558.98 nm. Estes *switchs* são controlados por um microcomputador, que usa interfaces TTL para tal. A Figura 5.5 mostra a configuração física do *optical cross-connect* (OXC) da rede OMEGA.

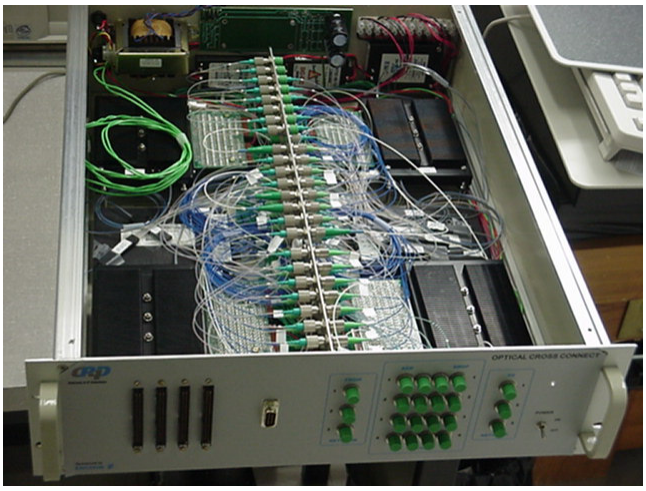

Figura 5.5 - *Optical cross-connect* (OXC) da rede OMEGA.

A Tabela 5.2 lista as características relativas a perdas e ganhos para cada dispositivo embutido no nó óptico.

Tabela 5.2 - Características típicas dos dispositivos no nó óptico

Dispositivo	**(dB)**
Perda no Demux, $Loss_{demux}$	3

Perda no Switch, $Loss_{sw}$	8
Perda no Mux, $Loss_{mux}$	3
Perda no Connector, $Loss_{con}$	0.5
Ganho no EDFA, G_{EDFA}	15 to 25

A rede OMEGA utiliza amplificadores ópticos nas três portas de saída de cada nó. Cada amplificador amplifica todos os comprimentos de onda de uma única vez, e isto pode acarretar diferença de amplificação entre os canais WDM, como já vimos anteriormente. Desta forma, existe a necessidade de ajustes para equalização da amplificação.

Um *transponder* ou adaptador de comprimento de onda é utilizado em cada nó da rede. Desta forma, permite inserir ou retirar até quatro sinais locais. A adaptação do comprimento de onda para a função de adição é feita através de quatro adaptadores de comprimento de onda que aceitam sinais de entrada desde baixas taxas até 2.5 Gbps, usando modulação direta. A Figura 5.6 apresenta um dos *transponders* usados na rede OMEGA.

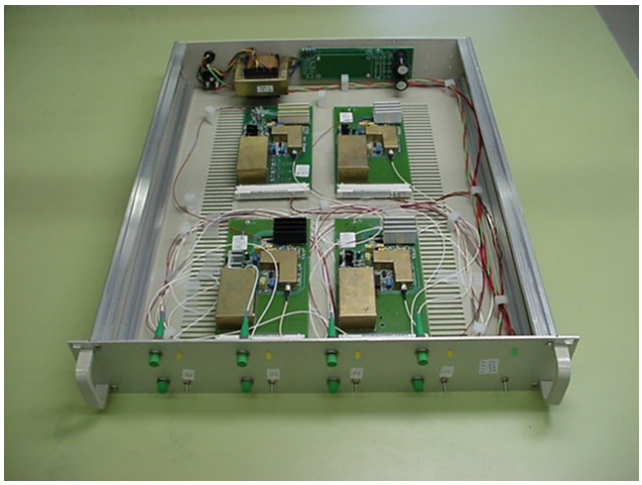

Figura 5.6 - Módulo *Transponder* (Quatro pares TX/RX).

5.1.2 Caracterização dos Elementos de Rede

No contexto do projeto de uma rede óptica ou da sua simulação é importante predizer a degradação do sinal devido à transmissão de múltiplos elementos. Os componentes físicos, elementos fundamentais de uma rede óptica não são ideais e os defeitos causados por

imperfeições destes implicam em limitações na transmissão. Estes temas têm sido extensamente estudados em [GILLNER, 1996] e [RAMAMMURTHY, 1999].

A base da análise da rede em questão foi encontrada em [ROCHA, 2002]. Assim, foram levadas em conta as limitações causadas por uma cascata de elementos. A escalabilidade tem sérias restrições no tamanho das redes em malhada impostas por parâmetros como comprimento dos enlaces e utilização de lasers de 2.5 Gbps moduladas diretamente. Esta técnica de modulação associada à transmissão através de vários nós resulta numa significante degradação por causa da dispersão. Além disto, outros efeitos tornam-se mais sérios na presença de ASE e acumulo de *cross-talk*.

5.1.2.1 Amplificadores

Nesta rede, cada nó faz uso de três amplificadores EDFA que atuam na banda C. As características ópticas e elétricas típicas são sumarizadas nas Tabela 5.3 e Tabela 5.4 respectivamente, que foram produzidas como decorrência da pesquisa realizada pelo CPqD.

Tabela 5.3 - Características ópticas

Parâmetro (@ 25°C)	**Min**	**Típico**	**Max**	**Unidade**
Operating wavelength	1532		1562	nm
Total nominal input power		-7		
Total output power at nominal input power	+13	+13.5	+14	dBm
Nominal gain value at nominal input power	20.0	20.5	21	dB
Gain flatness at nominal input power		± 0.5	± 0.7	dB
Noise figure at nominal input power		5.5	6.2	dB
Return loss looking into any amplifier port (amplifier off)	40			dB
Polarisation Dependent Gain			0.3	dB
Polarisation Mode Dispersion		0.5	1.0	ps

Tabela 5.4 - Características eletrônicas para bombeio de laser em 180 mW / 980 nm.

Parâmetro	Min	Típico	Max	Unidade
EOL operating bias current			0.39	A
Operating voltage		1.9	2.5	V
Monitor diode responsivity	1	15	50	μA/mW
Monitor dark current(-5V, T_{case} = 20°C)			0.15	μA
Laser element operating temperature	20	25	30	°C
Thermistor resistance (25°C)	9.5	10	10.5	kΩ
Laser temperature at 10 kΩ	23.5	25	26.5	°C
TEC *operating voltage*			2.7	V
TEC *operating current*			1.5	A
TEC *consumption*			3.5	W

5.1.2.2 Fibra Óptica

Cada um dos sete enlaces de fibra da Rede OMEGA comprende dois carretéis de 20 km de fibra monomodo (ITU-T G.652). Cada fibra foi caracterizada em termos de dispersão, atenuação e PMD.

5.1.2.3 *Transponders*

A caracterização do *transponder* foi feita através da avaliação de performance da taxa de erro de bits (BER) e não consta neste documento em função de tal informação não ter sido publicada de forma aberta (*papers*, revistas etc.).

5.1.2.4 *Optical Cross-Connect* (OXC)

No OXC, dois efeitos formaram o foco de pesquisa de caracterização: análise de *cross-talk* e *spectral clipping* (recorte spectral) devido ao estreitamento do filtro passa-faixa do mux/demux. Estas degradações podem limitar a aplicabilidade do OXC nas redes ópticas e dependem das propiedades do mux/demux e do *switch* óptico. Na rede OMEGA são usados modernos *switches* ópticos com nivel de cross talk de –35 dB, e filtros com faixa de passo suficientemente larga para não recortar os dados significativos.

a) Mux/Demux

O mux/demux foi caracterizado por medidas de nível de saída das oito portas de saída quando um sinal a – 3 dBm ingressa em cada uma das oito portas de entrada. A Tabela 5.5 apresenta o resultado de tais medidas em um mux/demux JDS.

Tabela 5.5 - MUX/DEMUX JDS

P_{in}= -3 dBm	P_{out}(dBm)							
λ_{in}	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	λ_8
λ_1	-4.17	-42.44	-42.2	-42.2	-42.12	-41.66	-42.06	-41.42
λ_2	-42.43	-4.55	-42.51	-42.6	-42.69	-41.95	-42.49	-41.65
λ_3	-42.52	-42.43	-4.39	-42.49	-42.59	-42.18	-42.45	-41.91
λ_4	-42.74	-43.09	-42.20	-4.88	-42.64	-42.4	-42.67	-41.95
λ_5	-42.81	-43.19	-42.67	-42.83	-4.13	-42.62	-42.72	-42.19
λ_6	-43.27	-43.64	-43.18	-43.44	-43.11	-4.81	-43.2	-42.61
λ_7	-43.7	-44.01	-43.59	-43.81	-43.62	-43.26	-5.11	-43.28
λ_8	-43.65	-44.02	-43.56	-43.84	-43.48	-43.27	-43.7	-4.87

b) Chave Óptica

Em relação a potência plana (*power flatness*) na porta de saída, a Figura 5.7 - Flutuação do nível de potência da porta de saída do *switch* Figura 5.7 apresenta os resultados obtidos para uma das chaves.

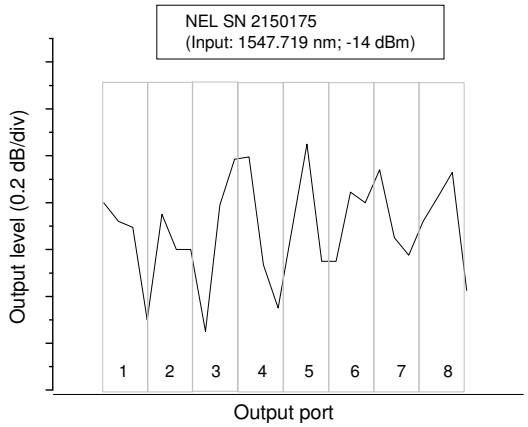

Figura 5.7 - Flutuação do nível de potência da porta de saída do *switch*

5.1.3 Arquitetura da Rede OMEGA

Na arquitetura da rede OMEGA cada nó esta composto por 4 portas (três para comunicação com nós adjacentes e uma para o ADM), unidades WDM para 8 comprimentos de onda operando entre 2,5 e10 Gbps (fazendo as funções de multiplexação e demultiplexação de comprimentos de onda sobre a fibra), o sistema comutador OXC (comutando comprimentos de onda de uma porta para outra), o ADM (que insere ou retira informação desde ou para a rede do usuário) e amplificadores ópticos, baseados em fibra dopada de Érbio (EDFA).

Nesta rede foram utilizados os canais ímpares de 23 até 37. Tais canais correspondem às freqüências 192,3 THz até 193,7 THz, com espaçamento de 200 GHz. Além disto, os nós possuem chaves ópticas que são capazes de escolher a porta de saída para cada comprimento de onda (cada cliente) entre quatro portas possíveis: uma porta leva o comprimento de onda para derivação local (drop), uma porta devolve o comprimento de onda para o nó de origem e duas portas são opções reais de encaminhamento. Assim, cada nó está conectado a três outros nós fazendo com que seja possível montar arquiteturas em malha ou em anel, bem como montar esquemas de proteção e restauração.

O plano de controle da rede OMEGA apresenta uma arquitetura distribuída. Cada nó possui um computador PC com três placas FastEthernet e duas placas para o controle dos comutadores ópticos. No modelo *overlay* usado nessa rede, as informações de topologia e recursos não são compartilhadas entre as camadas IP e WDM. Então, é definida uma interface usuário-rede (UNI) para acesso entre as camadas. Por meio de linha de comandos, essa interface habilita um usuário cliente a realizar aprovisionamento de caminho óptico, obter informação de estado da topologia e do protocolo de controle - LMP [ROSSI, 2002], [SACHS, 2002]. A UNI *server*, que é executada em cada PC, aceita conexões *telnet* de qualquer computador remoto conectado à rede de controle. As rotas são aprovisionadas usando RSVP simplificado e a rede possui, ainda, um esquema de proteção do tipo 1:N [IETF-1, 2003].

Na rede óptica transparente são atribuídos caminhos ópticos dinamicamente conforme necessidade de clientes que podem acessar a rede a partir de qualquer um dos seus nós. Todos os nós possuem a função de inserção e derivação de tráfego (*add/drop*).

O estado das chaves é controlado por computadores locais existentes em cada nó. Estes computadores se comunicam entre si através da mesma fibra óptica que é utilizada pelos oito canais de sinal, utilizando um comprimento de onda reservado para controle. Na versão utilizada para testes o comprimento de onda de controle é 1310 nm e este sinal de controle trafega no sentido oposto ao dos oito comprimentos de onda que transportam dados dos clientes.

Neste modelo, cada computador local tem a topologia da rede inserida manualmente, pois não está implementado nenhum algoritmo de descoberta de arquitetura. Contudo, se podem desabilitar portas de saída automaticamente em função de informações de tráfego ou de impossibilidade de operação por falta de sinal. Cada computador tem capacidade de calcular a rota para um dado cliente e enviar a rota solicitada para que todos os roteadores façam a reserva da mesma, tomem conhecimento do novo cliente que ocupa uma dada banda em alguns enlaces e executem o chaveamento necessário alterando o estado das chaves envolvidas para atender este novo cliente.

5.1.4 Protocolos de controle da Rede OMEGA

Entre dois nós adjacentes, são trocadas informações de controle. Automaticamente ou depois de alguma análise, ação ou correção, estas informações são divulgadas para nós adjacentes até que toda a rede esteja em um estado estável. Assim, foram criados vários tipos de mensagens trocadas entre roteadores.

O processo de criação de uma nova rota é iniciado em qualquer um dos nós, sem que os clientes que já utilizam a rede sejam afetados. Uma tabela dos recursos disponíveis já está armazenada em todos os nós no momento que é solicitada uma nova conexão, pois a mesma foi inserida manualmente. Todos os computadores já possuem as rotas de menor caminho obtidas pelo algoritmo Dijkstra executado sobre topologia disponível logo que o sistema de controle é colocado em execução. Sabendo o menor caminho disponível, bem como o comprimento de onda associado, esta rota é atribuída conforme solicitação de um novo cliente. Além dessa possibilidade, é permitido determinar manualmente a rota e o comprimento de onda.

Do ponto de vista prático, ao ligar um computador de controle o sistema operacional Linux solicita o nome do usuário e senha. Depois de entrar na conta do usuário, conecta-se

com o programa de controle associado à porta 1001 via *telnet*. Por exemplo, a partir do nó 5 digita-se: telnet node5 1001. Com este comando entramos no programa de controle de criação de rotas onde se pode criar rotas aleatoriamente ou as especificadas pelo usuário.

Exemplo:
wrnd@node3$ telnet node3 1001
Trying 127.0.0.1...
Connected to node3.
Escape character is '^)'.
wrnd@node3%

5.1.5 Aprovisionamento de caminho óptico

O protocolo de aprovisionamento de caminho óptico é uma espécie de RSVP simplificado desenvolvido especialmente para esta rede. O protocolo é responsável pela solicitação de reserva e posterior criação de uma nova conexão fim a fim sempre que houver uma nova demanda. As conexões existentes não são modificadas e somente os recursos disponíveis são utilizados para as novas requisições. As conexões são desfeitas, também sob demanda, caracterizando uma rede orientada a conexão e capaz de garantir qualidade de serviço.

O protocolo de aprovisionamento desenvolvido pelo CPqD é considerado como parcialmente distribuído já que todos os nós podem ser utilizados como pontos de acesso e não existe um nó central responsável pela gerência da rede. Cada nó mantém uma base de dados dos caminhos ópticos que estão sempre sincronizados entre si através de mensagens contendo informação do estado dos caminhos ópticos.

Consubstanciado na base de dados citada anteriormente cada nó pode calcular novas rotas evitando ultrapassar a capacidade da rede. Outras informações importantes também podem ser levadas em consideração fazendo com que este protocolo funcione como uma espécie de CR (*Constrain-based Routing*).

Depois de calculada a nova rota, um protocolo de sinalização é utilizado para informar e reservar esta. Assim, ao receber a informação de retorno do novo estado da rede contendo a reserva a rota é então estabelecida.

5.1.5.1 Procedimento para estabelecer um caminho óptico

A solicitação de uma nova conexão pode ser feita a partir de qualquer nó da rede. Quando uma nova demanda de tráfego é solicitada a partir de um dado nó (denominado de nó proprietário), esse nó passa a ser o responsável pelo cálculo das rotas apropriadas (rota principal e rotas de proteção) e pela reserva destes recursos na rede.

Para o cálculo das rotas é utilizado um algoritmo RWA (*Routing and Wavelength Assignment*) que escolhe a rota pelo caminho mais curto [GODRAN, 1979] e associa o comprimento de onda menos utilizado nesta rota [ZANG, 2000].

Após o cálculo das rotas, adequadamente realizado, o nó proprietário tenta fazer a reserva de recursos para a rota principal através do envio de uma mensagem LIGHTPATH_CREATE_TRY, pelo canal de controle, para o nó onde a rota se inicia. Assim, se conclui que o nó de origem não corresponde obrigatoriamente ao nó proprietário (aquele que está criando a rota).

A mensagem de tentativa de criação informa a seqüência de nós intermediários e o comprimento de onda associado. Dessa forma, quando um nó da rota recebe a mesma, ele verifica a disponibilidade do recurso e reserva as portas do OXC, em caso de sucesso. Após isto, este nó envia a mesma mensagem para o próximo que compõem a rota requerida.

Durante o processo de criação de rotas os nós intermediários atualizam suas base de dados com a nova reserva de recursos. Contudo, caso não exista disponibilidade do recurso solicitado, o nó responde com uma mensagem LIGHTPATH_CREATE_FAIL para o nó anterior.

Ao receber uma mensagem de falha na tentativa de criação de uma rota, o nó libera qualquer recurso reservado para esta demanda e envia esta mensagem para o nó anterior na seqüência da rota principal. Dessa forma, quando o nó origem recebe a mensagem LIGHTPATH_CREATE_FAIL, ele conclui que a rota foi bloqueada e descarta o pedido de conexão correspondente.

Por outro lado, quando uma mensagem LIGHTPATH_CREATE_TRY chega ao último nó da rota, este envia uma mensagem LIGHTPATH_CREATE_DONE para o nó origem. Isto indica o sucesso de reserva da rota principal e habilita o sistema ao início da alocação das rotas de proteção, caso haja.

O processo de criação da rota principal e de proteção é similar. Contudo, para o caso da rota de proteção, emite-se uma mensagem LIGHTPATH_CREATE_SUCCESS *broadcast* a rede. Além disso, as chaves ópticas não são configuradas no novo estado, mas sim apenas registrado que determinadas portas do OXC estão associadas com a rota de proteção relativa a rota principal. Obviamente, as chaves da rota de proteção serão configuradas somente após uma falha na rede.

O recebimento da mensagem LIGHTPATH_CREATE_SUCCESS caracteriza que o caminho principal e de proteção foram adequadamente criados. Por último, todo nó que recebe a mensagem LIGHTPATH_CREATE_SUCCESS atualiza sua base de dados incluindo a nova rota como recurso não disponível, pois esta informação é fundamental na execução do algoritmo RWA, que irá associar as rotas a um dado comprimento de onda.

5.1.5.2 Procedimento para liberação de um caminho óptico

Na implementação realizada pelo CPqD, o caminho óptico tem um número de identificação único, que é composto pelo número do nó proprietário e um número seqüencial interno devidamente atribuído pelo *software* de controle. Desta forma, o ID é utilizado nas mensagens subseqüentes (por exemplo, para comunicação de falha, restauração ou liberação do recurso).

Para destruir um caminho óptico, o nó proprietário envia uma mensagem LIGHTPATH_DESTROY para toda a rede, que processa tal informação em seus nós e atualiza a respectiva base de dados dos mesmos.

5.1.6 Emulação do Plano de Controle

Como cenário para os testes desta pesquisa, o plano de controle da rede OMEGA foi emulado por meio de cinco microcomputadores com configurações semelhantes. Em cada um deles, representando um dos nós ópticos da rede, instalou-se o sistema operacional

Linux *Red Hat* 9.0. A configuração física da rede de simulação inclui três placas Ethernet 10/100 Mbps por máquina, possibilitando uma topologia similar à apresentada pela rede OMEGA. A Figura 5.8 ilustra a rede emulada com endereços IP (192.168.0.0/24). Nas máquinas foi instalado um cliente do programa ZEBRA 0.94, que é um aplicativo livre que gerencia protocolos de roteamento TCP/IP, como BGP-4, RIPv1, RIPv2 e OSPFv2 [CRISPIM, 2004].

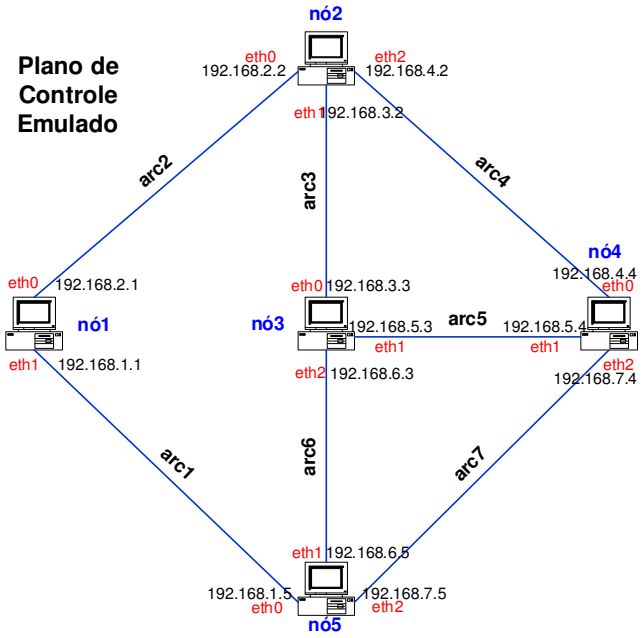

Figura 5.8 - Plano de controle emulado no Laboratório da UnB

Nesta configuração, mensagens *Hello* do LMP (*Link Management Protocol*) são trocadas periodicamente entre os nós para validar os enlaces de controle e a integridade da sessão.

Para que os protocolos de controle pudessem operar, foi necessário o carregamento, em cada ponto da rede de controle, de um arquivo com a topologia da rede física OMEGA. Nesse arquivo, são fornecidas informações acerca da quantidade de nós, ligação das fibras e esquema de proteção adotado. Assim, a criação de *lightpthts* pôde ser feita manualmente, desde uma interface UNI.

Toda esta rede foi simulada de forma a permitir entender e inspecionar as funcionalidades do software a fim de embasar o leitor para o desenvolvimento de um sistema centralizado. Vale ressaltar que o todo o software foi migrado na UnB da plataforma Linux *Red Hat* 7.3 para a versão 9, o que exigiu uma soma considerada de esforços por parte da equipe do LabCom envolvida no projeto.

6 DESENVOLVIMENTO DO SISTEMA DE CONTROLE CENTRALIZADO

6.1 APRESENTAÇÃO

Esta pesquisa tem como foco estudar a viabilidade da implementação de um sistema de controle centralizado para uma rede óptica transparente como solução alternativa para o uso de sistemas distribuídos. Desta forma, consolida-se como principal objetivo o diagnóstico da pertinência do uso de um sistema de controle e gerência centralizados numa rede óptica metropolitana como forma de implantar forte auditoria e melhor uso dos recursos da mesma.

Oliveira relata que a pesquisa descritiva, além de estudos bibliográficos, faz coleta de informações para consolidar o estudo a ser realizado. Segundo o mesmo autor, uma pesquisa que observa, registra, analisa e correlaciona fatos de forma isenta é dita descritiva, pois estuda fatos do mundo real sem a interferência do pesquisador [OLIVEIRA, 1998].

6.2 METODOLOGIA

Considerando a complexidade desse estudo, o autor realizará uma pesquisa descritiva e utilizará para a questão da ratificação da viabilidade da implementação de uma solução centralizada o critério de testes de performance e robustez da solução.

Do ponto de vista da análise dos resultados serão utilizados os mesmos requisitos adotados na pesquisa realizada pelo CPqD a fim de que se tenham parâmetros consistentes de comparação.

O levantamento de dados foi realizado através de um sistema automático de geração de demandas e registro das respectivas respostas do sistema de controle. Assim, foi possível a elaboração de gráficos que possibilitam uma visão rápida e intuitiva do comportamento da solução.

Por último, ressalta-se que todo o ambiente físico foi simulado com base na caracterização realizada pelo CPqD. Esta estratégia minimiza as limitações de ordem financeira que impedem a montagem de um cenário real da rede no Laboratório de Comunicações da UnB - LabCom, em curto prazo de tempo.

O método utilizado para a estruturação lógica da pesquisa e análise dos dados levantados foi o da dedução, que parte do geral para o particular. Segundo Gil [GIL, 1999], o método dedutivo é proposto por Descartes e outros considerados extremamente racionais, que acreditam na razão como a única forma capaz de levar ao conhecimento verdadeiro. Ainda segundo este autor, o método estatístico caracteriza-se por razoável grau de precisão, o que o torna bastante aceito por parte dos pesquisadores com preocupações de ordem quantitativa. Assim, considerando que tal estudo atua numa área eminentemente lógica, o método dedutivo foi considerado o adequado pelo autor da pesquisa, que utilizará modelos estatísticos para análise dos dados levantados.

6.3 UNIVERSO E AMOSTRA

Segundo Marconi [MARCONI, 1992] o universo ou população corresponde ao conjunto de seres animados ou inanimados que apresentam pelo menos uma característica em comum. Assim, este estudo deixa delimitados dois focos bem claros de estudo: os elementos físicos da rede (computadores) e os lógicos (programas). Para os elementos físicos da rede, o universo corresponde a todos os possíveis *sites*[5] que compõem uma rede óptica. Para os elementos lógicos, o universo compreende todos os programas utilizados na solução (gerência e controle da rede).

O processo de amostragem foi intencional e não probabilístico. Desta forma, foram escolhidas amostras, de maneira que elas equivalessem a maior representatividade possível do todo. Alguns autores, como Barros [BARROS, 1990], ratificam que não é possível extrapolar uma pesquisa realizada com base na seletividade não aleatória. Contudo, outros como Marconi (1992) aceitam como razoável que, a partir dos resultados obtidos numa

[5] Um *site* corresponde a um amplificador, um *transponder*, um *cross conect* e um computador para processar o sistema de controle.

amostra seletiva, pode-se inferir, o mais legitimamente possível, os resultados da população total.

Considerando os aspectos intrínsecos à pesquisa realizada o autor achou pertinente o delineamento de amostras não probabilísticas para o estudo em questão. Assim, as extrapolações poderão ser realizadas sem comprometer os aspectos científicos da pesquisa, que utilizará sobre as amostras, os preceitos da estatística descritiva.

6.3.1 Para os elementos físicos:

Dada a dificuldade da estruturação de uma rede com um maior número de nós, o pesquisador adotou o princípio da simulação dos elementos físicos da rede existente no CPqD. Desta forma, a rede simulada tem cinco nós que representam os elementos ópticos da rede OMEGA.

A Figura 6.1 apresenta o *layout* da simulação dos elementos físicos de um *site* através de três módulos de *software*, um para cada elemento.

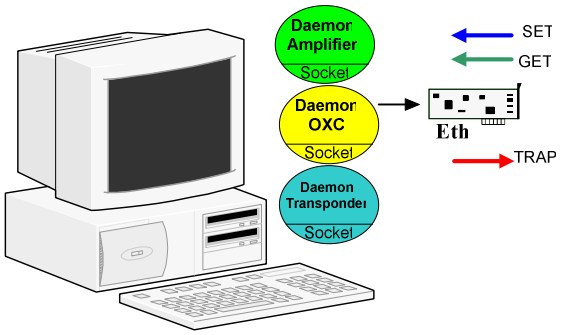

Figura 6.1 - Simulação dos elementos físicos

6.3.2 Para os elementos lógicos:

Todos os programas que compõem a solução foram estudados, validados e testados. Tal procedimento foi imperativo para testar o funcionamento ou não da solução como um todo. Neste contexto, também se inserem os programas desenvolvidos para realizarem o teste dinâmico das funcionalidades relativas ao controle da rede óptica. A solução foi

centralizada numa única máquina que recebeu os dados e os processou de acordo com os protocolos envolvidos.

Para a gerência, foi implementado um sistema no modelo *web* executado num único servidor http. Uma vez testadas as funcionalidades em termos de performance da solução de controle, por programas específicos, o sistema de gerência foi utilizado como proposta para uma melhor interação gráfica do usuário com o controle da rede, com as mesmas funcionalidades testadas automaticamente. Além disto, o referido sistema foi desenvolvido com o conceito de auditoria funcional, que tem como objetivo o registro, num banco de dados relacional, de todas as interações do usuário com o sistema de controle. A Figura 6.2 apresenta uma visão completa da arquitetura implementada.

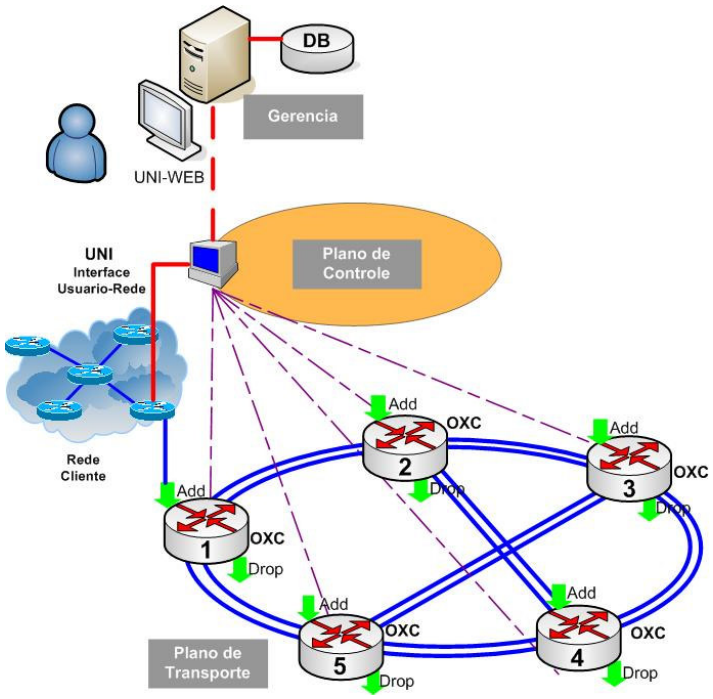

Figura 6.2 - Visão completa da arquitetura proposta.

6.4 PREMISSAS E HIPÓTESE

A seguir serão apresentadas as premissas nas quais se baseia o desenvolvimento da proposta centralizada, bem como as hipóteses que fundamentam o estudo em questão.

6.4.1 Premissas

O modelo centralizado foi desenvolvido de acordo com as premissas apresentadas abaixo, para cada um dos respectivos planos.

Plano de Gerência

— Todo o sistema foi desenvolvido no paradigma web e tanto as interações do usuário com o sistema de controle, quanto as ações automáticas do mesmo foram devidamente auditadas.

Plano de Controle

— Permite a criação (com proteção ou não) de uma rota de forma explícita ou implícita;

— Possibilita a destruição de uma rota na rede;

— Fornece, por demanda da gerência, dos caminhos que estão ativos, inativos, sob proteção ou não.

Plano Físico

— Cada equipamento (*transponder*, *amplifier* e OXC) tem uma interface ethernet (PHY, MAC) a partir da qual o plano de controle pode ler e ajustar seus parâmetros usando *socket* TCP/IP (PILHA TCP/IP). Estes equipamentos podem ter o IP modificado estaticamente ou dinamicamente;

— Os equipamentos têm o endereço IP da gerência configurados pelo operador;

— A mensagem get já traz o endereço IP de quem a solicitou;

— O endereço IP de gerência será único para um dado site;

— Os amplificadores e *transponders* são organizados em *arrays* específicos e de forma colapsada;

— Funcionalidades do *array* de Amplificadores:

- Ajuste (set)
    - Ligar e desligar (afeta o laser de bombeio permitindo ou não emissão);
    - Ajustar apenas o ganho (dB);

- Leitura (get)
  - Ler o valor do ganho (dB);
  - Ler status *on-off*;
  - Potência do sinal na entrada do amplificador (dBm);
  - Potência do sinal na saída do amplificador (dBm);
- Alarme (trap)
  - Crítico: Falta de potência de sinal na entrada e na saída;
  - Crítico: Falha no laser de bombeio;
  - Aviso: Envio de sinal de inserção e retirada;

— Funcionalidades do *array* de *Transponders*:

- Ajuste
  - Ligar e desligar (afeta o laser de saída permitindo ou não emissão);
  - Potência do sinal na saída do transponder (dBm);
- Leitura
  - Ler status *on-off*;
  - Potência do sinal na entrada do *transponder* (dBm);
  - Potência do sinal na saída do *transponder* (dBm);
- Alarme
  - Falta de potência de sinal na entrada e na saída;
  - Falha no laser de saída;
  - Aviso: Envio de sinal de inserção e retirada;

— OXC

- Ajuste
  - Fazer conexão do lambda de uma dada porta de entrada para uma dada porta de saída. Os parâmetros são: porta de entrada, porta de saída, e lambda –ID;
  - Desfazer conexão do lambda de uma dada porta de entrada. Os parâmetros são: porta de entrada e lambda –ID;
  - Apagar todas as conexões internamente realizadas;
- Leitura
  - Quais conexões estão setadas por porta ou todas de uma única vez;
  - Leitura da capacidade (lambdas e portas);
- Alarme

- Falha na chave óptica;
- Falha no enlace óptico, por fibra. Admite-se aqui que existe um elemento eletro-óptico que detecta a presença ou ausência de sinal em cada fibra individualmente. Na detecção de falha, é enviado um *trap* específico para o sistema de controle;
- Aviso: Envio de sinal de inserção e retirada;

— A topologia foi atribuída de forma semi-automática. Assim, os OXCs anunciam dinamicamente (*trap*) e o gerente configura a interligação física entre eles de maneira estática, informando via *software* o que está fisicamente implementado.

6.4.2 Hipóteses

Para a realização da referida pesquisa foram evidenciadas as seguintes hipóteses:

— A não pertinência da utilização de um sistema de controle e gerência centralizados;
— A pertinência da utilização de um sistema de controle centralizado como alternativa ao distribuído;
— A utilização de um modelo misto que incorpore a centralização dos aspectos gerenciais e a distribuição do sistema de controle;
— A ratificação do uso exclusivo de uma implementação distribuída.

6.5 DESCRIÇÃO GERAL DO SISTEMA – REDE SIMOMEGA

A solução centralizada desenvolvida nesse estudo é estruturada em três camadas: gerência, controle e simulação física. Assim, cada camada será descrita em termos das macro funcionalidades, bem como apresentados: o ambiente computacional utilizado para o desenvolvimento e teste das aplicações e o modelo computacional da solução.

Toda a solução foi desenvolvida sobre a plataforma operacional Linux com suporte da distribuição Fedora 4[6]. Para este tema específico, informações podem ser obtidas no site http://fedora.redhat.com.

A ferramenta CASE utilizada foi o Togheter Control Center, versão 6.0, desenvolvida na linguagem Java. Informações sobre esse produto podem ser obtidas no site http://www.borland.com/us/products/together/index.html.

A Figura 6.3 apresenta o diagrama geral do sistema, que evidencia três camadas distintas e que interagem entre si.

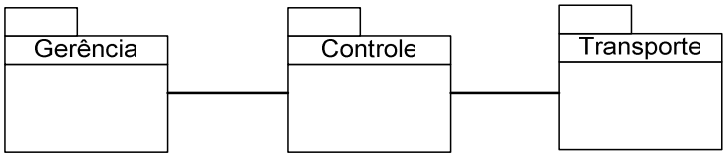

Figura 6.3 – *Deployment* do Sistema

6.6 GERÊNCIA

A gerência corresponde ao portal de acesso do usuário ao sistema de controle da rede óptica. Desenvolvida no conceito web, esta interface possibilita ao usuário um melhor conforto de interação, bem como suporta em *background* todas as funções de auditoria.

Os principais grupos de funcionalidades da gerência serão:

— Controle de usuário: permite a definição de diversos perfis de usuários;
— *Ligthpath*: permite a criação de caminhos na rede, de forma automática, manual ou aleatória. A eliminação de rotas também está disponível com esta utilidade;
— Inspecionar: mostra o número de caminhos por arco, o estado das portas de um dado nó e os grupos de risco compartilhado (SRG);

6 O projeto Fedora é aberto e desenvolvido pela Red Hat. Assim, tem-se um completo sistema operacional construído exclusivamente sobre o conceito de software livre, que fundamenta a liberdade dos usuários executarem, copiarem, distribuírem, estudarem, modificarem e aperfeiçoarem tal sistema.

— Controle: permite fazer *backup* e restore de rotas, envio e recebimento de avisos, ativar ou desativar um nó;

— Apresenta as rotas de serviço, as rotas de proteção, endereços e status de todos os equipamentos;

— Auditoria: permite auditoria de usuários e dos comandos realizados por testes.

A interface da gerência foi desenvolvida utilizando o conceito de classes, para implementar as funcionalidades listadas acima, e HTML.

O ambiente IDE[7] utilizado para esta camada foi o Eclipse, versão 3.1.1, com *plug-in* para o Tomcat[8].O *site* http://www.eclipse.org provê o *download* para o ambiente em questão, bem como apresenta um rico detalhamento de seu funcionamento.

As persistências dos dados da auditoria foram realizadas num banco de dados relacional PostgreSQL, versão 7.4.13. Informações detalhadas sobre o produto podem ser obtidas em http://www.postgresql.org.

A Figura 6.4 apresenta o Diagrama[9] de Caso de Uso com as funcionalidades do sistema e suas inter-relações [JACOBSON, 1999].

---

7 *Integrated Development Environment* – Ambiente Integrado de desenvolvimento.

8 *Apache Tomcat*, formalmente conhecido como *Apache Jacarta Project*, é um engenho web desenvolvido pela *Apache Software Fundation*. O Tomcat implementa tanto a tecnologia servlet, quanto as especificações JavaServerPages (JSP) da *Sun Microsystems*. Assim, tem-se um ambiente para código em Java que é executado em cooperação com um servidor web.

9 É um diagrama usado para se identificar como o sistema se comporta em várias situações que podem ocorrer durante sua operação. Assim, esse diagrama descreve o sistema, seu ambiente e a relação entre os dois. Os componentes do diagrama são os atores e os Casos de Uso.

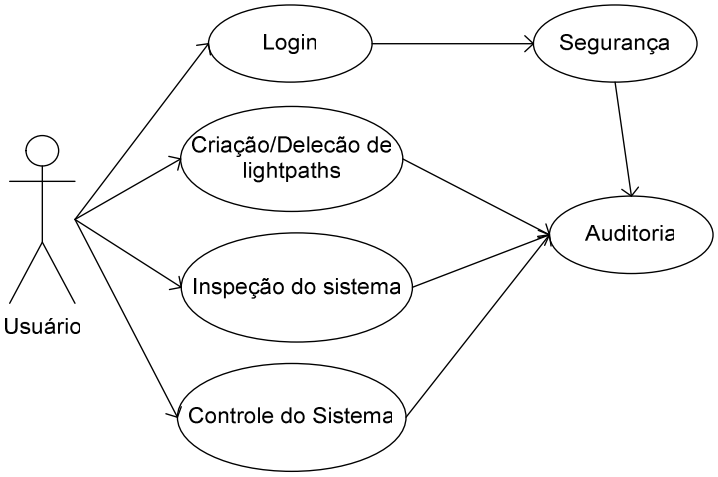

Figura 6.4 - Caso de Uso da Gerência

A integração do sistema de gerência com a camada de controle está ilustrada na Figura 6.5. Assim, o usuário faz as requisições junto ao servidor http, que possui conexão *socket* com o sistema de controle e jdbc com o banco de dados relacional. Após ser analisada, a requisição é atendida, registrada pela auditoria e o resultado final é informado para o usuário.

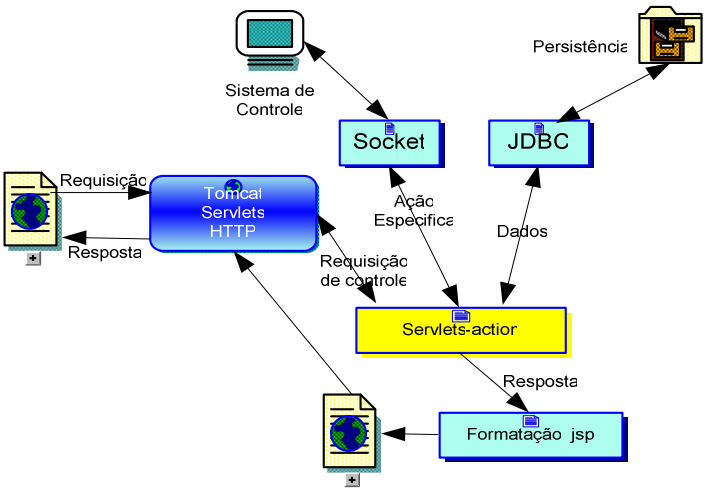

Figura 6.5 - Diagrama da arquitetura da camada de gerência

6.6.1 Apresentação das principais telas

Considerando a impropriedade de apresentar todas as telas do módulo de gerência, serão apresentadas abaixo as principais antecedidas de uma breve explicação de suas funções.

A Figura 6.6 apresenta a tela principal de *login* do sistema. Nela, o usuário informa sua identificação e senha. Nessa implementação foram usadas técnicas para evitar problemas de segurança como SQL Injection[10].

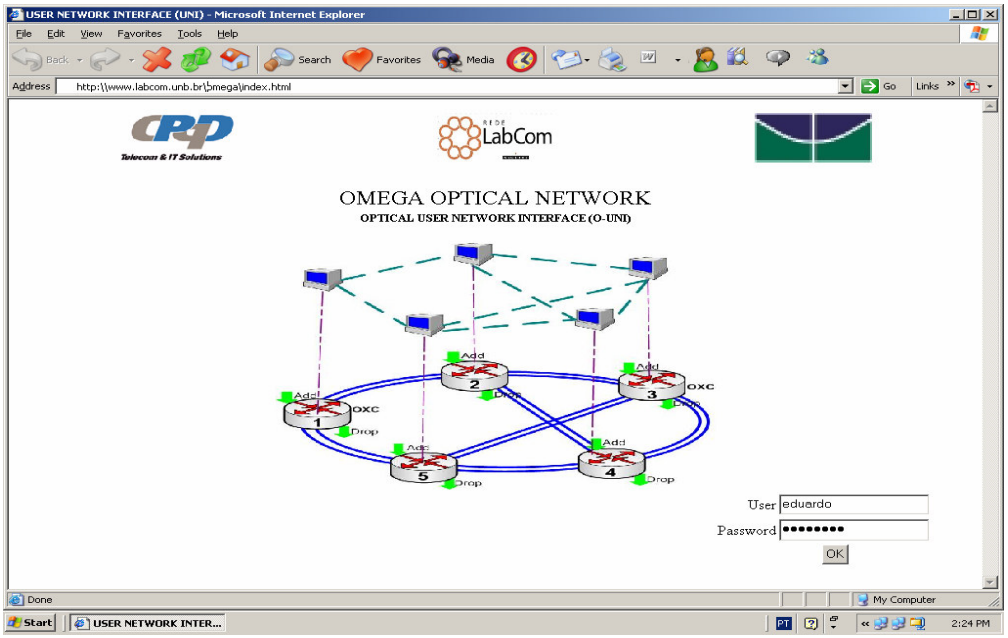

Figura 6.6 - *Login* do usuário

A Figura 6.7 apresenta a interface para criação e deleção de *lightpaths*. Essa interface possui mais usabilidade e torna a interação do usuário com o sistema mais imune a erros léxicos e semânticos. No caso da função específica de criação automática de um caminho óptico, os parâmetros nós de origem e destino, comprimento de onda e a obrigatoriedade de proteger a rota são informados de forma simples e direta.

[10] Corresponde a uma vulnerabilidade de segurança, que ocorre na camada da aplicação que interage com o banco de dados. Assim, o usuário pode entrar com uma seqüência de caracteres que representam declarações SQL não fortemente tipadas.

Figura 6.7 - Interface de criação e deleção de rotas

A Figura 6.8 apresenta as funcionalidades de administração de um dado nó óptico. A função específica de *show routes* mostra as rotas de trabalho criadas na rede, bem com se possuem proteção ou não. A tabela apresenta como resultado o número da requisição, os nós origem e destino, o lambda utilizado no caminho e toda a rota implementada pelo sistema de controle.

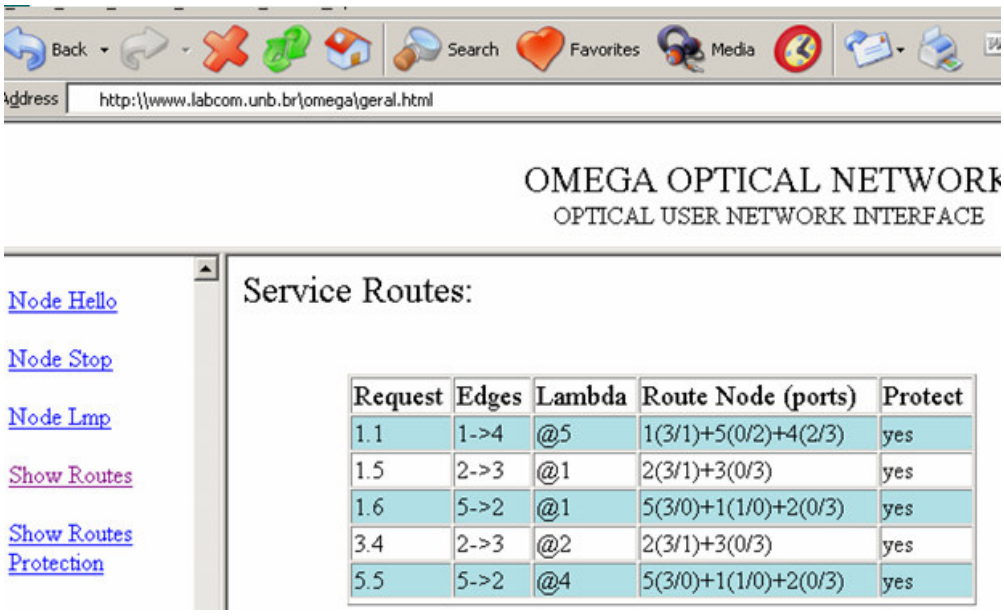

Figura 6.8 - Administração de um nó óptico

6.6.2 Segurança e auditoria

Auditoria corresponde à análise dos registros de um sistema a fim de validar sua exatidão de funcionalidade. Assim, a auditoria de sistemas de informações busca indicar quais controles e procedimentos devem ser estabelecidos, em um determinado sistema, bem como se os mesmos estão sendo utilizados corretamente [STAIR, 1998].

Todo sistema de segurança que se preocupe com violações deve implementar o conceito de auditoria. Desta forma, podem-se rastrear as interações do usuário com o sistema a fim de detectar fraudes, já que estas são causadas por um acesso autorizado.

Infelizmente, a auditoria é um dos processos de segurança que é mais desconsiderado na hora de se estabelecerem medidas corriqueiras de proteção. Os motivos para tal desinteresse são, principalmente, de ordem econômica.

Os objetivos da auditoria não são de impedir o acesso indevido, mas sim, de detectar possíveis violações que resistiram aos processos de identificação e de autorização e, se possível, determinar o caminho do violador e sua identidade [MARQUES, 2002].

As funções de segurança e auditoria implementadas nesse modelo são as seguintes:

— O administrador e o cliente deverão ter o *login* e senhas específicas que serão utilizadas durante todo o processo de auditoria;
— O administrador fará as requisições de criação e disponibilização de rota, além das demais ações previstas para o sistema;
— O cliente terá privilégio apenas de leitura dos status de seu enlace, do caminho relativo a ele e de seu SLA (*Service Level Agreement*);
— Todas as transações realizadas (com sucesso ou não) entre o gerente ou cliente e o sistema são persistidas numa base relacional.

Descrição detalhada do processo:

O módulo de segurança e auditoria é responsável pelo controle de acesso ao sistema e pela auditoria gerada pelas rotinas de inclusão, alteração, exclusão e leitura.

O registro da auditoria trabalha basicamente com funções e sub-rotinas incluídas antes e após os códigos de inclusão, alteração, exclusão, leitura ou qualquer outra ação que se queira auditar dentro do sistema.

O controle de acesso trabalha com o esquema de usuários, grupos e permissões. Desta forma, é necessário existir um módulo de cadastro de usuários, grupos, permissões e seus respectivos relacionamentos.

A Figura 6.9 apresenta o modelo Entidade/Relacionamento implementado para o módulo em questão. Assim, serão detalhadas abaixo as principais características da implementação e a conseqüente correlação com o modelo apresentado.

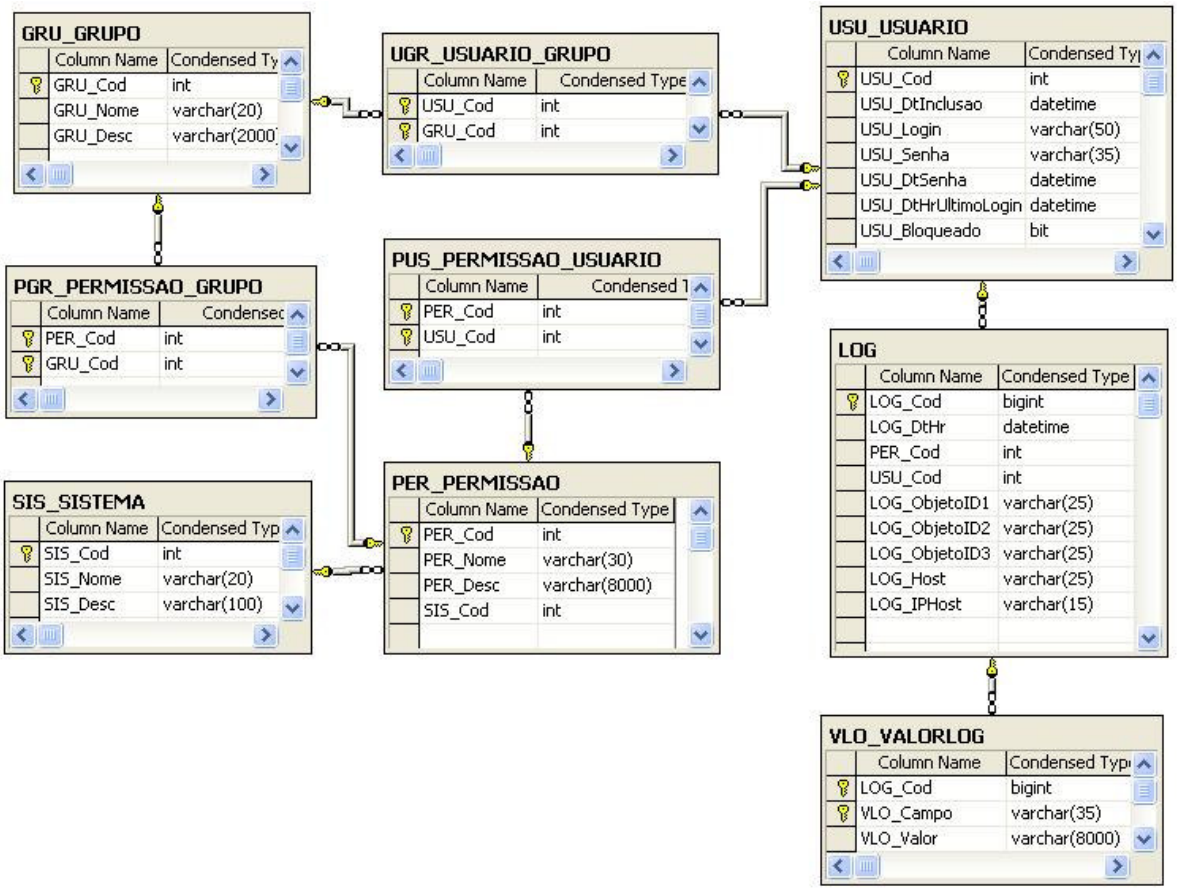

Figura 6.9 - Modelo Entidade Relacionamento

Controle de acesso utilizando usuários, grupos e permissões

Este tipo de controle, apesar de ser mais trabalhosa a sua implementação, permite administrar dinamicamente as permissões dos usuários e grupos de usuários. Neste modelo, é possível atribuir permissões a grupos de usuários ou a usuários individualmente. De uma forma geral, opta-se por atribuição de permissões a grupos de usuários devido à facilidade da administração permitida pelo uso do conceito de macro-perfil.

Os arquivos bases são: permissões, descrito na Tabela **6.1** - PER_PERMISSAO, onde são registradas todas as permissões relativas às ações que se queira auditar ou controlar o acesso, e o arquivo de usuários descrito na Tabela 6.8 - USU_USUARIO, onde são cadastrados os usuários do sistema.

O arquivo grupos de usuários, descrito na Tabela **6.1** - GRU_GRUPO, permite o cadastro de grupos, que podem ser traduzidos como níveis de acesso ou perfis. A idéia é que ao ser incluído em um grupo, o usuário herde todas as permissões daquele grupo. Isso é possível graças ao arquivo de permissões por grupo descrito na Tabela 6.4 - PGR_PERMISSAO_GRUPO.

Assim, para atribuir uma permissão a um determinado usuário, inclui-se no arquivo descrito na Tabela 6.5 - PUS_PERMISSAO_USUARIO, um registro com o código da permissão e com o código do usuário. Se deseja atribuir uma permissão a um determinado grupo, inclui-se no arquivo descrito na Tabela 6.4 PGR_PERMISSAO_GRUPO, um registro com o código do arquivo e com o código do grupo. E finalmente, pretendendo-se que um usuário herde a permissão de um grupo, inclui-se no arquivo descrito na Tabela 6.7 - UGR_USUARIO_GRUPO, um registro com o código do grupo e com o código do usuário.

Por exemplo, para uma função cadastrar usuário, deve ser incluído um registro no arquivo de permissões. Quando um usuário for executar a ação de cadastrar usuário, uma rotina no sistema verifica se o mesmo tem a permissão, buscando no aquivo PUS_PERMISSAO_USUARIO, ou na associativa de PGR_PERMISSAO_GRUPO com UGR_USUARIO_GRUPO, um registro que relacione o usuário à permissão verificada. Se

houver algum registro, o sistema prosseguirá com a inclusão do registro, caso contrário emitirá uma mensagem de permissão negada.

Abaixo é apresentado o extrato de um comando SQL executado quando não se está utilizando grupos de usuários:

```
Select PER_Cod from PUS_PERMISSAO_USUARIO
where PER_Cod = @PER_Cod
AND USU_Cod=@USU_Cod
Onde @PER_Cod = código da permissão e @USU_Cod = código do usuário.
```

Abaixo é apresentado o extrato de um comando SQL executado quando se está utilizando permissões de grupo:

```
Select PER_Cod from PGR_PERMISSAO_GRUPO
where PER_Cod =@PER_Cod
AND GRU_Cod in
(select GRU_Cod from UGR_USUARIO_GRUPO      where USU_Cod =@USU_Cod)
```

A verificação de permissão pode ser utilizada tanto para impedir uma ação dentro do sistema quanto para personalizar controles nos formulários, omitindo botões, itens de menu, etc.

Auditoria utilizando permissões

A auditoria tem por base o arquivo de permissões, onde a permissão verificada vai ser a mesma permissão relatada na auditoria, no aquivo descrito na Tabela 6.2 - LOG.

Ao executar a ação cadastrar usuário, o sistema irá incluir no arquivo LOG, um registro com o código da permissão executada, o código do usuário que executou, a data e hora, o IP da estação de trabalho utilizada, e o identificador do registro manipulado. O identificador pode ser um ou mais campos, de acordo com a chave primária do registro. Os campos de identificação do registro que não receberem valores ficam com valor = NULL.

Além de registrar a permissão executada, o sistema registra os valores dos campos manipulados. Isso é feito pela comparação de dois *snapshots* do registro manipulado. Um

snapshot feito antes da manipulação e outro feito depois. Da comparação, verifica-se quais campos foram modificados e, para cada campo modificado, inclui-se um registro no arquivo VLO_VALORLOG.

Tabela 6.1 - GRU_GRUPO

Campo	Tipo	Tamanho	Descrição
GRU_Cod	int	4	Código do Grupo. A tabela de grupos contém os grupos de ususários, que são perfis para efeito de permissões dentro do sistema. Os usuários que pertencerem a um determinado grupo herdam as permissões deste.
GRU_Nome	varchar	20	Nome do Grupo
GRU_Desc	varchar	2000	Descrição do Grupo

Tabela 6.2 - LOG

Campo	Tipo	Tamanho	Descrição
LOG_Cod	bigint	8	Código do Log. Esta tabela registra as operações auditadas do sistema. No caso de valores editados, as informações ficam na tabela VLO_VALORLOG
LOG_DtHr	datetime	8	Data e hora da operação
PER_Cod	int	4	Código da Permissão utilizada na operação
USU_Cod	int	4	Código do usuário que executou a operação
LOG_ObjetoID1	varchar	25	Identificador principal do objeto auditado (chave primária)
LOG_ObjetoID2	varchar	25	Segundo identificador do objeto auditado, no caso de chave primária composta por 2 campos
LOG_ObjetoID3	varchar	25	Terceiro identificador do objeto auditado, no caso de chave primária composta por 3 campos
LOG_Host	varchar	25	Nome da Máquina (estação) que foi utilizada pelo usuário para executar a operação auditada
LOG_IPHost	varchar	15	Endereço IP da Máquina (estação) que foi utilizada pelo usuário para executar a operação auditada

Tabela 6.3 - PER_PERMISSAO

Campo	Tipo	Tamanho	Descrição
PER_Cod	int	4	Código da permissão. Esta tabela contém a relação de todas as permissões verificadas pelo sistema.
PER_Nome	varchar	30	Nome da Permissão
PER_Desc	varchar	8000	Descrição da Permissão

SIS_Cod	int	4	Código do Sistema a que pertence a permissão. No caso do sistema ser modular este campo ajuda na busca da permissão.

Tabela 6.4 - PGR_PERMISSAO_GRUPO

Campo	Tipo	Tamanho	Descrição
PER_Cod	int	4	Código da Permissão. Esta tabela relaciona o grupo às permissões, indicando quais grupos possuem quais permissões
GRU_Cod	int	4	

Tabela 6.5 - PUS_PERMISSAO_USUARIO

Campo	Tipo	Tamanho	Descrição
PER_Cod	int	4	Código da Permissão. Esta tabela relaciona as permissões ao usuário, indicando quais permissões tem um determinado usuário.
USU_Cod	int	4	Código do usuário

Tabela 6.6 - SIS_SISTEMA

Campo	Tipo	Tamanho	Descrição
SIS_Cod	int	4	
SIS_Nome	varchar	20	
SIS_Desc	varchar	100	

Tabela 6.7 - UGR_USUARIO_GRUPO

Campo	Tipo	Tamanho	Descrição
USU_Cod	int	4	Código do usuário. Esta tabela relaciona o grupo aos usuários, indicando quais usuários pertencem a um determinado grupo
GRU_Cod	int	4	

Tabela 6.8 - USU_USUARIO

Campo	Tipo	Tamanho	Descrição
USU_Cod	int	4	Código do Usuário. A tabela de usuários contém os usuários do sistema
USU_DtInclusao	datetime	8	Data de inclusão do usuário
USU_Login	varchar	50	Login do usuário
USU_Senha	varchar	35	Senha do usuário. Este campo é criptografado, utilizando algoritmo MD5.
USU_DtSenha	datetime	8	Data da senha do usuário. Campo utilizado para controlar validade de senha
USU_DtHrUltimoLogin	datetime	8	Data e hora que o usuário efetuou o último login
USU_Bloqueado	bit	1	Indica se o usuário está bloqueado
USU_MotivoBloqueio	varchar	50	Motivo do Bloqueio
USU_DtExclusao	datetime	8	Data que o usuário foi excluído. Para garantir a integridade, o usuário não é excluído fisicamente, é somente marcado com este campo.
USU_ValidadeSenha	int	4	Validade da senha em dias.
USU_NomeCompleto	varchar	60	Nome completo do usuário
USU_DtNascimento	datetime	8	Data de nascimento
USU_Endereco	varchar	60	Endereço do usuário
USU_Bairro	varchar	50	Bairro
USU_Cidade	varchar	50	Cidade
USU_UF	char	2	Estado
USU_CEP	char	8	CEP
USU_Telefones	varchar	50	Telefones do usuario. Pode acumular neste campo quantos telefone puder em 50 posições.
USU_Email1	varchar	80	Email principal do usuário
USU_Email2	varchar	80	Email alternativo

Tabela 6.9 - VLO_VALORLOG

Campo	Tipo	Tamanho	Descrição
LOG_Cod	bigint	8	Código do Log. Esta tabela registra os valores dos campos editados.
VLO_Campo	varchar	35	Nome do campo editado
VLO_Valor	varchar	8000	Valor que o campo assumiu após a operação

6.6.3 Sistema de endereçamento

A gerência, por razões de segurança, permite uma única conexão por vez com o módulo de controle. Assim, num dado instante, apenas um administrador pode estar efetivamente usando o sistema.

Cada elemento físico (OXC, amplificadores e *transponders*) possui um endereço IP, que é obtido de forma dinâmica, via DHCP[11]. Os endereços do equipamento que executa o módulo de gerência, bem como do que executa o módulo de controle são pré-definidos. Assim, os elementos físicos devem ser informados do IP do equipamento de gerência a fim de que possam se anunciar.

6.6.4 Comunicação – Socket TCP/IP

Esse módulo se comunica com o de gerência e com o sistema de banco de dados realacional através de *sockets* TCP/IP específicos, que apresentam as características funcionais julgadas pertinentes para essa tarefa.

Na verdade, o TCP/IP é composto por um conjunto de diferentes protocolos e serviços de rede. Assim, esse nome aponta dois protocolos:

— IP (Internet Protocol), que é um protocolo de endereçamento de rede. Assim, esse protocolo tem como funções principais o endereçamento e roteamento. Desta forma, temos a maneira de identificar unicamente cada máquina da rede (endereçamento), bem como a de encontrar um caminho entre a origem e o destino (roteamento);

— TCP (Transmission Control Protocol), que é um protocolo de transporte, executa funções que garantem a entrega dos dados sem que os mesmos sejam corrompidos.

O TCP é um padrão definido na RFC 793, que especifica o fornecimento de um serviço de entrega de pacotes confiável e orientado por conexão. Assim, todos os aplicativos baseados em TCP como protocolo de transporte, antes de iniciar a troca de dados, devem estabelecer uma conexão [COMER, 1995].

---

11 O DHCP é o acrônimo de Dynamic Host Configuration Protocol, que corresponde a um serviço utilizado para automatizar as configurações do protocolo TCP/IP nos dispositivos de rede (computadores, switchs, etc.) Sem o uso do DHCP, o administrador e sua equipe deve configurar, manualmente, as propriedades do protocolo TCP/IP em cada dispositivo da rede.

A conexão fornece informações de *logon* (usuário e senha) para se estabelecer uma sessão. Assim, as informações colhidas na interface web serão diretamente utilizadas nessa conexão. Resumidamente, as principais características do TCP são:

— Garante a entrega de datagramas IP sem terem sido corrompidos e na ordem certa;

— Segmenta e reagrupa grandes blocos de dados enviados pelos programas e garante o seqüenciamento adequado e entrega ordenada de dados segmentados;

— Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação;

— Envia mensagens *ok* acusando o recebimento bem-sucedido dos dados. Assim, caso um pacote não tenha sido recebido ou apresente problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacotes;

— Representa o método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em sessões.

Por último, tem-se o conceito de portas que permite vários programas em funcionamento simultâneo, no mesmo computador, trocar informações com um ou mais serviços e/ou servidores. Assim, o lado do servidor de cada programa que usa portas TCP escuta as mensagens que chegam ao seu número de porta conhecido.

Todos os números de porta de servidor TCP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela *Internet Assigned Numbers Authority* (IANA, autoridade de números atribuídos da Internet). Por exemplo, o servidor Web utilizado escuta a porta 8080.

6.7 CONTROLE

O controle corresponde ao principal módulo da solução. Assim, essa camada apresenta as seguintes funcionalidades:

— Criação, com proteção ou não, de uma rota de trabalho de forma explícita ou implícita. Para a realização de tal ação têm-se os seguintes passos:

- Verificação léxica e sintática da solicitação recebida da gerência;

- Cálculo do melhor caminho e a associação deste a um lambda. O cômputo pode indicar a impossibilidade da criação de tal rota. Assim, esta informação deve ser enviada para a gerência;
- Enviar para os OXCs os sets das portas e aguardar os set_acks respectivos. Após todos os *acks* recebidos, informar a gerência do sucesso ou insucesso quanto à solicitação. No caso de insucesso, devem-se desfazer as comutações já realizadas e então reportar para a gerência o motivo de tal falha (código de erro);
- Para o caso da rota implícita, usa-se o algoritmo rwa (Dijkistra e first fit);

— Mecanismo de ativação das rotas de proteção que envolve a recepção da *trap*, análise de impacto da mesma sobre as rotas criadas e atuação sobre os OXCs a fim de ativar a proteção dos caminhos ópticos (rotas) em falha. Assim, tem-se que:

- O rwa, detalhado em tópico específico, já calculou a rota de proteção;
- Uma vez recebida a *trap* de falha busca-se na tabela de caminhos criados quais rotas passam por aquele nó e por aquela porta em falha;
- Para cada caminho encontrado nesta busca, recupera-se o caminho de proteção e ativa-o;
- A ativação corresponde ao envio de sets ajustando os OXCs de cada um dos nós do caminho de proteção, nos moldes da criação de uma rota principal.

— Mecanismo para reativação das rotas principais (chaveamento da rota de proteção para a rota principal associada). Este procedimento é manual, ou seja realizado pela gerência.

— Fornecimento de informações dos equipamentos que fazem parte da rede óptica para a gerência. Essa função é executada por demanda (*gets*).

Para a execução do rwa devem-se ter as seguintes informações: a topologia da rede (nós e conectividade por fibra), lambdas em cada fibra (esta informação é chamada de recursos da rede) e as informações do estado atual da rede (quais caminhos e lambidas que estão ocupados). Em síntese, a implementação segue a seguinte lógica:

— O algoritmo Dijkstra é executado uma única vez para calcular todas as possibilidades de conexão de um nó para todos os outros nós da topologia;

— O resultado do cálculo (rotas possíveis) é armazenado em uma tabela de alta performance para busca (hash table). No caso de desalocação de um caminho, a tabela hash será atualizada no sentido de disponibilizar o mesmo;
— Cada vez que é solicitado um caminho óptico, o wave assigment é executado com base no modelo First Fit.

A rota, principal ou de proteção, é o conjunto interligado (seqüencial) de enlaces já definidos pelo algoritmo Dijkstra. Assim, o caminho óptico é a rota acrescida de um lambda comum em todos os enlaces.

Nesse modelo, a representação do caminho corresponde a: nó1, porta de entrada1, porta de saída1; nó2, porta de entrada1, porta de saída2 .... nóN, porta de entrada3, porta de saída4 etc.

O ambiente IDE utilizado para implementar esse módulo foi o KDevelop, versão 3.1, disponível sob a licença GPL[12]. Assim, mais informações podem ser obtidas no site http://www.kdevelop.org.

6.7.1 Principais estruturas de dados utilizadas

O módulo de controle utiliza, para representar em memória a topologia da rede, o conceito de grafos. Um detalhamento teórico completo pode ser encontrado em [BIGGS, 1974], [BOLLOBÁS, 1998] e [GODSIL, 2001]. Assim, neste estudo, serão apresentados os conceitos julgados mínimos para o entendimento do assunto.

Um grafo é uma estrutura abstrata que representa um conjunto de elementos chamados nós (vértices) e suas interdependências chamadas arestas (ligações ou arcos). Desta forma, dado o conjunto N de vértices da estrutura e E o conjunto as ligações entre os vértices, um grafo pode ser representado por G=(N,E).

[12] A licença GPL - General Public License garante que uma vez o *software* inserido nela, a retirada do mesmo não é mais possível. Desta forma, preservam-se as liberdades inerentes ao conceito de *software* livre.

Grafo não direcionado G_{nd} = (N,A) é um conjunto finito e não vazio de nós N, bem como um conjunto A de pares não ordenados {n1,n2} de nós distintos. Assim, a ordem de ligação entre os vértices não é importante.

Grafo direcionado G=(N,E) é um conjunto finito e não vazio de nós N, bem como um conjunto E de pares ordenados {n1,n2} de nós distintos. Assim, a ordem de ligação entre os vértices é importante.

Em um grafo G=(N,E) um arco e = (n1,n2) corresponde ao par de nós chamados de origem e destino respectivamente. Contudo, para um grafo não direcionado estes termos não são usados. Desta mesma relação, conclui-se que o arco "e" sai do nó n1 e entra no nó n2.

O número de arcos que saem ou entram em um dado nó é chamado respectivamente de grau de entrada e grau de saída. Assim, a soma das entradas e saídas gera o conceito de grau do nó.

Num dado grafo o conceito de dois nós vizinhos é estabelecido se existe um arco "e", pertence a E, com uma das seguintes condições: e = (n1,n2) ou e = (n2,n1).

Uma rede pode ser definida como R = (N,E,F) a partir de um grafo direcionado G=(N,E) atravessado por um fluxo F = {f1,f2,f3...fm} que circula em suas m arestas. Numa dada rede, dois nós são destacados: o nó origem e o destino.

Para o modelo computacional implementado, um caminho em um grafo direcionado G=(N,E) é uma seqüência não vazia de arcos, que interligam os nós origem e destino.

A implementação prática de grafos exige que cada elemento, seja vértice ou arco, tenha informações associadas ao mesmo. Como exemplo, pode ser citada uma rede WAN, cujos vértices são os roteadores e os arcos o enlace entre os mesmos. A Figura 6.10 apresenta a topologia física de uma da rede WAN (N corresponde a uma rede local (nó), R a um roteador (nó), e os números aos pesos do enlace (arco)) e a Figura 6.11 o grafo dirigido correspondente à mesma.

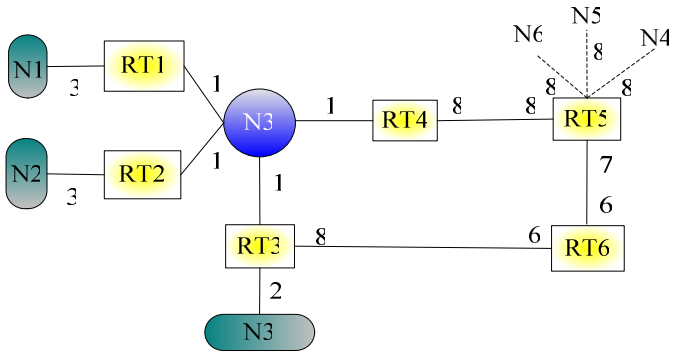

Figura 6.10 - Topologia física de uma rede

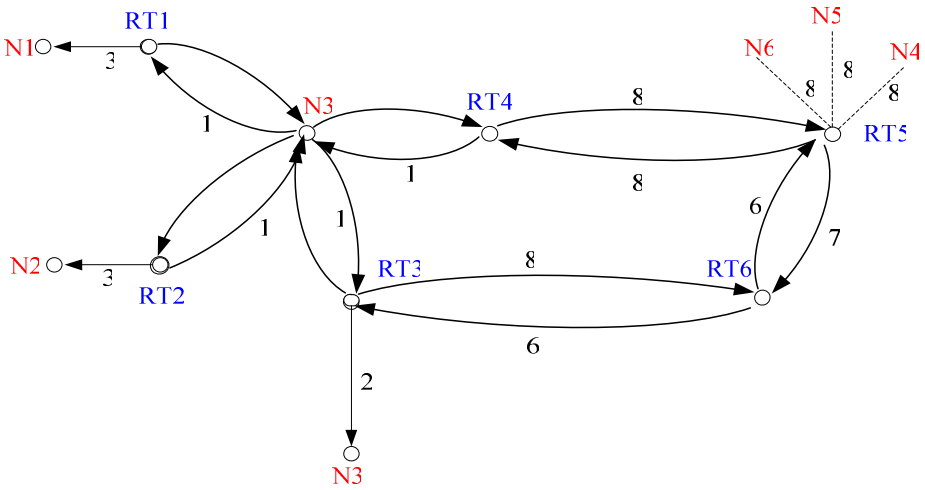

Figura 6.11 - Grafo resultante

Para a realização da implementação em questão foi estudado e usado como modelo, a biblioteca GTL - *Graph Template Library*, que pode ser vista como a extensão da STL *Standard Template Library* para grafos e seus algoritmos fundamentais. Esta biblioteca foi desenvolvida por pesquisadores da Universidade de Passau, no Departamento de Ciência da Computação (http://www.infosun.fmi.uni-passau).

Além de grafos, o modelo implementado incorpora estruturas como tabelas *hash*, *containers* com funcionalidades específicas para *string* e outras. Para um estudo mais profundo do princípio de funcionamento das principais estruturas são recomendadas as seguintes literaturas: para C++ [DROZDEK, 2005] e Java [PREISS, 2000] [GODRICH, 1997].

6.7.2 Interface entre a gerência e o controle

A interface web gera uma *string* com a síntese do comando desejado e então a envia, através da conexão *socket*, para o sistema de controle. Acoplado ao controle existe um tradutor capaz de efetuar as análises léxica e sintática do comando recebido. Assim, caso aconteça algum erro nesses dois estágios, a solicitação é negada e o erro é devidamente informado.

Após o sucesso dos dois estágios anteriores o comando é traduzido para uma seqüência lógica de eventos, que implementam a semântica da solicitação.

A análise léxica baseia-se no fato que certas seqüências de caracteres devem ser tratadas como um único símbolo. Por exemplo: identificadores, constantes, palavras-chave (BEGIN, END, IF...), um ou mais brancos, caracteres duplos (:=, <> ...) etc.

O analisador léxico (ou SCANNER) agrupa certos caracteres terminais em entidades únicas (TOKENS). A saída do SCANNER é uma sequência de pares da forma: (TIPO DO TOKEN, INFORMAÇÃO). O primeiro componente é uma categoria sintática (IDENTIFICADOR, CONSTANTE..) e o segundo uma cadeia que contém a informação relativa ao TOKEN (123, X, aux...).

Um exemplo específico de comando é o seguinte: action create 1 2 MustProtect. Ao receber esta *string* os identificadores são mapeados em TOKENS (“action”, “create”, “1”, “2” e “MustProtect”), que servem como base para a análise da sintaxe do comando. Nesta implementação, devido a simplicidade do conjunto de comandos, não são usadas tabelas de símbolo.

A cadeia de *tokens* produzida pelo analisador léxico forma a entrada para o analisador sintático (PARSER), que examina o tipo de cada *token* para determinar se certas convenções da linguagem são obedecidas. O *parser* produz a representação adequada da estrutura sintática da cadeia de t*okens* recebidos e então dispara o conteudo semântico.

6.7.3 Topologia da rede – estática

A topologia da rede, para o modelo implementado, é informada estaticamente pelo gerente da mesma nos moldes da rede OMEGA. Assim, o arquivo de topologia é também submetido a um PARSER.

Neste arquivo, entre outras informações, constam os nós pertencentes à rede e suas potencialidades, suas interligações e definição dos aspectos macro da infra-estrutura. Assim, pode-se implementar uma rede mash ou até mesmo em anel.

Um extrato do arquivo de topologia é mostrado abaixo. Na primeira parte são evidenciados os nós e suas respectivas capacidades em termos de lambdas. O início desse frame é indicado pelo TOKEN TOPOLOGY.

O TOKEN FIBER evidencia o início do contexto de interligação entre os nós. Assim, cada fibra possui uma identificação única e pertence a um dado grupo de risco. Como os equipamentos possuem quatro portas (0,1,2 e add/drop), tais conexões também devem ser evidenciadas para a origem e destino respectivamente. Este grupo de informações é encerrado pelo TOKEN END.

Por último vem o módulo que trata das características gerais da rede e do sistema. O TOKEN que dá início ao mesmo é o ACTION e o END delimita o final.

```
Arquivo de Topologia – extrato
TOPOLOGY
NODE    1      1:8x3
NODE    2      1:8x3
NODE    3      1:8x3
NODE    4      1:8x3
NODE    5      1:8x3
#       ID    ARC(SRG) NODE.PORT NODE.PORT
FIBER   1     1        1.1       5.0
FIBER   2     1        5.0       1.1
FIBER   3     2        1.0       2.0
FIBER   4     2        2.0       1.0
FIBER   5     3        2.2       3.2
FIBER   6     3        3.2       2.2
FIBER   7     4        2.1       4.1
FIBER   8     4        4.1       2.1
FIBER   9     5        4.0       3.0
FIBER   10    5        3.0       4.0
FIBER   11    6        3.1       5.1
FIBER   12    6        5.1       3.1
FIBER   13    7        4.2       5.2
FIBER   14    7        5.2       4.2
END
```

```
#
ACTION
PROTECTION-TYPE          1:N
PROTECTION-COLOR         SAME
PROTECTION-PORT          REUSE
MESH                     YES
END
```

6.7.4 Caminhos de serviço e proteção

O módulo de controle atua automaticamente em caso de falha. Desta forma, ocorre o redirecionamento automático do tráfego para rotas de proteção. Neste contexto, vale ressaltar que, por limitações do protocolo usado e da DNC[13], tal performance não atinge os intervalos de tempo inferiores a 50 ms.

Após a falha ser restaurada, a equipe de campo deve informar ao administrador para então este reconfigurar o sistema. Desta forma, restaura-se o caminho original e libera-se a rota de reserva para atender falhas futuras. Este tipo de operação de proteção de enlace é conhecido como 1:N, onde uma rota de proteção pode atender a várias de serviço.

O conceito de proteção exige, naturalmente, uma redundância dos enlaces para serem usados em caso de falha. Assim, todo o tráfego que pertence a um caminho óptico com restrições é dinamicamente alocado num caminho alternativo. Este tipo de estratégia é utilizada no SDH através do procedimento APS - *Automatic Protection Switching*.

Por outro lado, a restauração parte do pressuposto que o caminho de proteção é temporário e que, após resolvido o problema da rota principal, esta deva ser reativada. Assim, tem-se o conceito que a rota de proteção é temporária, pois a mesma também serve de reserva estratégica para outras rotas de serviço (1:N).

Como dito anteriormente o SDH, através do processo APS, é capaz de detectar a falha e corrigi-la num intervalo inferior a 50 ms. Neste contexto, a proteção oferecida ao cliente é fim a fim; ou seja, durante todo o caminho estabelecido entre a origem e o destino.

---

[13] *Data Network Control* , rede responsável pela tráfego do dados relativos aos seguintes protocolos: de controle e manutenção de enlace.

Em síntese, a proteção fim a fim pode ser de três tipos: 1+1, 1:1, 1:N. Assim, tem-se que:

— 1+1: contém a duplicação de todos os meios para atenderem a rota de serviço e a de proteção com o sinal enviado simultaneamente sobre ambas;

— 1:1: contém o recurso de proteção reservado para cada rota protegida, mas a transmissão não é duplicada. Assim, a rota de reserva pode ser utilizada por algum tráfego não prioritário;

— 1:N: generaliza o caso 1:1 prevendo-se apenas uma rota de proteção para N rotas principais.

Uma outra forma de proteção que vale ser ressaltado é a de enlace ou linha. Este tipo protege apenas um dado enlace, transferindo todo tráfego do mesmo para um ou mais enlaces de reserva.

Tanto os caminhos de serviço, quanto os de proteção, quando criados de forma implícita utiliza o algoritmo de Dijkstra para o cálculo do melhor caminho e o algoritmo *first fit* para a alocação do comprimento de onda.

Quando o caminho é construído de forma explícita, em que todos os nós e o respectivo lambda são apresentados pelo gerente da rede, é realizada apenas uma verificação da disponibilidade ou não de tal recurso.

6.7.5 RWA – Routing and Wavelength Assignment

Na teoria de grafos, o problema do melhor caminho consiste na minimização do custo de travessia de um grafo entre dois nós (origem e destino, respectivamente). O custo é dado pela soma dos pesos de cada arco percorrido.

Aos algoritmos especializados em solucionar o problema do melhor caminho são chamados de algoritmos de busca de caminhos. Entre os inúmeros algoritmos com tal funcionalidade, pode-se citar: o de Dijkstra, de Bellman-Ford, Floyd-Warshall e outros.

O algoritmo de Dijkstra[14] apresenta uma solução para o problema do caminho mais curto para um grafo dirigido com arestas de peso não negativo. Um algoritmo que serve para resolver o mesmo problema em grafos com pesos negativos é o algoritmo de Bellman-Ford.

No modelo implementado, esse algoritmo é utilizado para encontrar o menor caminho entre dois nós da rede, de acordo com os pesos de cada enlace.

O pseudo código do algoritmo Dijkstra é mostrado abaixo:

```
Considerando um grafo G=(V,E);
Um peso d:E->R+ e um vértice inicial s pertencente a V;
De s até cada vértice pertencente a V, o caminho mais curto é:
    Ajuste i=0; S0= {u0=s}; L(u0)=0; L(v)= infinito para v <> u0;
    Enquanto |V| != 1 {
    Para cada v em V\Si {
    Substitua L(v) por min{L(v), L(ui)+dvui};
    Se L(v) foi substituido, coloque um label (L(v), ui) em v;
    Encontre todos os vertices v que minimizem {L(v): v in V\Si}, como u;
    Ajuste Si+1 = Si proximo {ui+};
    Substitua i by i+1};
    i=|V|-1; }
```

Uma vez definido o melhor caminho deve ser associado a este um lambda disponível ao longo de todos os enlaces que o compõe. No caso do modelo implementado, foi utilizado o algoritmo *First Fit* para a escolha do referido comprimento de onda. De maneira resumida, o processo realizado é o seguinte:

— Toma-se o primeiro lambda disponível no primeiro enlace (nos dois nós pertencentes a este);
— Verifica-se no segundo enlace se o lambda do primeiro também está disponível e assim sucessivamente para os demais enlaces;
— Caso algum deles não atenda a disponibilidade daquele lambda, deve-se voltar a processar o primeiro enlace com o uso do próximo lambida disponível para ele;

[14] Nome que se origina do cientista da computação Edsger Dijkstra.

— Após o término do esgotamento do primeiro enlace da respectiva rota para todos os lambdas, caso não seja encontrado o lambda comum a todos os enlaces, deve-se passar pelo mesmo processo na próxima rota disponível.

— Ao final, se para todas as rotas disponíveis entre o nó origem e o destino não for possível reservar um lambda comum a todos os enlace, que compõem tais rotas, da-se a negativa quanto à solicitação. Caso positivo, tais recursos devem ser devidamente sinalizados como não disponíveis para uma próxima demanda de criação de um caminho óptico e respectivamente configurados no OXCs.

6.7.6 Comunicação – Socket TCP/UDP

O protocolo UDP - *User Datagram Protocol* é um padrão TCP/IP definido pela RFC 768. O UDP é usado, em alguns casos, em substituição ao TCP para o transporte rápido de dados entre *hosts* TCP/IP.

Este protocolo não fornece garantia de entrega e nem verificação de dados. Assim, o mesmo deve ser usado para atender alto desempenho, porém numa estrutura de rede que ofereça confiabilidade no tráfego dos dados. O serviço oferecido por este protocolo é sem conexão, logo as informações devem ser confirmadas pelo protocolo desenvolvido na solução implementada.

O conceito de porta UDP é igual ao das portas TCP. Contudo, existem diferenças quanto as maneiras de como as portas são utilizadas em cada protocolo. Todos os números de porta de servidor UDP menores que 1.024 (e alguns números mais altos) são reservados e registrados pela *Internet Assigned Numbers Authority* (IANA, autoridade de números atribuídos da Internet).

6.7.7 Protocolos

Para a realização do sistema de controle foram desenvolvidos três protocolos básicos. O primeiro implementa a criação e deleção de caminhos ópticos, o segundo a manutenção dos enlaces e o último a ativação da rota de proteção.

A Figura 6.12 apresenta o protocolo para a criação e deleção de caminhos ópticos. Assim, o sistema de controle envia uma mensagem *set* para cada nó ótico que faz parte do caminho informando a porta de entrada, a de saída e o respectivo lambda. O caminho óptico é considerado criado quando o sistema de controle recebe todos os Set_ack dos nós e então envia para a gerência a mensagem de sucesso quanto à solicitação de criação de um dado caminho. A partir deste instante, a informação pode ser transmitida.

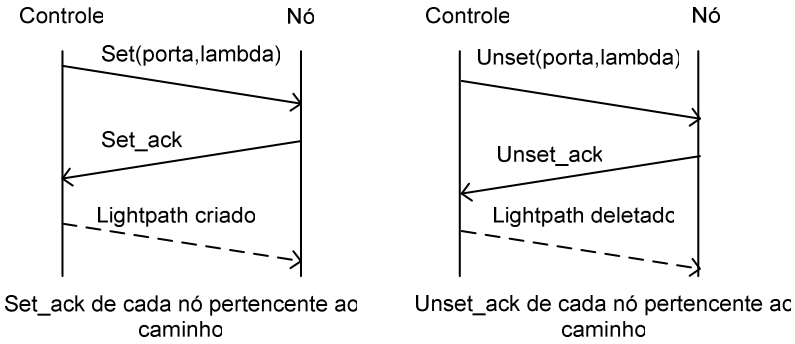

Figura 6.12 - Seqüência de eventos

A Figura 6.13 apresenta o diagrama de estado do protocolo para a manutenção dos enlaces. O mecanismo de proteção implementado corresponde ao envio e recebimento de mensagens Hello, que é um protocolo simples utilizado, por exemplo no OSPF[15].

O protocolo de manutenção de enlaces trabalha com UDP e envolve mensagens trocadas entre o controle e todos os nós que compõem a rede. Assim, uma mensagem HELLO é enviada a cada trinta segundos para todos os enlaces, que respondem a mesma ou não em caso de falha da DNC.

Quando a recepção do HELLO é interrompida por mais de quarenta segundos, o sistema passa de um estado "ATIVO" para o estado "FALHA". Desta forma, o administrador é imediatamente informado quanto à falha do respectivo enlace.

---

[15] OSPF - *Open Shortest Path First* é um protocolo de roteamento feito para redes com protocolo IP, que foi desenvolvido pelo grupo de trabalho de IGPs (Interior Gateway Protocol) da IETF (Internet Engineering Task Force). Mais detalhes: http://www.ospf.org

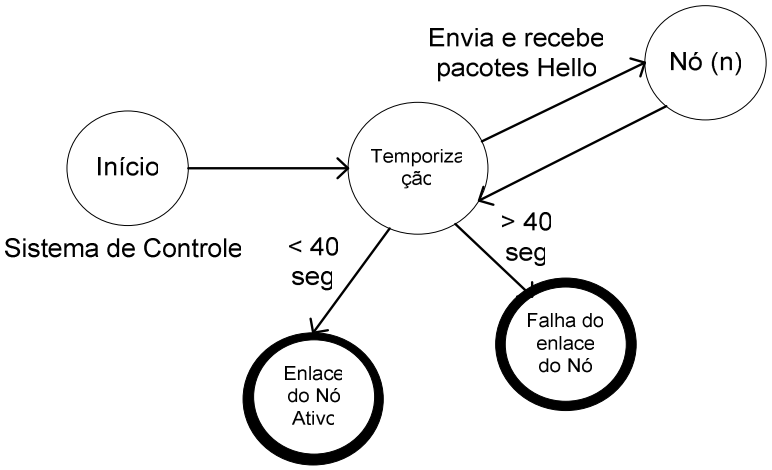

Figura 6.13 - Diagrama de estado do protocolo Hello

Por último, apresenta-se a lógica de ativação de rota de proteção, que corresponde a uma trap enviada pelo OXC que detectou a falha. De posse de tal informação, o sistema de controle dispara a criação da rota de proteção e avisa tal fato para a gerência. A Figura 6.14 apresenta o diagrama lógico de tais ações.

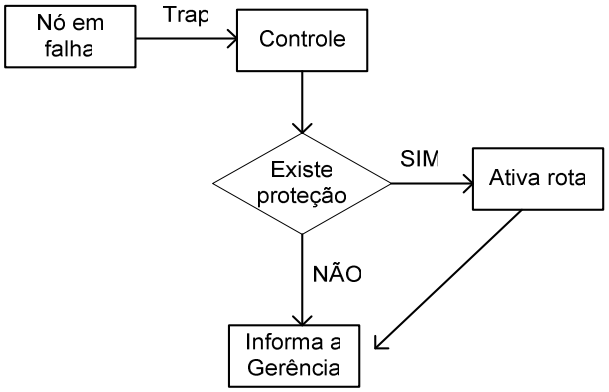

Figura 6.14 – Lógica de proteção

Diagrama de classes

A Figura 6.15 representa o diagrama UML simplificado das principais classes envolvidas na solução. A partir de tal ilustração, observa-se que o conceito de grafo está implementado intrinsecamente.

A classe No implementa o vértice ou nó, a Enlace o arco. Assim, todo o grafo fica representado na classe Topologia. As demais classes dão suporte ao algoritmo rwa (Dijkstra + First Fit), que em última instância representa a funcionalidade de criação e deleção de caminhos ópticos.

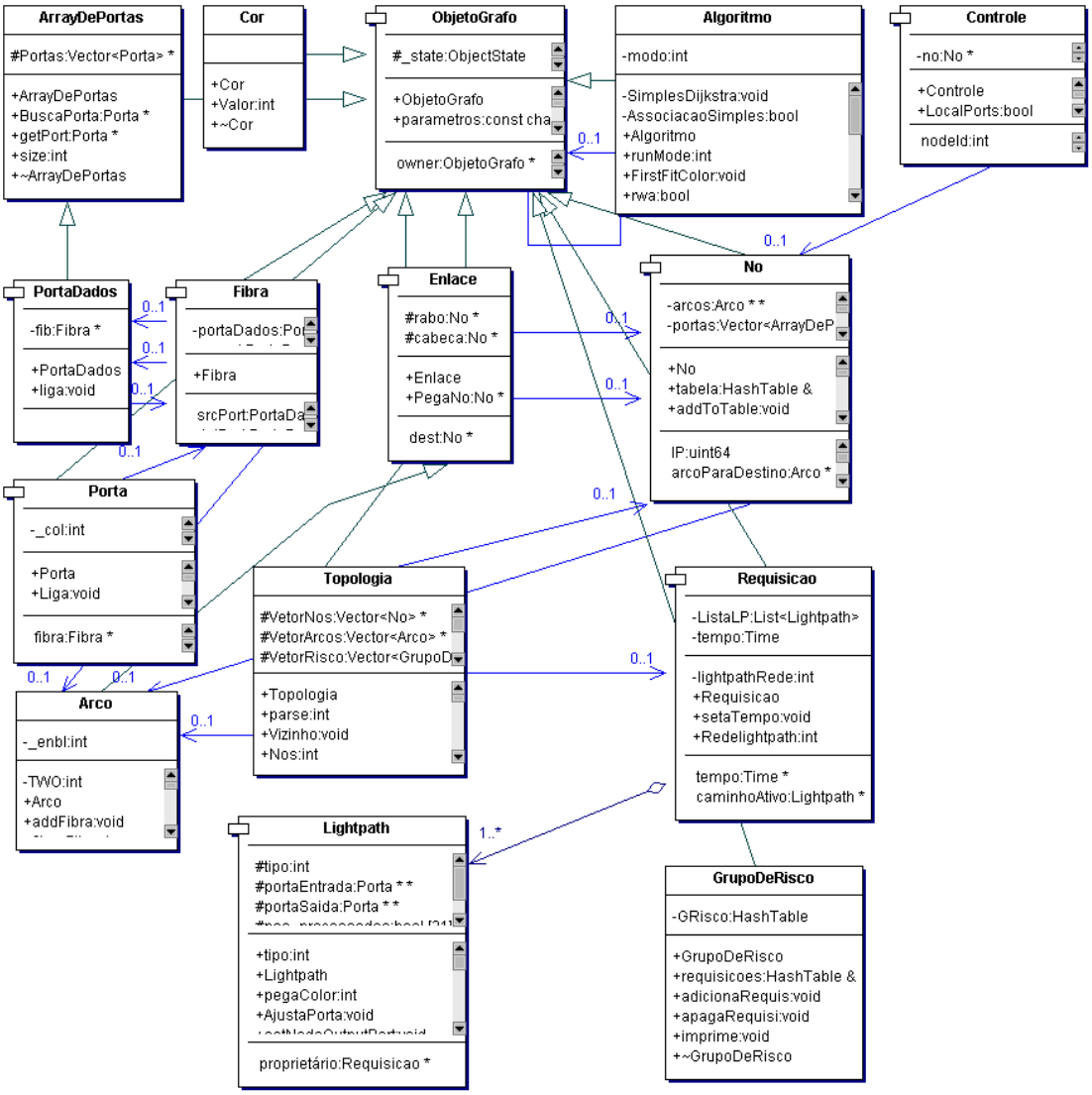

Figura 6.15 – Diagrama de Classes

6.8 SIMULAÇÃO FÍSICA

Optou-se por adotar uma simulação física da rede proposta por várias razões. Primeiro, a desativação da rede OMEGA no CPqD (devido a fatores que fogem ao escopo deste trabalho); segundo, limitações de tempo e receita do projeto, que inviabilizaram no momento a montagem de uma rede óptica no Laboratório de Comunicações (LabCom) da

Universidade de Brasília; e terceiro, mas não menos, a necessidade de se ter um ambiente de experimentação no LabCom.

A simulação dos elementos ópticos foi realizada através do desenvolvimento de uma interface gráfica que simulasse o funcionamento das chaves ópticas e dos amplificadores e *transponders*. Assim, cada computador passa a simular os três elementos acima e utiliza uma conexão ethernet para enviar e receber mensagens UDP do sistema de controle e da gerência.

As mensagens correspondem a *sets* e *gets* para ajustes e recebimento de informações dos elementos e traps para alarme. No caso das traps, estas são enviadas sempre do nó com problemas para o sistema de controle.

O ambiente utilizado para esta camada foi o Eclipse, versão 3.1.1, e a linguagem Java – *framework swing*.

A Figura 6.16 apresenta um elemento óptico com a respectiva configuração de sua chave. Neste caso, para melhor clareza das ações, são evidenciados os comandos enviados pelo controle.

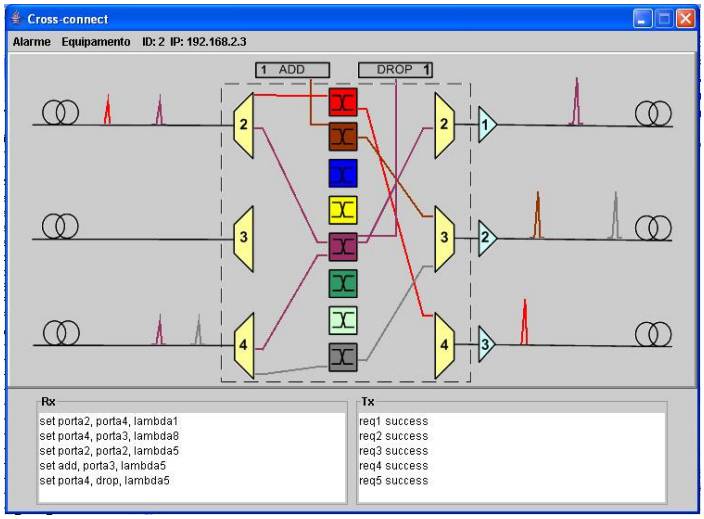

Figura 6.16 – OXC simulado

A Figura 6.17 apresenta a interface com os dados de um *transponder*.Assim, nesta interface podem ser alterados os valores de dadas informações, bem como forçar as *traps*.

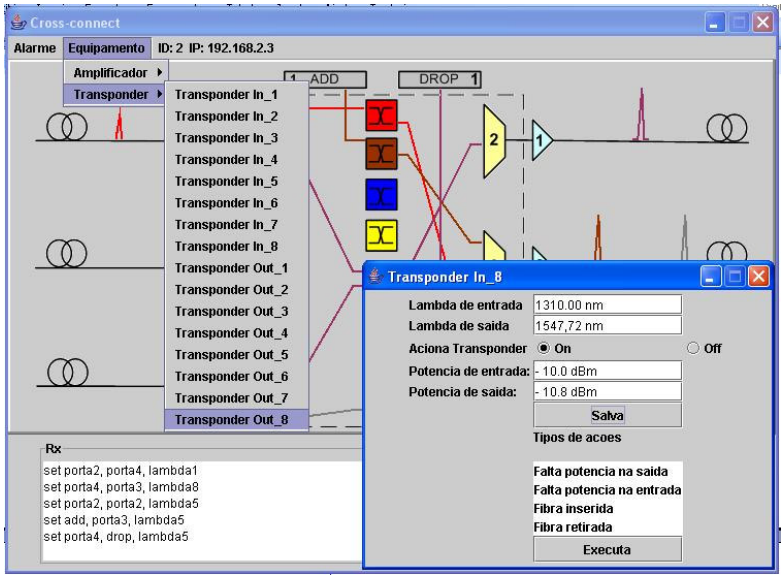

Figura 6.17 – Interface do *Transponder*

As informações sobre cada um dos elementos são persistidas em formato XML. Assim, quando a gerência requisita um get das mesmas, um *stream* XML é montado e enviado pela conexão *socket*. Este tipo de implementação confere simplicidade e leveza tanto no armazenamento das informações quanto no trâmite delas na rede.

6.9 CENÁRIO DE HARDWARE

O ambiente de teste para o sistema em questão possui a seguinte configuração:

— Cada elemento óptico (OXC, Amplificador e Transponder) é simulado num dado computador. Assim, para o ensaio realizado foram utilizadas seis estações de trabalho. Cinco para os nós ópticos e uma para o sistema de gerência e controle;

— A DNC foi simulada a partir de um *switch* Enterasys com capacidade para configuração de VLAN[16]s e limitação de banda nas portas a taxas de 1 Mbps a 10 Mps.

A Figura 6.18 representa o cenário montado.

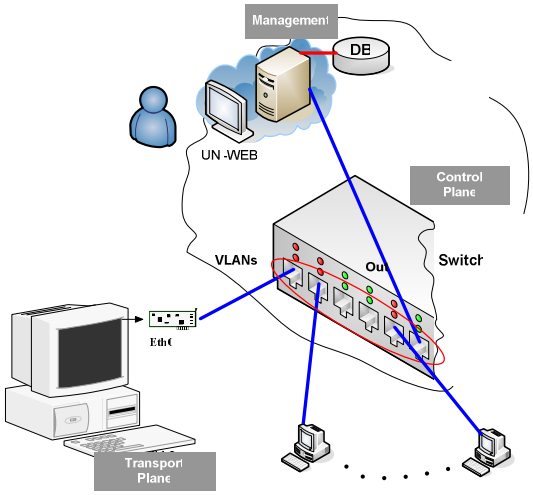

Figura 6.18 – Ambiente de teste

6.10 TESTES DA SIMULAÇÃO

Para a realização dos testes foram admitidas as seguintes premissas:

— Admitiu-se que a rede que interliga o sistema de controle aos sites está estável e que cada enlace de cada site tem uma característica de delay predeterminado entre um valor mínimo e um máximo em milisegundos;
— A trap do OXC informa apenas a porta, pois a fibra quem sabe é o sistema de controle;
— Após o sistema de controle receber a trap, ele decide sobre o que fazer. Neste contexto, o tempo de descida no enlace foi considerado o mesmo de subida, acrescido do tempo de execução da mensagem pelo OXC (em milisegundos) e o tempo de acionamento das chaves (valor diagnosticado pelo CPqD);

16 As VLANs são uma solução alternativa ao uso de roteadores para conter o tráfego broadcast. Assim, ocorre a segmentação das redes locais em diferentes domínios desta natureza.

— Todos os traps são logados, bem como todos os comandos. Essa etapa corresponde a auditoria do sistema, que também é realizada pelo o sistema de controle e tratada pela gerência;

— A estimativa do tempo de acionamento da proteção foi realizada da seguinte forma: ao receber a trap informando a falha de uma porta registrou-se o timestamp da trap, efetuou-se o lookup da rota de proteção e determinou-se as ações de comutação por sets específicos.

7 RESULTADOS E DISCUSSÃO

Neste Capítulo serão apresentados os resultados obtidos no cenário de testes, bem como realizadas as discussões julgadas pertinentes sobre os mesmos.

Por último, será apresentada a conclusão do trabalho, a conseqüente hipótese pertinente para a solução do problema estudado, bem como as propostas para trabalhos futuros.

7.1 RESULTADOS OBTIDOS NA REDE SIMULADA

A Tabela 7.1 apresenta os resultados do segundo experimento, dentre os três registrados e estudados. Cada experimento foi realizado com a submissão de 30 (trinta) requisições aleatórias, mas nem todas as requisições foram atendidas. No caso específico do experimento 2 apenas 26 (vinte e seis) foram atendidas. Este fenômeno se deu pela saturação da rede ocasionada pelo uso do First Fit como estratégia de alocação de comprimento de onda.

A primeira coluna da tabela apresenta o número da requisição, que possui valor crescente a partir de um. A segunda coluna apresenta o tempo em milissegundos, que foi consumido para criar um caminho, com o número de nós evidenciado em Num Nós. Todos os nós que pertencem a um dado caminho estão totalmente explicitados em *Lightpath.*

O caminho óptico, constante no campo *Lightpath*, pode ser entendido da esquerda para a direita com a seguinte lógica: o primeiro número corresponde ao nó de origem e o seguido pelo símbolo –> o nó destino. A palavra SERVICE indica que o caminho é de serviço e não de proteção. O número que segue o símbolo @ indica o lambda utilizado e o * declara que o caminho está ativo; permitindo assim o envio de dados pelo mesmo.

Os demais caracteres representam o detalhamento do caminho. Assim, para a requisição de número 30 (trinta) tem-se: o caminho começa no nó 4 (quatro) através do ADD, sai pela porta número 0 (zero) e entra na porta 2 (dois) do nó 2 (dois) onde sai através da porta DROP do mesmo.

Tabela 7.1 - Resultado das requisições de criação de *lightpaths.*

NumReq	Tempo – ms	Num. Nós	Lightpath
1	235	2	5->4 – SERVICE@1* 5(3/2)+4(2/3)
2	319	2	3->4 – SERVICE@2* 3(3/1)+4(1/3)
3	304	3	3->4 – SERVICE@3* 3(3/0)+2(1/2)+4(0/3)
4	304	4	3->2 – SERVICE@1* 3(3/2)+5(1/0)+1(1/0)+2(0/3)
5	240	2	5->3 – SERVICE@2* 5(3/1)+3(2/3)
6	257	2	2->1 – SERVICE@2* 2(3/0)+1(0/3)
7	364	3	2->5 – SERVICE@1* 2(3/2)+4(0/2)+5(2/3)
8	247	2	4->3 – SERVICE@1* 4(3/1)+3(1/3)
9	304	3	1->3 – SERVICE@3* 1(3/1)+5(0/1)+3(2/3)
10	295	3	4->3 – SERVICE@4* 4(3/0)+2(2/1)+3(0/3)
11	351	3	3->5 – SERVICE@4* 3(3/1)+4(1/2)+5(2/3)
12	370	3	5->2 – SERVICE@3* 5(3/2)+4(2/0)+2(2/3)
13	275	2	1->5 – SERVICE@2* 1(3/1)+5(0/3)
14	286	3	3->2 – SERVICE@5* 3(3/1)+4(1/0)+2(2/3)
15	307	3	4->5 – SERVICE@3* 4(3/1)+3(1/2)+5(1/3)
16	297	3	5->3 – SERVICE@5* 5(3/2)+4(2/1)+3(1/3)
17	426	4	3->5 – SERVICE@6* 3(3/0)+2(1/0)+1(0/1)+5(0/3)
18	435	4	1->5 – SERVICE@5* 1(3/0)+2(0/2)+4(0/2)+5(2/3)
19	344	3	4->3 – SERVICE@6* 4(3/2)+5(2/1)+3(2/3)
20	448	4	5->4 – SERVICE@4* 5(3/0)+1(1/0)+2(0/2)+4(0/3)
21	269	4	5->4 – SERVICE@6* 5(3/0)+1(1/0)+2(0/2)+4(0/3)
22	260	4	1->5 – SERVICE@7* 1(3/0)+2(0/1)+3(0/2)+5(1/3)
23	194	3	1->4 – SERVICE@8* 1(3/1)+5(0/2)+4(2/3)
26	434	3	5->4 – SERVICE@7* 5(3/1)+3(2/1)+4(1/3)
28	306	4	3->1 – SERVICE@8* 3(3/1)+4(1/2)+5(2/0)+1(1/3)
30	476	2	4->2 – SERVICE@2* 4(3/0)+2(2/3)

A Tabela 7.2 apresenta a quantidade de pacotes que foram capturados na rede quando da realização do experimento dois. Para realizar tal registro foi utilizado o Ethereal[17] 0.99.0 release de 24 de Abril de 2006. Nesta tabela são evidenciados todos os pacotes capturados, todos os pacotes UDP e as parcelas dos mesmos usados pelo protocolo em questão.

[17] Para mais detalhes sobre o *software*, acessar http://www.ethereal.com

A criação das VLANs acarretou o natural isolamento do domínio de *broadcast* e a conseqüente exclusão de transmissão de pacotes das aplicações típicas de *broadcast*. Assim, para o experimento dois foram obtidos os resultados listados na Tabela 7.2.

Tabela 7.2 - Total de pacotes UDP que transitaram na rede

Total packets captured on the network	207
Total UDP packets	78
Total UDP packets to node 1	11
Total UDP packets to node 2	13
Total UDP packets to node 3	16
Total UDP packets to node 4	19
Total UDP packets to node 5	19

A Figura 7.1 apresenta a configuração básica de um pacote UDP. Este pacote irá encapsular o pacote específico do protocolo e então formarão um único contexto.

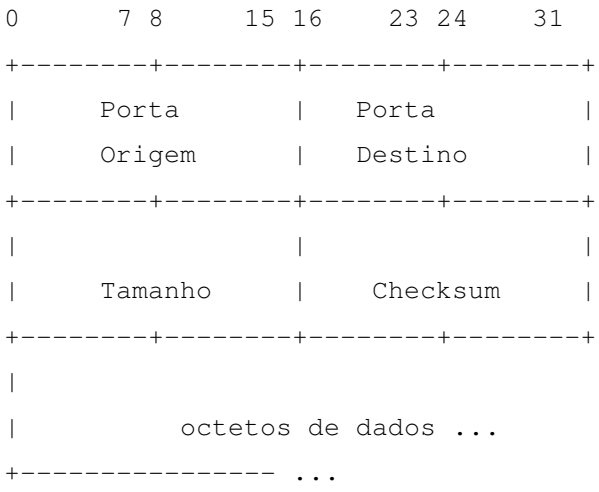

Figura 7.1 – Formato de um datagrama UDP

Cada pacote do protocolo de criação de caminho óptico tem a configuração apresentada na Figura 7.2. A síntese do cabeçalho é a seguinte:

```
Uint8 msgtype: SETPORT, UNSETPORT;
Uint8 tipo: SERVICO, PROTECAO;
Uint8 hops: número de saltos;
```

```
Uint8 npars: Número de parâmetros;
Uint8 nodeID: ID do Nó que receberá a mensagem;
Uint32 packetid: ID do pacote;
Uint32 ownerid: ID do proprietário da requisição;
Uint32 demandid: Número da demanda;
Uint32 time_sec: Tempo em segundos da origem;
Uint32 time_unsec: Tempo em milisegundos da origem.
Payload: npars * Uint8.
```

Total de 5 + 20 = 25 bytes fixos, mais o Payload.

A Figura 7.2 apresenta o pacote do protocolo para uma requisição típica SetPort. Neste exemplo, o lambda 8 será comutado entre a porta 0 e 1 do nó 5.

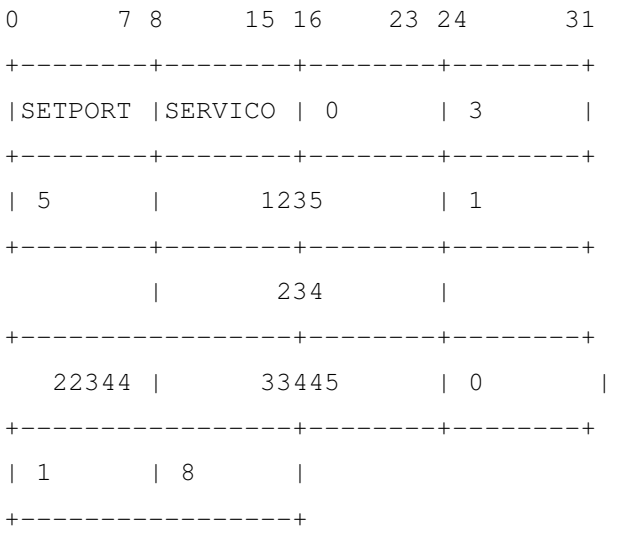

Figura 7.2 – Configuração de um pacote Set da requisição 234

Uma vez definido o pacote do protocolo, o mesmo será encapsulado num datagrama UDP, que ficará com a configuração mostrada na Figura 7.3.

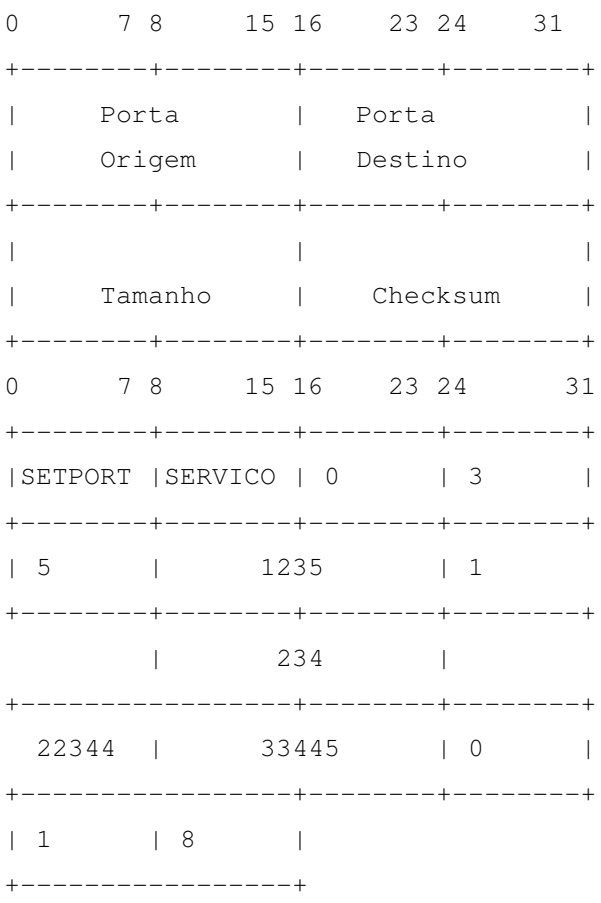

Figura 7.3 – Configuração de um pacote UDP para um Set

Para originar os parâmetros de consumo de rede do cenário montado, foram realizados os seguintes pings com a requisição de (25+8) = 33 bytes.

```
COMANDO UTILIZADO:

ping -s 25 -c x IP

PING 192.168.1.40 (192.168.1.40) 25(53) bytes of data.
33 bytes from 192.168.1.40: icmp_seq=0 ttl=64 time=0.181 ms
33 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.168 ms
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.168/0.174/0.181/0.014 ms, pipe 2

PING 192.168.1.40 (192.168.1.40) 25(53) bytes of data.
33 bytes from 192.168.1.40: icmp_seq=0 ttl=64 time=0.183 ms
33 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.168 ms
```

```
33 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.163 ms
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.163/0.171/0.183/0.013 ms, pipe 2

PING 192.168.1.40 (192.168.1.40) 25(53) bytes of data.
33 bytes from 192.168.1.40: icmp_seq=0 ttl=64 time=0.169 ms
33 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.169 ms
33 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.166 ms
33 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.166 ms
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.166/0.167/0.169/0.013 ms, pipe 2

LOOPBACK

PING 127.0.0.1 (127.0.0.1) 25(53) bytes of data.
33 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.037 ms
33 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.036 ms
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.036/0.036/0.037/0.006 ms, pipe 2

PING 127.0.0.1 (127.0.0.1) 25(53) bytes of data.
33 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.034 ms
33 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms
33 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.034/0.035/0.037/0.005 ms, pipe 2

PING 127.0.0.1 (127.0.0.1) 25(53) bytes of data.
33 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.034 ms
33 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms
33 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.049 ms
33 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.035 ms
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.034/0.039/0.049/0.006 ms, pipe 2
```

A Tabela 7.3 apresenta fragmentos dos caminhos de serviço e de proteção (disjuntos) calculados para uso em criação aleatória. Cada par de fibras que conecta dois OXCs dão origem a um enlace. Assim, para a topologia apresentada tem-se os seguintes enlaces:

— Enlace 1 = liga Nó 1 ao Nó 5;
— Enlace 2 = liga Nó 1 ao Nó 2;
— Enlace 3 = liga Nó 2 ao Nó 3;
— Enlace 4 = liga Nó 2 ao Nó 4;
— Enlace 5 = liga Nó 3 ao Nó 4;
— Enlace 6 = liga Nó 3 ao Nó 5;
— Enlace 7 = liga Nó 4 ao Nó 5;

Tabela 7.3 - Fragmentos de caminhos de serviço e de proteção

Caminhos de serviço:
Caminho: Nó origem = 1 Nó destino = 2 Enlaces: 2
Caminho: Nó origem = 1 Nó destino = 2 Enlaces: 1 6 3
Caminhos de proteção:
Caminho: Nó origem = 1 Nó destino = 2 Enlaces: 1 6 3
Caminho: Nó origem = 1 Nó destino = 2 Enlaces: 2
Caminhos de serviço:
Caminho: Nó origem = 1 Nó destino = 4 Enlaces: 1 6 5
Caminho: Nó origem = 1 Nó destino = 4 Enlaces: 2 3 5
Caminhos de proteção:
Caminho: Nó origem = 1 Nó destino = 4 Enlaces: 2 4
Caminho: Nó origem = 1 Nó destino = 4 Enlaces: 1 7
Caminhos de serviço:
Caminho: Nó origem = 1 Nó destino = 5 Enlaces: 1
Caminho: Nó origem = 1 Nó destino = 5 Enlaces: 2 3 6
Caminhos de proteção:
Caminho: Nó origem = 1 Nó destino = 5 Enlaces: 2 3 6
Caminho: Nó origem = 1 Nó destino = 5 Enlaces: 1
Caminhos de serviço:
Caminho: Nó origem = 2 Nó destino = 1 Enlaces: 2
Caminho: Nó origem = 2 Nó destino = 1 Enlaces: 3 6 1
Caminhos de proteção:
Caminho: Nó origem = 2 Nó destino = 1 Enlaces: 3 6 1
Caminho: Nó origem = 2 Nó destino = 1 Enlaces: 2
Caminhos de serviço:
Caminho: Nó origem = 2 Nó destino = 3 Enlaces: 4 7 6

Caminho: Nó origem = 2 Nó destino = 3 Enlaces: 2 1 7 5
Caminhos de proteção:
Caminho: Nó origem = 2 Nó destino = 3 Enlaces: 3
Caminho: Nó origem = 2 Nó destino = 3 Enlaces: 3
Caminho de serviço:
Caminho: Nó origem = 3 Nó destino = 2 Enlaces: 5 7 1 2
Caminho de proteção:
Caminho: Nó origem = 3 Nó destino = 2 Enlaces: 3
Caminho de serviço:
Caminho: Nó origem = 3 Nó destino = 4 Enlaces: 5
Caminho de proteção:
Caminho: Nó origem = 3 Nó destino = 4 Enlaces: 3 4
Caminho de serviço:
Caminho: Nó origem = 3 Nó destino = 5 Enlaces: 6
Caminho de proteção:
Caminho: Nó origem = 3 Nó destino = 5 Enlaces: 5 7
Caminho de serviço:
Caminho: Nó origem = 4 Nó destino = 1 Enlaces: 4 2
Caminho de proteção:
Caminho: Nó origem = 4 Nó destino = 1 Enlaces: 7 1
Caminho de serviço:
Caminho: Nó origem = 5 Nó destino = 1 Enlaces: 1
Caminho de proteção:
Caminho: Nó origem = 5 Nó destino = 1 Enlaces: 6 3 2
Caminho de serviço:
Caminho: Nó origem = 5 Nó destino = 2 Enlaces: 1 2
Caminho de proteção:
Caminho: Nó origem = 5 Nó destino = 2 Enlaces: 6 3
Caminho de serviço:
Caminho: Nó origem = 5 Nó destino = 3 Enlaces: 7 4 3
Caminho de proteção:
Caminho: Nó origem = 5 Nó destino = 3 Enlaces: 6

Caminho de serviço:
Caminho: Nó origem = 5 Nó destino = 4 Enlaces: 1 2 3 5
Caminho de proteção:
Caminho: Nó origem = 5 Nó destino = 4 Enlaces: 7

O tempo para ativar a proteção foi medido da seguinte forma: registra-se o tempo decorrido entre o acionamento da *trap* e a chegada desse pacote no sistema de controle. A partir desse instante, registra-se o tempo decorrido para o acionamento da rota de proteção. O sistema de proteção desenvolvido, que acompanhou os moldes do usado na rede modelo, apresenta estrutura de suporte para uma única pane por vez. Assim, todo o tráfego que está passando por um enlace é desviado para a rota de proteção.

Uma diferença significante entre proteção fim a fim e uma proteção local é que a última corresponde a uma proteção por enlace. Assim, a proteção local comuta todo o tráfego do enlace para o correspondente de proteção. Conexão fim a fim comuta as conexões individuais que possuem um caminho de serviço e um de proteção.

Tanto a solução desenvolvida pelo CPqD, quanto a solução centralizada utiliza o conceito de Grupo de Enlaces de Risco Compartilhado - *Shared Risk Link Group* (SRLG) [RAMAMMURTHY, 2003], [MOUFTAH, 2002]. O SRLG corresponde a uma identificação única associada a um grupo de enlaces ópticos que compartilham o mesmo enlace físico. Dessa forma, todos os enlaces ópticos que passam por uma fibra pertencem ao mesmo grupo de risco.

No caso de falha num enlace, o OXC detecta a falta de sinal na sua porta de entrada e envia a mensagem de falha para o sistema de controle. Quando o sistema recebe esta mensagem ele encontra a SRLG associado com o enlace em falha. O SRLG contém a lista de todas as conexões passando através do enlace falho. Para aquelas conexões em que o caminho de serviço passa através do nó ele conecta a porta apropriada do OXC. Então quando todos os nós de uma dada requisição terminam seus processos a conexão está estabelecida.

Para a restauração, o procedimento é realizado pelo sistema de gerência. Dessa forma, o operador de campo informa ao gerente que o enlace foi restabelecido e então as conexões originais voltam a operar e os caminhos de proteção ficam novamente em *stand by*, quando ele reativar a operação.

Nos testes realizados com o caminho de serviço entre o nó origem 5 e o nó destino 2, com os enlaces 1 2 e o respectivo caminho de proteção com os enlaces 6 3 foram observados valores que variaram entre 0,3 ms de subida da *trap* mais um tempo na ordem de 286 ms para criação da rota de proteção. Os valores obtidos não apresentaram uniformidade nas respostas, mesmo para a mesma situação de origem.

A Figura 7.4 apresenta o histograma do tempo consumido para criação de um caminho óptico no modo aleatório para o experimento dois. Nesta Figura observa-se que a mediana é menor que a média. Assim, a curva de Gauss está deslocada à direita das faixas mais representativas do histograma o que revela uma assimetria positiva.

Todos os dados estatísticos foram produzidos através do *software* estatístico SPSS[18].

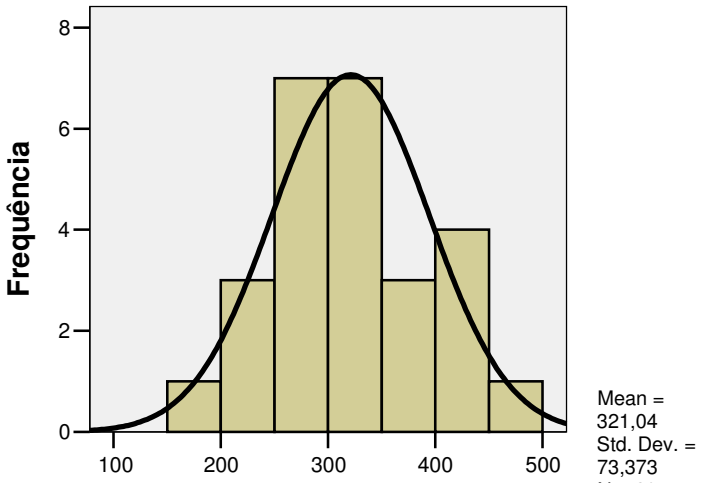

Figura 7.4 – Histograma do tempo da requisição para o experimento dois

[18] SPSS originalmente acrônimo de Statistical Package for the Social Sciences, mas hoje para Statistical Product and Service Solutions de propriedade da SPSS Inc.

A Figura 7.5 apresenta o histograma do tempo consumido para criação de um caminho óptico no modo aleatório para todos os experimentos.

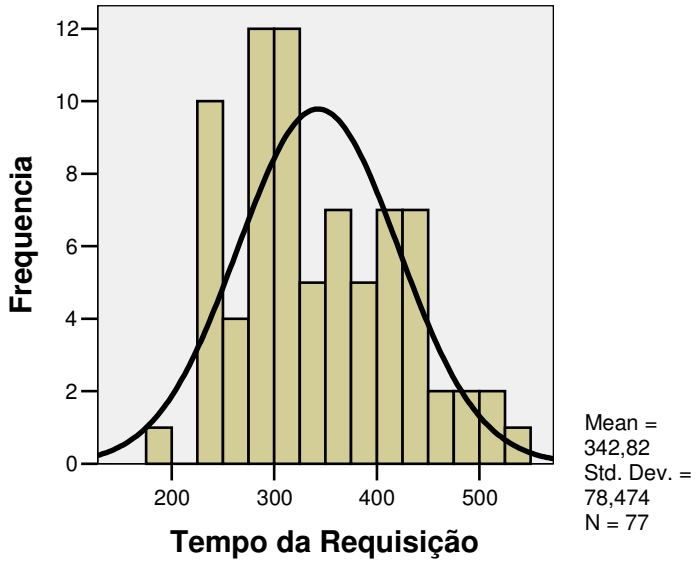

Figura 7.5 – Histograma do tempo da requisição para todos os experimentos

A Figura 7.6 apresenta o gráfico de linha que representa a correlação entre o número de nós e o tempo consumido para a requisição.

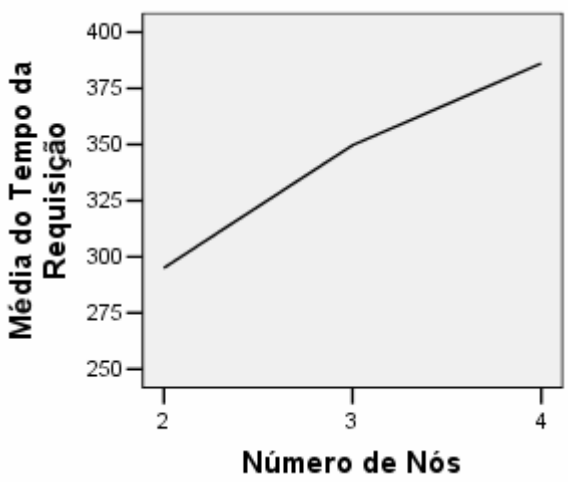

Figura 7.6 – Correlação entre número de nós e tempo da requisição em ms

A Tabela 7.4 apresenta o resumo do cenário estudado. Assim, são registrados os três experimentos, bem como a contribuição quantitativa de cada um.

Tabela 7.4 – Sumário dos casos

		Cases					
		Valid		Missing		Total	
	Experimento	N	Percent	N	Percent	N	Percent
Tempo da Requisição	Experimento 1	27	100,0%	0	,0%	27	100,0%
	Experimento 2	26	100,0%	0	,0%	26	100,0%
	Experimento 3	24	100,0%	0	,0%	24	100,0%

A Tabela 7.5 apresenta o detalhamento do cenário estudado. Desta forma, são apresentadas as principais análises descritivas de cada experimento.

Tabela 7.5 - Detalhamento do cenário estudado

Experimento				Statistic	Std. Error
Tempo da Requisição	Experimento 1	Mean		354,04	14,352
		95% Confidence Interval for Mean	Lower Bound	324,54	
			Upper Bound	383,54	
		5% Trimmed Mean		351,57	
		Median		349,00	
		Variance		5561,114	
		Std. Deviation		74,573	
		Minimum		232	
		Maximum		521	
		Range		289	
		Interquartile Range		101	
		Skewness		,523	,448
		Kurtosis		,048	,872
	Experimento 2	Mean		321,04	14,390
		95% Confidence Interval for Mean	Lower Bound	291,40	
			Upper Bound	350,67	
		5% Trimmed Mean		319,32	
		Median		304,00	
		Variance		5383,638	
		Std. Deviation		73,373	
		Minimum		194	
		Maximum		476	
		Range		282	
		Interquartile Range		99	

		Skewness		,618	,456
		Kurtosis		-,355	,887
	Experimento 3	Mean		353,79	17,560
		95% Confidence Interval for Mean	Lower Bound	317,47	
			Upper Bound	390,12	
		5% Trimmed Mean		351,40	
		Median		347,00	
		Variance		7400,694	
		Std. Deviation		86,027	
		Minimum		231	
		Maximum		526	
		Range		295	
		Interquartile Range		141	
		Skewness		,151	,472
		Kurtosis		-1,060	,918

Os textos abaixo apresentam o diagrama *Stem-and-Leaf* (ramo e folhas) de cada experimento. Este diagrama foi criado por John Tukey com o objetivo de armazenar os dados de um experimento sem perda de informação.

```
Tempo da Requisição Stem-and-Leaf Plot for
NumExpe= Experimento 1

 Frequency    Stem &  Leaf

     2,00        2 .  33
     6,00        2 .  688999
     6,00        3 .  012334
     7,00        3 .  5677899
     3,00        4 .  112
     1,00        4 .  5
     2,00        5 .  12

 Stem width:   100
 Each leaf:       1 case(s)
```

```
Tempo da Requisição Stem-and-Leaf Plot for
NumExpe= Experimento 2

 Frequency    Stem &  Leaf

     1,00        1 .  9
     3,00        2 .  344
     7,00        2 .  5667899
     7,00        3 .  0000014
     3,00        3 .  567
     4,00        4 .  2334
     1,00        4 .  7

 Stem width:   100
 Each leaf:       1 case(s)


Tempo da Requisição Stem-and-Leaf Plot for
NumExpe= Experimento 3

 Frequency    Stem &  Leaf

     5,00        2 .  34444
     3,00        2 .  799
     4,00        3 .  1223
     2,00        3 .  57
     7,00        4 .  0022223
     2,00        4 .  57
     1,00        5 .  2

 Stem width:   100
 Each leaf:       1 case(s)
```

A Figura 7.7 apresenta o gráfico de caixas e *whiskers* dos três experimentos. Os valores apresentados serão discutidos no tópico seguinte.

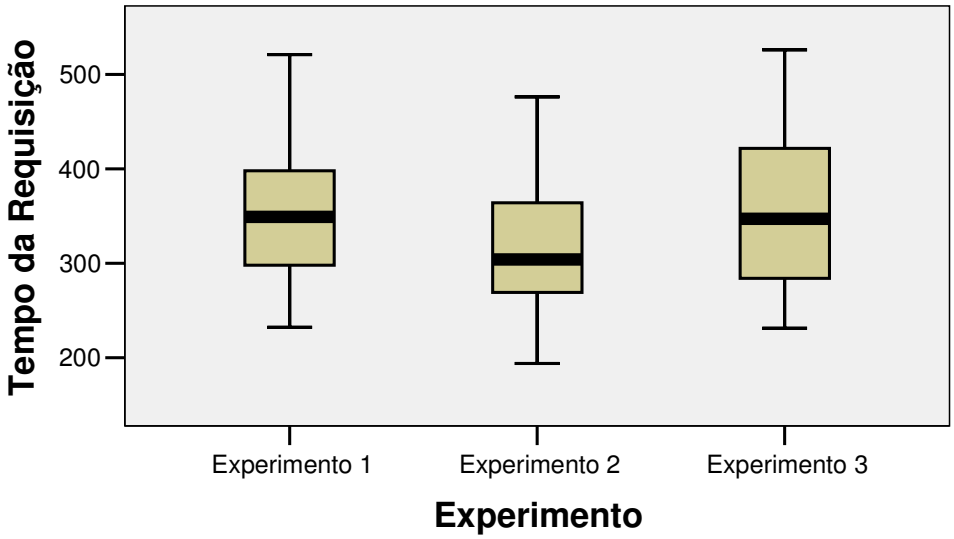

Figura 7.7 – Gráfico de caixas

7.2 DISCUSSÃO DOS RESULTADOS

O software desenvolvido apresentou, nas três camadas, um comportamento integrado e homogêneo. De uma forma geral, apesar da complexidade de integração dos módulos de gerência, controle e simulação física foi observado uma forte coesão e um baixo acoplamento dos mesmos.

Acoplamento corresponde ao grau de interdependência entre os componentes de um sistema. Desta forma, a engenharia de *software* considera uma boa prática um acoplamento fraco, possibilitando uma maior flexibilidade na mudança das partes sem ocasionar a mudança no todo.

No caso específico desse estudo, melhorias no processo de desenvolvimento podem ser realizadas numa das três camadas com pouca implicação de mudanças nas demais. Para a gerência, por exemplo, podem ser desenvolvidos mecanismos do cliente monitorar seus enlaces com base no seu SLA - *Service Level Agreement*.

No desenvolvimento de *software*, coesão diz respeito à consistência interna dos elementos de um sistema. Assim, quando há coesão forte os elementos do sistema têm a menor distância conceitual possível entre si. Esta característica confere ao produto uma

robustez funcional baseada no fato que cada parte do sistema faz bem aquilo para o qual foi projetado.

O sistema de controle, por exemplo, apresenta uma alta coesão a partir da visão clara que sua função é extremamente especializada e só permite interação com o mesmo através de uma rigorosa interface (análise léxica, sintática e semântica).

A Tabela 7.1, que apresenta os resultados do segundo experimento, registra um grupo de resultados coerentes e bem estruturados. Desta forma, percebe-se que as funcionalidades desejadas estão presentes nos resultados.

Os requisitos básicos funcionais para este contexto foram:

— Registro da requisição através de um identificador único, permitindo assim rastreabilidade;
— Computo do tempo necessário para a realização de uma requisição e o respectivo atendimento da mesma;
— Explicitação dos caminhos criados de forma a permitir um fácil entendimento do mesmo.

Além dos requisitos acima, foram agregadas as informações relativas ao lambda utilizado, a atividade ou não do caminho e sua caracterização (serviço ou proteção).

A Tabela 7.2, que apresenta a quantidade de pacotes capturados na rede a partir do experimento dois evidencia um consumo mínimo de pacotes UDP por parte do protocolo de criação de enlaces ópticos. O fragmento da captura de todos os pacotes, apresentado abaixo, indica o trâmite de fragmentos intrinsecamente ligados às questões de camada dois (por exemplo, spanning tree). Assim, pode-se considerar que tal protocolo agindo numa DNC com uma boa performance (enlaces acima de 2 Mbps) e livre de outros tráfegos pode muito bem suportar níveis de tempo exigidos para sistemas desta natureza.

```
                                          Spanning-tree-(for-
20  25.739.321  Enterasy_94:ac:57             bridges)_00
                                          Spanning-tree-(for-
21  27.719.269  Enterasy_94:ac:57             bridges)_00
22  29.562.936  CompalEl_02:79:b8    AcctonTe_ec:8d:2b
```

				ARP
				CompalEl_02:79:b8
23	29.563.031	AcctonTe_ec:8d:2b		ARP
				Spanning-tree-(for-
24	29.699.217	Enterasy_94:ac:57		bridges)_00
				01:80:c2:00:00:21
25	30.721.377	Enterasy_94:ac:57		GVRP
				01:80:c2:00:00:21
26	30.870.436	Enterasy_94:ac:57		GVRP
				Spanning-tree-(for-
27	31.679.741	Enterasy_94:ac:57		bridges)_00
				192.168.1.20
28	32.769.292	192.168.1.9		UDP
				192.168.1.40
29	32.769.877	192.168.1.9		UDP
				192.168.1.9
30	32.769.901	192.168.1.20		UDP

Os comandos *ping* realizados tanto para um dado equipamento (estação quatro), quanto em *loopback* evidenciaram um rtt na ordem de (0.163 a 0.181 ms) e (0.034 a 0.039 ms) respectivamente. Contudo, o tempo total para o processamento e apresentação dos dados do *ping* apresentou um crescimento médio de 1000 ms para cada pacote acrescentado (2,3 e 4 pacotes). Assim, conclui-se que o tempo de processamento do *ping*, apesar de ser um protocolo extremamente simples, é que representa a verdadeira contribuição do acréscimo do tempo consumido pelo processo como um todo.

O rtt é o acrônimo de *Round Trip Time*, que é a medida de tempo que um pacote leva para ir de um computador a outro na rede e retornar. O cômputo desse valor é realizado através da subtração entre o tempo registrado no recebimento da mensagem e o tempo inicialmente registrado no envio desta.

No sistema de controle, o algoritmo rwa é o principal responsável pelo consumo de tempo de processamento. Apesar dos caminhos estarem registrados numa tabela *hash*, a alocação do lambda por *First Fit* é realizada de forma dinâmica. Esta estratégia implica num natural *overhead* computacional, que será discutido sob o prisma da análise de complexidade.

Para um dado algoritmo pode-se medir a complexidade do mesmo através de estratégias que caracterizem o comportamento assintótico das funções que o implementam. Uma forma clara de tal análise é o uso da notação O, inventada em 1892 por P. Bachmann.

Para a análise de complexidade, tem-se a restrição do uso de funções *assintoticamente não-negativas*, ou seja, funções f tais que $f(n) \geq 0$ para todo n suficientemente grande. Assim, f é assintoticamente não-negativa se existe N tal que $f(n) \geq 0$ para todo n maior que N.

Assim, tem-se a seguinte definição para a notação O, que segundo Knuth trata-se do ômicron grego maiúsculo: tendo duas funções assintoticamente não-negativas f e g, dizemos que f *está na ordem O de* g, e escrevemos f = O(g), se $f(n) \leq c \cdot g(n)$ para algum c positivo e para todo n suficientemente grande [KNUTH, 1998]. Desta forma, existe um número positivo c e um número N tais que $f(n) \leq c \cdot g(n)$ para todo n maior que N.

Na prática, após o cálculo da complexidade, tem-se a convergência para notações do seguinte tipo:

- O(1) : valor constante;
- O(log n) : logaritmo;
- O(n) : linear;
- $O(n^2)$: quadrático;
- $O(n^3)$: cúbico;
- $O(2^n)$: exponencial;

Para o algoritmo Dijkstra a complexidade está associada à implementação da lista de vértices, que neste caso foi implementada com estrutura dinâmica de ponteiros.

Considerando que haverá a cada iteração a extração do valor mínimo, esta operação irá tomar um tempo O(n), com n extrações. Assim, esta operação irá consumir $O(n^2)$, mesmo que o tamanho da fila seja decrementado teremos após cada iteração $O(1) + O(2) + ...+ O(n) = O(n^2)$.

Como o algoritmo, neste caso, visita uma dada aresta mais de uma vez, pois tem-se a extração de todos os possíveis caminhos, tem-se que a visita de uma aresta irá consumir O(E) e consequentemente terá o mesmo custo computacional anterior $O(E^2)$. Assim, tem-se $O(E^2) + O(n^2) = 2\ O(n^2)$. Como a implementação foi realizada na *heap*, o tempo passa a m x O(lg n).

Considerando as iterações sobre cada vértice se repetir de acordo com as m derivações dos mesmos tem-se que $O(n \log(n) + n + m \log(n))$. Logo, tem-se que $O((n+m) \log(n))$.

Para otimizar a alocação do comprimento de onda, que só pode ser realizada de forma dinâmica, calculou-se todos os caminhos e os respectivos disjuntos. Todos os caminhos foram armazenados uma tabela *hash*, que apresenta performance na ordem de O(n) para inserção e deleção [PREISS, 1999].

Para o algoritmo de alocação de comprimento de onda (*First Fit*), tem-se uma dedução direta de sua complexidade, pois os caminhos já foram calculados e resta ao sistema percorrer todos os vértices e verificar a alocação ou não de um dado lambda. Dado que um caminho tem um número n de nós e a rede um potencial m de lambdas terá: m * log(n).

Desta forma, observa-se que para a implementação centralizada a performance do rwa (Dijkstra e *First Fit*) é o fator limitante, e não somente os enlaces dos nós junto ao sistema de controle. Para este contexto, tanto mais rápida será a resposta quanto mais otimizada for a implementação do rwa e melhor banda possuir o enlace mais restrito da DNC.

Outro fator importante a ser observado é que a partir do crescimento sensível de n (numero de nós na rede) o sistema rwa terá sua performance mais afetada. Assim, a soma dos dois fatores representará um óbice ao sistema como um todo. Esta análise também é valida para o sistema distribuído, que será afetado na convergência da tabela de vizinhos quando o número de nós da rede aumentar (sobrecarga no *flooding*).

A Tabela 7.3 apresenta fragmentos dos caminhos de serviço e de proteção (disjuntos) calculados para uso em criação aleatória. Como mencionado anteriormente, o conjunto de todos os caminhos de serviço e proteção são calculados assim que a rede é tornada ativa.

Esta estratégia permite uma melhora significativa na performance do rwa, contudo acarreta uma alocação não otimizada após um número razoável de lambdas utilizados.

Para o caso do caminho de serviço entre o Nó origem = 1 e o Nó destino = 4 tem-se os seguintes enlaces: 1 6 5 . O respectivo caminho de proteção corresponde ao caminho disjunto dado pelos enlaces 2 4. Esta abordagem não permite a associação de outros enlaces caso existam. Assim, deve-se privilegiar o desenvolvimento de soluções que possibilitem a exploração de todas as possíveis rotas de proteção e que a escolha seja arbitrada por mecanismos inteligentes a fim de obter a otimização do uso dos recursos da rede óptica como um todo.

A Figura 7.4 com o histograma do tempo consumido para criação de um caminho óptico no modo aleatório para o experimento dois apresenta um valor médio de tempo de 321,04 ms e desvio padrão de 73,373 ms. Como evidenciado através dos *pings* realizados, grande parte do tempo de processamento deve-se ao computo realizado pelo sistema centralizado.

A média geral dos três experimentos foi de 342,82 ms e o desvio padrão de 78,474 ms, evidenciada na Figura 8.5, indicam certa homogeneidade no custo computacional. Diante de tais fatos, percebe-se que o reaproveitamento do *kernel* da solução distribuída não correspondeu a uma boa estratégia de implementação. A manutenção dos estados de cada nó óptico no sistema centralizado causa uma sobrecarga tanto na memória da máquina (mais estruturas de dados armazenadas localmente) quanto no processamento de tais informações.

De todos os experimentos realizados e sumarizados na

Tabela 7.4 observou-se a clara correlação entre o número de nós e o aumento do tempo de processamento, haja visto que o tempo associado ao protocolo UDP permanece com uma média constante para o cenário estudado. Esta situação evidencia a necessidade do redesenho do kernel de forma que todas as estruturas sejam otimizadas no caso de uma implementação centralizada.

A Tabela 7.5 apresenta o detalhamento do cenário estudado através da evidência das principais métricas da estatística descritiva. De uma forma geral, o resumo de tais experimentos pode ser visualizado através da Figura 7.7, que evidencia as diferenças entre os três experimentos com relação a variável tempo de requisição.

A Figura 7.7 nos permite compreender a distribuição dos valores em cada grupo e a correspondente significância estatística. Logo, não se observaram nos três experimentos resultados atípicos.

De forma resumida, os limites inferior e superior das caixas representam os quartis superior e inferior da distribuição de dados, respectivamente. Assim, o comprimento da caixa é a distância entre o 25º percentil e o 75º percentil de forma que a caixa contem 50 % dos valores centrais dos dados.

Graficamente, tem-se que, quanto maior a caixa, maior é a dispersão das observações. Logo, percebe-se uma homogeneidade na distribuição. As linhas que se estendem nas caixas, chamadas de *whiskers,* representam a distância em relação à maior e menor observação que estão a menos de um quartil da caixa.

Os experimentos 1 e 2 apresentaram assimetria e o experimento 3 uma distância mais simétrica. Assim, apesar da aleatoriedade empreendida aos experimentos, o *software* apresentou resultados globais que não fogem da média esperada.

Quanto ao contexto da gerência valem ser citados a leitura e controle das informações sobre os elementos da rede, bem como o sistema de auditoria e segurança.

Para as informações gerenciais sobre os dispositivos foi usado o paradigma XML em detrimento do SNMP. Considerando que o aspecto velocidade não está ligado a este contexto, não foram realizados testes de performance com base na variável tempo, mas sim realizada uma análise com base na flexibilidade de representação das informações.

O SNMP - *Simple Network Management Protocol* por mais de dez anos tem sido a base para todos os sistemas de administração de rede IP. Contudo, como em todo *software*

legado, ele necessita romper com o passado e ter compromisso com as novas demandas [DZUBECK, 2004].

Inúmeros são os trabalhos que sugerem uma reengenharia do SNMP com vista a movê-lo dos padrões de administração do IETF para o *World Wide Web Consortium* (W3C). Dessa forma, teria-se o XML como principal componente de desenvolvimento de *software* dessa natureza. Assim, se conclui que a indústria de TI não necessita de um melhor protocolo, mas de padronização dos serviços web para aplicações de gerência.

Atualmente, sistemas desenvolvidos baseados em XML e serviços web contribuem acentuadamente para a interoperabilidade e comunicação entre os mesmos. Contudo, a grande base SNMP legada dita a necessidade de compatibilidade entre este e o protocolo sucessor, que pode ser obtida através do uso dos conceitos de metadados, intimamente ligado ao XML.

O SNMP é dependente de mensagens UDP e este protocolo de rede não requer reconhecimento e autenticação das mensagens recebidas. Assim, as aplicações SNMP necessitam de complementos para garantir a segurança adequada quanto ao recebimento das mesmas. Assim, observa-se uma ineficiência computacional baseada no fato que a IETF privilegia a precisão e a segurança das mensagens SNMP.

O uso do paradigma XML neste modelo propiciou uma rápida adequação das informações de cada elemento da rede a medida que os requisitos funcionais foram evoluindo. Então, a complexa tarefa de gerar uma assinatura SNMP passou a uma simples redefinição do esquema de um arquivo XML.

Quanto ao sistema de auditoria e segurança, foi consignada a clara visão da necessidade da implementação de um forte conceito de monitoramento das ações tanto dos gestores da rede, quanto dos clientes que podem ter níveis de serviços cada vez mais elaborados.

As implementações realizadas para o sistema de auditoria utilizaram o conceito de associar o controle das ações ao código de cada funcionalidade implementada. Assim, pode-se ter numa mesma interface mais de um controle de interação com o sistema.

Nesse contexto, deve-se ter em mente que implementações alternativas com *triggers* no banco relacional não cabem, pois todas as iterações são realizadas com o sistema de controle, que está fora do escopo relacional. Diante de tais assertivas observa-se que a solução proposta pode ser perfeitamente aplicada a sistemas com maior dimensão e requisitos mais robustos de segurança.

8 CONCLUSÃO

Wavelength Division Multiplexing (WDM) é entendida como a solução de melhor custo benefício quando se trata de aumentar a capacidade da rede de transporte sem ter que instalar novos cabos de fibra óptica. Dessa forma, redes desta natureza exigem constantemente que novas funcionalidades sejam adicionadas, como roteamento óptico, proteção de enlaces, administração e manutenção dos dispositivos ópticos.

Numa rede convencional os serviços têm que ser configurados manualmente. Assim, os engenheiros têm que estudar cada elemento da rede óptica e fisicamente configurar os mesmos. Numa rede óptica inteligente serviços podem ser colocados em produção em pouco tempo através de uma administração centralizada e otimizada dos recursos. A interface gráfica, notadamente no *design* Web, possibilita uma rápida produtividade e alta mobilidade.

De uma forma simples, para atender a demanda de um dado cliente, primeiro se analisa os requisitos do serviço solicitado, selecionam-se as rotas e então as aloca. Sendo o *software* de roteamento inteligente ele providencia todo o resto.

Roteamento com tolerância a falha em redes WDM corresponde a computar um par de rotas disjuntas entre um dado par de nós na rede sendo que ambas as rotas não podem falhar simultaneamente. Todimala estudou e propôs heurísticas iterativas para computar caminhos disjuntos ótimos sob o aspecto de proteção compartilhada [TODIMALA, 2005].

Diagnóstico remoto e recuperação de erros são possíveis em toda a rede inteligente, o que faz o trabalho *on-site* menos necessário. Contudo, atualmente, as redes instaladas por múltiplos fornecedores exigem tantas interfaces de gerência quanto forem às grandes empresas proprietárias dos dispositivos, o que ocasiona baixa taxa de aproveitamento da solução integrada.

Requisitos como otimização do uso dos recursos físicos da rede com vistas à obter-se grande retorno econômico, facilidade na administração da rede como um todo, provimento

de enlaces com alto grau de confiabilidade, diagnóstico e recuperação remota representam as principais exigências do mercado.

Para atender todos estes citados requisitos, se busca efetuar a divisão das funcionalidades em camadas e a adoção de protocolos abertos e bem estruturados nas mesmas. Contudo, existem tensões em todas as camadas causadas pela busca de algumas empresas em definir infra-estrutura de *software* e *hardware* próprios. Apesar de não ser considerada uma boa prática, o que se vê no mercado é a continuação de tal procedimento.

Por outro lado, o mundo acadêmico, como de praxe, busca construir cenários que fujam ao contexto meramente comercial e proponha mudanças na direção de um ambiente aberto. Apesar de todos os esforços, esta faceta não consegue ser atendida por razões que passam pela falta de recursos ou, até mesmo, de conhecimentos proprietários das grandes empresas.

Assim, de posse deste impasse, soluções que consigam simular um cenário proprietário e caro e que atendam aos preceitos acadêmicos de vanguarda acabam fazendo a diferença. Posta tal situação, se pode entender claramente o contexto desta pesquisa.

Considerando que a solução centralizada desenvolvida foi estruturada em três camadas (gerência, controle e simulação), as conclusões serão apresentadas na mesma ordem.

Para a camada de gerência observou-se que a solução Web, acrescida das funcionalidades de segurança e auditoria corresponde às boas práticas do mercado. Apesar de soluções WWW apresentarem limitações quanto aos objetos utilizados na interface, comparados com ambientes de desenvolvimento convencionais, a alta mobilidade permitida associada à simplicidade da interface representam os grandes diferenciais.

O desenvolvimento de código seguro corresponde a uma importante característica a ser atendida, notadamente quando o código e os dados trafegam pela internet. Assim, as soluções web que integram controle de acesso e auditoria necessitam de especial atenção quanto ao aspecto de segurança no desenvolvimento de software.

Na camada de gerência, todos os requisitos citados foram atendidos guardadas as proporções do trabalho e levando-se em consideração o tamanho da equipe de desenvolvimento de *software* alocada para esta pesquisa. Assim, conclui-se para esta camada que uma gerência parcial centralizada corresponde a uma solução sub-ótima, partindo-se do pressuposto que uma gerência centralizada de toda a rede de uma companhia seja o alvo a ser atingido.

Ainda no domínio da gerência, destaca-se o uso do paradigma XML que corresponde, atualmente, a principal vertente de troca de dados na internet. Desta forma, optou-se por usar uma solução simples e flexível, quando comparada com as idiossincrasias do SNMP.

A camada de controle, que corresponde ao núcleo da solução no que diz respeito às questões de performance, apresentou resultados que não se coadunam com o esperado no mercado. De uma forma geral, o que se pretende é o provimento de um enlace seguro com tempo de proteção na ordem de 50 ms, dado que este é o valor típico do SDH.

O aprovisionamento do caminho ótico, por outro lado, não necessita de uma performance na mesma ordem de grandeza que o de proteção. Assim, para esta faceta a solução desenvolvida apresentou um resultado excelente e na ordem de 350 ms.

Os algoritmos utilizados no rwa (Dijkstra e First Fit) correspondem a alternativas que podem ser mudadas, à medida que novas composições lógicas forem sendo apresentadas e implementadas. Desta forma, para a camada de controle, observou-se a restrição quanto ao mecanismo de proteção, notadamente quando são exigidos padrões de alta performance.

A camada de simulação apresentou o comportamento básico esperado, pois nela não foram simuladas transmissão óptica de dados, mas somente a comutação das chaves do OXC. Assim, a solução implementada foi considerada adequada para o que se propôs no estudo em questão.

Esta pesquisa foi nivelada com base nas quatro hipóteses descritas abaixo:

1. A não pertinência da utilização de um sistema de controle e gerência centralizados;

2. A pertinência da utilização de um sistema de controle centralizado como alternativa ao distribuído;
3. A utilização de um modelo misto que incorpore a centralização dos aspectos gerenciais e a distribuição do sistema de controle;
4. A ratificação do uso exclusivo de uma implementação distribuída;

De posse de tais resultados apresentados e discutidos, pode-se inferir que a primeira hipótese está rejeitada quando se exige alta performance no fornecimento de mecanismos de proteção. Vale ressaltar, que associado ao contexto do peso computacional acarretado pelo protocolo UDP está a fragilidade de ter o mecanismo de proteção associado aos enlaces de dados da DNC. Desta forma, pode haver dano tanto no enlace óptico quanto em algum dos enlaces de administração, o que aumenta o potencial de risco da solução.

Com base nas argumentações apresentadas acima, considera-se inadequada na mesma proporção a hipótese dois. Contudo, deve-se ressaltar que o sistema de controle totalmente distribuído também apresenta restrições.

No caso de soluções que envolvam convergência de topologia usa-se, invariavelmente, algoritmos que realizam constantes trocas de informações na DNC, seja ela *in-bound* ou *out-off bound*. Para tais comunicações, soluções clássicas que envolvem *flooding* de pacotes corroboram a natural degradação de performance quando o número de nós na rede aumenta.

Um exemplo clássico de sistema distribuído na camada IP é o OSPF, que atua num sistema autônomo – AS. Um AS é um grupo conectado de um ou mais prefixos do Internet Protocol administrado por um ou mais operador de rede e que tem uma única e bem definida política de roteamento. Este protocolo é baseado na tecnologia de manutenção dos estados dos seus enlaces e tem sua performance degradada quando o número de nós na rede aumenta. Assim, soluções práticas recomendam como boa prática o número máximo entre quarenta e cinquenta roteadores por sistema autônomo [HALABI, 1996].

Com base em tais restrições, a hipótese quatro também está descartada. Uma solução distribuída confere elegância ao sistema como um todo, mas exige da codificação tratamentos complexos e uso de protocolos que, por mais eficientes que sejam, acabam

criando impedância para atingir alta performance em toda a solução (de redes de pequeno a grande porte).

Assim, com base nos experimentos realizados e nas inspeções lógicas apontadas, conclui-se que a adoção de um modelo híbrido seja a melhor solução para um problema de tamanha complexidade.

A solução mista deverá ter o seguinte conjunto mínimo de requisitos: gerência centralizada com auto nível de segurança e auditoria, controle centralizado parcialmente para o cálculo das rotas e utilização de algoritmos mais elaborados (Algoritmo Genético, Inteligência Artificial, Funções heurísticas etc.), controle distribuído para o mecanismo de proteção a fim de obter a performance desejada e evitar a dependência da rede DNC para este caso.

O desenho de uma solução híbrida está longe de ser trivial e apresenta ser um desafio a ser enfrentado por pesquisadores da área.

8.1 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

As soluções que envolvem redes WDM exigem pesquisas em todos os âmbitos da área que vão dos aspectos físicos dos dispositivos aos detalhes de usabilidade dos softwares associados ao contexto.

Considerando que este estudo foi focado no desenvolvimento de um completo modelo que abordasse as três camadas, serão apresentadas propostas que visem complementar os desenvolvimentos realizados.

Assim, na camada de gerência sugere-se a implementação de uma interface que permita a visualização dinâmica de todos os elementos da rede tanto do ponto de vista do funcionamento individual como interconectados. Associadas a esta interface estariam todas as conexões físicas, suas ocupações com lambdas, suas características operacionais e demais informações que permitissem ao gerente da rede o completo conhecimento de sua utilização.

Na camada de controle poderiam ser acrescentadas funcionalidades que permitissem o gerente escolher os algoritmos a serem utilizados tanto para a definição do caminho, quanto para o preenchimento deste com os lambdas possíveis. Neste contexto, existem inúmeras possibilidades de pesquisa, pois se permite o uso de algoritmos inteligentes, abordagens genéticas, processamentos funcionais e demais estruturas de computação exploradas nesta área.

Em novas pesquisas se pode implementar a solução híbrida apontada como a adequada para permitir o equilíbrio entre uma gerência sólida e segura e a alta performance exigida para redes desta natureza quanto tratamos de mecanismos de proteção e restauração.

As simulações da camada física são um terreno fértil para a área acadêmica. Inicialmente, se propõe a criação de um completo *framework* de simulação de elementos ópticos. Estes componentes de software facilitariam a criação de diversos cenários e também o estabelecimento de testes que são inviáveis economicamente em ambientes que não tenham os elementos simulados.

A reconstrução de toda a arquitetura, numa visão mais abrangente e que envolva uma equipe maior de desenvolvedores é um passo importante a ser tomado. Composições de times de desenvolvimento podem ser realizadas com participantes de todos os níveis acadêmicos e o trabalho conjunto permitirá a geração de uma base de conhecimento que servirá não só para Universidade de Brasília, mas para outras do país que estejam em menor nível de desenvolvimento.

De fato não é fácil construir toda a estrutura proposta de forma aberta, discutida e consolidada por pesquisadores da engenharia elétrica, computação e outros. Contudo, a consolidação de um trabalho dessa natureza pode ser interessante no alinhamento das produções científicas de determinados grupos de pesquisas acadêmicas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMSON N. **The Aloha System - Another Alternative for Computer Communications.** Proceedings of Fall Joint Computer Conference, AFIPS Conference, 1970.

AWDUCHE, Daniel O.; Jabbari, Bijan. **Internet Traffic Engineering Using Multi-Protocol Label Switching (MPLS)**. Elsevier Science B.V, 2002.

CISCO SYSTEMS, Inc. **Internetworking Technologies Handbook** – Chapter 7, 2005.

CISCO SYSTEMS, Inc. **Internetworking Technologies Handbook** – Chapter 9, 2005.

ABBADE, M. L. F.**Contribuição para o Estudo de Não-Linearidades em Fibras Ópticas Monomodo.** 2001.Tese de Doutorado apresentada à FEEC da UNICAMP.

ASO, O. et al. **Efficient FWM based broadband wavelength conversion using a short high-nonlinearity fiber**. [s.l.] IEICE Trans. Electron., vol. E83-C, 2000.

AWDUCHE, D.; REKHTE, **Multiprotocol Lambda Switching: Combining MPLS Traffic Engineering Control with Optical Crossconnects**. IEEE Communications Magazine, 2001.

BANERJEE, A. Et al. **Generalized Multiprotocol label switching: an overview of routing and management enhancements**. IEEE Communications Magazine , v.39, 2001.

___. **Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques**. IEEE Communications Magazine, volume: 39, 2001).

BARROS, A. de J. P. de. **Projeto de pesquisa: propostas metodológicas**. Vozes, Petrópolis, 1990.

BIGGS, N. **Algebraic Graph Theory**. Cambridge University Press, 1974.

BIRD, J.L. **British Patent 285, 738, 1927**

BLACK, U. **Optical Networks – Third Generation Transport Systems**. Prentice Hall. 2002.

BLACK,U. **MPLS and label switching networks**. Prentice Hall, 2001.

BOLLOBÁS, B. **Modern Graph Theory**, Springer-Verlag, 1998.

COMER, Douglas E. and STEVENS, David L.. **Internetworking with TCP/IP Vol II: Design, Implementation, and Internals**. Prentice Hall, New Jersey, 1995.

CRISPIM, H.. et. al. XXI SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES-SBT'04. **Otimização de Alocação de Rotas e Comprimentos de Onda em redes WDM .** Belém - PA, 2004.

DESURVIRE, E.; SIMPSON, J. R.; BEKER, P. C. **High-gain erbium-doped traveling-wave fibre amplifier**. Opt. Lett., no. 12, vol. 11, 1987.

DROZDEK, A. **Estruturas de dados e algoritmos em C++.** São Paulo: Pioneira Thomson Learning, 2005.

DZUBECK, F. **Is it time to re-engineer SNMP?** Network World, 2004.

ELSENPETER, R.. **Optical Networking: A beginner's guide**. McGraw-Hill/Osborne, 2002.

FRENCH, W.G. et al. **Optical waveguides with very low loss**. The Bell System Technical Journal, 1974.

GARRET, C.G.B.; MCCUMBER, D.E. **Propagation of a gaussian light pulse through an anomalous dispersion medium**. Phys. Rev. A, vol. 1970.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas,1999.

GILLNER, L. 22nd EUROPEAN CONFERENCE ON OPTICAL COMMUNICATION, ECOC´96. **Transmission limitations in the all-optical network.** Proceedings of the, paper TuB.2.3, 1996.

GILLNER, L.; LARSEN, C. P.; GUSTAVSSON, M. **Scalability of Optical Multiwavelength Switching Networks: Crosstalk Analysis**. J. of Lightwave Technol., V. 17. 1999.

GILLNER, L. **Scalability of Optical Multiwavelength Switching Networks: Power Budget Analysis**. IEEE Journal on Selected Areas in Communications, 1996.

GODSIL, C. R.,Gordon. **Algebraic Graph Theory**. Springer, 2001.

GODRAN, M.; MINOUX, M. **Graphs and algorithms**. Wiley Interscience,1979.

GODRICH, M. T.; TAMASSIA, R. **Data Structures and Algorithms in Java**. John Wiley & Sons, 2nd edition,1997.

GREEN Jr., P.E.. **Fiber Optic Networks**. Prentice-Hall, 1993.

HAYEE, M.I.; WILLNER, A.E. **NRZ Versus RZ in 10-40 Gb/s dispersion managed WDM transmission systems.** IEEE Photon. Technol. Lett., vol. 11, 1999.

HALABI, SAM. **OSPF Design Guide**. Cisco Systems, Network Supported Accounts Rev: 1.0 April, 1996.

HELD, G. **Ethernet Networks: Design, Implementation, Organization and Management**. Wiley: Fouth Edition., 2005.

IETF-1 CCAMP Working Group**. Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)**, work in progress, 2003.

IETF-2 CCAMP Working Group. **Link Management Protocol (LMP)**, work in progress, 2003.

ITU-T-1 Recommendation G.652. **Characteristics of a single-mode optical fibre cable**. Revision Oct 2000.

ITU-T-2 Recommendation G.653. **Characteristics of a dispersion-shifted single-mode optical fibre cable.** Revision Oct. 2000.

ITU-T-3 Recommendation G.692. **Optical interfaces for multichannel systems with optical amplifiers**. Oct, 1998.

JACOBSON, I.; RUMBAUGH, J.; BOOCH, G. **Unified Software Development Process**. Addison-Wesley, Reading - MA, 1999.

K.__ Y.-J. et al. 22nd EUROPEAN COFERENCE ON OPTICAL COMMUNICATION, ECOC´2000. **Scalability of a metropolitan multifiber bidirectional WDM-ring network**", paper 8.1.4. ,2000.

KAPANY, N.S. **Fiber Optics. VI. Image Quality And Optical Insulation**, J. Opt. Soc. Am., vol. 49, 1959.

___. **Fiber Optics: Principles and Applications.** New York: Academic Press, 1967.

KAPRON, F.P.; KSCK, D. B.; Maurer, R. D. **Radiation losses in glass optical waveguides**. Appl. Phys. Lett., vol. 17, 1970.

KNUTH, D. E. **The Art of Computer Programming**. Addison-Wesley, v. 1, 2, and 3, 3rd edition, 1998.

KOMPELLA, K. **Extensions to IS-IS/OSPF and RSVP in support of MPL(ambda)S**. draft-kompella-mpls-optical-00.txt. 2000.

LANG, J. **Link Management Protocol (LMP)**. Editor - draft-ietf-ccamp-lmp-10.txt. October, 2003.

LEE, D.L. **Electromagnetic Principles Of Integrated Optics**. Krieger Publisinhg Company, 1986.

MANNIE, E. **Generalized Multi-Protocol Label Switching Architecture**. Editor - draft-ietf-ccamp-gmpls-architecture-07.txt – Maio, 2003.

MARCONI, M. de A.; LAKATOS, E. M. **Técnicas de pesquisa**. São Paulo: Atlas,1. ed. 1992.

MARQUES, M. T. M. **Auditoria em bancos de dados relacionais**. Brasília: UNB, 2002.

MEARS, R. J. et al. **Low-noise erbium-doped fibre amplifier operanting at 1.54 µm.** Electron. Lett., no. 23, vol. 19. 1987.

MILO, S. **Análise de desempenho de topologias de amplificadores ópticos a fibra dopada com érbio**. 2003. Dissertação de mestrado. Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação – Campinas.

MIYA, T. et al. **Ultimate low loss single-mode fiber at 1.55 µm**. Electronic Letters. 1979.

MOUFTAH, H. T.; HO, Pin-Han. **Optical Networks – Architectures and Survivability**. Kluwer Academic Publishers, September. 2002.

MURTHY, C. S. R.; GURUSAMY, M**. WDM Optical Networks – Concepts, Design and Algorithms.** Prentice Hall, 2002.

NORTEL NETWORKS. **MPLS and ASTN: Extending multiprotocol label switching for automatically switched transport networking**. White Paper, 2001.

OLIVEIRA, S. L. **Elaboração de projetos de pesquisa científica**. São Paulo: Atlas, 6ª ed. 1998.

PAPADIMITRIOU, D. **Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control**.Editor - draft-ietf-ccamp-gmpls-sonet-sdh-08.txt – August, 2003.

___. **Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration).** draft-ietf-ccamp-gmpls-recovery-analysis-02.txt - Dimitri Papadimitriou (Editor) – September, 2003.

PASTOR, E. et al. **Optical Transparent IP/WDM Network Simulation**. Brasília: IMOC, 2005.

___. **Redes Convergentes: Tecnologias e Protocolos**. Projeto Anatel-UIT/UnB-Finatec, Distrito Federal, Abril 2004.

PAYNE, D.N.; GAMBLING, W.A. **New silica-based low-loss optical fibre**. Electron. Lett., 1974.

PREISS, Bruno R. **Data Structures and algorithms with object-oriented design patters in Java**. New York: John Wiley & Sons, Inc. 1999.

RAJAGOPALAN, B. Et al. **IP over Optical Networks: Architectural Aspects**. Tellium,

Inc. - IEEE Communications Magazine.September, 2000.

RAMAMMURTHY, B. et. al. **Impact of transmission impairments on the teletraffic performance of wavelength-routed optical networks**. Journal of Lightwave Technology, V. 17, 1999.

RAMAMMURTHY, S.; SAHASRABUDDHE, L.; MUKHERJEE, B. Survivable WDM Mesh Networks. **Journal of Lightwave Technology**, vol. 21, no.4, April 2003, pp. 870-883.

RAMASWAMI, R. and SIVARAJAN, K.N. **Optical routing and wavelength assignment in all-optical networks**. IEEE/ACM Trans. Networking, vol. 3, 1995.

___. **Optical Networks, A Pratical Perspective.** San Diego: Academic Press, CA., 1998.

ROCHA, M.L.; et al. X SIMPÓSIO BRASILEIRO DE MICROONDAS E FOTOELETRÔNICA - SBMO. **Experimental characterization of optical nodes in a mesh network**, in Proceedings of., , 2002.

ROSSI, S. M. et al. X SIMPÓSIO BRASILEIRO DE MICROONDAS E FOTOELETRÔNICA – SBMO. **Optical WDM Networks with Distributed IP-Centric Control Plane** . 2002.

ROUSKAS, G. N.; PERROS, H. G. **A tutorial on Optical Networks**. Department of Computer Science, North Carolina State University, Raleigh, NC, USA ,2002.

ROUSSEAU, B. PAPADIMITRIOU, D. **Generalized Multiprotocol Label Switching**. Strategy White Paper, Alcatel, 2003.

SACHS, A.C. **Sistema de Proteção e Restauração, Demonstração de Protótipo de Laboratório**. Campinas: CPqD, 2002.

SATO, K. **Photonic Network Technology Development. Global Optical Communications**._,_, 2002.

SOMANI, Arun K. **Survivability and Traffic Grooming in WDM Optical Networks**. Cambridge University Press, Cambridge, 2006.

STAIR, R. M. **Princípios de Sistemas de Informação – Uma Abordagem Gerencial.** Livros Técnicos e Científicos,. 2ª ed., 1998.

STERN, T. E. and BALA, K. **Multiwavelength Optical Networks**. Addison-Wesley, 1a ed., EUA, 1999.

SUDO, S. **Optical Fiber Amplifiers – Material, Devices, and Applications**. Artech House, 1a ed, EUA, 1997.

THOMPSON, K.; MILLER, G. e WILDER, R. **Wide Area Internet Traffic Patterns and Characteristics** – IEEE Network, November-Dezember, 1997, p.13.

TODIMALA A.;RAMAMURTHY B.A. **Heuristic with Bounded Guarantee to Compute Diverse Paths under Shared Protection in WDM Mesh Networks.** In Proc. of IEEE GLOBECOM, St. Louis, MO, Nov. 2005.

TOMKOS, I. et al. **Mechanisms of wave mixing and polarization sensitivity of the wavelength conversion in semiconductor optical amplifiers using two parallel polarized pumps**. Opt. Commun., vol. 163, 1999.

YAKAMAKA, N.; et al. **GMPLS-based photonic multilayer router (Hikari router) architecture: an overview of traffic engineering and signaling technology**. - IEEE Communications Magazine**,** v.40, 2002.

ZANG, H., J. J.; MUKHERJEE, B. **A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical Networks**. Optical Networks Magazine, January, 2000.

APÊNDICES

A. PADRÕES

A.1. Padrão SONET/SDH

SONET é um padrão de multiplexação e transmissão para sinais de alta velocidade, dentro da infra-estrutura de telecomunicações nos Estados Unidos, e está vigente até nossos dias. Uma tecnologia similar, o SDH (*Synchronous Digital Hierarchy*), tem sido adotado na América Latina, Europa e Japão. Embora SONET e SDH tenham similaridades como a mesma taxa de bit e organização do formato do frame (elemento básico de transmissão); esquemas idênticos de sincronização de *frames*; as mesmas regras de multiplexação e demultiplexação, entre outras, trata-se de dois padrões distintos. Contudo, uma vez que o interesse está nas características de multiplexação e de transmissão desses sistemas, que são idênticas, costuma-se tratá-los como um único sistema denominado SONET/SDH.

A infra-estrutura SONET/SDH foi baseada em Hierarquia Digital Plesiócrona[19] (PDH: *Plesiochronous Digital Hierarchy*), tecnologia implementada em meados dos anos 60, e também conhecida como hierarquia digital assíncrona.

O PDH nasceu focado nos serviços de telefonia pública, especificamente na multiplexação de canais digitais de voz. Esse sistema utiliza a técnica da multiplexação por divisão no tempo (TDM) para formar seus níveis hierárquicos, que são baseados na capacidade de transmissão de canais de 64 kbps.

Um canal de voz analógico com largura de banda de 4 KHz, pelo teorema de Nyquist, deve ser amostrado a 8 KHz no mínimo. Quantizando cada amostra com 8 bits de precisão, se consegue uma taxa de transmissão de 64 Kbps. Nos Estados Unidos uma taxa de 64 Kbps é designada como DS-0 (*Digital Signal* – 0). A Tabela A. 1 apresenta as taxas de transmissão para o PDH.

Tabela A. 1 - Taxas de transmissão para PDH.

Nivel	Estados Unidos	Europa	Japão
0	64 Kbps	64 Kbps	64 Kbps

[19] Plesiócrono significa ”quase síncrono”.

1	1,544 Mbps	2,048 Mbps	1,544 Mbps
2	6,312 Mbps	8,448 Mbps	6,312 Mbps
3	44,736 Mbps	34,368 Mbps	32,064 Mbps
4	139,264 Mbps	139,264 Mbps	97,728 Mbps

A tecnologia PDH apresentou algumas deficiências que levaram ao desenvolvimento de novos padrões como SONET/SDH. Nos processos de multiplexação com PDH, era dificil escolher um *stream* de baixa taxa de dados em relação a um *stream* de alta velocidade, sem passar por um significativo processamento do sinal de alta velocidade, que era derivado da maneira como os *streams* de baixa velocidade eram multiplexados. Em PDH, os níveis estabelecidos não são múltiplos inteiros de 64 Kbps. Assim, não existe um sincronismo perfeito destes *streams* e bits adicionais são necessários para aliviar retardos entre os diferentes *clocks*.

Devido às suas características de multiplexação, bem como uma falta de padronização adequada para a interoperabilidade dos padrões que surgiram, o próprio PDH fez despertar interesses por um novo padrão de transmissão e multiplexação que pudesse resolver tais dificuldades.

Pelo exposto, conclui-se que os sistemas SONET/SDH surgiram com uma melhor alternativa ao PDH. Dentre as melhorias em vários aspectos, se pode destacar:

— Multiplexação: em PDH, devido à forma como os canais de baixa velocidade são multiplexados, torna-se muito difícil extraí-los quando estão multiplexados em hierarquias superiores (canais com taxas de transmissão mais elevadas), sendo necessário desmontar toda a hierarquia para o sucesso da extração. Além disso, a necessidade de se preencher os *slots* com *bits* extras, responsáveis por acomodar a discrepância entre os diferentes relógios de cada tributário, torna os Mux/Demux PDH relativamente complexos. Nos padrões SONET/SDH, conforme descrito a seguir, emprega-se um esquema de multiplexação muito mais sofisticado, o qual facilita a extração de canais de baixa velocidade dos canais de alta velocidade.

SONET/SDH define métodos de multiplexação explícita para que todos os clocks na rede sejam perfeitamente sincronizados a um único *master clock.* Desta forma, a implementação de um Mux/Demux SONET/SDH é muito mais simples de ser realizada, quando comparada com a dos equivalentes PDH.

— Utilização da banda: no padrão PDH, o *time slot* designado ao estabelecimento de uma conexão permanecerá exclusivo ao transporte de dados desta única conexão durante todo o tempo em que ela se mantiver ativa (funcionalidade característica de um sistema determinístico).

Entretanto, como os dados não fluem continuamente durante a conexão, uma subutilização de banda é acarretada nesses sistemas. Já nos padrões SONET/SDH, os dados são mapeados dentro de um conjunto específico de *bytes* (designado *synchronous payload envelope* – SPE), aos quais é acrescido um cabeçalho responsável pela sua identificação e seu endereçamento. Dessa forma, se pode alocar os dados em diferentes pontos dentro do *frame*, o que ocasiona um uso muito mais eficiente de banda.

— Interoperabilidade: devido a não padronização de um formato em nível de transmissão (códigos de linha, interfaces ópticas e outros), os sistemas PDH de diferentes fabricantes encontravam bastante dificuldades para a conexão de seus equipamentos via enlaces de transmissão. Contudo, nos sistemas SONET/SDH, dada uma única padronização para suas interfaces ópticas, tornou-se bem mais facilitada a interoperabilidade (em nível de transmissão) entre equipamentos de diferentes fabricantes. Apesar disso, aspectos como os canais de comunicação para o gerenciamento da rede ainda não foram padronizados, mantendo a interconexão um tanto difícil.

— Gerenciabilidade: ao contrário do padrão PDH, o SONET/SDH utiliza informações de gerenciamento para a monitoração da performance do tráfego.

De forma diferente do PDH, SONET/SDH acrescenta informação de gerência para monitoramento de performance de tráfego e padronizam interfaces ópticas para permitir interoperabilidade entre equipamentos de diferentes fabricantes. Nos aspectos relativos a

rede, tem-se evoluído para topologias e esquemas de proteção específicos. Como conseqüência, o tempo de restauração do serviço após falha é menor a 60 ms, que em PDH eram da ordem de alguns segundos e até minutos (RAMASWAMI, 1998).

O SONET/SDH usa um sofisticado esquema de multiplexação. Um *stream* PDH é mapeado num SPE (*Synchronous Payload Envelope* ou *Synchronous Container* em SDH). Um conjunto de bytes de cabeçalho, denominado *path overhead,* permite monitorar o *stream* fim-a-fim; quando adicionados ao SPE, formam um tributário virtual (VT: *Virtual Tributary*), ou contêiner virtual (VC: *Virtual Container*). O termo virtual é aplicado porque o contêiner pode estar em diferentes pontos dentro de um *frame*. Um *frame* tem 125 μs de duração, correspondente aos 8 KHz de amostragem do circuito de voz.

Na estrutura hierarquica de multiplexação, VTs têm sido definidos em quatro tamanhos: VT1.5, VT2, VT3 e VT6 que transportam 1,5, 2, 3 e 6 Mbps. Para SONET, a taxa básica é de 51,84 Mbps, chamado de STS-1 (*Synchronous Transport Signal Level 1*). Sinais de alta taxa (STS-n) são obtidos por *interleaving* dos bytes de n STS-1. Para SDH, a taxa básica é 155 Mbps, e é denominada STM-1 (*Synchronous Transport Module-1*).

Quando é necessário mapear sinais não-SONET, por exemplo, 150 Mbps ATM, sinais STS-N_c com um *payload* fechado são definidos no padrão. Vale ressaltar que tais sinais não podem ser demultiplexados em *streams* de baixa velocidade. Desta forma, sinais ATM a 150 Mbps são mapeados em sinais STS-3_c.

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

Assim, a interface óptica correspondente a STS-3 é o OC-3, para STS-12, STS-48, STS-192, tem-se definidas OC-12, OC-48 e OC-192. As taxas de operação SONET/SDH são mostradas na Tabela A. 2.

Tabela A. 2 - Taxas de transmissão para SONET/SDH

Sinal SONET	Sinal SDH	Taxa de bits (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.1.1. Elementos da infra-estrutura SONET/SDH

As redes SONET/SDH utilizam dois elementos fundamentais para a realização de multiplexação, demultiplexação e roteamento. São eles: o *Digital Crossconnect* (DCS) e Add/Drop Multiplexer (ADM). A função dos DCSs é demultiplexar, rotear e remultiplexar os sinais que chegam a ele. Os ADMs realizam as mesmas operações que os DCSs, diferenciando-se apenas por possuírem duas portas para conexão entre nós, em detrimento aos DCSs, os quais são formados por mais de duas.

Na prática, dispõe-se basicamente de três tipos essenciais de configurações de rede: ponto-a-ponto, linear e anel. As primeiras redes foram implantadas na forma ponto-a-ponto. Posteriormente, com a necessidade de se extrair ou adicionar um ou mais canais de um feixe de alta velocidade, *Add/Drop multiplexers* (ADMs) foram inseridos no meio de enlaces ponto-a-ponto, formando as configurações lineares. Contudo, a necessidade de permanecer disponibilizando serviços quando da ocorrência de falhas, vinculada à simplicidade do modelo anel, que pode prover meios de neutralizar alguns tipos de falhas, fez desta topologia a configuração mais adotada pelos padrões SONET/SDH.

Novos componentes estão amadurecendo, como é o caso dos *crossconnects* que, quando conectados aos ADMs, não só fornecem conectividade entre anéis, como também podem fazer parte do mesmo.

A.2. Interconexão de Computadores

Diferentemente das redes SONET/SDH descritas no tópico anterior, as redes de computadores são encontradas principalmente no ambiente corporativo. Elas têm como principais características à utilização de componentes ópticos de baixo custo operando a taxas de *bits* modestas, além de não apresentarem qualquer mecanismo de proteção contra falhas. Desta forma, depende-se da camada óptica para suprir tal tarefa.

A seguir, serão descritos de forma sucinta três padrões de redes comumente empregados na interconexão de computadores entre si e/ou com seus periféricos (por exemplo, unidades controladoras de terminais, discos rígidos, impressoras etc.)

A.2.1. ESCON (Enterprise Serial Connection)

Padrão criado pela IBM (*Internacional Business Machine*) a fim de substituir as interfaces de entrada e saída de baixa velocidade, que usavam fios de cobre, por interfaces ópticas. Esta tecnologia é usada principalmente em ambientes à base de *mainframes*, os quais chegam a possuir centenas de canais ESCON de entrada e saída, e que podem ser ligados a outros mainframes ou a dispositivos periféricos.

A taxa de transmissão por cada canal ESCON é de 200 Mbps. Para enlaces de transmissão com distância inferior a 3 Km, é possível a utilização de LEDs operando em fibras multimodo na janela de 1310 nm. Para distâncias de 20 Km ou superiores, mantendo a taxa de transmissão no mesmo valor, recomenda-se o uso de lasers juntamente com fibras monomodo.

A.2.2. Fiber Channel

Fiber Channel é um padrão desenvolvido para ser usado nas mesmas aplicações que o ESCON, porém com maiores taxas de transmissão de dados úteis (200, 400 e 800 Mbps). Na taxa de 800 Mbps, são utilizados lasers operando a 1310 nm em fibras monomodo, mesmo para distâncias curtas.

A.2.3. HIPPI (High Performance Parallel Interface)

HIPPI é um padrão de interface paralela de entrada e saída que, anteriormente ao surgimento do *Fiber Channel*, fora desenvolvida para operar a 800 Mbps. Contudo, devido a possíveis variações no relógio de sincronismo, sua distância máxima ficava limitada a apenas 25m. Para transmissão em distâncias superiores, seus dados eram serializados e transmitidos sobre fibras monomodo.

Dado tal limitação, um novo padrão, designado Serial HIPPI foi recentemente definido para suprir tal propósito. Nele os dados já são serializados na própria interface e são transmitidos em fibra monomodo a 1,2 Gbps, após a codificação de linha.

A.3. Redes Locais (LAN) e Metropolitanas (MAN)

A.3.1. FDDI (Fiber Distributed Data Interface)

FDDI é um padrão para redes metropolitanas, o qual opera a taxas de 100 Mbps, possui topologia comumente implementada na forma de anel de duas fibras e, assim como SONET/SDH, também incorpora mecanismos de proteção. Ele é considerado como uma extensão do padrão *Token Ring* para redes locais, sendo adotada uma maior velocidade de transmissão e meios ópticos para tal.

Visto que fora desenvolvido com o intuito de se obter implementações de baixo custo, as especificações padrões adotam LED´s operando em 1310nm sobre fibras multimodo e fotodiodos PIN na recepção, limitando o comprimento máximo entre duas estações a 2 Km. Entretanto, distâncias maiores (tais como 40 Km) podem ser atingidas, bastando para isso a utilização de fibras monomodo e lasers.

A.3.2. ATM (Asynchronous Transfer Mode)

Tradicionalmente, as redes de comunicações apresentaram-se especificamente voltadas ou para a comunicação de voz ou para a comunicação de dados. Mesmo com o advento da tecnologia digital na infra-estrutura pública de telefonia, esta continua a disponibilizar seus recursos e esforços a fim de fornecer padrões de serviços compatíveis com os exigidos pela transmissão de voz.

ATM surgiu, pois, como um padrão de rede capaz de permitir a convergência de uma variedade de serviços, tais como: serviços de faixa estreita e de faixa larga; síncrono e assíncrono, em tempo real ou não. Desta forma, esta tecnologia possibilitou a tão esperada integração das redes de voz e de dados.

O modo de transmissão assíncrono, como o próprio nome sugere, provém do fato de que as informações geradas numa determinada origem chegam ao sistema assincronamente, ou seja, os intervalos de tempo entre as unidades de informação são irregulares. Entretanto, embora possa parecer que a rede em si irá operar de uma forma assíncrona, internamente, a comunicação se procede de forma síncrona, o que acarreta a necessidade da utilização de *buffers* nos nós comutadores ATM.

Toda a informação a ser transportada pela rede é agrupada em forma de pacotes (ou células) de tamanhos fixos, formados por 53 bytes, dentre os quais 5 constituem o campo de cabeçalho (responsável principalmente pelo endereçamento do pacote e pela identificação da classe de serviço pretendida pela requisição), e 48 o campo de informação propriamente dito.

O tamanho dos pacotes ATM é o resultado de um compromisso entre as necessidades conflitantes das aplicações de voz e de dados, visto que a utilização de pacotes pequenos torna-se preferível à transmissão de voz, pois seriam entregues com pequenos atrasos, enquanto, caso se utilize pacotes grandes, a transmissão de dados passa a ser a beneficiada, tendo em vista uma melhor relação de aproveitamento do campo de informação frente ao campo de cabeçalho. Além desse fato, o tamanho fixo do pacote é particularmente vantajoso, dado uma maior facilidade para o desenvolvimento de comutadores de baixo custo e de alta velocidade.

Tipicamente, a conectividade ATM entre dois assinantes quaisquer consiste basicamente da identificação de um caminho virtual (*Virtual Path* – VP), agindo como enlaces virtuais entre os nós, e de um canal virtual (*Virtual Channel* – VC), responsável por suportar cada conexão fim-a-fim. Essas identificações encontram-se no campo de cabeçalho e são identificadas por VPI e VCI, respectivamente. Cada VP é dimensionado de forma a transportar vários VCs multiplexados. A comutação da informação se processa da seguinte forma: os nós comutadores possuem uma tabela que é atualizada todas as vezes

que uma conexão do circuito é ativada ou desativada. Dessa forma, ao chegar uma célula no comutador por uma determinada porta de entrada, de acordo com os valores presentes nos campos VPI e VCI e da informação contida na tabela de roteamento, esta célula será encaminhada para uma determinada porta de saída com novos valores de VPI e VCI, os quais serão utilizados pelo próximo nó comutador.

Uma das grandes vantagens da tecnologia ATM é sua habilidade de dispor de serviços de diferentes classes (taxa de *bit* constante ou não, em tempo real ou não, etc.) e com diferentes garantias de qualidade de serviços (perda de células, atrasos, etc.), os quais pertencem a um conjunto de parâmetros a serem negociados.

Para que possam ser oferecidos os serviços, a rede ATM faz uso das características *a priori* da conexão pretendida (por exemplo, a taxa média e de pico de envio de células), vinculado ao comprometimento da rede em assegurar tal serviço. Essa função é desempenhada por um algoritmo chamado de controle de admissão de conexão (CAC), que é capaz de bloquear novas conexões quando necessário, a fim de satisfazer os requisitos de qualidade de serviço garantidos às conexões presentes no momento de seus estabelecimentos.

Mesmo com as diversas vantagens da utilização do padrão ATM, sua disseminação está sendo mais lenta do que o esperado, sendo uma das grandes razões a concorrência de outros padrões. Neste caso, se pode citar, no âmbito das redes de longa distância, a utilização do padrão IP (*Internet Protocol*).

O padrão IP, além de continuar a ser suficiente para dar suporte à grande maioria das aplicações atuais, está evoluindo para prover as mesmas funcionalidades que o ATM. No âmbito das redes locais, a concorrência vem do surgimento de novas redes LAN´s, bem como da evolução de alguns padrões já amplamente estabelecidos, como as versões a 100 Mbps e 1 Gbps da Ethernet.

A.4. IP (Internet Protocol)

Atualmente, o protocolo IP é a tecnologia de rede mais utilizada nas redes de longa distância. Uma das razões para o seu grande sucesso deve-se ao fato de ter sido projetada

para operar sobre uma grande variedade de camadas inferiores; estas, designadas camadas de enlaces de dados na arquitetura clássica de camadas OSI (*Open System Interconnection*) da ISO (*International Standardization Organization*). Algumas dessas camadas de enlace de dados sobre as quais o IP opera estão associadas aos padrões de redes locais mais populares, tais como Ethernet e *Token Ring*; aos padrões de redes metropolitanas, por exemplo, FDDI, como também aos protocolos destinados à operação sobre linhas alugadas de operadoras públicas, como é o caso do HDLC (*High Level Data Link Control*).

Um dos mais conhecidos protocolos da camada de transporte, o qual atua diretamente sobre o IP, é o TCP (*Transmission Control Protocol*), razão pela qual essas redes são comumente conhecidas como TCP/IP.

Quando comparada ao ATM, o qual provê uma comutação de pacote no modo de circuito virtual, o protocolo IP fornece para suas camadas superiores apenas serviços em modo datagrama. Esse tipo de serviço, embora seja mais simples do ponto de vista de processamento nos nós, não se compromete a entregar os pacotes de dados, como também não apresenta qualquer preocupação no que se refere à ordenação entre os pacotes entregues.

Como fora concebido com o propósito voltado para a comunicação de dados, os pacotes IP são de tamanhos variáveis e geralmente muito maiores quando comparados aos ATM. Portanto, quando uma rede IP estiver fazendo uso de uma rede ATM como sua camada imediatamente inferior, seus pacotes de tamanhos variáveis deverão, no lado da transmissão, serem segmentados em tamanhos fixos correspondentes aos da célula ATM e reagrupados, no lado da recepção, a fim de que os pacotes IP originais possam ser devidamente entregues.

A rede IP é formada por roteadores com função de examinar os pacotes recebidos, reconhecer os endereços de destino, compará-los com o conteúdo presente numa tabela de roteamento que fica armazenada no próprio roteador, e repassar o pacote para a saída apropriada. Devido à característica altamente dinâmica da Internet, a qual é composta de inúmeras redes individuais, cuja forma de interconexão e a própria topologia estão sob freqüente mudança, os roteadores IP possuem a capacidade de criar tabelas de roteamento que se ajustam automaticamente em decorrência de mudanças nas topologias das redes.

Estas mudanças são causadas tanto por falhas nos enlaces e/ou nos próprios equipamentos, quanto pela adição ou remoção de fibras ou comprimentos de onda entre roteadores.

Como dito anteriormente, o protocolo IP, embora seja o mais utilizado nas redes de longa distância, não possui qualquer garantia de qualidade de serviço (QoS - *Quality of Service*). Contudo, com o crescimento explosivo do tráfego de serviços de Internet, tanto os usuários quanto os operadores das redes têm sentido a necessidade de serviços que disponham dessas garantias. Este fato vem gerando um grande esforço entre os desenvolvedores do padrão IP no sentido de acrescentar tais funcionalidades a ele. Assim, protocolos como o RSVP (*Resource Reservation Protocol*) têm sido desenvolvidos para tal. Uma outra alternativa é simplesmente manter o protocolo existente e aumentar a largura de banda disponível e a velocidade dos roteadores, de modo a assegurar a taxa de transmissão do usuário.

A.5. Arquitetura de uma rede IP Fotônica

Uma arquitetura de rede híbrida, chamada de arquitetura de rede IP Fotônica (YAMANAKA, 2002), combina comutadores ópticos e eletrônicos (de pacotes) num só comutador para acomodar flexivelmente o tráfego. Aqui, o roteador integrador ou roteador MPLS fotônico (MPΛS) é o elemento principal da rede. Assim, comprimentos de onda são usados como rótulos, acomodando pacotes IP que trafegam pela mesma rota e o roteador MPΛLS comuta os caminhos ópticos.

Esta proposta de arquitetura visa conjugar a alta capacidade oferecida pela comutação óptica, com o eficiente uso de recursos de rede e a granularidade oferecida pela comutação de pacotes (eletrônica), que comuta pacote por pacote. Roteadores IP (MPLS) reconhecem roteadores MPLS fotônicos e integram operações de roteamento e sinalização. A gerência e controle da rede são feitos com um plano de controle com sinalização estendida GMPLS [YAKAMAKA, 2002]. A Figura A. 1 apresenta este cenário.

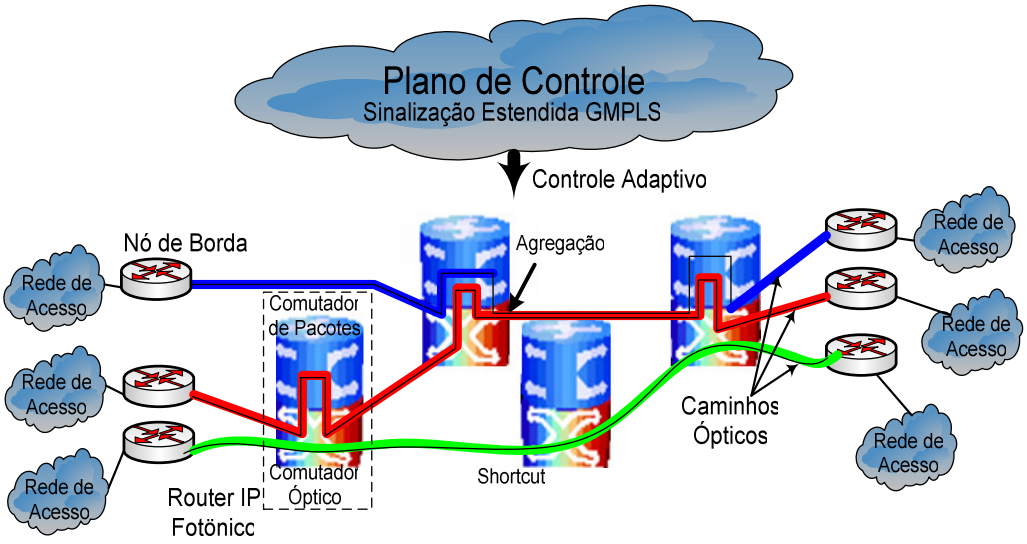

Figura A. 1 - Rede Fotônica IP

Estas duas funções de comutação devem ser usadas dinamicamente de acordo com o estado e tráfego na rede, sendo estabelecido um caminho óptico direto entre nós de borda quando transportado um alto volume de tráfego. Quando o tráfego é menor, é estabelecido um caminho salto-por-salto, com operação dos roteadores de pacotes, principalmente em operações de agregação e distribuição de tráfego sobre caminhos ópticos. Esses processos são gerenciados pelo plano de controle. O controle e gerência do trafego IP precisa da incorporação deste plano de controle, fisicamente desagregado do plano de transporte, encarregado dos processos de roteamento, sinalização e gerência na rede WDM (RAJAGOPALAN, 2000).