UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE SEMICONDUTORES, INSTRUMENTOS E FOTÔNICA

DISSERTAÇÃO DE MESTRADO

Análise de Tráfego, Capacidade e Proteção em Redes de Pacotes Ópticos com Chaveamento Fotônico

Indayara Bertoldi Martins
Orientador: Prof. Dr. Edson Moschim
Co-orientador: Dr. Felipe Rudge Barbosa

Campinas, SP – Brasil
Setembro - 2007

UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE SEMICONDUTORES, INSTRUMENTOS E FOTÔNICA

DISSERTAÇÃO DE MESTRADO

Análise de Tráfego, Capacidade e Proteção em Redes de Pacotes Ópticos com Chaveamento Fotônico

Dissertação apresentada à Faculdade de Engenharia Elétrica
e de Computação da Universidade Estadual
de Campinas, como parte dos requisitos exigidos
para a obtenção do título de Mestre em Engenharia Elétrica.

Indayara Bertoldi Martins
Orientador: Prof. Dr. Edson Moschim
Co-orientador: Dr. Felipe Rudge Barbosa

Banca Examinadora (prevista):
Prof. Dr. Edson Moschim – (presidente)
Prof. Dr. Iguatemi Fonseca (UFERSA-RN)
Prof. Dr. Marcelo Abbade (PUC-Campinas – SP)
Prof. Dr. Yuzo Iano (FEEC/Unicamp)
Prof. Dr. Furio Damiani (FEEC/Unicamp)

Campinas, SP – Brasil
Setembro - 2007

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

Martins, Indayara Bertoldi
M366a Análise de tráfego, capacidade e proteção em redes de pacotes ópticos com chaveamento fotônico / Indayara Bertoldi Martins. --Campinas, SP: [s.n.], 2007.

Orientadores: Edson Moschim, Felipe Rudge Barbosa.

Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Telecomunicações. 2. Análise de redes (Planejamento). 3. Topologia. 4. Interconexão de redes (Telecomunicações). 5. Telecomunicações – Proteção. I. Moschim, Edson. II. Barbosa, Felipe Rudge. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Título em Inglês: Analysis of traffic, capacity and protection in optical packet networks with photonic switching
Palavras-chave em Inglês: Photonic switching, Topology of optical network, Network protection
Área de concentração: Telecomunicações e telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Marcelo Abbade, Yuzo Iano, Furio Damiani
Data da defesa: 12/9/2007
Programa de Pós-Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidata: Indayara Bertoldi Martins

Data da Defesa: 12 de setembro de 2007

Título da Tese: "Análise de Tráfego, Capacidade, e Proteção em Redes de Pacotes Ópticos com Chaveamento Fotônico"

Prof. Dr. Felipe Rudge Barbosa (Presidente): _____

Prof. Dr. Iguatemi Eduardo da Fonseca: _____

Prof. Dr. Marcelo Luis Francisco Abbade: _____

Prof. Dr. Yuzo Iano: _____

Prof. Dr. Furio Damiani: _____

Resumo

Neste trabalho investigamos o desempenho de redes ópticas avançadas, em particular redes de chaveamento de pacotes ópticos (*Optical Packet Switching Network*-OPSN), constituídos por arquiteturas com topologias em malha e nós ópticos sem armazenador. Utilizou-se distribuição de tráfego uniforme, na qual todos os nós geram a mesma quantidade de tráfego para todos os outros nós. Foram avaliados vários parâmetros de redes OPSN, principalmente número médio de saltos e capacidade efetiva da rede, bem como comparações entre topologias anel e malha, considerando como parâmetros principais vazão e desempenho, e os impactos causados por falhas de enlaces. Demonstrou-se também que o aumento do número de nós em OPSNs, não necessariamente aumenta o desempenho ou capacidade.

Palavras-chave: Chaveamento Fotônico, Topologia de Rede Óptica, Proteção de Redes.

Abstract

In this work we have investigated the performance of advanced optical networks, more specifically optical packet switched networks (OPSN), with architectures comprising fully connected mesh topologies and optical bufferless nodes. We have adopted uniform traffic distribution, in which all nodes generate the same traffic to every other node. Several parameters of the OPSNs have been evaluated, mainly average number of hops and effective network capacity, as well as comparisons between the ring and mesh network topologies, considering as main parameters the network throughput and performance, and the impacts caused by failures of links. We demonstrate that increasing the number of nodes in OSPNs does not necessarily increase performance or capacity.

Keywords : Photonic Switching, Topology of Optical Network, Network Protection**.**

Ninguém é tão grande que não possa aprender,
nem tão pequeno que não possa ensinar.

AGRADECIMENTOS

Foram muitas as pessoas que de alguma forma contribuíram para que eu pudesse concluir este trabalho, de grande importância para mim.

Agradeço primeiramente aos meus pais e irmãos que sempre apoiaram e acreditaram em mim, principalmente nos momentos de dificuldades, sempre me dando força e coragem para enfrentar os obstáculos da melhor forma possível.

Agradeço também a todos os amigos do LE-25 que conheci e convivi durante esses 2,5 anos em especial: Luiz Bonani Juliana Batista, Jackson, Celso, Lídia, Kleber, Hudson, Carol, Érika, Mariana que foram os mais presentes e me apoiaram e me ajudaram de alguma forma.

Agradeço muito também ao prof Marcelo Abbade que foi quem me indicou e me incentivou a iniciar o mestrado, além de ter sido um ótimo professor no curso de graduação.

E para finalizar, quero agradecer infinitamente aos meus orientadores Edson Moschim e Felipe Rudge que me ensinaram conduzir este trabalho de forma adequada. Agradeço até os puxões de orelha que levei, pois foram merecidos e úteis para a conclusão deste trabalho.

Enfim, agradeço a Deus por ter me dado saúde e perseverança, possibilitando assim realizar todas as etapas não só deste trabalho, mas de toda minha vida.

Sumário

Lista de Figuras

LISTA DE ACRÔNIMOS

ATM : Modo de Transferência Assíncrono - (*Asynchronous Transfer Mode*);

CATV: TV a cabo - (*Cable TV*);

CBR: Taxa Constante de Bit – (*Constant Bit Rate*);

DR : Roteamento por deflexão – (*Deflection Routing*) ;

DWDM: Multiplexação densa por comprimento de onda – (*Dense Wavelength Division Multiplexing*);

DPP: Proteção de caminho dedicado- (*Dedicated path Protection*);

FDM: Modulação por divisão de freqüência – (*Frequency Division Modulation*);

FDL: Linha de atraso de fibra – (*Fiber Delay Line*);

FNT: Fundo Nacional de Telecomunicações;

FW: *Floyd-Warshall*;

FPP: Fração de Perda de Pacotes;

ISO: *International Standard Organization*;

IP: Protocolo Internet;

KEOPS: *Keys to Optical Packet Switching;*

LAN: Rede de área local – (*Local Area Network*);

MAN: Rede de área metropolitana – (*Metropolitan Area Network*);

MPLS: *Multiprotocol Label Switching;*

MS: Topologia *Manhattan Street* ;

MTBF: Tempo Médio entre falhas - (*Mean Time Between Failures*);

MTTR: Média de tempo para reparo - (*Mean Time to Repair*);

NS: *Network Simulator®;*

OCDM: Multiplexação por divisão de código óptico-(*Optical Code Division Multiplexing);*

OPS: Chaveamento de pacote óptico – (*Optical packet Switching*);

OBS: Chaveamento de rajada óptica - (*Optical Burst Switching*);

OPSN: Redes de chaveamento de pacotes ópticos – (*Optical Packet Switching Network);*

OSI: *Open System Interconnection*;

OSPF: Primeiro menor Caminho aberto – (*Open Shortest Path First);*

OTDM: Multiplexação óptica por divisão de tempo– (*Optical Time Division Multiplexing);*

PCIC: Pacote de tamanho Constante e Intervalo entre pacotes Constante;

PCIV: Pacote de tamanho Constante e Intervalo entre pacotes Variável;

PDH: *Plesiochronous Digital Hierarchy*;

P-Cycles: Proteção de p-ciclos pré configurados;

PR: Restauração de Caminho- (*Path Restoration*);

QoS: Qualidade de Serviço - (*Quality of Service*);

RF: Rádio Freqüência ;

RV: Variável aleatória – (*Random Variable*);

SCM: *Subcarrier Multiplexing* ;

SDH: Hierarquia Digital Síncrona-(*Synchronous Digital Hierarchy)* ;

SF: Armazena e encaminha – (*Store-and-Forward*);

SONET: Rede Óptica Síncrona **-***(Synchronous Optical Network)*;

SP: Proteção de enlaces - (*Span Protection*);

SBPP: Proteção por compartilhamento de caminho sobressalente -(*Shared Backup Path Protection*);

SR: Restauração de enlaces - (*Span Restoration*);

TTL: Tempo de vida - (*Time to live*);

UDP: Protocolo de Datagramas de Usuário -(*User Datagram Protocol)*;

WAN: Rede de Área Ampla -(*Wide Area Network)*;

WDM: Multiplexação por divisão de comprimento de onda - (*Wavelength Division Multiplexing)*;

1. Introdução

Conforme a cronologia da evolução das comunicações no mundo [1.1], pode-se ver que cada um dos últimos três séculos foram marcados por um tipo de tecnologia. O século XVIII foi a época dos grandes sistemas mecânicos, que levaram à Revolução Industrial. O século XIX foi a era das grandes invenções, da descoberta da eletricidade, em particular, o início das telecomunicações, com a invenção do telégrafo e do telefone.

No campo das comunicações e da informação, houve grandes conquistas tecnológicas no século XX. Dentre outros desenvolvimentos, vimos a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento da indústria de computadores e o lançamento dos satélites de comunicação.

A fibra óptica é também outra inovação revolucionária, surgida no final do século XX. Essa tecnologia das comunicações e da informação permite a transmissão rápida e simultânea de milhares de chamadas telefônicas e dezenas de imagens por um filamento de vidro, sílica, microscópica de altíssima transparência e com espessura do fio de cabelo humano. Para se ter uma idéia de seu impacto, um cabo de fibra óptica (com apenas uma dúzia de fibras em seu interior) pode substituir até milhares de cabos coaxiais de cobre (pesando e custando muito menos).

Com o crescimento de tráfego, o aparecimento de novos serviços e o avanço tecnológico [1.2], surge a necessidade de melhorar a velocidade de processamento e transporte da informação a qual é transportada nas redes, sejam elas ópticas, sem fio, ou até mesmo a cabo.

Com o atual cenário das telecomunicações, pode-se antecipar que se trata de uma tarefa difícil para as empresas de tecnologias oferecerem serviços aos seus usuários com qualidade de serviço (QoS), ou seja, um serviço que tenha confiabilidade, segurança, integridade, e rapidez a um custo operacional que esteja ao alcance de seus clientes.

Foi com vista neste cenário que vem provocando novos desafios para o desenvolvimento tecnológico das comunicações ópticas, que surgiu a idéia de trabalhar com redes de chaveamento de pacotes ópticos (*Optical Switching Packet Network*- OPSN) e mecanismos de proteção e sobrevivência de serviços [1.3].

As redes fotônicas permitem baixa latência e grande banda passante, proporcionando um ambiente favorável ao crescimento da Internet e a proliferação de aplicações cada vez mais sofisticadas que exigem maior desempenho da rede [1.2][1.4][1.5]. As aplicações, tais como os jogos interativos, os programas de compartilhamento de arquivos e as conferências de áudio e vídeo, entre outras, estão presentes no cotidiano de praticamente todos os usuários de computadores que utilizam a Internet. Além da necessidade de maior disponibilidade de banda e de baixo atraso de transmissão, existe também uma tendência para que estas aplicações apresentem um comportamento cada vez mais dinâmico, modificando ao longo do tempo o conjunto de origens e destinos de tráfego na rede para uma única instância de aplicação [1.6].

Na próxima seção iremos mostrar os marcos mais importantes da evolução das comunicações ópticas no mundo e no Brasil.

1.1. Evolução das Comunicações ópticas

As idéias para Comunicações Ópticas como conhecemos hoje, surgiram na década de 60. Nesta data o Brasil apenas assistia os avanços internacionais nas pesquisas em óptica e fotônica.

Procurava-se, principalmente uma tecnologia alternativa para otimizar os sistemas de comunicação quanto à sua capacidade, custo e confiabilidade. A transmissão de dados por sinais luminosos através da fibra óptica era uma firme candidata a substituir gradualmente, muitos sistemas baseados em fios de cobre ou microondas.

Havia duas limitações que impediam o deslanche das comunicações ópticas: as grandes perdas de luz que as fibras ópticas apresentavam durante a transmissão e o excessivo calor que os lasers geravam. Em 1970, estas limitações foram vencidas nos Estados Unidos pela empresa *Corning* onde foi fabricada a primeira fibra óptica com perda de luz suficientemente baixa para viabilizar a comunicação e nos laboratórios *Bell*, onde foi desenvolvido um laser que operava continuamente à temperatura ambiente. Em 1970, *Kapron e Kech*, da *Corning Glass Works* , nos Estados Unidos, anunciaram a fabricação de centenas de metros de fibra óptica de sílica do tipo monomodo com atenuação inferior a 20dB/Km, que foi um marco fundamental na história das comunicações ópticas. Na década de 80 conseguiu transmitir pela fibra a distância mais longas e com perdas de 0,25 dB/Km e somente na década de 90 com a chegada dos amplificadores ópticos e o desenvolvimento da optoeletrônica de alta velocidade, é que foi viabilizada a transmissão óptica. Nesta mesma década e ínicio de 2000, ainda vieram as tecnologias *Dense Wavelength Division Multiplexing* (WDM) e *Dense Wavelength Division Multiplexing* (DWDM). Desde então os estudos referentes a transmissão óptica são direcionados e focalizados para um sistema que seja inteiramente fotônico.

A seguir os marcos em nível mundial serão apresentados resumidamente, e depois serão apresentados os marcos no Brasil, que é de nosso interesse.

Evolução por década mundialmente

Década de 70

- Melhoria da tecnologia do laser semicondutor;
- Aparecimento e melhoria da tecnologia da fibra;
- Primeiros sistemas *Plesiochronous Digital Hierarchy* (PDH);

Década de 80

- Uso das janelas de 850 e 1300 nm;
- PDH até 560 MB/s e desenvolvimento do *Synchronous Optical Network* (SONET);
- Sistemas de longa distância e 1° sistema submarino;

- Desenvolvimento da janela de 1550 nm;
- Aparecimento do amplificador óptico a fibra;
- Sistemas WDM de baixa densidade;

Década de 90

- Uso das janelas de 1300 e 1550 nm;
- Criação do *Synchronous Digital Hierarchy* (SDH) e evolução das taxas de 155 MB/s até 10 GB/s;
- Fibra no acesso, em *Cable TV* (CATV) e em *Local Area Network* (LAN);
- Uso em larga escala de DWDM em longa distância;
- Proliferação de sistemas submarinos;

Década de 2000

- DWDM metropolitano e no acesso;
- Interfaces de transporte DWDM abertas para: SDH/SONET, PDH, *Asynchronous Transfer Mode* (ATM), *Internet Protocol* (IP), Gigabit Ethernet, etc. Taxas até 40 GB/s;
- Nascimento da Camada óptica;

O Brasil deu início as comunicações ópticas no governo militar, instituído pelo golpe de 1964, que criou mecanismos institucionais e destinou fundos para viabilizar as pesquisas no país. Foram criadas instituições governamentais, como a Embratel e o Fundo Nacional de Telecomunicações (FNT). Em novembro de 1972, foi criada a Telebrás (Telecomunicações Brasileiras, S.A), que passou a controlar todas as operadoras e com isto possibilitou a padronização da tecnologia usada para a comunicação entre as cidades e estados. Com isto, a situação das telecomunicações brasileiras era de melhoria contínua.

Os principais marcos históricos do desenvolvimento das comunicações ópticas ocorridas no Brasil foram:

- 1964 – Início das pesquisas;

- 1972 – Criação de instituições governamentais;
- 1973-75 - Lab. Laser e Lab. Fibras Óticas (Unicamp)/Telebrás;
- 1978-1980 - Lab. Laser e Lab. Fibras Óticas (CPqD)/Telebrás;
- 1982 - Primeiro Teste de Campo (Cetel-RJ)/Telebrás;
- 1991 - Primeiro Entroncamento Longa Distância (CPqDTelesp - SP)/Telebrás ;
- 1993 - Primeiro Enlace Amplificado (Telesp- SP) /Telebrás ;
- 1994 - Primeiro Sistema WDM Longa Distância (CPqD/Embratel) /Telebrás ;
- 1997 - Primeiro Sistema Submarino Alta Capacidade (Embratel) /Telebrás;

A Figura 1 ilustra as principais evoluções mundiais a partir da década de 70 até 2000.;

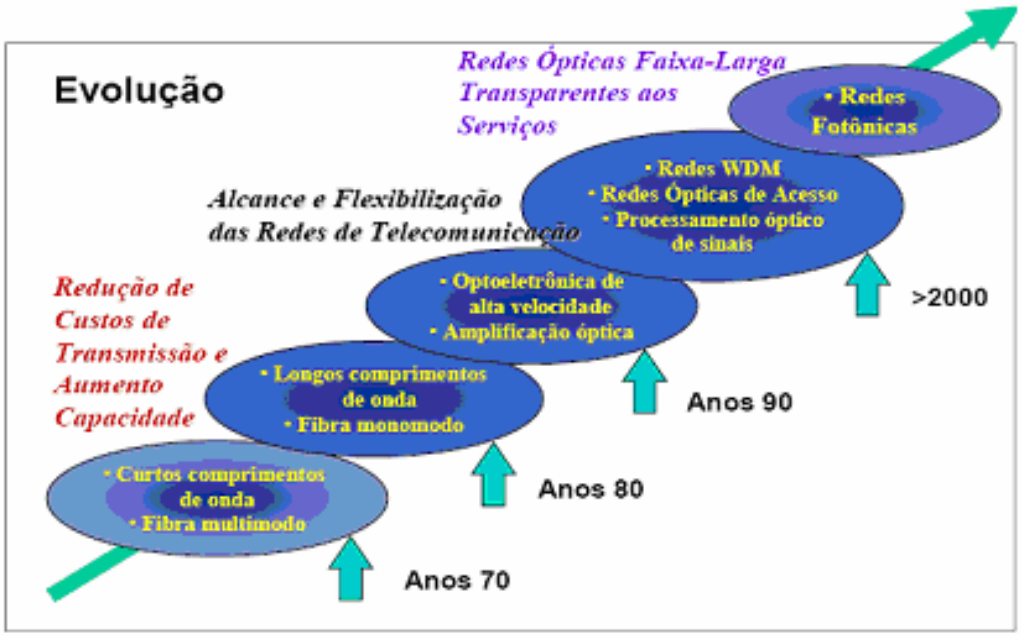


Figura 1 : Marcos importantes na evolução das comunicações ópticas mundialmente

1.2. Motivação do trabalho e Organização

A crescente demanda de novos serviços e de serviços de banda larga ao assinante vem acarretando um aumento acelerado do tráfego das diversas redes de comunicações e

também o aparecimento de novas tecnologias. Tendo em vista este cenário, surgiu a proposta de trabalhar com redes OPSN e mecanismos de proteção e sobrevivência de serviços aplicados em redes Metro-Acesso.

No desenvolvimento deste trabalho utilizamos algumas idéias já abordadas em trabalhos anteriores de nosso grupo (Laboratório de Tecnologia Fotônica-LTF), entretanto, buscando novos rumos e novos resultados. Nesse sentido, desenvolvemos estudos de mecanismos de proteção, abrangendo primeiramente uma análise de comportamento de redes ópticas em situações de falha de enlace *(link).*

O trabalho está estruturado da seguinte forma. O capítulo 1 trata-se de uma breve contextualização da evolução tecnológica das comunicações em geral, sendo focalizadas principalmente as tecnologias ópticas.

No capítulo 2 serão abordados conceitos e definições básicas dos elementos mais relevantes que constituem uma rede OPSN, assim como também o processo de transporte de informações nestas redes.

No capítulo 3 serão apresentadas as definições e implementações na obtenção dos resultados deste trabalho, além de uma análise de acordo com o aumento de tráfego nestas redes.

O capítulo 4 introduz conceitos e definições teóricas dos principais mecanismos de proteção e sobrevivência.

O capítulo 5 trata-se de uma extensão do capítulo 2, porque também se refere a resultados, mas com o intuito de melhorar a qualidade de entendimento, optou-se por criar outro capítulo. Nele iremos apresentar os resultados de medida de utilização de *links,* mostrando assim quais as rotas mais vulneráveis às falhas e que, no entanto, devem ser protegidas por algum mecanismo estudado no capítulo 4.

E finalmente, no capítulo 6 será feita uma conclusão geral de todo o trabalho e também sugestão de trabalhos futuros.

Os Anexos deste trabalho foram disponibilizados após a Conclusão.

1.3. Referências:

[1.1] A. S. Tanenbaum, *Redes de Computadores* .Editora Campus,Tradução da 3º ed .

[1.2] L.H. Bonani, "Contribuição ao Estudo de Redes Fotônicas de Pacotes", Dissertação de Mestrado, FEEC/Unicamp, 2003.

[1.3] R. Ramaswami e K. N. Sivarajan, *Optical Networks: Practical Perspective,* Morgan Kaufmann Publisher, 2002.

[1.4] L. H Bonani, "Proposta de Arquitetura Inovadora para Redes de Pacotes Ópticos baseadas em Chaveamento Fotônico", Dissertação de Doutorado, FEEC/ Unicamp, 2006.

[1.5] D.Maia Jr, "Desenvolvimento de Nós de Chaveamento de Pacotes Ópticos para aplicação em Redes Metropolitanas de Metropolitanas de Acesso", Dissertação de Mestrado, FEEC/Unicamp,2005.

[1.6] T. S. El-Bawab,. *Optical Switching,* Springer, 2006

.

2. Estudo de Redes Ópticas em Malha

As redes de comunicação estão em constante evolução tecnológica, visando sempre à melhoria dos serviços por elas transportados. As redes ópticas, em particular, devido a sua altíssima capacidade, configuram em anel ou malha, sendo que no acesso, pode ser anel ou estrela. Entretanto, a topologia de malha tem sido hoje, apresentada como uma melhor solução para o acesso, pois se caracteriza por ser rede robusta mais resistente à ocorrência de falhas de enlaces, devido ao maior número de caminhos disponíveis.

Em particular, as tecnologias de chaveamento de pacotes fotônicos (*Optical Packet Switching* – OPS) e de rajadas de pacotes (*Optical Burst Switching* - OBS) podem oferecer uma maior flexibilidade, funcionalidade e granularidade às redes ópticas [2.1][2.2][2.3] [2.4][2.5]. Os estudos e pesquisas envolvendo essas tecnologias têm ganhado importância para as redes ópticas atuais e futuras, tendo em vista que o tráfego nas diversas redes impõe cada vez mais demanda, pelo aumento de usuários e serviços da Internet, necessitando assim, de maior disponibilidade de banda e agilidade de provimento.

Neste capítulo apresentaremos os itens mais relevantes da estrutura física e lógica das redes ópticas em malha, e o processo de chaveamento fotônico, com o objetivo de preparar a apresentação dos resultados e aplicações que serão vistos no capítulo 3.

2.1. Histórico da topologia malha Manhattan Street (MS)

A rede *Manhattan Street* (MS) foi inicialmente proposta por Maxemchuk em 1985,[2.6][2.7], como uma alternativa para uma rede *backbone* de área metropolitana. Hoje

temos visto que essa topologia aplica-se melhor às redes metro-acesso de distribuição e de coleta dos tráfegos de clientes e sub-redes locais.

Essas redes MS pertencem à família das chamadas redes multipassos (*multihop networks*), nas quais há mais de uma rota entre quaisquer pares de nós. Ou seja, o tráfego gerado em um determinado nó pode passar por diversos nós intermediários antes de atingir o nó de destino. Em cada nó de uma rede *multihop* deve, portanto, ser tomada uma decisão sobre o roteamento de cada pacote recebido. As características das regras de roteamento adotadas determinam o desempenho da rede.

Este tipo de rede é constituído de uma malha regular bidimensional, sendo que cada nó tem dois enlaces (*links*) de entrada e dois enlaces de saída. Os braços paralelos e adjacentes, verticais e horizontais possuem sentidos alternados (daí a idéia de ruas e avenidas de Manhattan). Os nós extremos são sempre interligados aos nós (i, 1) ligados aos nós (i, m) e nós (1, j) ligados aos nós (n, j), onde n é o número de linhas, m o número de colunas, i = 1, ..., n e j = 1,..., m. A rede MS pode ser do tipo regular (MS) quando o número de nós da rede for par [2.7] e quase-regular (MSq) quando o número de nós da rede for ímpar. A Figura 2 apresenta uma rede MS-q de 9 nós.

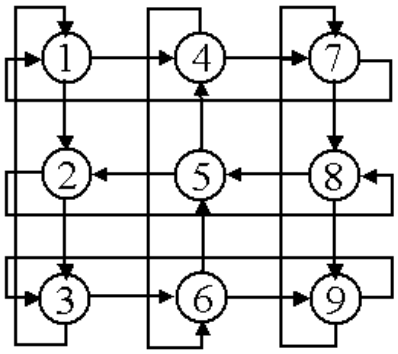


Figura 2 :Rede Manhattan Street 9 nós.

As redes MS podem ser divididas em duas classes: as redes MS síncronas (*slotted* MSN) e as redes MS assíncronas (*unslotted* MSN). Nas redes MS síncronas, novos pacotes só podem ser inseridos dentro do *slot* de tempo previamente determinado; assim, dois pacotes atingem os nós sempre em um instante múltiplo do valor do *slot*. Já nas redes

assíncronas, os pacotes podem ser inseridos em qualquer instante, logo, a probabilidade de disputa é maior nas redes assíncronas.

2.2. Pacote Óptico

Um pacote óptico é a unidade de informação tratada pela rede, contendo um campo de dados que é preenchido com uma carga útil e um cabeçalho onde estão registradas todas as informações necessárias ao seu correto encaminhamento através da rede [2.3][2.5]. O cabeçalho contém informações de roteamento, e é processado em cada nó óptico que o pacote passar e a carga útil, que é a informação a ser entregue ao destinatário, é processada apenas no nó de destino final. A Figura 3 mostra a estrutura de um pacote óptico.

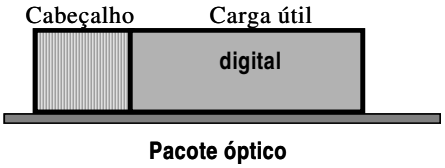


Figura 3 : Estrutura do pacote óptico

Durante o chaveamento fotônico, o nó óptico realiza a leitura do cabeçalho óptico que está codificado em TDM/FDM e este é processado eletronicamente enquanto a informação útil do pacote (*payload*) estará circulando por uma linha de retardo (FDL).

O cabeçalho óptico TDM/FDM, utilizado como endereçamento, pode ser composto por vários tons em baixa freqüência e em *slots* de tempo diferentes, constituindo assim o endereço do nó de destino. A carga útil do pacote é totalmente digital.

2.3. Protocolos para endereçamento de Pacotes Ópticos

Algumas técnicas de codificação do endereço (contido no cabeçalho) dos pacotes ópticos foram estudadas, sendo as mais utilizadas [2.1][2.3][2.4] :

- Multiplexação óptica por divisão de código (OCDM);
- Multiplexação por sub-portadora (SCM);

- Multiplexação óptica por divisão de tempo (OTDM);
- Multiplexação no domínio do tempo e multiplexação por divisão de freqüência (TDM/FDM);

Essas técnicas serão descritas nas sub-seções a seguir.

2.3.1. OCDM

Trata-se de uma técnica de multiplexação óptica, usando divisão de códigos (OCDM). Nela a codificação do endereçamento dos pacotes ocorre no nível de bit, onde o endereço de destino do pacote é representado por uma série de bits (*chirps*), contidos no cabeçalho do pacote. O código óptico de bit é usualmente gerado com fibras ópticas, atuando como linhas de retardo, que determinam o endereço de destino do pacote contendo bits [2.8][2.9].

Vantagens:

- ✓ codificadores ópticos podem ser implementados com dispositivos muito simples comparado com OTDM.
- ✓ Não requer sistema de controle para a sincronização de tempo
- ✓ Podem ser conectados a redes sem fios;

Ultimamente, o interesse em OCDM tem caído bastante em comparação com outros métodos de codificação .

2.3.2. SCM

Esta é uma técnica [2.10] de sinalização fora da banda de informação do pacote, que envolve a transmissão de um sinal ou canal de controle em uma freqüência separada do canal de dados. Dois tipos de sinalização fora da banda foram demonstrados, com a carga de informação e o cabeçalho do pacote sendo transmitidos em paralelo. No primeiro, o método SCM é usado para codificar a informação e o cabeçalho de endereçamento como bandas laterais de rádio-freqüência (RF) na portadora óptica, cada uma com uma banda diferente. A separação das bandas é determinada pelas taxas de dados da informação e do

cabeçalho do pacote fotônico. Na segunda abordagem, a informação e o cabeçalho dos pacotes são codificados com dois comprimentos de onda distintos.

Na transmissão da informação e do cabeçalho em paralelo, a vazão é acrescida desde que o cabeçalho ocupe a mesma duração que a informação, o que implica que, nestes casos, a sincronização entre informação e cabeçalho é importante durante o processo de roteamento. Quando à distância entre os nós roteadores é conhecida, uma compensação de atraso pode ser implementada utilizando dois comprimentos de onda para o realinhamento do cabeçalho e da informação. Contudo, a degradação do sinal devido a não-linearidades pode ocorrer, especialmente com o efeito de *crosstalk*, que pode limitar esses sistemas quando o espaçamento entre canais SCM é muito pequeno. Em um sistema com dois comprimentos de onda, o cabeçalho pode ser extraído utilizando-se filtros ópticos passivos; no entanto duas fontes ópticas sintonizadas devem ser usadas em cada transmissor, sendo que a estabilidade da fonte e do filtro ópticos, bem como da dispersão das fibras, são também parâmetros críticos.

2.3.3. OTDM

No método OTDM, os pacotes ópticos são chaveados em cada nó de acordo com o endereço de encaminhamento, carregado por cada pacote. Os pacotes ópticos são separados por pulsos que delimitam as fronteiras entre cada pacote [2.11]. Espera-se que, nas redes OTDM, sejam agregadas vazões da ordem de Tb/s em um canal com um simples comprimento de onda, pelo compartilhamento e processamento de uma grande quantidade de dados simultaneamente. A maioria das pesquisas em OTDM foi voltada para o desenvolvimento de dispositivos ultra-rápidos para a demultiplexação e sincronização do fluxo multiplexado no tempo, assim como de pulsos ultracurtos em altas velocidades. Espera-se com isso que o chaveamento óptico de pacotes possa permitir funções de roteamento, como adicionar e remover pacotes em uma rede de múltiplos nós. Assim, a função de adicionar é feita pela checagem de um espaço vazio e, a partir daí, insere-se um pacote. A função de remoção de pacotes acontece quando estes chegam ao nó de destino e, como outras funções de roteamento, requer a demultiplexação da informação contida no cabeçalho dos pacotes.

O processamento óptico pode acontecer muito rapidamente, mas a limitação está nos algoritmos ainda não muito robustos que até agora podem ser implementados, envolvendo, em alguns casos, não mais que um bit para a tomada de decisões [2.10]. Por outro lado, tem havido propostas onde o processamento do cabeçalho dos pacotes pode ser feito no domínio eletrônico. No entanto, nesses casos o controle de roteamento torna-se muito mais lento em altas taxas de pacotes.

2.3.4. FDM/TDM

A multiplexação por divisão de freqüência (FDM) é uma técnica que permite o chaveamento óptico de pacotes, além de apresentar uma baixa complexidade de sistema, devido ao fato de que tanto o cabeçalho de informação de endereçamento como a informação útil (*payload*) do pacote podem ser multiplexados no mesmo comprimento de onda. Neste esquema, a informação é codificada com uma alta taxa de bits na banda-base, enquanto o cabeçalho, numa taxa de bits muito menor, é codificado utilizando um tom com uma baixa freqüência de RF. A informação do cabeçalho é extraída pela detecção de uma fração do sinal do pacote e filtrando a freqüência RF da subportadora [2.10]. Uma grande vantagem da técnica FDM é a transparência da taxa em que a informação do pacote está comprimida. Além disso, a possibilidade de utilização de tons em baixa freqüência permite a identificação do cabeçalho do pacote, podendo cada tom ser entendido como um bit de endereçamento. A possibilidade de uma maior simplicidade de implementação também chama a atenção, pois, desde que o cabeçalho FDM tenha uma baixa taxa de bits (poucos tons), o processamento da informação contida no cabeçalho pode ser feito com circuitos eletrônicos de baixo custo. Aliada à técnica FDM pode-se optar por uma multiplexação no domínio do tempo (TDM), em que além da informação de endereçamento, poderiam ser colocados outros bits de informação, como prioridade de tráfego e sinalização para QoS, ainda como um tom de RF a baixa freqüência, mas em *slots* de tempo diferentes, inclusive daquele adotado para a informação útil dos pacotes. Esse sistema utilizando TDM torna o sistema de detecção um pouco mais complexo do que quando se utiliza apenas FDM. No entanto, experiências [2.13][2.4] mostraram que o sistema utilizando TDM/FDM mostrou-se mais robusto para detecção do endereço e, desta forma, para o roteamento correto do pacote.

2.4. Arquitetura do nó óptico

O nó óptico é um dos elementos principais que constitui uma rede óptica, isto devido as suas funcionalidades que é processar o cabeçalho, reconhecendo assim o endereço final do pacote óptico e, portanto, verificando a qual nó da rede o pacote pertence. Outra funcionalidade do nó é o envio ou encaminhamento do pacote óptico para uma de suas portas de saída que pode ser preferencial ou não; quem irá definir qual porta o pacote irá escolher é o protocolo de roteamento que será definido mais adiante.

O nó óptico é provido de configuração 2x2, ou seja, possui duas portas de entrada e duas portas de saída, mais as funcionalidades para adicionar e remover pacotes (*Add-Drop*) em cada *link*[2.3][2.4][2.5][2.14][2.15]. Além disso, o nó possui uma linha de retardo (FDL) em cada uma das portas de entrada, e um controle eletrônico, que juntos realizam o chaveamento fotônico dos pacotes, onde, enquanto o cabeçalho é lido eletronicamente, a carga útil do pacote ficará circulando pela linha de retardo. Veja que este processo é seguro, pois a carga do pacote é desempacotada somente no endereço de destino final, não sendo desempacotada nos nós intermediários ao seu destino.

A Figura 4 mostra a arquitetura do nó óptico.

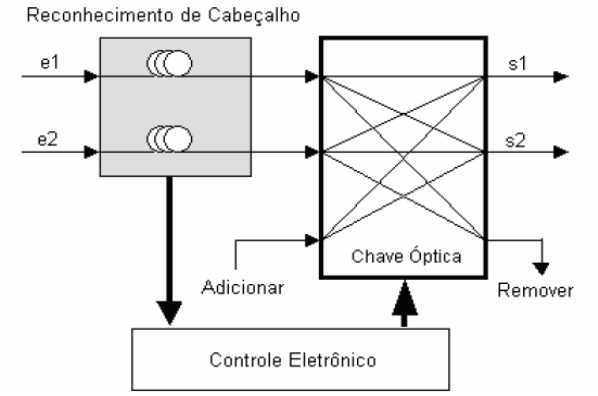


Figura 4 : Arquitetura do nó óptico

Resumidamente, os elementos mais importantes deste nó são:

- Portas de entrada (e1, e2) e saída (s1 e s2): por onde os pacotes acessam e deixam os nós;

- Portas Add/Drop (adicionar/remover) por onde os pacotes são adicionados ao nó de origem e retirados ao nó de destino;
- Linha de retardo: atrasa a carga útil do pacote para processamento do cabeçalho;
- Controle eletrônico: processa e reconhece o cabeçalho;

2.5. Roteamento em Redes Ópticas

Roteamento é definido como sendo o processo de encaminhamento de tráfego em redes de comunicação, estando diretamente relacionado com a topologia física e lógica das redes. O roteamento pode ser realizado tanto no domínio óptico como no eletrônico.

Os roteamentos escolhidos neste estudo adotam a política do caminho mínimo fim a fim para cada aplicação da rede, ou seja, o pacote tem como meta sempre realizar o menor caminho para chegar ao seu nó destino. O estabelecimento do caminho óptico é definido através da utilização de alguns algoritmos como protocolos de roteamento, os quais podem ser estáticos ou dinâmicos, dependendo do tipo de aplicação.

O roteamento estático sempre escolhe o mesmo caminho para cada nó de origem-destino. Este caminho é estabelecido conforme uma rota pré-determinada. Se todos os recursos como total de banda disponível, armazenadores e comprimentos de ondas, disponíveis ao longo de determinado caminho óptico estiverem sendo utilizados, pode ocorrer perda de pacotes. Outro problema do roteamento fixo é que este, por si só, não é tolerante à falhas, o que equivale a dizer que um esquema de roteamento alternativo deve ser implantado dinamicamente no caso da necessidade de implantação de um sistema de proteção quanto à falhas nos enlaces.

No roteamento estático, como dito anteriormente, a escolha do caminho é feita através da escolha de rotas previamente estabelecidas (orientadas a conexão), proporcionando um melhor planejamento da disponibilidade de rotas na rede. No entanto, este tipo de roteamento tem limitações para rotear tráfego aleatório.

No caso de roteamento dinâmico, a escolha do caminho é feita em tempo real (não orientadas a conexão), procurando naquele instante da requisição da conexão o melhor caminho a percorrer.

Em geral foi utilizado roteamento do tipo armazenar e encaminhar (*Store and Foward*) onde os pacotes são armazenados em um *buffer* e despachados preservando o caminho mínimo. O pacote sempre percorrerá o menor caminho que existe entre seu nó de origem até seu nó destino. Aqui seu caminho é definido ainda no seu nó de origem e caso alguma das rotas entre o caminho que o pacote irá percorrer estejam ocupadas por outro pacote, o pacote fica armazenado no *buffer* até que seu caminho preferencial esteja desocupado. Este tipo de roteamento é utilizado apenas para verificar qual o melhor caso de roteamento de pacotes, pois aqui desconsidera disputa entre pacotes, ou seja, resolução de contendas. O outro tipo de roteamento usado e que se trata de uma boa solução para resolução de contenda é roteamento por deflexão, também conhecido por batata quente (*Hot Potato)*. Neste caso, os pacotes nem sempre percorrem o menor caminho entre o nó de origem até o nó destino. O pacote quando entra no nó de origem pode ser enviado para a porta preferencial, ou seja, a porta que leva ao menor caminho até seu destino, mas caso esta porta esteja ocupada, este pacote será defletido para a outra porta do nó, lembrando que o nó óptico tem configuração 2x2, ou seja, é provido de duas portas de entrada e duas de saída.

2.6. Resolução de Contendas

Em redes fotônicas a questão da resolução de contenda pode ocorrer de 3 formas[2.3][2.4][2.14]:

- Temporal que utiliza *bufferização* óptica;
- Freqüêncial utilizando conversão de comprimento de onda;
- Espacial, que utiliza roteamento por deflexão.

A utilização da *bufferização* óptica e a conversão de comprimento de ondas requerem uma alta complexidade tecnológica, aumentando assim o custo das redes. A resolução espacial é uma alternativa simples e atraente, possibilita a implementação de uma

rede de pacotes ópticos sem armazenadores e conversores em cada nó, com topologias em malha e com um critério de resolução de contenda eficiente, sendo a disputa entre os pacotes, ou melhor, a contenda, resolvida pelo roteamento de um dos pacotes envolvidos para o enlace desejado e outro defletido para outra porta disponível.

2.6.1. Armazenamento óptico (*Optical Buffering*)

O congestionamento em roteadores eletrônicos convencionais é resolvido através de armazenamento dos pacotes eletrônicos, em *buffers*, ou seja, usando o domínio do tempo. Em óptica, este tipo de armazenamento devido à natureza intrinsicamente dinâmica dos fótons, é feita utilizando-se linhas de atraso constituídas de segmentos mais ou menos longos de fibras ópticas *(Fiber Delay Line* - FDL*).* Uma FDL pode atrasar um pacote por um período de tempo específico, ajustando-se o comprimento da linha de retardo.

Existem soluções de armazenamento eletrônico (*e-buffer*) que podem complementar a ação das FDL, mas não serão abordadas neste trabalho.

2.6.2. Comprimentos de Onda

Em WDM vários comprimentos de onda são disponibilizados em um enlace de fibra que conectam dois roteadores ópticos, podendo assim diminuir as contenções com a transmissão de pacotes conflitantes em outros comprimentos de onda.

Este método torna-se muito atrativo, particularmente porque o número de comprimentos de onda que podem ser acoplados em uma única fibra continua crescendo. A conversão de comprimento de onda pode reduzir a probabilidade de descarte de pacotes devido às contenções. Entretanto, nem todos os pacotes precisam de conversão, e, portanto a conversão poderia ser otimizada para reduzir o número de conversores e melhorar a qualidade dos sinais através da redução de conversões desnecessárias.

2.6.3. Roteamento por Deflexão

Roteamento por deflexão foi inventado inicialmente por Baran em 1964 e foi estudado e implementado no contexto de interconexão de redes em 1980 [2.16]. Este tipo de roteamento conhecido também como *Hot Potato* tornou-se uma técnica atrativa em

questões de resolução de contenda, pois dispensa a utilização de *buffers*, reduzindo assim o custo destas redes. Algumas das suas propriedades atraentes são:

- Simplicidade dos nós: o roteamento implementado em cada um dos nós da rede é bastante simples. Primeiro cada nó deve rotear os pacotes que chegam, para o caminho mais curto. Para que o nó encaminhe o pacote para a porta que o levará pelo caminho mais curto ao seu destino final, basta que este nó faça uma pesquisa em uma tabela saída de roteamento. A ausência de *buffers* para realizar o *Deflection Routing,* livra os nós de terem que realizar complexas tarefas de gerenciamento de *buffers*. Nenhum pacote é perdido devido a falta de capacidade do *buffer;*
- Congestionamento da rede: caso um trecho da rede apresente-se congestionado, os pacotes serão automaticamente defletidos para outro caminho, aliviando assim o tráfego nos locais congestionados;
- Tolerância à falhas: com rotas alternativas as redes tornam-se mais robustas;

A resolução de contenda espacial resolvida com este roteamento, os pacotes que sofrerem disputas e não vencerem, não serão descartados e sim defletidos para a porta de saída disponível. Neste contexto temos que levar em consideração três parâmetros importantes:

- Atraso de pacotes entre fonte e destino final;
- Ordem da chegada dos pacotes;
- Tempo de vida máximo que um pacote possa ter (*Time to live* -TTL);

2.7. Condições de Tráfego (PCIC e PCIV)

Os tráfegos adotados na etapa de simulação deste trabalho e que serão descritos nos próximos itens, utilizaram pacotes de mesmo tamanho. Os intervalos de transmissão entre os pacotes foram de tempos constantes e variados. A Figura 5 mostra o diagrama dos tempos onde T_p, t_B e t_i representam tempo de duração do pacote, duração de cada bit que constitui a carga útil do pacote e o intervalo entre os pacotes transmitidos sucessivamente, caracterizando assim os tipos de tráfegos.

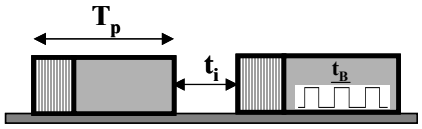


Figura 5 :Diagrama dos tempos que caracterizam os tipos de tráfego

2.7.1. Tráfego com pacotes de mesmo tamanho e intervalos de transmissão constante

Neste tipo de tráfego, os pacotes gerados são de tamanhos constantes, ou seja, T_p tem sempre o mesmo tamanho e os intervalos de transmissão entre cada pacote consecutivo (t_i) são também constantes.

A Figura 6 mostra o comportamento do tráfego PCIC.

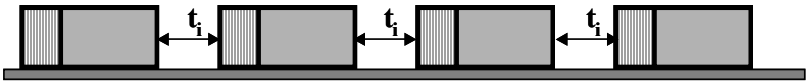


Figura 6 : Tráfego com transmissão de pacotes em tempos constantes

2.7.2. Tráfego com pacotes de mesmo tamanho e intervalos de transmissão variada.

No tráfego PCIV, os pacotes gerados possuem tamanhos constantes, mas o intervalo de transmissão entre cada pacote consecutivo é variável. O intervalo foi tratado como uma variável aleatória (RV), distribuída uniformemente no intervalo de (0, t_{max}). A distribuição é calculada em função do máximo intervalo entre os pacotes t_{max} que por sua vez é calculado através da taxa de bits da fonte de tráfego R (em bits/s), do tamanho do pacote P (em bits) e da largura de banda do enlace S (em bits/s), segundo a equação 2.1.

$$t_{\max} = \frac{P}{R} - \frac{P}{S} = \frac{P}{R} * \left(1 - \frac{R}{S}\right) \qquad 2.1$$

O intervalo efetivo entre cada pacote gerado, segundo a natureza de tráfego PCIV, é então dado por:

$$t = t_{\max} * Uniform[0,1] \qquad 2.2$$

onde Uniform[0,1] é um valor entre 0 e 1 obtido através de uma distribuição uniforme.

A Figura 7 mostra como se comporta o tráfego PCIV levando em consideração os intervalos de tempo entre os pacotes transmitidos.

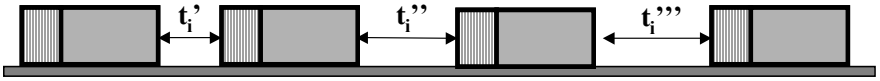


Figura 7 : Tráfego com transmissão de pacotes com tempos variados

2.8. **Referências**:

[2.1] L.H. Bonani, "Contribuição ao Estudo de Redes Fotônicas de Pacotes", Dissertação de Mestrado, FEEC/Unicamp, 2003.

[2.2] L.H. Bonani "Uma Proposta Inovadora para a Arquitetura de Redes Fotônicas de Pacotes", Monografia apresentada para teste de qualificação do programa de doutorado da FEEC/Unicamp

[2.3] F. R. Barbosa, D. Maia Jr, L. Pezzolo, A. C. Sachs, M. R. Salvador, "Optical Packet Switching Node for Metro-Acess Networks", Proc. Of European Conference on Optical Communications ECOC'2003, 2003.

[2.4] L. H. Bonani, F. L. Pádua, Edson Moschim and F. Rudge Barbosa, "Optical Packet Switching Access Networks using Contention Resolution without Wavelength Conversion", *11th Intl. Conf. on Telecomm.– ICT '2004*, paper TS-25-3, Fortaleza, Brasil, Aug. 2004; and Springer-Verlag , Nov.2004.

[2.5] F. Rudge Barbosa, et al, "Optical Packet Switching Node for Metro-Access Networks", paper PD-160, *Proceed. 29th. ECOC'2003*, Rimini, Italia, Sept. 2003.

[2.6] N. F. Maxemchuk, "The Manhattan Street Network", *Proc. Globecom* 85, New Orleans, LA, pp.255-261, Dec. 1986.

[2.7] N. F. Maxemchuk, "Routing in the Manhattan Street Network"*, IEEE Trans. Com*., Vol. Com-35, No. 5, pp 503-512,1987.

[2.8] D. J. Blumenthal, P. R.Prucnal, and L. Thylen and P. Granestrand, "Perfomance of an 8x8LiNbO3 Switch matrix as a Gigahertz self Routing Switching node", Eletronic Letter vol.23, no.25, pp.1359-1360, 1997.

[2.9] I. Daeki, S. Nishi and K. Murakami, "All Optical Code Division Multiplexing Switching Network Based on Self Routing Principle", IEICE Transactions on Communications vol.16, no.2, pp.239-245, 1999.

[2.10] F. R. Barbosa, A. C. Sachs, M. T. Furtado, J. B. Rosolem, "Optical Packet Switing: a transmission and recovery demonstration using an SCM header", SBrT'2001, Fortaleza, Brazil, Sept. 2001; and Special Issue, Rev. Soc. Bras. Telecom., June 2002.

[2.11] R. Ramaswami and K. N. Sivarajan, Optical Networks: A Practical Perpective, Morgan Kaufman Publisher Ed. D. Clark, (1998).

[2.12] F. R. Barbosa, A. C. Sachs, R. S. Ferreira, M. T. Furtado, "New Photonic System for Optical Packet Switing", Proc. 6th World Conference on Systemics, Cybernetics, and Informatics- SCI'2002. Orlando, FLA, USA, July 2002

[2.13] F. R. Barbosa, D. Maia Jr, E. Moschim, L. Pezzolo, A. C. Sachs, "Optical Packet Switching and Routing Using RF Frequency Header Label for Application in Metropolitan Acess Networks", SPIE-ITCom'2003, paper 5247-20, Florida USA, Sept. 2003.

[2.14] L. H. Bonani, F.J.L. Pádua, E. Moschim, and F. Rudge Barbosa, "Optical Packet Switching Access Networks using Contention Resolution without Wavelength Conversion", *11th International Conference on Telecomm – ICT'2004*, paper TS-25-3, Fortaleza, Brazil, Aug. 2004; Springer-Verlag.

[2.15] L. H. Bonani, F. R. Barbosa, E. Moschim, "Performance and Dimensioning Analysis of Optical Packet Switching Access Networks with Variable Traffic Demands", *Proceedings of the 11th International Conference on Telecomunications*, August 2004, Fortaleza- CE, Brazil.

[2.16] P. Baran, "On Distributed Communications Networks", *IEEE Transactions on communications*, pages 1-9, March 1964.

3. Análise da Evolução de Tráfego em Redes OPSN

Prevendo a implantação e utilização de redes totalmente ópticas em um futuro próximo, foram realizados estudos e simulações, baseados em OPSN, a fim de se obter resultados analíticos e numéricos de simulação, envolvendo parâmetros específicos para avaliação de capacidade, desempenho e vazão.

Neste capítulo, portanto, abordam-se definições específicas aos cálculos de parâmetros e variáveis como, por exemplo, capacidade total (C_t), número de usuários (N*(N-1)), número médio de saltos (*hops)* (E[*hops*]), fator desempenho (F_d) e vazão (Tp) que são importantes para o entendimento dos resultados teóricos e de simulações.

Os *softwares* utilizados em nossas simulações e para plotagem de gráficos foram *Network Simulator* (NS) e o *Matlab.*

3.1. Conceitos e Definições

Os parâmetros e variáveis considerados e que serão definidos nesta seção são: número médio de *hops* (E[*hops*]), capacidade total da rede (C_t), capacidade efetiva (Ce), carga na rede (Lc) e vazão (T_p) [3.1] [3.2]. Através destes parâmetros e variáveis foi criada uma nova métrica para avaliar o desempenho da rede analiticamente, nomeado por fator de desempenho (F_d), exclusivo deste trabalho e que utiliza a relação entre C_t e E[*hops*] para ser calculado.

O número médio de *hops* (E[*hops*]) trata-se do valor médio de saltos que os pacotes realizam para chegar ao seus endereços de destinos . Ele é calculado com a finalidade de encontrar a rota de menor caminho que o pacote pode percorrer para chegar ao seu destino. O cálculo deste parâmetro não é igual para os dois tipos de roteamento (*Store and Forward* -SF e *Deflection Routing* -DR) por isto será detalhado na próxima seção deste capítulo.

O E[*hops*], tanto no roteamento SF quanto no DR, calcula o número médio de saltos realizados pelos pacotes entre o nó origem e o nó destino, sendo que para o SF esse cálculo é realizado no início (nó origem), obtendo assim uma média de menor caminho que o pacote irá trafegar antes de ser roteado, definindo assim, sua rota. Para o roteamento DR [3.2][3.3][3.4][3.5] os pacotes não possuem uma rota determinada no seu nó de origem e, em cada *hop*, ele pode tomar um certo caminho que levará a um maior ou menor número de saltos (*hops)* até seu destino. A escolha do caminho dos pacotes no DR é ocasionada pela disponibilidade da sua porta de saída do nó em que o pacote se encontra, podendo ser preferencial ou não.

O roteamento DR é uma alternativa para a resolução de contenda entre pacotes ópticos em redes multi-caminhos, como já foi visto no capítulo 2. Quando ocorre disputa por uma porta de saída, uma solução eficiente e barata é a utilização do roteamento DR, onde os pacotes que chegam primeiro ganham a disputa e são roteados para a porta preferencial e os que chegam após é defletido para a porta de saída disponível, pois se trata de redes sem *buffer (bufferless).*

O número de usuários, também conhecido como fontes de tráfegos de uma rede, foi definido por Acampora (1992) [3.2], como sendo todos os nós gerando tráfego uniforme para todos os outros nós da rede, menos para si mesmo. Desse modo, para N nós, o número de usuários se calcula utilizando a equação (3.1), onde N_u corresponde ao número total de tráfegos ou usuários e N é o número de nós existente na rede. Ex: rede com 16 nós, Nu = 240, ou seja, 15 usuários por nó.

$$N_u = N * (N - 1) \qquad \textbf{(3.1)}$$

Para rede do tipo MS, com tráfego unidirecional nos enlaces, o número total de caminhos mínimos Nc é dado pelo número de menores caminhos possíveis, que será único para cada nó, então Nc= N*(N-1) que é igual a Nu.

No caso de enlaces bidirecionais, a situação difere para pacotes e circuitos. Pacotes, tendo por definição seus próprios cabeçalhos e mecanismos de endereçamento, sempre seguem o menor caminho disponível. Circuitos, por sua vez são estabelecidos pela rede, e uma vez realizada a conexão, esta permanece. Assim, estabelecida uma conexão de caminho mínimo do nó de origem para o nó de destino, o caminho de volta será o mesmo. Ou seja, nesse caso Nc= Nu/2. Exemplo: o trabalho de Cho&Kim [3.6] possui 25 nós, 80 enlaces bidirecionais, isto resultaria em um Nu= 600, sendo o número de diferentes caminhos ou conexões Nc=300, pois a ida é igual à volta.

A capacidade total da rede (C_t), corresponde à quantidade de pacotes que a rede pode suportar. Este parâmetro é dado pela equação (3.2) [3.1][3.2][3.9],

$$C_t = \frac{2 * N * S}{E[hops]} \qquad \textbf{(3.2)}$$

na qual S é a capacidade do *link* (Gb/s), N é a quantidade de nós da rede, e E[*hops*] é número médio de *hops*; o fator "2" é devido a existência de 2 enlaces que estão saindo de cada nó, conforme mostra a Figura 8. Nota-se pela equação (3.2) que C_t pode ser maximizada sempre que E[*hops*] for minimizado; isto também impacta no fator de desempenho (F_d) e na vazão da rede.

Vale a pena salientar que existe um limite máximo da capacidade da rede, designado C_{max}, e que é definido como C_{max}= 2NS obtido na situação idealizada em que toda a comunicação da rede é feita com um salto.

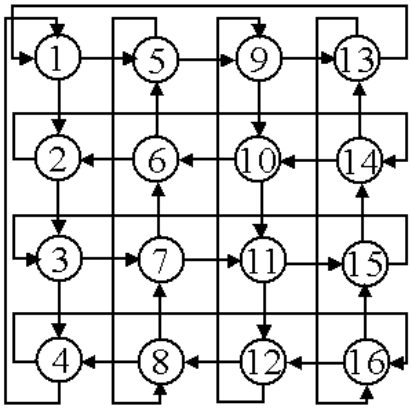


Figura 8 : Topologia de rede MS de 16 nós.

A carga na rede (L_c), é uma variável que define o quanto está sendo utilizada a capacidade da rede, sendo variado entre "0 a 1".

A capacidade efetiva da rede (C_{ef}) como em [3.9] é a capacidade que está sendo utilizada em um momento, dada pela equação (3.3).

$$C_{ef} = C_t * L_c \qquad \textbf{(3.3)}$$

Do mesmo modo da C_{ef} , a taxa efetiva por usuário da rede (Re) é calculada utilizando a equação (3.4) [3.9]:

$$R_e = \frac{C_{ef}}{Nu} = \frac{(C_t * L_c)}{(N * (N-1))} \qquad \textbf{(3.4)}$$

Finalmente, a especificação do fator de desempenho (F_d), considerado neste trabalho como uma métrica para dimensionamento das redes de pacotes ópticos, é calculado através da equação (3.5).

$$F_d = \frac{C_t}{E[hops]} \qquad \textbf{(3.5)}$$

A lógica para a compreensão desta nova métrica é que, quanto menor o caminho percorrido pelo pacote para chegar ao seu endereço de destino, menos tempo o pacote alocará banda e, portanto, mais pacotes podem trafegar nesta rede, sendo a capacidade efetiva calculada maior.

Observa-se que, de fato, uma rede com alto desempenho não só tem C_t alto, como E[*hops*] baixo, o que significa também alta vazão (T_p).

A vazão (T_p) também conhecida de *throughtput é* um parâmetro que mede o fluxo de tráfego de pacotes que circulam na rede [3.2]. Pela equação (3.6), T_p é C_{ef} pelo E[*hops*], visto anteriormente que $C_{ef} = C_t * L_c$.

$$T_p = \frac{2NS}{E[hops]} * L_c \qquad \textbf{(3.6)}$$

3.2. Procedimento de cálculos

O cálculo do E[*hops*] para o roteamento SF utiliza o algoritmo *Floyd Warshal* (FW) e segue as seguintes etapas e suas descrições, conforme mostra a Figura 9.

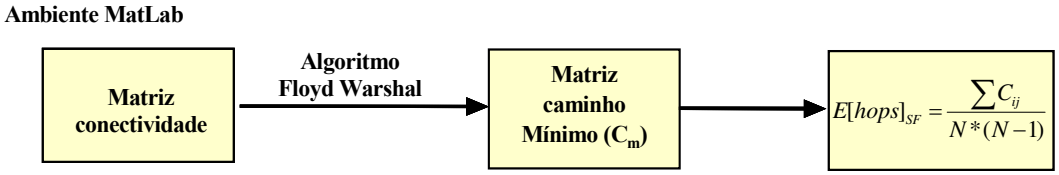


Figura 9 :Etapas do cálculo do E[*hops*] utilizando algoritmo FW.

- Definição pelo usuário da matriz conectividade da topologia que se pretende utilizar. Por exemplo, para uma topologia MS-4 nós, o dimensionamento da matriz segue a quantidade de nós da rede (4 nós = matriz conectividade 4x4) onde as linhas e colunas representam as ligações entre os nós da rede (coloca-se "1" para quando houver ligação e "0" para quando não houver ligação).

$$MC = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

- Em seqüência utilizando o algoritmo FW é gerada uma matriz de caminho mínimo;

$$C_m = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix}$$

- Após os cálculos de quantos saltos (mínimo) entre os nós da rede, é realizado o somatório de todos estes nós e depois dividindo pelo número de usuários (N*(N-1)).
- Após este último cálculo, obtem-se o número médio de *hops*.

$$E[hops]_{SF} = \frac{\sum C_{ij}}{N*(N-1)} \qquad \textbf{(3.7)}$$

No cálculo do E[*hops*] utilizando roteamento DR[3.1][3.3][3.4][3.5] é necessário calcular as probabilidades de deflexão e não deflexão de um pacote, quando não existir contenda (disputa entre pacotes) e quando existir contenda (disputa entre pacotes).

O cálculo da probabilidade de não deflexão, quando um pacote é encaminhado para porta preferencial (P_p), foi calculado partindo da análise de 3 possibilidades de chegadas de pacotes adotadas, considerando que para estas possibilidades não existiria contenda.

- **Caso-1:** Chegada de apenas um pacote: este é direcionado sem problemas, para sua porta preferencial como mostra a Figura 10. A probabilidade do pacote chegar sozinho em um certo nó é calculada pela (3.8):

$$P_a = (1 - L_c) \qquad \textbf{(3.8)}$$

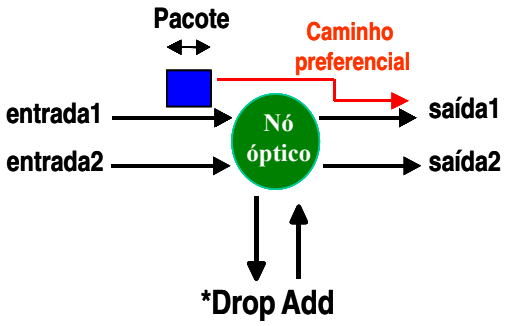


Figura 10 : Chegada de 1 pacote no nó (sem contenda)
(*Drop/Add=retirar/adicionar)

- **Caso 2:** Chegada de 2 pacotes juntos no nó sendo que cada um possui destino em portas preferenciais diferentes, conforme ilustrado a seguir.

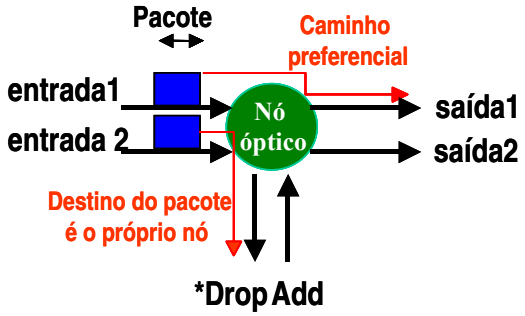


Figura 11 : Chegada de 2 pacotes sem disputa (sem contenda)
(*Drop/Add=retirar/adicionar)

A probabilidade de não deflexão de um dos pacotes para o caso 2 é dada pela equação (3.9):

$$P_b = L_c * P_n \qquad \textbf{(3.9)}$$

Na qual P_n é calculado pela equação (3.10):

$$P_n = \frac{(N-1)}{2N} \qquad \textbf{(3.10)}$$

- **Caso 3:** Chegada de 2 pacotes juntos sendo que um tem como destino final o próprio nó, portanto o outro terá as duas portas de saída liberadas.

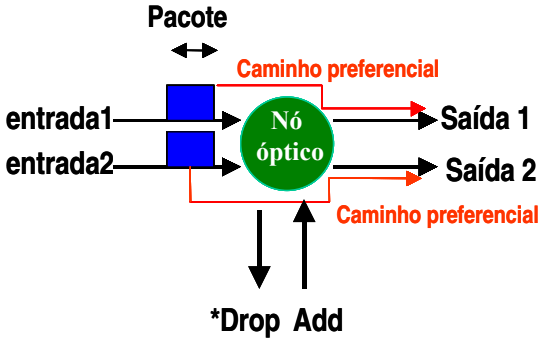


Figura 12 :Chegada de 2 pacotes juntos (sem contenda)
(*Drop/Add=retirar/adicionar)

A probabilidade de não deflexão do pacote para esta possibilidade é dada por:

$$P_c = L_c * (1 - P_n) * \frac{1}{2} \qquad \textbf{(3.11)}$$

Para calcular a probabilidade de não deflexão, quando não há contenda, basta somar P_a, P_b e P_c, de acordo com a equação (3.12)

$$P_{n-deflexão} = P_a + P_b + P_c \qquad \textbf{(3.12)}$$

Quando houver contenda, a probabilidade de um pacote vencer a disputa (P_{vdp}) e ser encaminhado para a porta preferencial é calculado pela equação (3.13):

$$P_{vdp} = \frac{1 - P_{n-deflexão}}{2} \qquad \textbf{(3.13)}$$

A probabilidade do pacote ser encaminhado para a porta preferencial (P_p) é a soma das probabilidades de não deflexão do pacote, não havendo contenda ($P_{n\text{-}deflexão}$) e a probabilidade do pacote vencer a disputa quando houver contenda (P_{vdp}). Assim temos a equação (3.14):

$$P_p = P_{n-deflexão} + P_{vdp} \qquad \textbf{(3.14)}$$

Portanto a probabilidade de deflexão do pacote calculada através da equação (3.15)

$$P_{np} = 1 - P_p \qquad \textbf{(3.15)}$$

As probabilidades calculadas acima foram substituídas na matriz de tráfego. Nela as colunas representam o nó em que o pacote está localizado em um determinado momento e as linhas, as probabilidades de deflexão e não deflexão daquele pacote para que ele chegue no nó destino, ou seja, a probabilidade de o pacote alcançar cada um dos N nós no momento seguinte.

Quando um pacote tem 2 possibilidades de caminhos de mesmo tamanho (com o mesmo número de *hops*), tanto direcionado para porta preferência, quanto para porta não preferencial de saída até o nó destino, nomeamos esta situação de tanto faz (*don´t care).* Neste trabalho, a escolha da porta de saída, quando ocorreu este tipo de situação, foi feita de acordo com NS, ou seja, o caminho adotado pelo simulador durante as simulações foi a escolhida no trabalho teórico.

Exemplo de matriz tráfego para rede MS-9 nós

$$T=\begin{pmatrix} 0 & 0 & P_{nd} & 0 & 0 & 0 & P_{nd} & 0 & 0 \\ 0 & 0 & 0 & 0 & P_{nd} & 0 & 0 & 0 & 0 \\ 0 & P_{nd} & 0 & 0 & 0 & 0 & 0 & 0 & P_{nd} \\ 0 & 0 & 0 & 0 & P_{d} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & P_{d} & 0 & P_{d} & 0 \\ 0 & 0 & P_{d} & P_{d} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & P_{nd} & 0 & 0 & 0 & 0 & P_{nd} \\ 0 & P_{d} & 0 & 0 & 0 & 0 & P_{d} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & P_{nd} & 0 & P_{nd} & 0 \end{pmatrix}$$

Analisando um pacote(teste) em um determinado momento inicial (k=1), verifica-se que a probabilidade de encontrá-lo em algum outro nó da rede $(N-1)$ é de 1/N-1 e a probabilidade de encontrar no nó referente ao destino final é de zero, pois considera-se que quando o pacote chega no destino final, este já seja retirado da rede. Com isto podemos calcular a probabilidade para k=1:

$$P_1=\begin{pmatrix} 0 \\ 1/N-1 \\ 1/N-1 \\ \vdots \\ \vdots \\ \vdots \end{pmatrix} \qquad \textbf{(3.16)}$$

Uma vez calculada a probabilidade no instante k=1, o cálculo da probabilidade de encontrar o pacote em um determinado nó para os demais instantes k>1 é calculada utilizando a equação:

$$P_k = T * P_{k-1} \qquad \textbf{(3.17)}$$

Finalmente o cálculo de E[hops] pode ser realizado:

$$E[hops]_{DR} = \sum_{k=2}^{\infty} k * P_k(1) \qquad \textbf{(3.18)}$$

Obs.: Lembrando que este cálculo leva em consideração que o pacote teste citado acima tem como destino final o nó 1.

3.3. Resultados analíticos

Os resultados que veremos a seguir foram obtidos utilizando o *software Matlab* [3.13] e em uma máquina Pentium 4 com processador Intel X86 de aproximadamente 3391MHz , 512 MB de memória e HD de 80 GB.

Como já citado e explicado no início deste capítulo, o fator de desempenho (F_d) das redes de topologia MS-4, 16, 36, MSq-9, 25, nós e redes irregulares de 6, 8 nós foi medido através dos parâmetros E[*hops*] e C_t, que são utilizados no contexto de OPSN de nosso trabalho .

A tabela 1 e as Figura 13 e Figura 14 resumem os resultados analíticos obtidos sendo utilizado o roteamento SF.

Topologias	**Número de nós (N)**	**Número médio de hops E[*hops*]**	**Capacidade da rede Ct (Gb/s)**	**Fator desempenho (F_d)**
MS-4	**4**	1,3333	15	11,27
MI	**6**	1,7000	17,64	10,35
MI	**8**	2,2857	17,5	7,67
MSq-9	**9**	2,0139	22,34	11,09
MS-16	**16**	2,9333	27,27	9,28
MSq-25	**25**	3,2800	38,10	11,61
MS-36	**36**	3,7143	48,46	13,04

Tabela 1. **:** Resumo dos resultados de parâmetros de rede de pacotes ópticos na topologia em malha.

Tomando a rede de 4 nós como referência, é observado que:

- ➔ Rede de 6 nós teve um aumento de 17,64% da capacidade;
- ➔ Rede de 8 nós teve um aumento de 16,66% da capacidade;
- ➔ Rede de 9 nós teve um aumento de 48,9% da capacidade;
- ➔ Rede de 16 nós teve um aumento de 81,8% da capacidade;
- ➔ Rede de 25 nós teve um aumento de 154,06% da capacidade;
- ➔ Rede de 36 nos teve um aumento de 223,07% da capacidade

Obs.: Na tabela acima foi mostrado também resultado para topologias de 6 e 8 nós que são de outros trabalhos e autores[3.9][3.11].

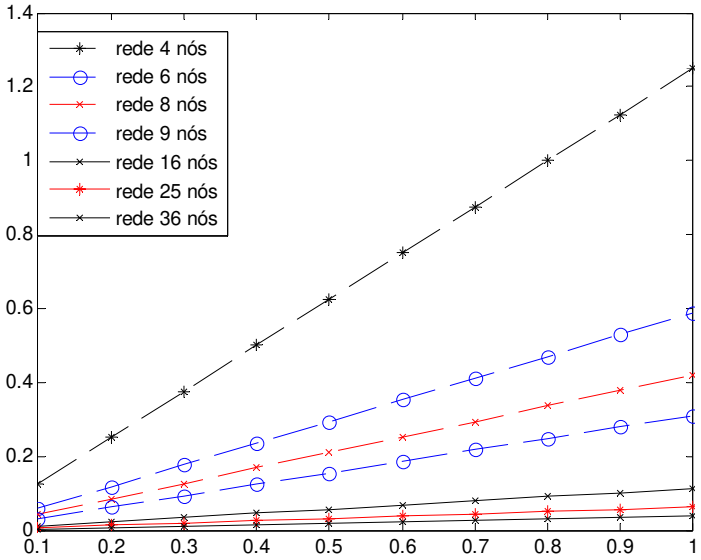


Figura 13 :Evolução da taxa de bits por usuário R_e, em função da carga nas redes.

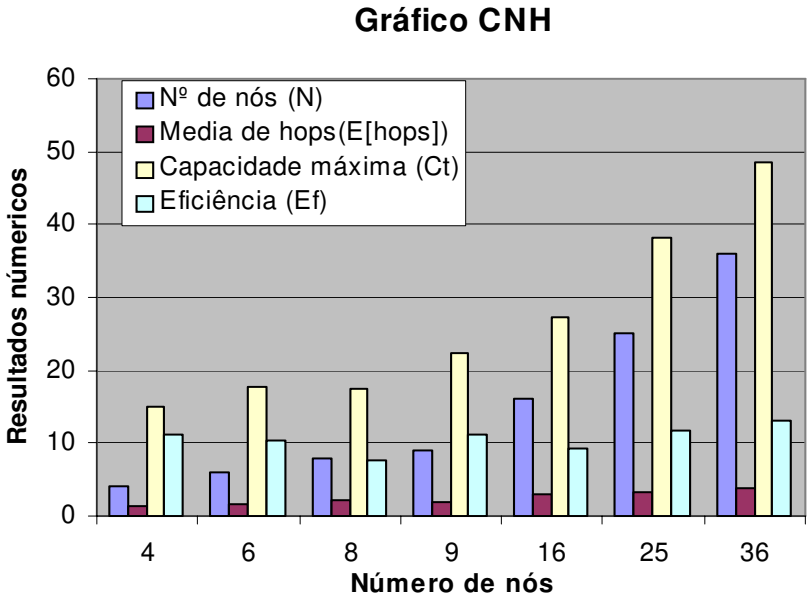


Figura 14 : Gráfico representando nº de nós/cap max/ nº médio de saltos/desempenho para cada topologia (MS-4, 16, 36; MSq-9, 25; MI-6,8 nós).

De acordo com a tabela 1, verifica-se que a solução de rede de 8 nós (resultados obtidos em outro trabalho e autor [3.9]) não é muito razoável, pois, apesar de ter aumento significativo de capacidade em relação a 4 nós, em relação a de 6 nós, a capacidade da rede diminui.

O fator de desempenho da rede (F_d) também aponta a rede irregular de 8 nós como uma má solução, com o pior desempenho de todos os casos estudados.

A razão E[*hops*] x N decresce com o aumento do número de nós (N), exceto para 8 nós.

Portanto, no caso de demanda de ampliação de uma rede de 4 ou 6 nós, qual deve ser a topologia seguinte ? Claramente, a de 8 nós não deve ser escolhida, enquanto a de 9 nós, nos dá um grande aumento de capacidade, além de dar alta eficiência.

No gráfico da Figura 13 observa-se que a taxa máxima na rede de 4 nós é de 1250 Mb/s (carga de 100%), e coincide com a metade do valor da taxa total (2.5Gb/s). Isto é mera coincidência numérica, porque a heurística de cálculo segue, na verdade, a fórmula de Re, definida anteriormente.

Outro aspecto relevante que deve ser destacado é a proposta da nova métrica para avaliação e escolha de topologias, e decisão do número de nós para redes de pacotes ópticos. O número de nós dá entrada ao tamanho da rede desejada; o fator de desempenho define a melhor rede. Os únicos limitantes estabelecidos dessas redes são o número de nós (atual máximo 36) e o tempo de vida dos pacotes ópticos (TTL)(=1 ms), porque se pretende uma solução direcionada para redes metropolitanas de acesso, com alta granularidade e baixa latência.

Os próximos resultados referentes as Figura 15 e Figura 16 apresentam os gráficos de E[*hops*] em função da carga da rede (L_c) e T_p em função da carga da rede (L_c) respectivamente. Analisando as duas figuras, nota-se que o número de nós é diretamente proporcional ao número de *hops* realizado por um pacote, ou seja, quanto maior o número de nós, maior o número de *hops* que os pacotes tem que realizar para chegar no seu nó destino, apesar de que para a rede de 9 nós,particularmente, o E[*hops*] apresentado foi inferior a de 8 nós.

Este resultado do E[*hops*] da MS-9 veio reforçar a coerência da nova métrica criada neste trabalho o F_d , pois quando calculada, já havia mostrado um melhor desempenho para MS-9 comparada com a de 8 nós .

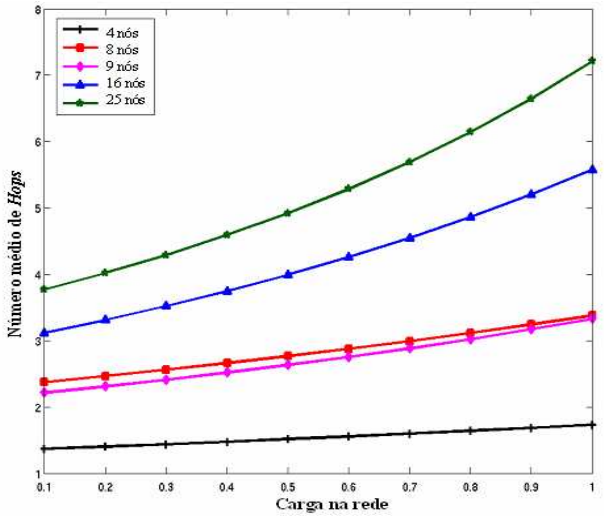


Figura 15 : Número médio de *hops* da rede

Os resultados referentes à vazão (inversamente proporcional a E[*hops*]) mostram que, quanto maior o tamanho físico da rede (número de nós), maior será o fluxo de tráfego e os pacotes terão de realizar em média, mais saltos para chegarem ao seu endereço de destino. Portanto, observa-se que a vazão tende a saturar mais rápido para redes maiores. O gráfico da vazão, assim como o do número médio de *hops*, tiveram comportamentos iguais levando em consideração, o formato das curvas de cada gráfico, porém com pesos diferente para cada rede. Nota-se que o traçado das curvas, se manteve para todas as redes, mudando apenas o deslocamento no eixo que representa a vazão.

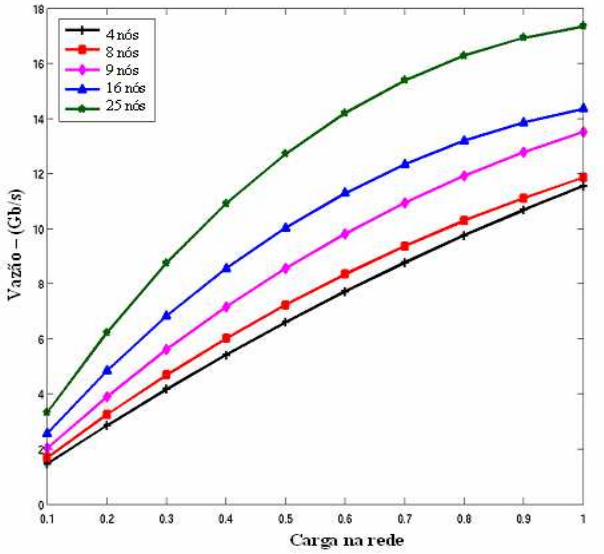


Figura 16 :Vazão da rede

3.4. Processo de simulação

As etapas do processo de simulação estão descritas detalhadamente no Anexo A, desde a preparação dos scripts até o resultado gráfico final.

3.5. Características da OPSN simulada

A estrutura física da rede montada no *script* para a simulação é constituída de nós com configurações 2x2 interconectados em *links* unidirecionais iguais, com tamanho equivalente a (2km ou 10μs). Os nós são com e sem armazenamento de pacotes. Para a rede com armazenamento, os pacotes serão roteados utilizando SF, portanto, serão encaminhados sempre para a porta preferencial, percorrendo assim, sempre o caminho mais curto. Para a rede sem armazenamento óptico (*bufferless optical node*) utiliza fila do tipo *Droptail* com limite de 2 pacotes e roteamento DR onde os pacotes que perdem a disputa, quando chegam junto com outro pacote e são defletidos para a porta de saída não preferencial. O fluxo de tráfego gerado é uniforme, ou seja, gera-se a mesma quantidade de tráfego para todos os nós, e a carga do *link* (L_c) foi variada de 0.1 a 1. Considerou-se um *delay* de 10μs para cada pacote .

Os nós ópticos possuem também uma linha de retardo (FDL) em cada uma das portas de entrada, com funcionalidade de melhorar o processamento eletrônico do cabeçalho do pacote. A Figura 17 abaixo apresenta a arquitetura do nó utilizado nas simulações, com todas suas portas de entradas e saídas, FDL.

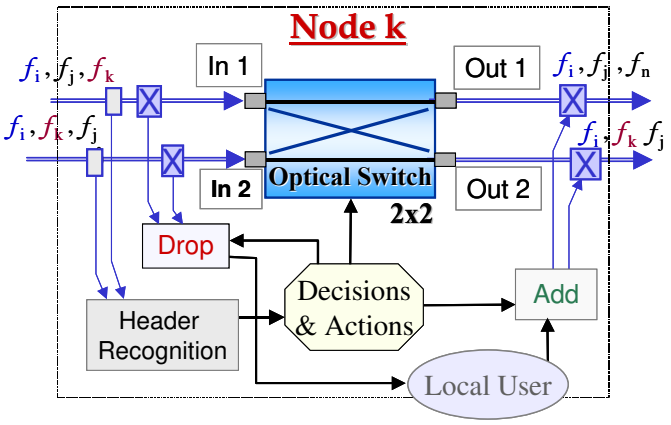


Figura 17 : Arquitetura do nó óptico de chaveamento fotônico.

Foram adotados dois tipos de tráfego e para cada um deles, foram utilizados dois tipos de roteamento SF e DR. Os tipos de tráfegos foram nomeados como PCIC e PCIV e já foram descritos e definidos no capítulo 2 .

Nos dois tipos de tráfego (PCIC e PCIV) a taxa de bits é constante (CBR – *Constante Bit Rate*) 2,5Gb/s e o tamanho de cada pacote utilizado é de 500 *bytes*. Na camada de transporte foi utilizado o protocolo UDP (*User Datagram Protocolo*) para evitar retransmissão de pacotes perdidos.

Resumo das características

Topologia : MS-4, 16, 36; MSq- 9, 25, nós;

Link Load : variação de 0.1 a 1;

Tipo de Tráfego:

1- PCIC : Pacotes constantes com intervalos constantes;

2- PCIV : Pacotes constantes com intervalos variados;

Roteamento: *no deflection, droptail* (tem as mesmas características do *deflection routing*);

Protocolo camada transporte: UDP;

Taxa de transmissão dos *links*: 2,5 Gb/s ;

Delay: 10μs

Tipo de Fila: *droptail* (limite de 2);

Taxa de transmissão de bits: CBR;

Tamanho do pacote: 500 bytes;

Quantidade de pacotes gerados: 200000 ($2*10^5$)

Perdas de Pacotes

Na OPSN caracterizada no item anterior e por onde os pacotes são transportados, existem alguns problemas os quais podem acarretar perdas de pacotes, principalmente, quando a rede está trabalhando com sua capacidade máxima.

É importante conhecermos as causas que provocam a perda de pacotes. Essas perdas podem ocorrer por:

- Final do tempo de vida do pacote óptico: este é um problema causado geralmente pelas várias deflexões dos pacotes para as portas não preferenciais. Os pacotes defletidos podem trafegar por caminhos muito longos, ficando assim muito tempo trafegando na rede, sem chegar ao seu destino final e em conseqüência disto, estourando o tempo máximo de vida (TTL) que o pacote pode ter. Por isto, escolheu-se um valor máximo de *hop*s (TTL), limitando assim o tempo de vida de um pacote e evitando também o congestionamento da rede, comprometendo, no entanto, sua Qualidade de Serviço (QoS);
- Por adicionamento de pacotes no nó de entrada: trata-se das perdas quando está se adicionando um pacote no nó. Estas perdas podem ocorrer de duas formas:
  - Perda do pacote que já trafegava na rede;
  - Perda do pacote que seria adicionado à rede;

Essas duas formas de perdas de pacotes ocorrem principalmente em condições de alta carga, devido ao fator de não haver critério seguro para adicionar os pacotes, sem evitar assim, as colisões. Nas duas situações de perdas de pacotes por adicionamento, um pacote é adicionado ao mesmo tempo em que um outro pacote está atravessando o nó, causando assim, a colisão dos pacotes. Este tipo de perda somente ocorre nas simulações, por isto será desconsiderado nos nossos resultados simulados. A Figura 18 abaixo mostra estas situações:

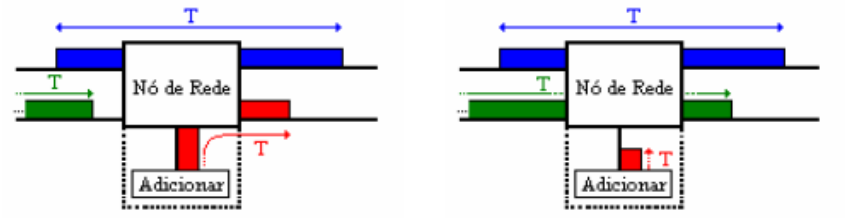


Figura 18 :Perdas de pacotes pela adição de novos pacotes.

3.6. Resultados e discussão de simulação

Aqui serão apresentados os resultados adquiridos com o simulador NS, constituído por arquivo ".txt" que contém "m linhas" e "n colunas", sendo que cada coluna representa os seguintes parâmetros.

- ***Event*:** esta coluna refere-se a ação ocorrida com o pacote que pode ser dos tipos pacotes recebidos, pacotes enviados para a fila, pacotes retirados da fila, pacotes perdidos, que são representados pelos seguintes símbolos respectivamente (r, +, -, d);
- ***Time*:** tempo em que o evento ocorre;
- ***From node*:** nó de entrada do nó no link em que o evento ocorre;
- ***To node*:** nó de saída do link em que o evento ocorre;
- ***Pkt type*:** tipo de pacote;
- ***Pkt size*:** tamanho do pacote;
- ***Flags*:** parâmetro não utilizado; mantido em zero;
- ***Fid (flow id):*** este é o fluxo id (fid) do IPv6 representado por um número inteiro que um usuário pode ajustar para cada fluxo na entrada do script OTcl;
- ***Src addr*:** endereço de uma determinada fonte em forma de porta de nó;
- ***Dst addr*:** endereço de destino de uma fonte em forma de porta nó;
- ***Seq Num*:** número seqüencial de pacotes de protocolos na camada de rede;
- ***Pkt id*:** id original do pacote;
- ***TTL (time to live):*** que é o tempo de vida de um pacote na rede;
- ***Prior:*** quando há prioridade de pacotes;
- ***Número de deflexões:*** número de deflexões dos pacotes ópticos;

Os resultados referentes aos parâmetros definidos acima foram utilizados para realização de outros cálculos no *script* awk. Os resultados calculados através deste *script* awk foram:

- **Número de pacotes recebidos (Tpckt_r):** para obter esta variável é necessário apenas contar os **"r"** contidos na primeira coluna **(EVENT)** do arquivo.txt gerado pelo NS .

- **Número de pacotes perdidos (Tpckt_d):** semelhante a variável calculada acima, aqui teremos apenas de contar a letra **"d"** referente aos pacotes perdidos do arquivo ".txt" gerado pelo NS.
- **Número de pacotes considerados (Tpckt_consid):** esta variável foi calculada baseando-se no número médio de *hops* que cada pacote tenha realizado. Caso o pacote houvesse realizado zero *hops,* interpreta-se que o pacote foi perdido no nó de origem (Tpckt_d_src) e, portanto, este pacote seria descartado de nossa contagem de pacotes considerados. Assim, no final da transmissão de todos os pacotes, conseguimos contar os Tpckt_consid que são todos os pacotes transmitidos, menos os que foram perdidos no nó de origem.
- **Fração de pacotes recebidos (prf):** esta variável foi calculada utilizando o número Tpckt_r e dividindo pelo Tpckt_consid;
- **Fração de perda de pacotes (plf):** o mesmo cálculo realizado para **prf** foi utilizado para calcular **prf**, trocando apenas a variável Tpckt_r por Tpckt_d;
- **Número médio de *hops* (avhops):** com o número de *hops* realizados por cada pacote o Avhops é facilmente calculado somando todos *hops* realizados por todos os pacotes e dividindo esta soma pelo total de pacotes.
- **Tempo médio de transmissão de cada pacote (avdelay)**: foi calculado o tempo de transmissão de cada pacote, e após este cálculo foi realizado o calculo médio que é o tempo total de transmissão de todos pacotes pelo número total de pacotes.

Obs.: Desconsideramos os pacotes perdidos no nó de entrada para os cálculos **prf e plf**, pois trata-se de uma perda ocorrida por fatores internos do simulador que, apesar de se tratar de um software bastante confiável, ainda possui suas limitações.

Os gráficos e comentários dos resultados estão apresentados a seguir.

A Figura 19 é referente ao número total de pacotes recebidos em seus endereços de destino, utilizando o tráfego PCIC e PCIV e o roteamento SF e DR. Os gráficos que transmitem os seus pacotes em intervalos de tempo constantes, sendo os pacotes também de tamanho constante (PCIC), e utilizando tanto o roteamento SF quanto DR, mostraram valores baixos para todas as redes analisadas, exceto, para a MS-4 nós, que por ser muito

pequena e suas conexões de nós coincidirem com a de um anel, já eram esperadas as pequenas perdas comparadas com as de outras redes. A justificativa deste resultado é o fato de se tratar de transmissão de pacotes com intervalos constantes (PCIC), sendo que bastaria a perda de um pacote para causar as perdas de todos os outros pacotes transmitidos posteriormente. Considerando-se, portanto, a principal causa destas perdas obtidas com a simulação, devido ao sincronismo na transmissão dos pacotes.

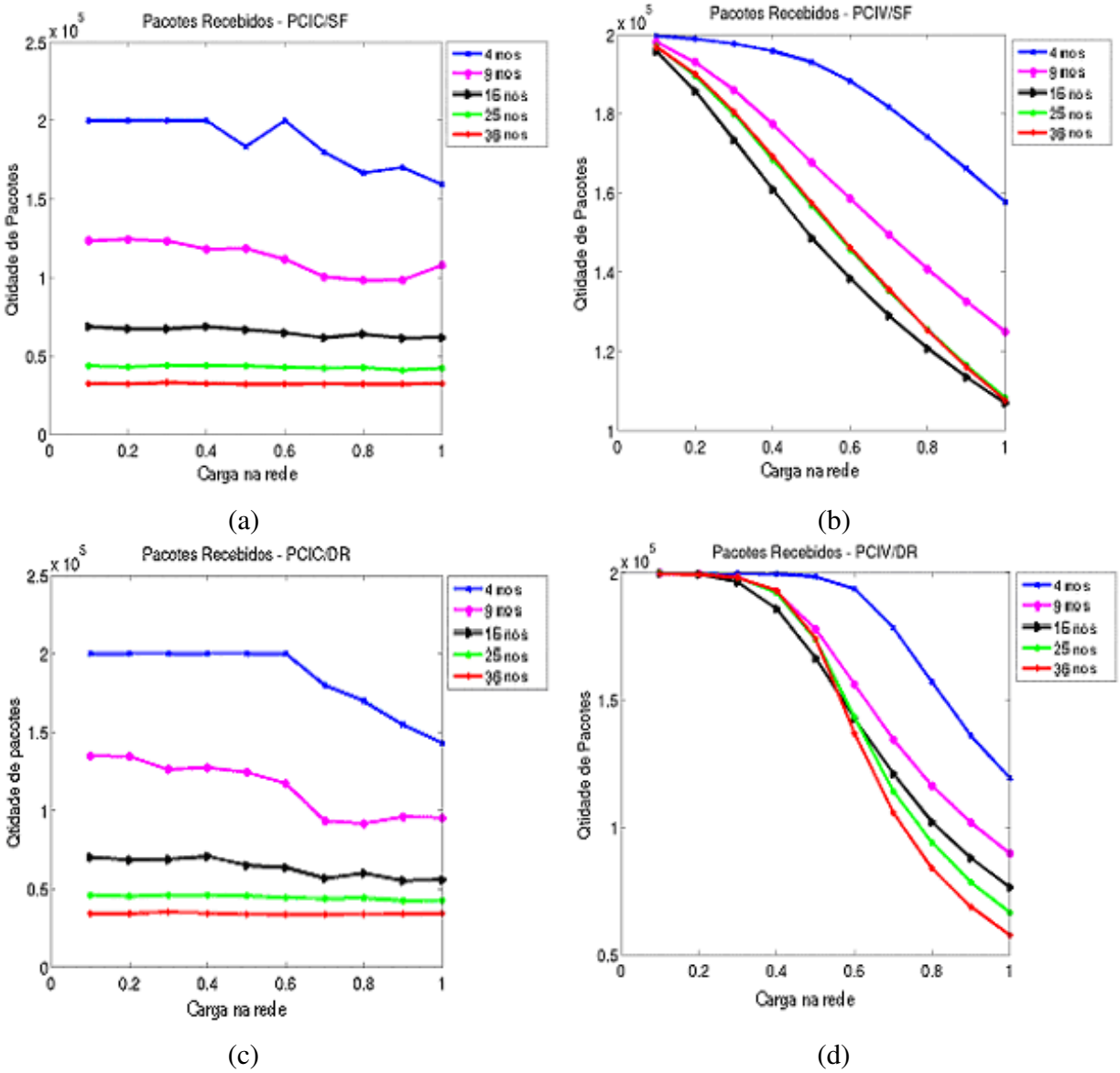


Figura 19 : Quantidade total de pacotes recebidos com (a) tráfego PCIC e roteamento SF; (b) tráfego PCIV e roteamento SF, (c) tráfego PCIC e roteamento DR e (d) tráfego PCIV e roteamento DR.

Outra informação importante da Figura 19 (Pacotes Recebidos) é a diferença entre os gráficos que utilizam tráfegos PCIC dos que utilizam tráfego PCIV. Pode-se notar que eles se diferem pelo formato de suas curvas. Para o PCIC a quantidade de pacotes recebidos é praticamente a mesma para todas as cargas da rede, apresentando uma pequena variação. Para PCIV, quanto mais carregada a rede mais perda terá, sendo este resultado mais lógico, pois quanto maior a quantidade de pacotes que estiver circulando na rede, seja ela de 4, 9 16, 25 ou 36 nós, a probabilidade de colisões, perdas devido a resolução de contenda espacial e grandes atrasos de transmissão, será bem maior.

Verificou-se também que para tráfego e roteamento PCIV/SF, o número de pacotes recebidos na rede MS-16 nós particularmente, tendo carga máxima (Lc = 100%) foi aproximadamente igual ao das redes MS-25 e 36 nós.

A Figura 20 representa o número de pacotes perdidos causados por adicionamento de pacotes no nó de entrada. Nota-se para todos os gráficos desta Figura 20, valores significativos referentes a este tipo de perdas de pacotes, que já foi explicado anteriormente neste capítulo.

O gráfico PCIV/SF da Figura 20 apresenta perdas de pacotes no nó de entrada que não seguem a ordem do número de nós, como acorre para os gráficos PCIC desta figura. Verifica-se que a rede MS-16 nós obteve a maior perda de pacotes na entrada. Entretanto, para PCIV/DR as perdas foram praticamente as mesmas para todas as redes, exceto para MS-4 que mostrou perdas inferiores em todas as cargas entre 40% a 90% aproximadamente.

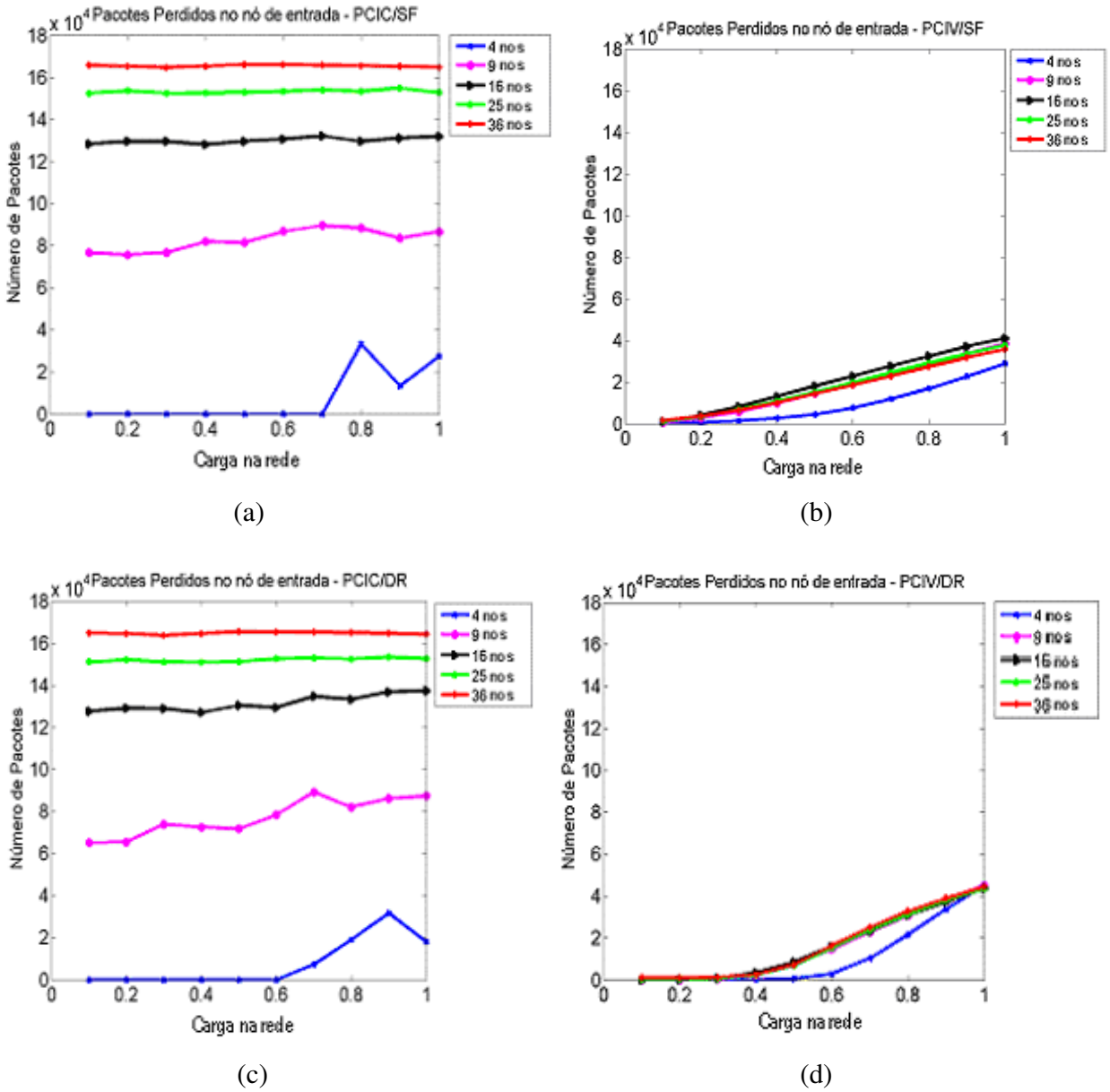


Figura 20 : Quantidade total de pacotes perdidos no nó de entrada com: (a) tráfego PCIC, (b) tráfego PCIV, com roteamento SF; (c) tráfego PCIC, (d) tráfego PCIV, com roteamento DR.

A Figura 21 refere-se a porcentagem de pacotes recebidos, desconsiderando os pacotes que foram perdidos na entrada do nó. Observa-se que para o tráfego PCIC há uma variação de valores, tornando as curvas instáveis. Isto ocorre porque o tráfego PCIC transmite os pacotes em intervalos de tempo fixos e, com isto, caso ocorrer uma perda de

pacote, todos os outros pacotes que serão transmitidos posteriormente serão perdidos, devido ao sincronismo de transmissão, como já falado e explicado anteriormente.

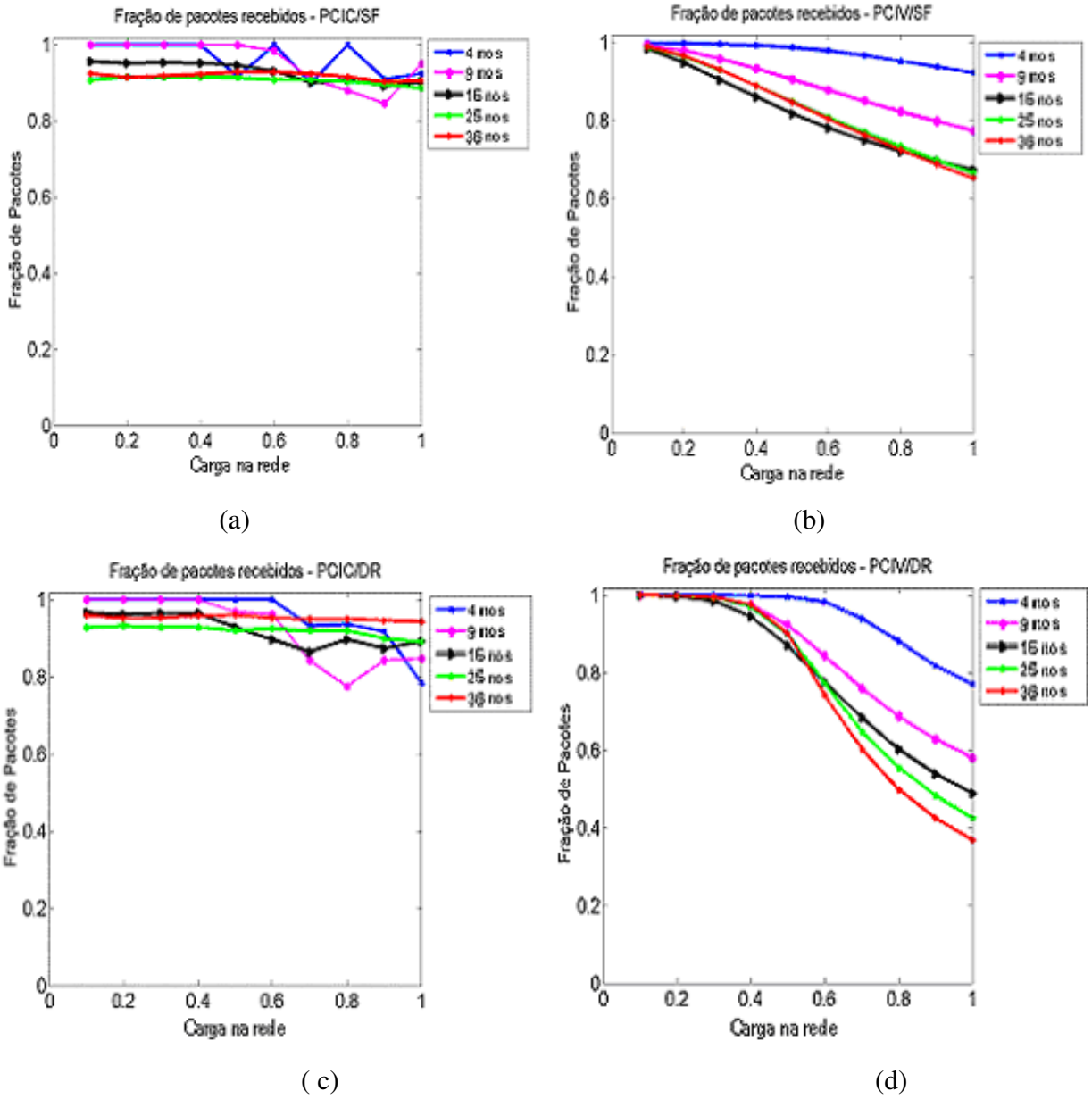


Figura 21 : Fração de pacotes recebidos desconsiderando os perdidos no nó de entrada com (a) tráfego PCIC e roteamento SF; (b) trafego PCIV e roteamento SF, (c) tráfego PCIC e roteamneto DR;e (d) tráfego PCIV e roteamento DR.

Percebe-se que nos gráficos onde o intervalo de transmissão de pacotes é variado (PCIV), as curvas das 5 redes analisadas são semelhantes, sendo possível verificar que,

quanto maior a carga e número de nós de uma rede, menor é o número de pacotes recebidos, tanto para o roteamento SF, quanto para o DR (gráficos b,d).

A Figura 22 representa a porcentagem de pacotes perdidos desconsiderando a perda de pacotes na entrada do nó, como feito para os gráfico de fração de pacotes recebidos.

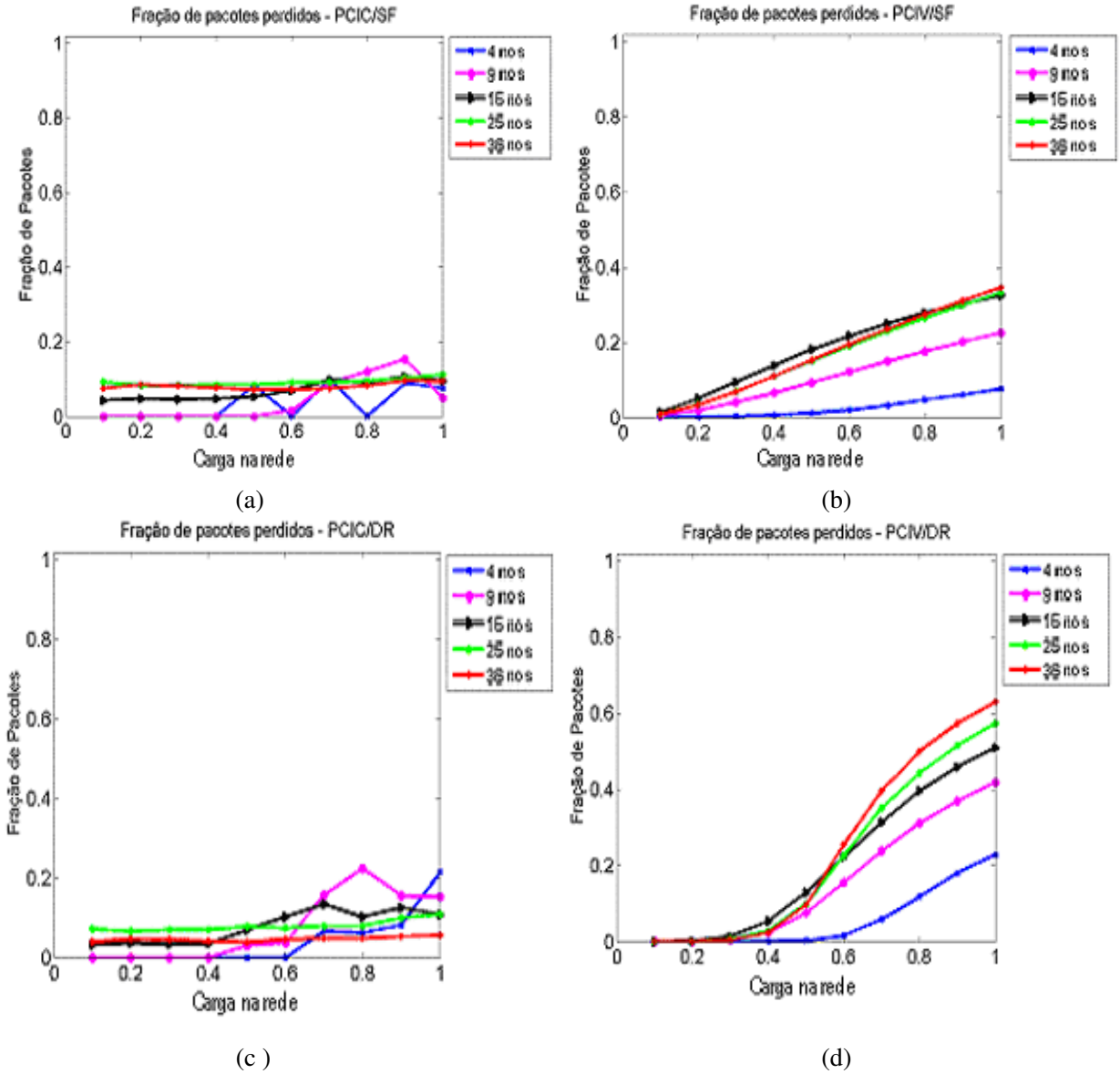


Figura 22 : Fração de pacotes perdidos desconsiderando os perdidos no nó de entrada com (a) tráfego PCIC e roteamento SF e (b) tráfego PCIV e roteamento SF, (c) tráfego PCIC e roteamento DR e (d) tráfego PCIV e roteamento DR.

Nos gráficos de tráfego PCIC da Figura 22, utilizando tanto roteamento SF, quanto o DR nota-se que suas curvas têm o mesmo comportamento. As perdas de pacotes ficaram abaixo de 20% para todas as redes em todas as cargas. Já para os gráficos de tráfego PCIV, verificou-se que, quando se utilizava roteamento DR, as perdas eram muito baixas para as cargas de 1 a 50% da capacidade total das redes, sendo o comportamento destes gráficos de tráfego PCIV mais homogêneos, com curvas crescendo com o aumento da carga das redes. Todas as curvas possuem o mesma forma, diferenciando-se apenas por seu deslocamento no eixo.

A Figura 23 mostra o número médio de *hops* que os pacotes realizam para chegar ao seu endereço de destino. Estes gráficos mostram qual o tipo de tráfego e roteamento que tem o melhor desempenho, levando em consideração o parâmetro distância entre nó de origem e destino que um pacote percorrerá.

Verifica-se que o número médio de *hops* apresenta uma pequena variação com o aumento da carga da rede em quase todos os gráficos, sendo que somente para PCIV/DR que o número médio de *hops* houve um aumento para 9, 16, 25, 36 nós quando a rede estava com uma carga acima de 50%.

No gráfico PCIC/DR da Figura 23 foi notado que a rede de 16 nós quebra a homogeneidade das curvas, apresentando um aumento significativo do valor médio de *hops* na carga de 40% e 80%.

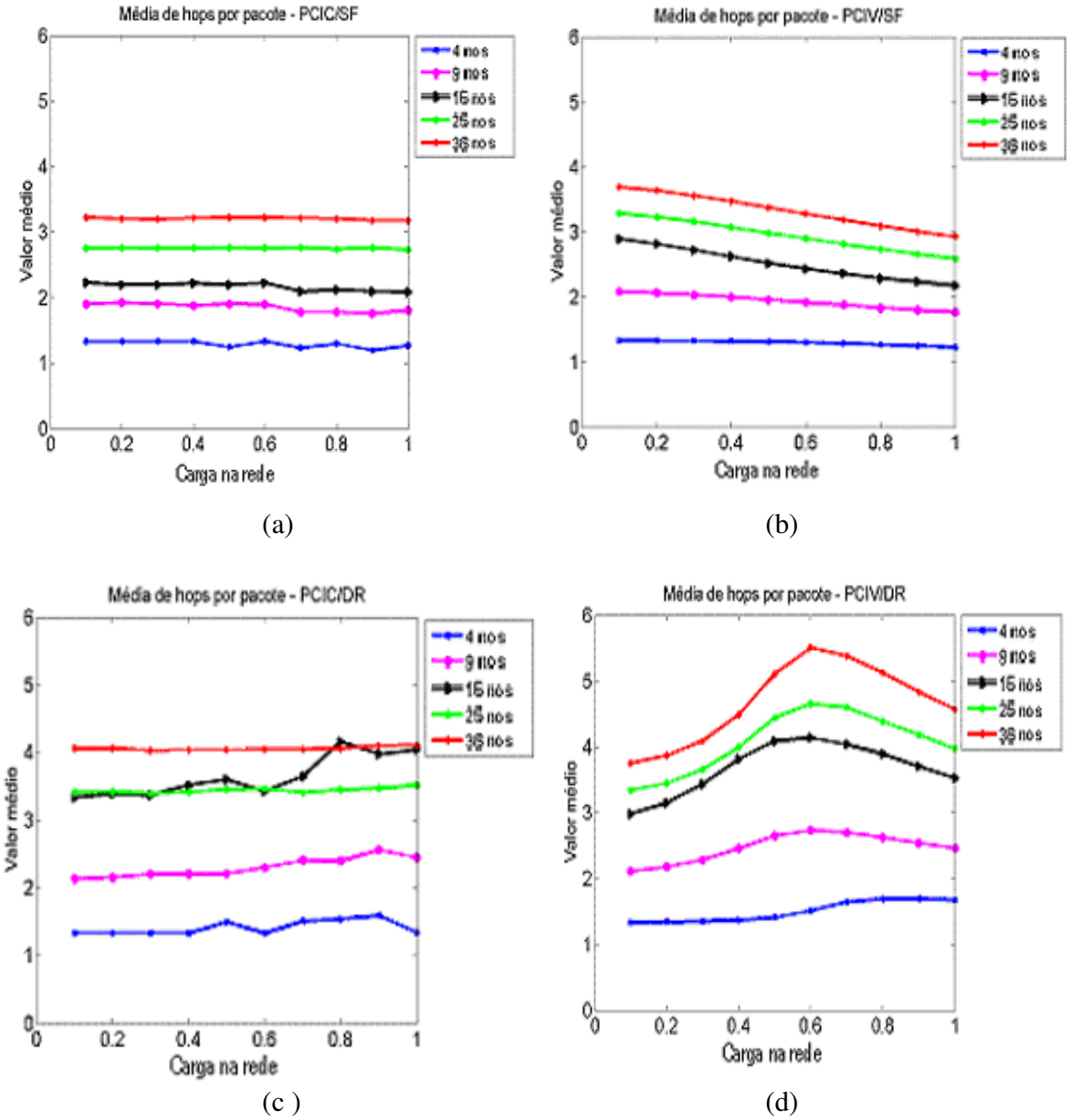


Figura 23 : Número médio de *hops* por cada pacote, com (a) tráfego PCIC e roteamento SF e (b) tráfego PCIV e roteamento SF, (c) tráfego PCIC e roteamento DR e (d) tráfego PCIV e roteamento DR.

A Figura 24 pode ser considerada uma extensão da Figura 23, pois o tempo médio de transmissão de cada pacote é calculado de acordo com o número médio de *hops* realizados pelos pacotes considerados.

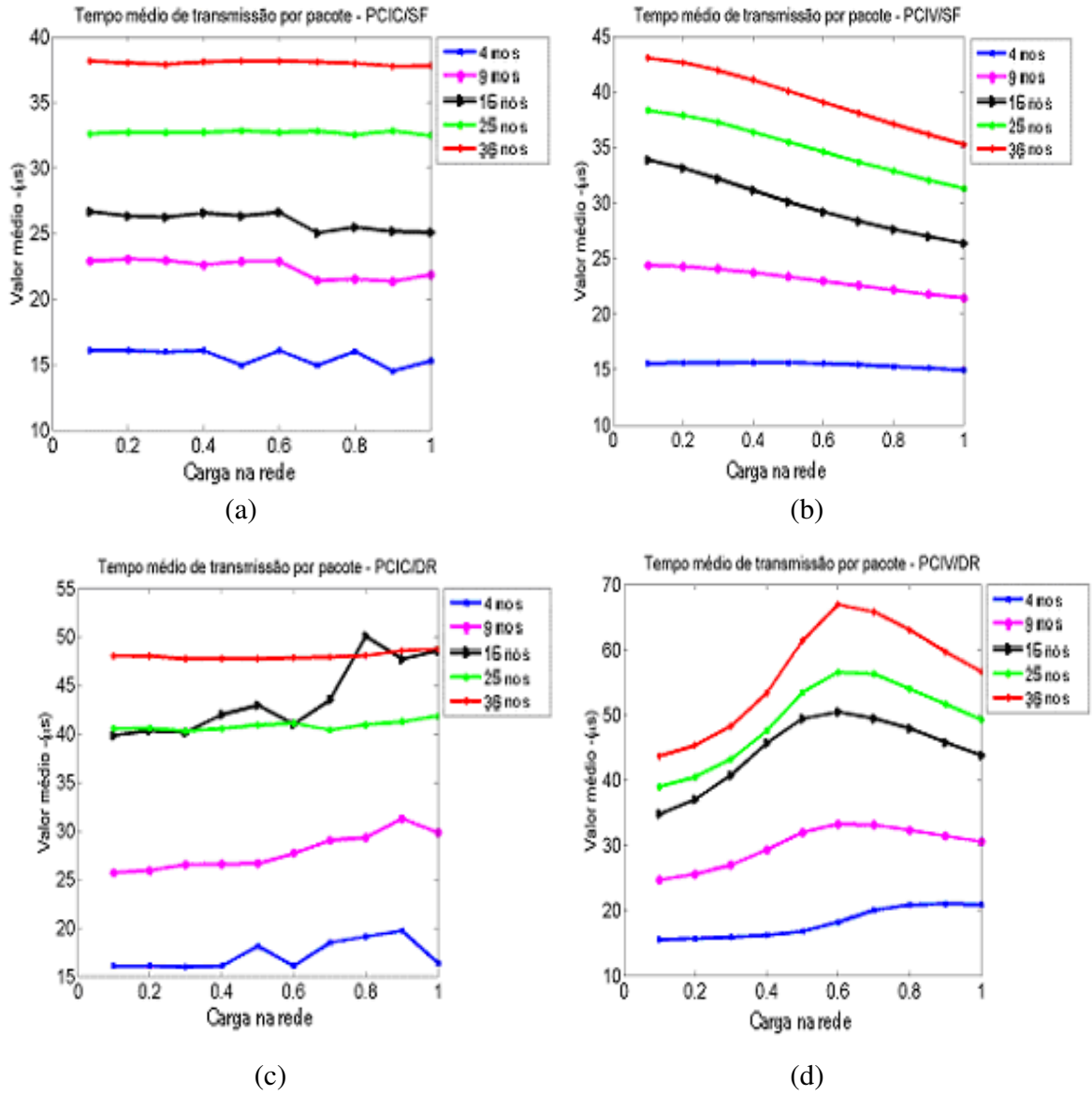


Figura 24 : Tempo de transmissão por cada pacote, com (a) tráfego PCIC e roteamento SF e (b) tráfego PCIV e roteamento SF, (c) tráfego PCIC e roteamento DR e (d) tráfego PCIV e roteamento DR.

A Figura 25 refere-se ao número de pacotes normalizados, ou seja, trata-se da razão entre pacotes considerados e o número total de pacotes simulados (desconsiderando as perdas por adicionamento de pacotes na entrada do nó de origem).

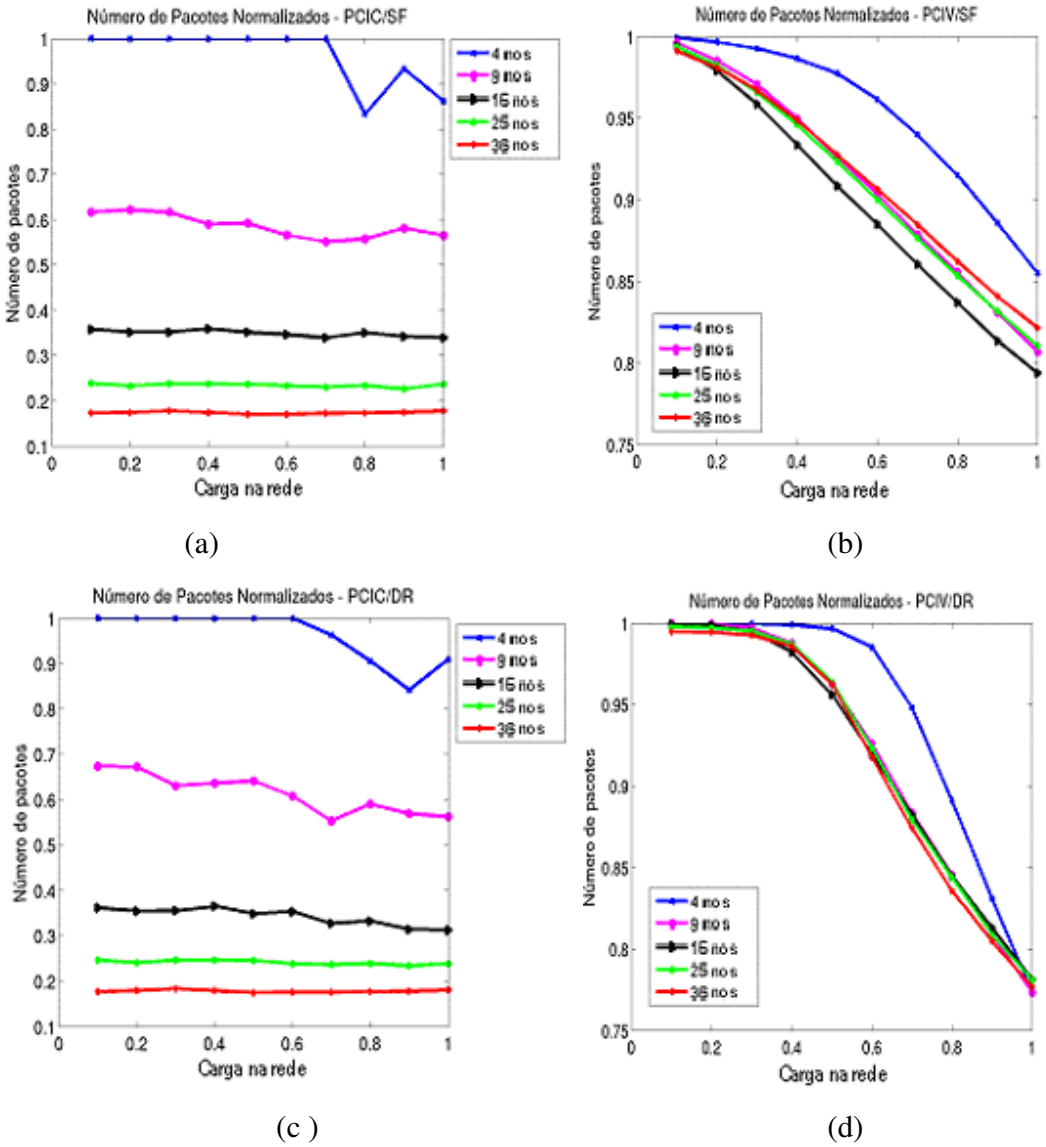


Figura 25 : Número de Pacotes Normalizados (a) tráfego PCIC e roteamento SF e (b) tráfego PCIV e roteamento SF, (c) tráfego PCIC e roteamento DR e (d) tráfego PCIV e roteamento DR.

Neste capítulo, vimos os resultados teóricos e de simulações que foram analisados. Nos próximos capítulos serão apresentados estudos e resultados dando enfoque em mecanismos de proteção de redes e analisando os mesmos parâmetros deste capítulo, considerando falha de *link.*

3.7. Referências

[3.1] A. S. Acampora, "A multichannel multihop local lightware networks", in Proc. IEEE GLOBECOM'87 *Conf.,* Nov. 1987, pp. 1459-1467.

[3.2] A. S. Acampora and S. I. A. Shah, "Multihop lightwave network: a comparison of store-and-forward and hot potato routing", *IEEE Trans. Communications*, vol.40, no.6, pp.1082-1090 (1992).

[3.3] F. Rudge Barbosa, A.C.Sachs, "Transparent Optical Packet Switching Node based on Bottom-up Organization Network", *XXI Simp. Brasileiro Telecom – SBT'2004*, Belém PA, Brasil, Set. 2004.

[3.4] I. B. Martins, L. H. Bonani, F.R. Barbosa, E. Moschim, "Dynamic Traffic Analysis of Metro Access Optical Packet Switching Networks having Mesh Topologies", *Proceedings of the International Telecommunications Symposium, ITS'2006*, September 2006, Fortaleza, Brazil.

[3.5] L. H. Bonani, F.R. Barbosa, E. Moschim, "Modelling And Analysis of Optical Packet Switched Networks in Mesh Topology", *Proceedings of the International Telecommunications Symposium, ITS'2006*, September 2006, Fortaleza, Brazil.

[3.6] Y. H. Cho and K. Kim, "Impact of 3R Wavelength Converters on the Blocking Probability of WDM Networks with Finite Signal Impairment Threshold", *IEEE Communications Letters*, vol.9, no.11, November 2005.

[3.7] L. H. Bonani, F. L. Pádua, Edson Moschim and F. Rudge Barbosa, "Optical Packet Switching Access Networks using Contention Resolution without Wavelength Conversion", *11th Intl. Conf. on Telecomm.– ICT '2004*, paper TS-25-3, Fortaleza, Brasil, Aug. 2004; and Springer-Verlag , Nov.2004.

[3.8] F. Rudge Barbosa, et al, "Optical Packet Switching Node for Metro-Access Networks", paper PD-160, *Proceed. 29th. ECOC'2003*, Rimini, Italia, Sept. 2003.

[3.9] L.H. Bonani, "Contribuição ao Estudo de Redes Fotônicas de Pacotes", Dissertação de Mestrado, FEEC/Unicamp, 2003.

[3.10] D. J. Blumenthal, P. R. Prucnal and J. R. Sauer, "Photonic packet switching: architectures and experimental implementations", *Proceedings of the IEEE*, vol.82, no.11, pp.1650-1667 (1994).

[3.11] L.H. Bonani "Uma Proposta Inovadora para a Arquitetura de Redes Fotônicas de Pacotes", Monografia apresentada para teste de qualificação do programa de doutorado da FEEC/Unicamp

[3.12] L.H.Bonani, F.Rudge Barbosa, Edson Moschim., "Fully Optimized Mesh Topologies for Optical Packet Switching Network Architectures", *accepted for presentation at ICT 2006*, paper ON1-2, Madeira, Portugal, 2006.

[3.13] www.mathworks.com.br

4. Mecanismos de Proteção e Restauração em Redes Ópticas

Hoje em dia, sejam os usuários residenciais ou empresariais de pequeno ou grande porte, redes de comunicações são utilizadas dia e noite, dificultando a realização de manutenção dessas redes. A simples interrupção do sistema acarretaria uma enorme perda de quantidade de dados que trafegam pelas redes e com isto, a perda de receita e insatisfação dos usuários. Por este aumento de tráfego de dados nas redes em geral, torna-se essencial a implantação de métodos de sobrevivência, caso haja algum tipo de falha, evitando assim que muitas informações (pacote ou rajada) sejam perdidas, além de preservar o desempenho parcial no pior dos casos ou até mesmo total, nestas redes.

Neste capítulo abordaremos apenas a parte conceitual, explicitando alguns mecanismos tradicionais de proteção e restauração em redes ópticas em malha, Os resultados numéricos de simulação serão apresentados no capítulo 5.

4.1. Conceitos básicos

Definiremos a seguir alguns conceitos básicos utilizados na implementação de proteção em redes ópticas, devido, como visto, a grande quantidade de informações e serviços que nelas trafegam.

Uma grande variedade de técnicas de proteção são usadas nas redes atuais. Definem-se caminhos de trabalho, aquele que carrega tráfego sob operação normal; e caminhos de proteção, o que fornece um caminho alternativo para o tráfego em caso de falhas [4.1].

Boa parte dessas técnicas foi desenvolvida no ambiente SDH durante a década de 80. A tecnologia SDH permite implementar mecanismos variados de proteção nos equipamentos e na própria rede, oferecendo serviços com alta disponibilidade e efetiva segurança no transporte de informação.

As técnicas de proteção são projetadas para operar de forma dedicada ou compartilhada. Na proteção dedicada, aloca-se, a cada conexão um caminho de trabalho e um caminho de proteção, que são disjuntos e dedicados. Na proteção compartilhada aloca-se, a cada conexão, um caminho de trabalho e um caminho de proteção que pode compartilhar capacidade com outros caminhos de proteção, cujos caminhos de trabalho são disjuntos.Tanto a proteção dedicada como a compartilhada pode ser do tipo 1+1(trilha exclusiva para uso de proteção) e 1:1 (trilha de proteção pode ser usada para tráfego extra, descartando em situação de contingência).

Técnicas de proteção também podem ser reversíveis e não reversíveis[4.1] [4.2] [4.3]. Em ambas, se houver falha na rede, o tráfego é chaveado do caminho de trabalho, para o de proteção. No esquema não reversível, o tráfego é chaveado para o caminho de proteção, quando houver alguma falha e voltará a trafegar no caminho de trabalho em condições normais, caso o gerente da rede realizar este chaveamento, que é feito manualmente. Já para o reversível, o caminho de trabalho quando é reparado, o tráfego é chaveado automaticamente para o caminho normal. Ainda neste capítulo entraremos mais em detalhes sobre assunto de reversibilidade dos mecanismos de proteção.

Outro detalhe importante para as técnicas de proteção de rede, é o tipo de chaveamento de proteção que pode ser unidirecional ou bidirecional [4.1] [4.2]. No chaveamento de proteção unidirecional, cada direção de tráfego é independente do outro. Assim, no evento de um corte de uma fibra, somente um tráfego é chaveado para a fibra de proteção e outro permanece na fibra de trabalho original. Em chaveamento de tráfego bidirecional, ambas as direções seriam chaveadas para a fibra de proteção. A Figura 26 apresenta o caminho de proteção de um anel bi/unidirecional.

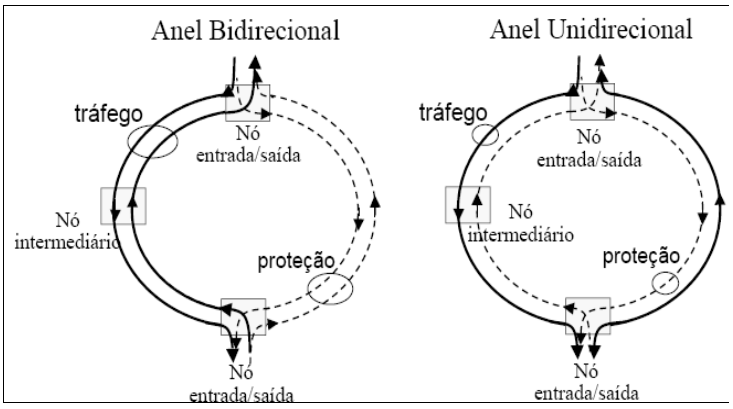


Figura 26 : Anéis /enlaces uni- e bi-direcionais (2 ou 4 fibras com proteção)

Bidirecionais:

- Há tráfego bidirecional em cada enlace entre nós;
- Proteção em rota diversificada;
- Duas fibras: um braço leva tráfego de linha; outro braço tráfego de proteção;
- Quatro fibras: cada braço carrega tráfego de linha e de proteção;

Unidirecionais:

- Anel unidirecional o tráfego circula em sentido único ao redor do anel;
- Proteção circula no sentido oposto;
- Uma direção leva tráfego, outra direção leva proteção;
- Bastam duas fibras para realizar proteção em anéis unidirecionais;

Sistemas de proteção em redes Ópticas estão presentes nas camadas físicas, rede óptica, transporte e acesso; são nessas camadas que podem existir algum mecanismo de proteção e também de restauração.

As falhas podem ocorrer por vários motivos como, cortes de cabos de fibras, falhas de componentes, mau funcionamento de *software,* incêndios ou inundações em centrais e nós.

As redes ópticas utilizam planejamento de sobrevivência de serviços que pode ser categorizado em 4 fases para assegurar continuidade e minimizar o nível de impacto

causado pela interrupção de serviço. As fases são: prevenção, detecção rápida, auto-reparação da rede através de projetos robustos, restauração manual.

- A 1º fase focaliza a prevenção de falhas nas redes. Nesta fase, esforços são localizados para minimizar problemas criados por pessoas. Por exemplo: fogo em centrais.
- A 2º fase focaliza em uma rápida detecção de falhas de componentes de rede. Solução nesta fase seria incluir sistemas de alarmes.
- A 3º fase focaliza a capacidade da própria rede reparar a falha do componente. Aqui focaliza-se o planejamento e a prática de restauração em casos de a rede não poder solucionar a falha.

4.2. Parâmetros de qualidade de serviço

Aqui apresentaremos a definição de alguns dos principais parâmetros de qualidade de serviço em redes ópticas.

- **Confiabilidade**

A confiabilidade de uma conexão é a probabilidade de uma conexão operar ininterruptamente, ou seja, sem falhas, por um período de tempo. A confiabilidade está associada ao tempo médio entre falhas (*Mean Time Between Failures* – MTBF) que o sistema apresenta.

- **Disponibilidade**

A disponibilidade de uma conexão é a probabilidade da conexão estar operando. Ao contrário da confiabilidade, a disponibilidade leva em conta o tempo que uma falha deixou a conexão inativa. Portanto, o tempo que se gasta em recuperar uma falha da conexão é levado em consideração. A confiabilidade está relacionada ao número de interrupções que sofre uma conexão em um período de tempo e a disponibilidade está também relacionada à porcentagem de tempo que a conexão ficou interrompida. A disponibilidade pode ser computada analiticamente levando-se em conta o tempo médio entre falhas e a taxa de recuperação de falhas. É importante ressaltar que, como o tempo de recuperação de falha de

uma conexão é computado no cálculo da disponibilidade, a política de operação e o mecanismo de proteção de conexão utilizado, passam a influir diretamente na disponibilidade. A Figura 27 ilustra a disponibilidade de uma conexão, onde C é o início da conexão, D é o término da conexão, F é o início de uma falha na conexão e R é o início do restabelecimento da conexão.

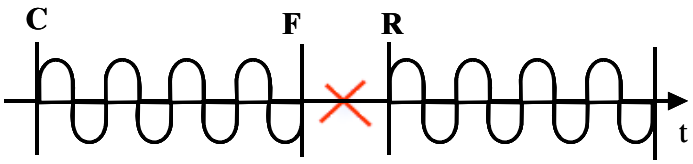


Figura 27 : Disponibilidade de conexão no tempo.

- **Probabilidade de Bloqueio**

A probabilidade de conexão é a probabilidade de um pedido de conexão não ser atendido por falta de recursos da rede. A probabilidade de bloqueio é um parâmetro de grande utilidade para as operadoras, pois quanto menor é a quantidade de bloqueio, maior é o número de clientes que estão utilizando os serviços com os mesmos recursos da rede, sem nenhuma implementação extra. Outro ponto que deve ser citado é que a baixa probabilidade de bloqueio resulta em uma maior confiabilidade dos clientes.

4.3. Diferenças entre Proteção e Restauração

Os mecanismos de proteção e restauração são classificados como mecanismos de sobrevivência a falhas e são abordados distintamente pela literatura [4.2]. Antes de começar a diferenciar proteção de restauração, conceitos de *computação, reserva* e *configuração* da capacidade utilizada pela conexão, quando houver alguma falha na rede (capacidade alternativa) serão introduzidos, a fim de que o leitor compreenda de forma fácil outras definições que virão ao longo desta e de outras seções e que são essenciais para este trabalho.

O conceito *computação* é puramente lógico e define a capacidade alternativa a ser adotada em caso de falha. *Reserva* aloca capacidade alternativa e só permite que ela

também seja utilizada por outras conexões em condições especiais de compartilhamento. A *configuração* atua nos nós da rede e estabelece o caminho físico para a transmissão.

Foram classificados como mecanismos de proteção como em [4.5] aqueles em que a capacidade para o re-roteamento da conexão(enlace ópticos) no caso de ocorrência de falha é pré computada e reservada. Já mecanismo de restauração é aquele em que a capacidade para o re-roteamento da conexão é pós-computada e configurada. Os mecanismos de proteção normalmente possuem um tempo de recuperação menor, uma vez que a capacidade alternativa já é conhecida antes da ocorrência da falha. Entretanto o intervalo de recuperação do tráfego exclui a fase de computação. Já os mecanismos de restauração tendem a ser mais eficientes em capacidade, pois dispõem do estado da rede no momento da falha (enlaces disponíveis) para o cálculo da capacidade alternativa, mas por outro lado, eles não oferecem garantias de que haverá capacidade ociosa suficiente para recuperar a conexão afetada.

A proteção é conveniente por oferecer garantias contra alguns tipos de falhas como, por exemplo, falhas simples em fibra. Já a restauração aplica um algoritmo em tempo real para encontrar a capacidade alternativa, independente do estado da rede.

4.4. Mecanismos de sobrevivência a falhas em redes ópticas em malha

Os mecanismos de sobrevivência a falhas (proteção e restauração) [4.6] podem ser aplicados em enlaces, caminhos e sub-caminhos. Para enlace, a conexão segue um trajeto alternativo entre os nós adjacentes à falha nodal ou de enlace. O mecanismo age localmente de forma que o restante do caminho que não é afetado pela falha permanece o mesmo. Nos mecanismos de proteção e restauração de caminhos, em caso de falha, a conexão segue um caminho alternativo entre os nós origem-destino da conexão. Neste, o mecanismo age de forma global, utilizando a capacidade alternativa disponível da rede. No mecanismo de proteção ou restauração de sub-caminhos, o caminho original é dividido em sub-caminhos, e um trajeto alternativo é adotado entre os nós nas extremidades do sub-caminho. Caso o

sub-caminho seja o caminho completo, tem-se a proteção de caminho; caso cada sub-caminho seja um enlace, tem-se a proteção de enlace.

Uma vez sabendo onde aplicar a proteção e restauração, podemos classificá-las e defini-las em:

- Proteção Dedicada: trajeto da proteção é disjunto dos trajetos de trabalho e proteção de todas as conexões ativas.
- Proteção Compartilhada: o trajeto de proteção, também disjunto do trajeto de trabalho, pode não ser disjunto de outros trajetos de proteção, desde que certas condições sejam satisfeitas.
- Proteção Dependente a falha [4.2]: são reservados caminhos de proteção alternativos, que não são necessariamente disjuntos dos caminhos de trabalho e proteção das conexões roteadas na rede. O caminho de proteção a ser adotado, depende do enlace que vier a falhar. A proteção, dependente da falha, é um mecanismo novo e que não aparece nas classificações tradicionais publicadas na literatura.

A diferença entre as três proteções citadas acima é relacional, pois refere-se às relações de compartilhamento entre os caminhos de trabalho e proteção das conexões.

A proteção dedicada e a compartilhada se aplicam aos três casos de classificação espacial (enlace, caminho e sub-caminho), mas a proteção dependente da falha só é aplicada à de caminho. A Figura 28 mostra a classificação de proteção e restauração

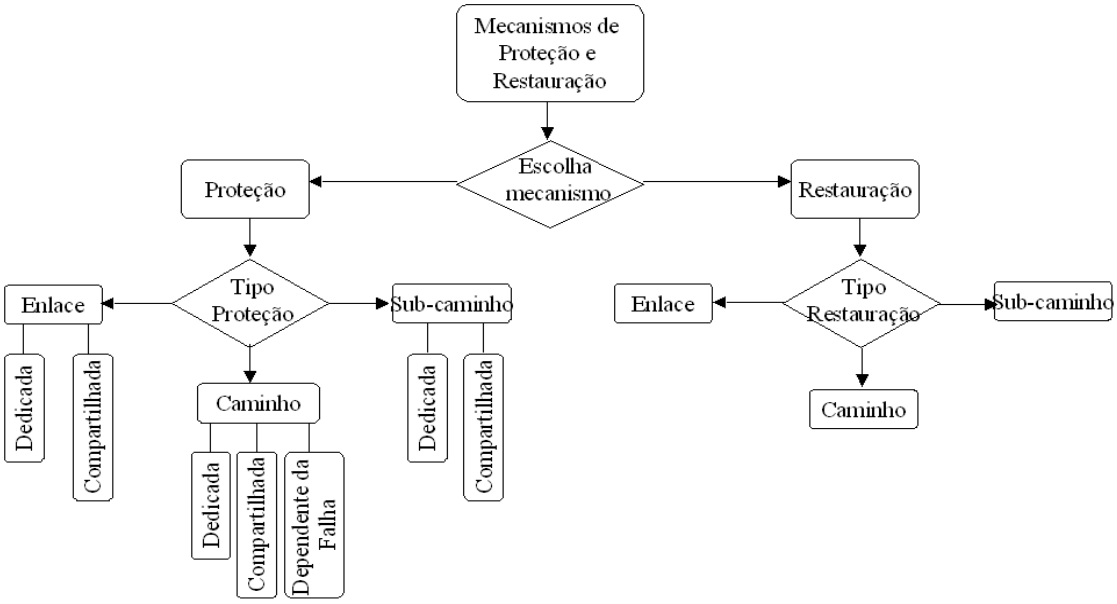


Figura 28 :Classificação de proteção e restauração

4.5. Exemplos de proteção e restauração

Nos sub-itens abaixo foram definidos e apresentados alguns exemplos de mecanismos de proteção e restauração, baseando-se em trabalhos já realizados e publicados [4.2].

4.5.1. Proteção de Enlaces (SP - *Span Protection*)

Na proteção SP um caminho de trabalho (*w*) e trajetos alternativos que conectam os nós adjacentes a cada enlace de *w* são alocados a cada conexão. Na Figura 29, a linha contínua representa a conexão entre A e B e a linha tracejada é a capacidade alocada para proteção. As figuras menores ilustram os caminhos adotados no caso de alguma falha em diferentes enlaces.

OBS: em caso de falha, o caminho só não segue seu trajeto inicial entre os nós adjacentes à falha.

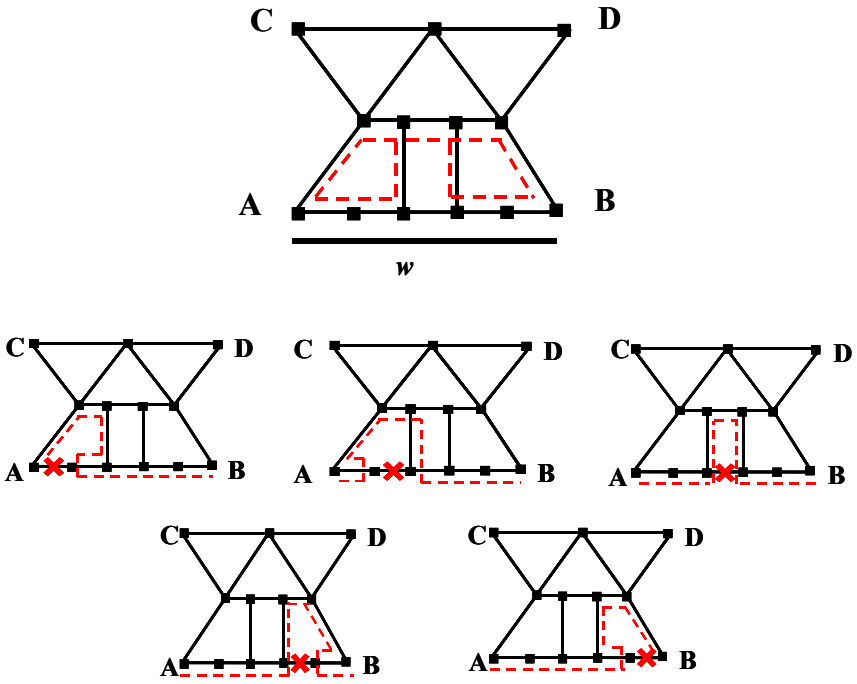


Figura 29 : Proteção de enlace (*Span Protection*-SP)

4.5.2. Proteção por Ciclos Pré-Configurados (*P-Cycles*)

As topologias em malha permitem que mais conexões compartilhem recurso de proteção, mas o tempo de recuperação é geralmente maior. A proteção utilizando p-cycles foi concebida para conciliar a velocidade de recuperação das redes em anel à eficiência em capacidade dos mecanismos de proteção em malha. O p-cycles é um anel pré-configurado que protege enlaces de caminhos que atravessam fibras por onde passa o p-cycle e por enlaces de caminhos que atravessam fibras cujas extremidades estão conectadas a nós que fazem parte do p-cycle, mas não são atravessados por ele. Em caso de falha a conexão é re-roteada para um dos arcos do p-cycle pelos nós adjacentes à falha. A eficiência em capacidade do mecanismo está no compartilhamento de recursos de proteção por enlaces internos e enlaces apoiados, no compartilhamento de recursos de proteção por enlaces internos e enlaces apoiados, estes inexistentes nas redes em anel. Na Figura 30 a linha tracejada representa um p-cycles, e as linhas sólidas representam dois caminhos de trabalho roteados na rede. Os enlaces de W1 são internos ao p-cycle e o enlace de W2 é apoiado. As duas conexões são protegidas contra falhas simples de enlaces.

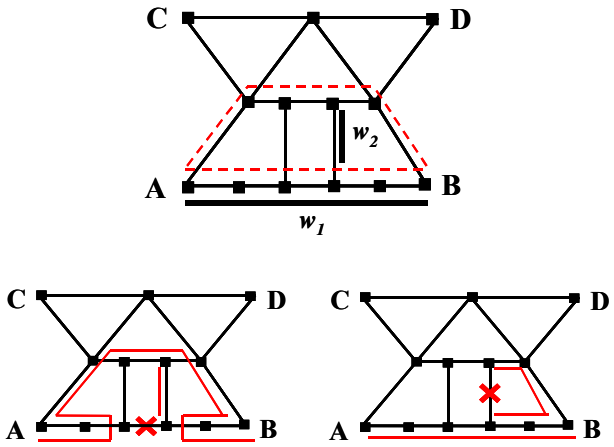


Figura 30 : Proteção por ciclos pré configurados (*p-cycles*)

4.5.3. Proteção de Caminho Dedicada (*Dedicated Path Protection – DPP*)

A DPP aloca a cada conexão um caminho de trabalho w e um caminho de proteção b, disjuntos e dedicados mostrados na Figura 31. Ela pode ser 1+1 quando no caminho de trabalho e proteção trafegarem simultaneamente a mesma informação; ou 1:1, no caso do caminho de proteção transportar apenas dados de w depois de ele falhar. A DPP 1+1 tem como vantagem o curtíssimo tempo de recuperação, que é gerada por chaveamento local junto ao receptor. Mas a 1: é mais eficiente porque permite que os enlaces ópticos alocados para proteção sejam usados para o transporte de tráfego não prioritário, enquanto w estiver íntegro.

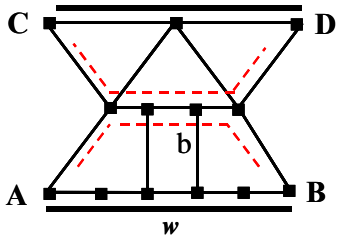


Figura 31 : Proteção de caminho dedicada

4.5.4. Proteção por compartilhamento de Caminhos de Reserva (*Shared Backup Path Protection* – SBPP)

A SBPP aloca a cada conexão um caminho de trabalho w e um caminho de proteção b, que pode compartilhar capacidadde com outros caminhos de proteção cujos caminhos de trabalho são disjuntos de w. Por disjuntos entendem-se caminhos de proteção que não percorrem enlaces comuns. Esta condição para o compartilhamento é conhecida como restrição de grupo de enlaces com risco compartilhado. Na Figura 32 as conexões A-B e C-D compartilham capacidade de proteção (tracejada), o que economiza três enlaces em comparação a DPP .

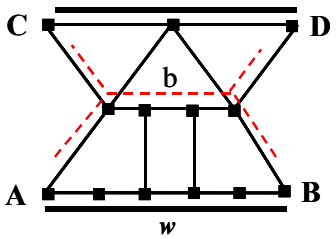


Figura 32 : Proteção por compartilhamento de caminhos de reserva

4.5.5. Restauração de Enlaces – (*Span Restoration* – SR) e Restauração de Caminho (Path Restoration – PR)

Como foi dito anteriormente, nos mecanismos de restauração a capacidade para o re-roteamento da conexão é pós-computada e pós –configurada. A reserva de recurso não é feita. A restauração de enlaces calcula o menor trajeto entre os nós adjacentes à fibra que falhou. Enquanto a restauração de caminho calcula o menor caminho entre os nós de origem-destino do caminho que passa pela fibra que falhou.

4.6. Reversibilidade dos Mecanismos de Proteção

A reversibilidade para mecanismos de proteção dedicados (1+1) é um fator preponderante, porque o canal secundário não é compartilhado, já para proteção

compartilhada (1:1 ou 1:N) pode influenciar no desempenho, uma vez que os canais secundários ou caminhos de proteção são compartilhados[4.3].

Como foi explicado no início deste capítulo, um mecanismo de proteção é classificado como reversível se, após a recuperação de um enlace (que falhou), as conexões afetadas pela falha, voltam ao seu caminho de trabalho ou canal primário. Entretanto o não-reversível, mesmo após a recuperação do enlace (que falhou) não reverte ao canal primário.As Figura 33 e Figura 34 são eventos de um mecanismo reversível e de um não-reversível respectivamente. Os Cs representam os instantes de tempo em tempo de ocorrência de eventos de conexão; F representa falha, R recuperação da falha, D Deslocamento. São mostradas 2 conexões ópticas C_1 e C_2 que vão comutar do canal primário para o secundário (S) que é compartilhado. A vantagem da não reversibilidade é a redução da quantidade de comutações entre o canal primário e o canal secundário que são efetuadas para oferecer sobrevivência às possíveis falhas das fibras ópticas e outros componentes da rede. As Figura 33 e Figura 34 mostram apenas duas comutações entre canal enquanto o mecanismo reversível utiliza quatro comutações. O efeito das comutações na disponibilidade depende do tempo necessário para realizar as comutações. Caso as comutações sejam realizadas em um curto período de tempo, a disponibilidade não é muito afetada. No entanto, as reconfigurações das redes ópticas são, em geral, lentas, pois os comutadores totalmente ópticos não apresentam um hardware com tempo de resposta baixo o suficiente. Como conseqüência, a comutação entre canais ópticos usualmente acarreta na desordenação na entrega de pacotes ao destino e até na indisponibilidade do serviço por um período de tempo. Portanto, em redes nas quais que se pretende garantir alto índice de disponibilidade, esta comutação de canais deve ser evitada.

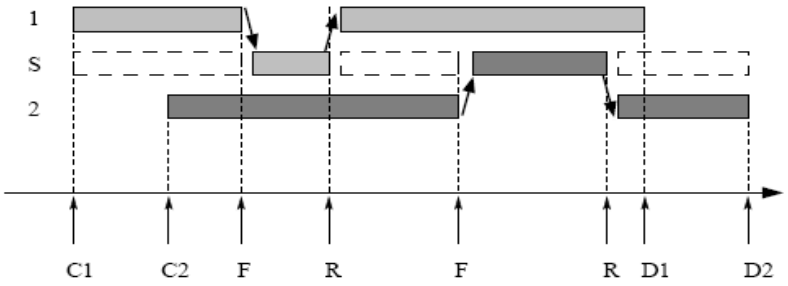


Figura 33 : Mecanismos de proteção reversível.

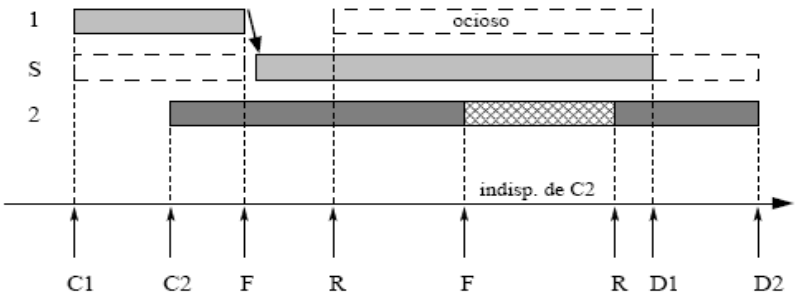


Figura 34 : Mecanismos de proteção não-reversível

A não-reversibilidade dos mecanismos de proteção influi em alguns parâmetros de desempenho. A probabilidade de bloqueio não é afetada. A disponibilidade das conexões pode ser prejudicada, se o mecanismo de proteção compartilhar recursos, ou ainda pode ser beneficiada, se o tempo de permanência da conexão for pequeno o suficiente. Em uma rede que utiliza proteção 1:N não reversível, o canal secundário de uma conexão que foi afetada por falhas não é liberado até que a desconexão seja efetuada. Esta ocupação desnecessária de recursos de proteção, aliada à ocorrência de uma falha, mesmo que após a recuperação da primeira falha, pode acarretar na indisponibilidade de uma conexão óptica que compartilha estes recursos de proteção, como é apresentado na Figura 34. Enquanto esta conexão não for liberada, as conexões que compartilham recursos com ela não poderão requisitar o canal secundário. Nesta situação, além da desnecessária indisponibilidade do canal secundário, existe ainda a ociosidade do canal primário, pois este recurso não é compartilhado.

Se esta ineficiência no uso dos recursos de proteção afeta negativamente a disponibilidade, por outro lado, a não-reversibilidade também afeta positivamente, dependendo do tempo médio de duração da conexão e do período desnecessário à configuração dos comutadores ópticos da rede. Se o tempo médio de duração de conexão for pequeno o suficiente, a conexão que ocupa o canal secundário desnecessariamente pode afetar a desconexão e liberar os recursos compartilhados antes que outra conexão os requisite, como mostra a Figura 35 . Assim o impacto negativo na disponibilidade será, na média, atenuada e a resultante do desempenho geral da rede pode ser majoritariamente positiva.

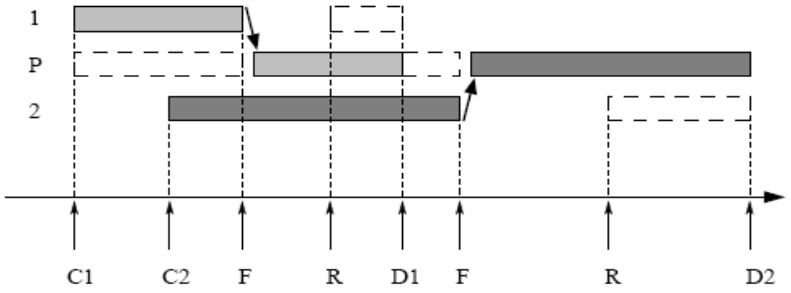


Figura 35 : Efeito do menor tempo de duração de uma conexão

4.7. Probabilidade de múltiplas falhas

Conforme referido no início deste capítulo as redes ópticas são vulneráveis a muitos tipos de falhas principalmente aquelas causadas por falhas de *hardware* e erros operacionais. O tipo de falha considerada mais importante é causada por corte de fibras [4.7]. Normalmente as redes ópticas são projetadas com proteção contra uma única falha, principalmente para as de pequeno e médio porte. Já para as redes de tamanho maiores deve ser considerada a ocorrência de duplas falhas. Diante disto segue abaixo como é tratado o cálculo da probabilidade de ocorrência de k falhas de uma determinada rede.

Primeiramente é necessário o conhecimento do comprimento do enlace *l* em *km,* e o número de enlaces que compõem a rede. O tempo médio entre falhas (*Mean time between failures*- MTBF) e o tempo médio de reparo (*Mean time to repair*- MTTR) conforme [4.8] pode assumir valores como 1000, 570 e 360 anos para MTBF, e MTTR varia tipicamente entre 1 a 48 horas.

Com estas variáveis é calculada a disponibilidade da rede *"a",* definida no início deste capítulo, utilizando a equação abaixo,

$$a = \left(\frac{MTBF}{MTBF + MTTR} \right)^{l} \qquad (3.1)$$

E finalmente a probabilidade de ocorrência de k falhas simultâneas é calculada por:

$$P = \binom{m}{k} (1-a)^{k} a^{m-k} \qquad (3.2)$$

4.8. Referências

[4.1] R. Ramaswami e K. N. Sivarajan. *Optical Networks: Practical Perspective*. Morgan Kaufmann Publishers, 2002

[4.2] D. A. A. Mello, "Suporte ao tráfego Heterogêneo pela Rede Óptica: Habilidade de Sobrevivência", Dissertação de Doutorado, FEEC/Unicamp,2006.

[4.3] M. D. Bicudo, "Sobrevivência em Redes Ópticas Transparentes", Dissertação de mestrado, COPPE/UFRJ, 2005.

[4.4] W. D. Zhong, New Bi-Directional WDM Ring Networks with Dual Hub Nodes, *IEEE Globocom, 1997.*

[4.5] J. Zhang e B. Mukherjee. A Review of Fault Management in WDM Mesh Networks: basic concepts and reserch challenges. *IEEE Network*, 18(2);41-48, março/abril.

[4.6] PAPADIMITRIOU, D., E MANNIE, E. Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanisms (including Protection and Restoration).*Internt Draft* (abril de 2005). INFORMATIONAL.

[4.7] D. A. Schupke and R. Prinz. " Capacity Efficiency and Restorability of Path Protection and Rerouting in WDM Networks Subject to Dual Failures", Proceeding of the Journal: Photonic Network Communications, Publisher: Springer Netherlands, Vol 8, number 2 /september,2004

[4.8] D. A. Schupke , A. Autenrieth, e T. Fischer "Survivability of Multiple Fiber Duct Failures". *Proc. DRCN'01*, Budapest, Hungary October 2001.

5. Análise de Proteção em Redes OPSN

Para as redes fotônicas que utilizam tecnologias OPSN e OBS mesmo sendo redes robustas e apresentando assim excelente capacidade de sobrevivência em caso de ocorrência de falhas é importante a implementação de mecanismos de proteção e restauração nestas redes, garantido o funcionamento de pelo menos parte do tráfego de pacotes ou rajadas.

Para utilizar os mecanismos de proteção e restauração das redes estudado no capítulo 4, foram analisados primeiramente a freqüência de utilização de cada *link* durante as simulações do NS, para os tipos de topologias anel e MS-4, 16, e MSq-9, 25, 36 nós. Mostra-se assim qual ou quais os *links* com maior e menor freqüência de utilização, uma vez que os enlaces mais sensíveis às falhas na rede serão aqueles mais utilizados. Além de mostrar a vulnerabilidade crítica desses *links* nas topologias citadas, realizou-se uma comparação entre as topologias malha e anel levando em consideração o valor de E[*hops*].

5.1. Topologias de Redes: Malha vs. Anel

As topologias malha e anel, citadas no início deste capítulo, foram utilizadas para medir o quanto foi utilizado cada link que as constituem. Esta informação de quanto foi utilizado cada link é importante para realizar implementação de proteção e restauração em redes.

A topologia da rede MS é totalmente conectada em malha. Dependendo de sua quantidade de nós, ela pode ser regular (par) (MS), quase regular (ímpar) (MSq) ou irregular(MI). As topologias conectadas em malha são redes robustas, assim pacotes e rajadas possuem opções de caminhos para chegar em seu endereço de destino. Esta é uma

característica favorável para as redes em malha, pois caso ocorra falha em algum *link* ou congestionamento de tráfego, o pacote poderá mudar sua rota e chegar ao seu endereço de destino, utilizando outros caminhos. Porém, para topologias em anel, esta característica não é apresentada, pois existem somente duas opções de caminho para o pacote (sentido horário ou anti-horário) e caso um *link* falhar, o sentido que estiver em funcionamento normal poderá ficar sobrecarregado, dependendo da quantidade de pacotes que estiverem trafegando na rede. A Figura 36 apresenta uma rede em anel com 9 nós.

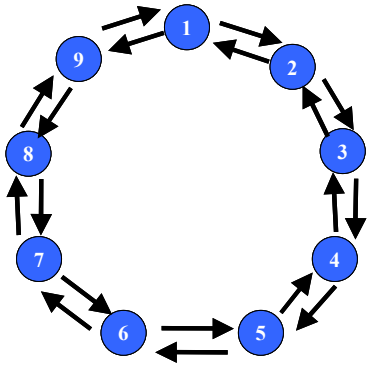


Figura 36 : Topologia em anel de 9 nós

5.2. Resultados numéricos e análise

Os resultados foram obtidos baseando-se nos mesmos parâmetros e variáveis já definidos em capítulos anteriores, tais como Ct, E[*hops*], F_d, e Tp. Embora estes parâmetros sejam calculados utilizando a mesma equação anteriormente definida, aqui foi considerada falha de *link* mais utilizado.

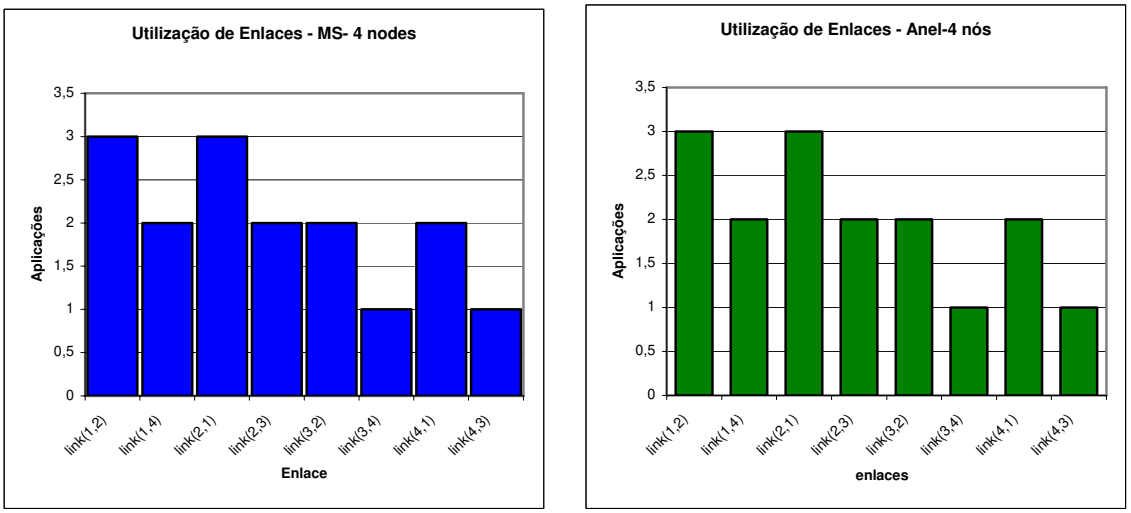
Nossos resultados são referentes à freqüência de utilização de cada *link* que constituem as topologias MS e MSq -9,16,25,36 e Anel-9,16,25,36. Para se obterem estes resultados, foi considerado o roteamento SF tendo largura de banda de 2,5Gb/s. A escolha do tipo de roteamento se deu, porque o número de deflexões apresentados nos resultados de simulação foram baixos, utilizando o roteamento DR. Além disso para nossa análise de aumento de número médio de *hops* e diminuição de capacidade da rede é necessário somente uma estimativa estatística dos valores das medidas de utilização de *link.*

A Tabela 2, e os gráficos abaixo são referentes à ocupação de cada enlace, ou à distribuição de aplicações na rede. Entende-se por aplicação, o total fluxo de tráfego gerado por cada nó para toda a rede, por isto as quantidades de aplicações são diferentes para cada rede.

Topologia	No. enlaces	∑aplicações	No. Médio Aplics/enlace E[aplics]	Desvio padrão ΔE[aplics]
MS-4	8	16	2	0,75
Anel-4	8	16	2	0,75
MSq-9	18	151	8,38	3,14
Anel-9	18	180	10	0
MS-16	32	704	22	13,85
Anel-16	32	988	30,9	3,2
MSq-25	50	1984	39,68	12,27
Anel-25	50	3900	78	0
MS-36	72	4680	65	8,83
Anel-36	72	11664	162	8,11

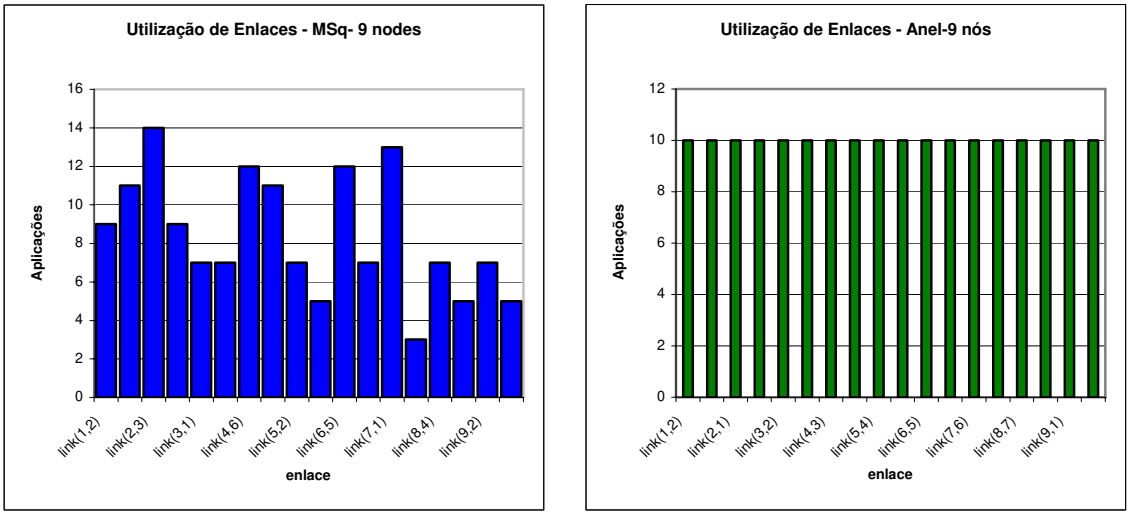
Tabela 2. Estatística para distribuição de tráfego

Entende-se por aplicação o fluxo de tráfego gerado por cada nó da rede, por isto as quantidades de aplicações são diferentes para cada rede.



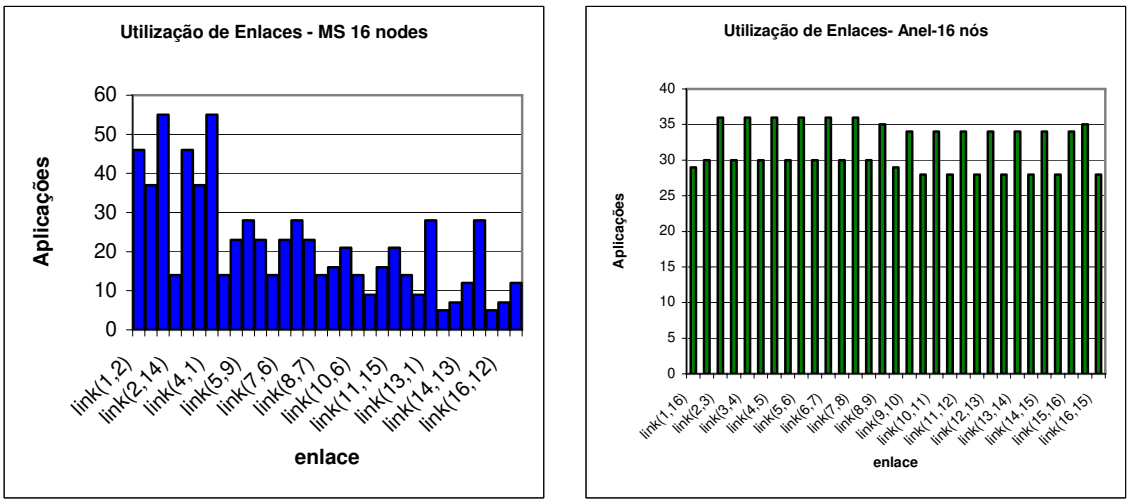
(a) (b)

Figura 37 : Utilização de Enlaces: (a) topologia MS-4 nós, (b) topologia anel-4 nós



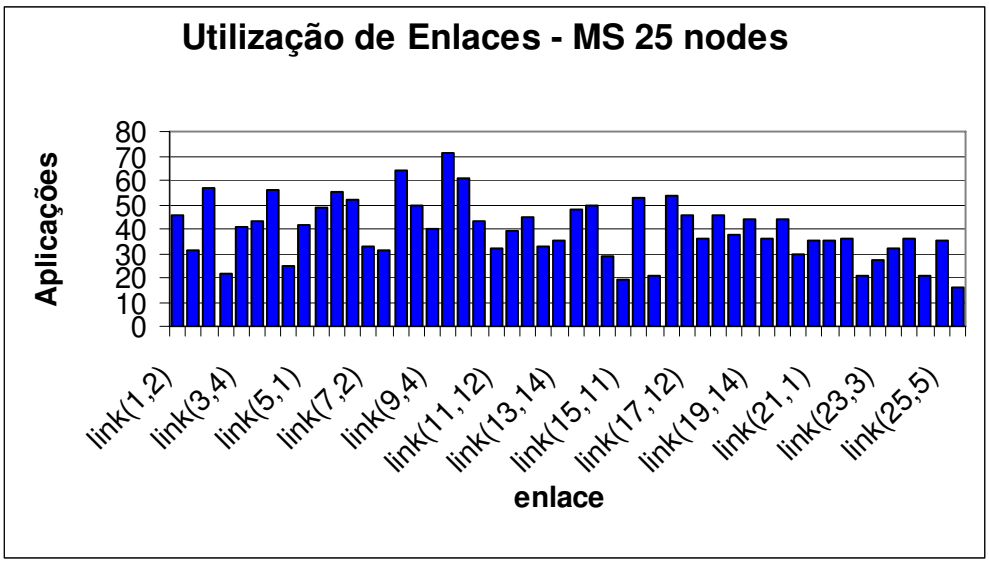
(a) (b)

Figura 38 :Utilização de Enlaces: (a) topologia MSq-9 nós, (b) topologia anel-9 nós

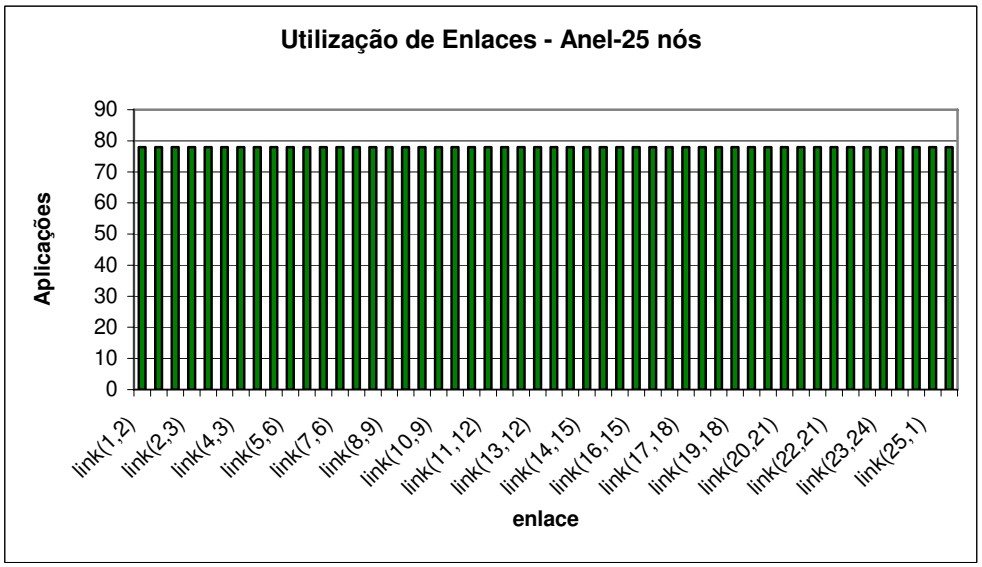


(b) (b)

Figura 39 :Utilização de Enlaces: (a) topologia MS-16 nós, (b) topologia anel-16 nós

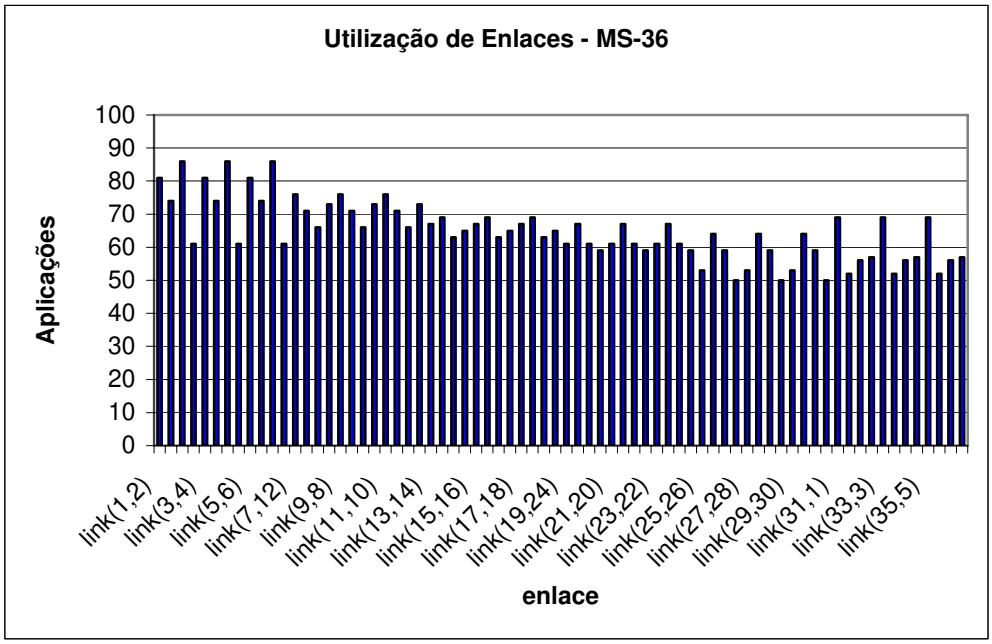


(a)

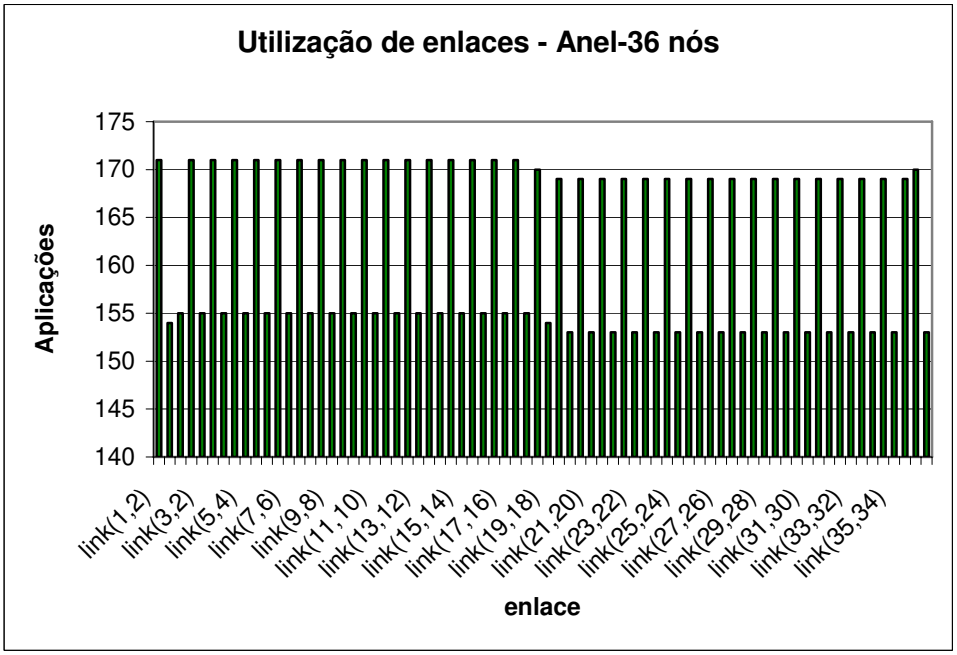


(b)

Figura 40 :Utilização de Enlaces: (a) topologia MSq-25 nós, (b) topologia anel-25 nós



(a)



(b)

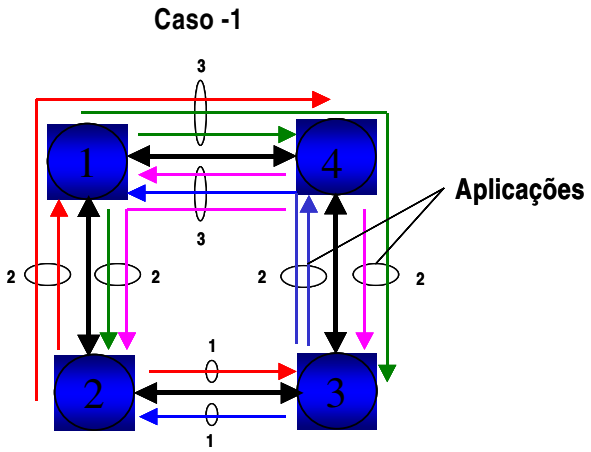
Figura 41 : Utilização de Enlaces: (a) topologia MS-36 nós, (b) topologia anel-36 nós

Os gráficos referentes aos resultados que mostram o quanto foi utilizado cada *link* tendo como topologia de rede a MS, coincidem com os resultados obtidos em trabalhos anteriores e de outro autor , sendo os resultados para a topologia anel originais deste trabalho.

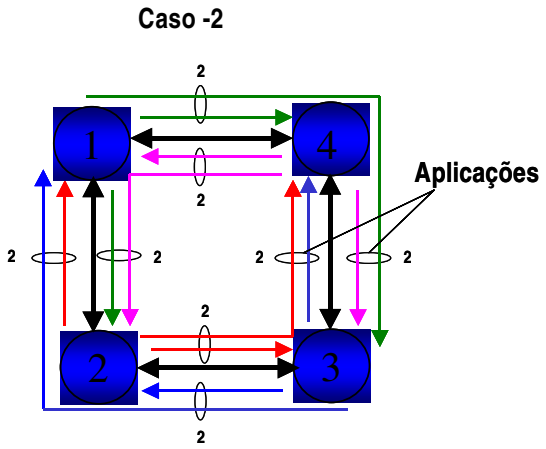
Analisando os resultados, verificamos que a utilização de *link* para a topologia anel com número de nós ímpar, é a mesma para todos os *links*, mas para anel com número par de nós a utilização de cada *link* tem uma pequena variação. Isto ocorre porque em redes com número ímpares, tanto faz uma aplicação percorrer o sentido horário ou anti-horário da rede óptica para chegar ao seu nó destino, o caminho sempre terá o mesmo tamanho. Em anéis com números pares de nós, o sentindo do caminho (horário/anti-horário) pode mudar o tamanho do caminho. Um exemplo prático foi ilustrado na Figura 42 que representa a distribuição das aplicações geradas em um anel de 4 nós. Percebe-se que no caso –1 a utilização de cada *link* não está balanceada. Para o caso-2 os *links* tiveram o mesma freqüência de utilização. Nota-se que todos os nós geram aplicações para todos os outros nós da rede menos para si mesmo.

No exemplo, é importante entender que em redes em anel com números pares de nós, o sentido que as aplicações irá percorrer define o valor de utilização de link, e o simulador, será o responsável pela escolha do sentido do caminho.

Distribuição de aplicações



(a)



(b)

Figura 42 : Distribuição de Aplicações: (a) distribuição não homogênea; (b) distribuição homogênea

Sem falha de *link* topologia MS:

Topologia	No. Enlaces (2N)	No. Médio hops E[*hops*]	Capacidade (Gb/s)	Fator de Desempenho F_d
MS-4	8	1,33	15	11,2
MSq-9	18	2,01	22,34	11,1
MS-16	32	2,93	27,27	9,3
MSq-25	50	3,28	38,11	11,6
MS-36	72	3,71	48,41	13,0

Tabela 3. **:** Parâmetros relevantes para topologia MS (desconsiderando falha)

Sem falha de *link* topologia anel:

Topologia	No. Enlaces (2N)	No. Médio hops E[*hops*]	Capacidade (Gb/s)	Fator de Desempenho F_d
Anel-4	8	1,33	15	11,2
Anel-9	18	2,50	18	7,9
Anel-16	32	4,27	18,75	5,7
Anel-25	50	6,50	19,23	2,9
Anel-36	72	8,76	20,55	2,34

Tabela 4. **:**Parâmetros relevantes para topologia anel (desconsiderando falha)

Falha de *link* mais utilizados MS:

Topologia	Links quebrado (falha)	No. Médio de *hops* E[*hops*]		Variação ΔE[*hops*] (%)	Capacidade C (Gb/s)		Variação ΔC(%)	Fator de Desempenho F_d		Variação ΔF_d(%)
		S/f *	C/f *		S/f *	C/f *		S/f *	C/f*	
MS-4	(1,2)	1,33	1,5	+12,53	15	13,3	-11,13	11,25	8,86	-21,24
	(2,1)	1,33	1,5	+12,53	15	13,3	-11,13	11,25	8,86	-21,24
MSq-9	(2,3)	2,014	2,15	+6,76	22,34	20,9	-6,33	11,09	9,72	-12,35
	(7,1)	2,014	2,12	+5,27	22,34	21,1	-5,00	11,09	10,00	-9,82
MS-16	(2,3)	2,93	3,02	+2,96	27,27	26,5	-2,87	9,29	8,77	-5,60
	(4,1)	2,93	3,02	+2,96	27,27	26,5	-2,87	9,29	8,77	-5,60
MSq-25	(9,8)	3,28	3,38	+3,05	38,10	36,9	-2,96	11,61	10,94	-5,77
	(10,9)	3,28	3,38	+3,05	38,10	36,9	-2,96	11,61	10,94	-5,77
MS-36	(2,3)	3,78	3,78	+1,77	48,41	47,6	-1,74	13,04	12,60	-3,37
	(4,5)	3,71	3,78	+1,77	48,41	47,6	-1,74	13,04	12,60	-3,37
	(6,1)	3,71	3,78	+1,77	48,41	47,6	-1,74	13,04	12,60	-3,37

Tabela 5. :Resultados de parâmetros sem falha e com falha para MS (considerando falhas simples)

Falha de *link* mais utilizados em topologia anel:

Topologia	Link quebrado (falha)	No. Médio de *hops* E[*hops*]		Variação ΔE[*hops*] (%)	Capacidade C (Gb/s)		Variação ΔC(%)	Parâmetro Eficiência F_d		Variação ΔF_d (%)
		S/f*	C/f*		S/f*	C/f*		S/f*	C/f*[1]	
Anel-4	(1,2)	1,33	1,5	+12,5	15,00	13,3	-11,13	11,2	8,89	-20,06
	(2,1)	1,33	1,5	+12,5	15,00	13,3	-11,13	11,2	8,89	-20,06
Anel-9	Qualquer Link	2,5	2,9	+16,8	18,00	15,42	-14,44	7,2	5,27	-26,80
Anel-16	Qualquer Link	4,26	4,9	+16,4	18,75	16,11	-14,08	4,4	3,24	-26,3
Anel-25	Qualquer Link	6,5	7,5	+16,6	19,23	16,5	-14,19	2,96	2,18	-26,3
Anel-36	(2,3)	8,75	10,3	+17,5	20,55	17,5	-14,84	2,35	1,70	-27,65
	(17,18)	8,75	9,7	+11,5	20,55	18,4	-10,46	2,35	1,88	-20,00

Tabela 6. **:**Resultados de parâmetros sem falha e com falha para anel (considerando falhas simples)

*S/f : sem falha,
*C/f: com falha

Conforme os resultados da Tabela 3, 4,5,6, nós verificamos que o desempenho das redes analisadas com topologia em malha é melhor, comparando com os resultados da topologia anel. Os resultados da tabela 5 e 6 mostraram que, caso o link mais utilizado falhar, considerando a topologia MS e MSq -4, 9,16, 25,36 seu fator de desempenho reduziria em média de aproximadamente 21%,11%,5%,5%,3% respectivamente levando em consideração os resultados de F_d desconsiderando as falhas. Já para Anel, este fator de desempenho decresce em média 20%, 26%,26%, 26%, 27%, mostrando assim o melhor desempenho das redes em malha.

A Figura 43 é uma complementação da carga de vazão estudada [5.1][5.4][5.6] em que foram reproduzidos os resultados da vazão para redes MS e MSq -4, 9,16, 25 nós e adicionados os resultados para a topologia anel.

A análise do gráfico da vazão mostra que as redes em malha apresentam uma maior vazão comparada com a topologia anel.

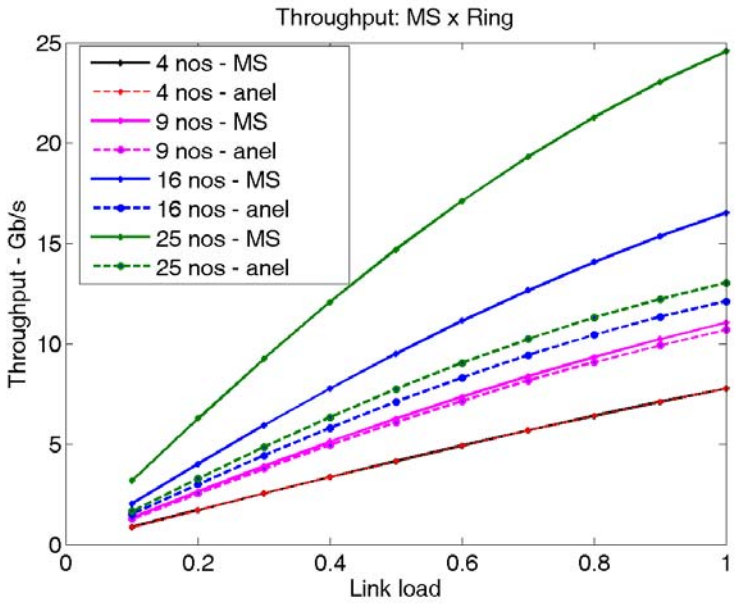


Figura 43 : Vazão : MS x Anel

5.3. Referências

[5.1] A. S. Acampora and S. I. A. Shah, "Multihop lightwave network: a comparison of store-and-forward and hot potato routing", *IEEE Trans. Communications*, vol.40, no.6, pp.1082-1090 (1992).

[5.2] D. Maia Jr, L. Pezzolo, A. C. Sachs, F. Rudge Barbosa, "Optical Packet Switching and Routing using in-band frequency header labeling", *IMOC'2003 Joint IEEE-SBMO Intl. Symposium*, Foz Iguaçu, Brasil, Sept.2003.

[5.3] D. J. Blumenthal, P. R. Prucnal and J. R. Sauer, "Photonic packet switching: architectures and experimental implementations", *Proceedings of the IEEE*, vol.82, no.11, pp.1650-1667 (1994).

[5.4] F. Rudge Barbosa, A.C.Sachs, "Transparent Optical Packet Switching Node based on Bottom-up Organization Network", *XXI Simp. Brasileiro Telecom – SBT'2004*, Belém PA, Brasil, Set. 2004.

[5.5] I. Chlamtac, A. Fumagalli, "An Optical Switch Architecture for Manhattan Networks", IEEE J.Select. Areas Communic. vol.11, no. 4, .550, May 1993.

[5.6] I. B. Martins, L. H. Bonani, F.R. Barbosa, E. Moschim, "Dynamic Traffic Analysis of Metro Access Optical Packet Switching Networks having Mesh Topologies", *Proceedings of the International Telecommunications Symposium, ITS'2006,* September 2006, Fortaleza, Brazil.

6. Conclusão

De acordo com o planejamento, realizou-se neste trabalho um estudo teórico dos principais elementos que constituem as redes OPSN. Foram abordados também técnicas de roteamento, critérios de resolução de contenda com enfoque em resolução de contenda espacial, utilizando o roteamento por Deflexão para solucionar a disputa entre os pacotes.

Depois de finalizado os estudos teóricos e compreendidas todas as definições relevantes ao estudo de OPSN em redes com topologia em malha, foram feitos estudos que envolvem os cálculos dos principais parâmetros tais como C_t, E[*hops*], T_p , com o objetivo de verificar o fator de desempenho (F_d) de cada rede adotada neste trabalho.

O fator desempenho (F_d) foi medido utilizando a razão entre dois parâmetros (capacidade máxima (C_t) por número médio de *hops* (E[*hops*]))

Através deste fator que mede o desempenho das redes adotadas neste trabalho, foi possível verificar através de seus resultados, que a rede MSq-9 nós tem um bom desempenho comparada com as redes de 8 e 16 nós, verificando assim que, apesar da capacidade da rede de 8 nós e MS-16 terem aumentado, a conectividade entre os enlaces não favoreceu os pacotes a realizarem um menor caminho,(menor E[*hops*] até seus destinos) ocasionando um baixo desempenho para estas topologias.

Os resultados que envolveram cálculos da vazão e número médio de *hops* utilizando roteamento DR comprovam a credibilidade deste fator desempenho, onde o gráfico referente a E[*hops*] mostrou que a MS-9 tinha uma menor número de saltos comparada com a topologia de 8 nós e uma melhor vazão, portanto o fator de desempenho se mantém também melhor.

Nos resultados de simulação das redes OPSN adotadas, utilizando roteamento SF e DR e transmissão de pacotes em intervalos constantes e variados, foram plotados vários gráficos referentes aos pacotes recebidos, perdidos por adicionamento de pacotes no nó, número de deflexões e outros resultados foram comentados no capítulo 3.

Para finalizar nosso trabalho foi analisada a freqüência de utilização de cada link das redes adotadas, verificando assim que redes em malha são mais resistentes à falha comparada com redes em anel, levando em consideração a diminuição do fator desempenho e a vazão dos dois tipos de topologia. Em ambos resultados a topologia em malha se mostrou superior.

.

6.1. Trabalhos Futuros

Para os próximos trabalhos pretende-se continuar analisando o comportamento de tráfego, já realizado no presente trabalho, porém com a modificação de parâmetros e estruturas referente a topologia física e lógica da rede, tais como a utilização de pacotes do tipo *burst*, implantação de enlaces bidirecionais e, assumindo tráfego com pacotes de tamanhos variados. Pretendem-se também, melhorar o estudo de casos já realizado para o roteamento DR, com a utilização de mais casos, visando melhor a distribuição de tráfego na rede e evitando a perda de pacotes provocados por congestionamentos de pacotes.

Pretende-se também aperfeiçoar os estudo referente à proteção das redes com utilização de técnicas de redes neurais para detecção de falhas em *links* ópticos.

Atualmente o re-roteamento rápido em redes ópticas quando ocorre alguma falha, é um problema. Por isto tem-se como objetivo aplicar os conceitos de redes neurais (agentes inteligentes) para prever as falhas e, desta forma, garantir maior agilidade no processo de re-roteamento, sendo que o tráfego antes da ocorrência de falha deve ser desviado para outra rota possibilitando que todos os pacotes sejam entregues a seus destinatários.

Trabalho Publicado

I. B. Martins, L. H. Bonani, F. R. Barbosa, E. Moschim, “Dynamic Traffic Analysis of Metro Acess Optical Packet Switching Networks Having Mesh Topologies”, *Proceeding of the International Telecommunications Symposium, ITS’2006*, September 2006, Fortaleza, Brazil

Anexo A

Etapas do processo de simulação

A seguir apresentaremos na Figura 44 o fluxograma que descreve todas as etapas do processo de simulação, desde a preparação dos scripts para a primeira rodada de simulação até o resultado final na forma gráfica.

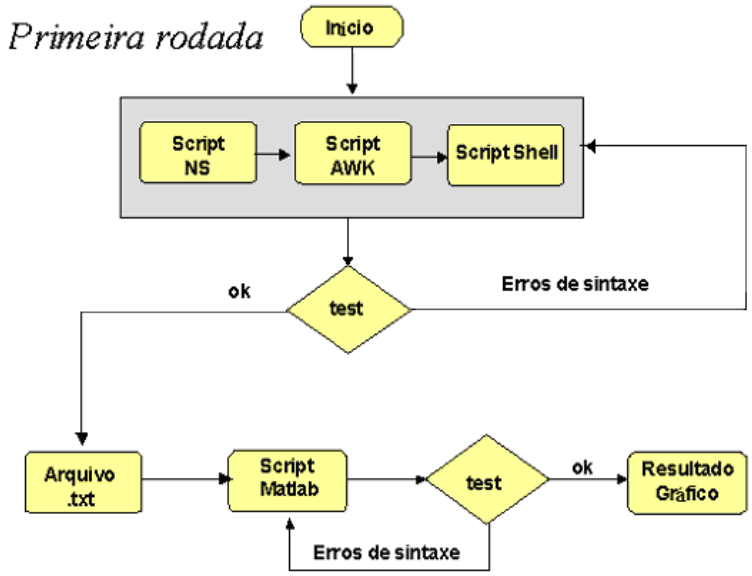


Figura 44 Fluxograma do processo para a 1º simulação

- ✓ **Início:** para dar início ao processo de simulação no NS, é necessário definir algumas características da rede que deseja construir, como, número de nós, tipos de topologias, *link load*, tipo de tráfego, tipo de roteamento, tamanho dos pacotes, número de pacotes que deseja que seja transmitido, taxa de transmissão, além da estrutura física da rede como, por exemplo, o tipo e tamanho de enlace (bidirecional ou unidirecional) que conecta dois nós, se o nó terá *buffer* ou não,e topologias. Estas informações são importantes para montar corretamente a rede de pacotes ópticos pretendida e esta funcionar, tendo assim simulações com resultados reais e coerentes com os teóricos.

- ***Script* NS**: depois de caracterização da rede que se pretende simular, é necessário escrever um *script* (seqüência de códigos) usando linguagem *tcl* (*Tool Command Language*) descrevendo todas as características e estruturas físicas definidas no início. A primeira etapa trata-se de uma modelagem do sistema estrutural da rede e a escolha de suas características (protocolos de comunicação, tipo de tráfego, tipo de filas, tamanho do pacote, número de pacotes a ser transmitidos e outros).

  Depois de construído o *script* na linguagem *tcl*, este será testado, colocado para simular e caso haja algum erro de sintaxe do código o simulador apresentará mensagens de erros, bloqueando assim a simulação. Caso não apresente erros, a simulação será concluída. Os resultados desta simulação ficarão salvos em um arquivo "*.txt*" cujo nome fica a critério do programador do *script.*

- ***Script* AWK:** O arquivo "*.txt"* resultado da simulação no NS é um arquivo constituído por muitas informações, e por isto se utiliza um mecanismo para aproveitar apenas as informações que interessam ao trabalho. Com o objetivo de filtrar o arquivo "*.txt"* (NS) para obter apenas os resultados de interesse, é montado um outro *script* utilizando a linguagem AWK (Aho, Weinberger e Kernighan). Neste *script* serão calculados outros resultados a partir dos que existem e escolha dos resultados gerados pelo NS os de interesse. Quanto à sintaxe do código AWK, o procedimento é o mesmo da etapa anterior, caso haja algum erro, este terá que ser corrigido porque ao executar o *script* aparecerá mensagens de erro, caso esteja tudo correto, esta etapa resultará a um outro arquivo também .txt.

- ***Script* Shell**: como as simulações são executadas utilizando uma janela *prompto* de comando, em ambiente Linux, para facilitar o processo de simulação e evitar a digitação da linha de comando para executar a simulação a todo instante, foi criado um novo *script* utilizando linguagem Shell. Este *script* executa a simulação de uma vez só para todas as cargas e tipos de roteamento.Quanto a escrita do código o procedimento é idêntico aos anteriores. O resultado final deste script fica salvo em um arquivo .txt que será utilizado pelo Matlab para a plotagem dos gráficos desejados.

- ✓ ***Script Matlab* (*Matrix Laboratory*)**: nesta etapa serão montados *scripts* para plotagem de gráficos levando em considerações os resultados da etapa anterior. O mesmo procedimento das etapas 2 e 4 é feito aqui, caso *script* tenha algum erro aparecerá mensagens de erros, e caso esteja tudo correto o resultado gráfico final é impresso na tela.

Observações-Os *scripts* NS, AWK, SHELL e *Matlab* são salvos com extensão "**.tcl", ".awk", ".sh", ".m"** respectivamente.

O processo de simulação depois de corrigido e ajustado todos os *scripts* (NS, AWK, Shell), a etapa de escrita de *script* fica finalizada, sendo necessário apenas alguns ajustes nestes *scripts* para definir alguns parâmetros de entrada que define a simulação da rede desejada, como, por exemplo, taxa de transmissão dos pacotes, tamanho do pacote, tempo de simulação e outros. A Figura 45 abaixo mostra o fluxograma de simulação depois que já se tem os scripts escritos ou seja o processo otimizado de simulação .

O fluxograma em questão pode ser executado porque já se tinha realizado todas as etapas do 1° fluxograma descrito acima, onde foram eliminadas as falhas eventuais de programação. Designa-se "outras rodadas" porque são as rodadas otimizadas, onde os resultados são repetitivos e confiáveis.

No caso de novas simulações, com outros parâmetros, o processo é reiniciado, seguindo o fluxograma completo descrito anteriormente.

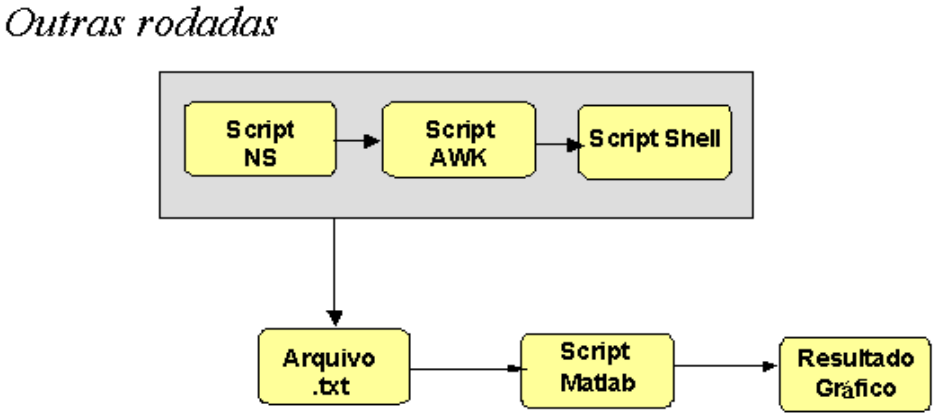


Figura 45 :Fluxograma do processo otimizado das simulações

Anexo B

Apresenta-se neste anexo, os scripts de simulação utilizados para a obtenção dos dados relativos ao roteamento SF e ao roteamento DR. Deve-se notar que o script descreve todo cenário da simulação, e é inteiramente escrito na linguagem Tcl (linguagem interpretada de alto nível).

```
#############################################################################
# Creating a simulator object

set ns [new Simulator]

#inputs parameters of script

set lload [lindex $argv 0];             # set the network load (store-and-forward)
set numnode [lindex $argv 1];                   # set the number of nodes
set noise [lindex $argv 2];             # set the noise
set seed [lindex $argv 3];              # set the seed
set appp [lindex $argv 4];              # set the % of priority traffic
set topology [lindex $argv 5];                  # set the topology
set mttl [lindex $argv 6];              # set the time to live between 32 since 100

#Simulation parameters
#clk_ = 0 -> No defletion routing
#clk_ = 10 -> DTJGT/DropTail (DR1)
#clk_ = 20 -> PRIO (DR2)

$ns rtproto Static;                     # dynamic links
Classifier set clk_ 0;                  # type of classifier

#Setting auxiliary variables
#
#set mttl 36                            #tempo maximo de vida de um pacote 32 hops
set normaltraff 18
set priotraff 18
set appnode [expr $numnode-1]
set numus [expr $numnode*$appnode];
set bw 2.5e9;
set delay 10us;
```

```
set qtyp DropTail;
set qlim 2;
set size 500;
set tp [expr 8 * $size / $bw];
set t1 [expr 10 * $tp];
set aux1 1;
set aux2 1;


#Setting Number of packets
#

set qpkts 200000;

#Setting paramenters for random number generator
#
set rngen [new RNG]
#$rngen seed $seed
set rng [new RandomVariable/Uniform]
#$rng use-rng $rngen
#$rng set min_ 1
#$rng set max_ $numnode

#Setting output files

#set fbuff [open buff$topology-$lload.txt w]
if {$noise ==1} {
        set f [open m$topology-numnode$numnode-cr$lload.txt w];        # open trace file

} else {
        set f [open m$topology-numnode$numnode-sr$lload.txt w];        # open trace file

}

$ns trace-all $f

#Setting nam
#
#set nf[opem m16dr.nam w];          #open nam file
#$ns namtrace-all $nf

#Creating <numnode> nodes
#
for {set i 1} {$i <= $numnode} {incr i} {
        set n($i) [$ns node]
}
```

```
#Matrix of zeros for the topology generation,
#priority traffic and queue monitor of the more
#loaded links (mll) and less loaded links
#
for {set i 1} {$i <= $numnode} {incr i} {
  for {set j 1} {$j <= $numnode} {incr j} {
        set top($i,$j) 0
        set vep($i,$j) 0
        set mll($i,$j) 0
        set lll($i,$j) 0
        set buffmax($i,$j) 0
        set bufftime($i,$j) 0
   }
}

#Connecting matrix
#
switch $topology {

        4ms {
                set top(1,2) 1; set top(2,1) 1; set top(3,2) 1; set top(4,1) 1;
                set top(1,4) 1; set top(2,3) 1; set top(3,4) 1; set top(4,3) 1;
        } 9ms {
                set top(1,2) 1; set top(4,6) 1; set top(7,1) 1;
                set top(1,4) 1; set top(4,7) 1; set top(7,8) 1;
                set top(2,3) 1; set top(5,2) 1; set top(8,4) 1;
                set top(2,8) 1; set top(5,4) 1; set top(8,9) 1;
                set top(3,1) 1; set top(6,5) 1; set top(9,2) 1;
                set top(3,6) 1; set top(6,9) 1; set top(9,7) 1;
        } 16ms {
                set top(1,2)  1; set top(5,8)  1; set top(9,10)  1; set top(13,1)  1;
                set top(1,5)  1; set top(5,9)  1; set top(9,13)  1; set top(13,16) 1;
                set top(2,3)  1; set top(6,2)  1; set top(10,6)  1; set top(14,10) 1;
                set top(2,14) 1; set top(6,5)  1; set top(10,11) 1; set top(14,13) 1;
                set top(3,4)  1; set top(7,6)  1; set top(11,12) 1; set top(15,3)  1;
                set top(3,7)  1; set top(7,11) 1; set top(11,15) 1; set top(15,14) 1;
                set top(4,1)  1; set top(8,4)  1; set top(12,8)  1; set top(16,12) 1;
                set top(4,16) 1; set top(8,7)  1; set top(12,9)  1; set top(16,15) 1;

                set mll(4,1)   1; set mll(2,3)   1;
                set lll(15,14) 1; set lll(13,16) 1;
        } 25ms {
                set top(1,2)  1; set top(6,10)  1; set top(11,12) 1; set top(16,20) 1; set
top(21,1)  1;
                set top(1,6)  1; set top(6,11)  1; set top(11,16) 1; set top(16,21) 1; set
top(21,22) 1;
```

```
                set top(2,3)  1; set top(7,2)   1; set top(12,6)  1; set top(17,12) 1; set
top(22,17) 1;
                set top(2,22) 1; set top(7,6)   1; set top(12,13) 1; set top(17,16) 1; set
top(22,23) 1;
                set top(3,4)  1; set top(8,7)   1; set top(13,14) 1; set top(18,17) 1; set
top(23,3)  1;
                set top(3,8)  1; set top(8,13)  1; set top(13,18) 1; set top(18,23) 1; set
top(23,24) 1;
                set top(4,5)  1; set top(9,4)   1; set top(14,9)  1; set top(19,14) 1; set
top(24,19) 1;
                set top(4,24) 1; set top(9,8)   1; set top(14,15) 1; set top(19,18) 1; set
top(24,25) 1;
                set top(5,1)  1; set top(10,9)  1; set top(15,11) 1; set top(20,19) 1; set
top(25,5)  1;
                set top(5,10) 1; set top(10,15) 1; set top(15,20) 1; set top(20,25) 1; set
top(25,21) 1;
        } 36ms {
                set top(1,2)  1; set top(10,4)  1; set top(19,24) 1; set top(28,22) 1;
                set top(1,7)  1; set top(10,9)  1; set top(19,25) 1; set top(28,29) 1;
                set top(2,3)  1; set top(11,10) 1; set top(20,14) 1; set top(29,30) 1;
                set top(2,32) 1; set top(11,17) 1; set top(20,19) 1; set top(29,35) 1;
                set top(3,4)  1; set top(12,6)  1; set top(21,20) 1; set top(30,24) 1;
                set top(3,9)  1; set top(12,11) 1; set top(21,27) 1; set top(30,25) 1;
                set top(4,5)  1; set top(13,14) 1; set top(22,16) 1; set top(31,1)  1;
                set top(4,34) 1; set top(13,19) 1; set top(22,21) 1; set top(31,36) 1;
                set top(5,6)  1; set top(14,8)  1; set top(23,22) 1; set top(32,26) 1;
                set top(5,11) 1; set top(14,15) 1; set top(23,29) 1; set top(32,31) 1;
                set top(6,1)  1; set top(15,16) 1; set top(24,18) 1; set top(33,3)  1;
                set top(6,36) 1; set top(15,21) 1; set top(24,23) 1; set top(33,32) 1;
                set top(7,12) 1; set top(16,10) 1; set top(25,26) 1; set top(34,28) 1;
                set top(7,13) 1; set top(16,17) 1; set top(25,31) 1; set top(34,33) 1;
                set top(8,2)  1; set top(17,18) 1; set top(26,20) 1; set top(35,5)  1;
                set top(8,7)  1; set top(17,23) 1; set top(26,27) 1; set top(35,34) 1;
                set top(9,8)  1; set top(18,12) 1; set top(27,28) 1; set top(36,30) 1;
                set top(9,15) 1; set top(18,13) 1; set top(27,33) 1; set top(36,35) 1;


                set mll(2,3)   1; set mll(4,5)   1; set mll(6,1)   1;
                set lll(26,27) 1; set lll(28,29) 1; set lll(30,25) 1;
        }
}


#Generate Random Priority Connections
#
if {$priotraff == 10} {
        set ind 1;
```

```
        set ptrf [open priortraffic$seed.txt w];
        set apprio [expr $numnode * $appp];
        while {$ind <= $apprio} {
                set stest [$rng value]
                set sourc [expr round ($stest)]
                set dtest [$rng value]
                set desti [expr round ($dtest)]
                if {($sourc != $desti) && ($vep($sourc,$desti) != 1)} {
                        set vep($sourc,$desti) 1;
                        incr ind
                }
        }
}

#Connect the nodes and define queue monitors
#
for {set i 1} {$i <= $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                if {$top($i,$j) == 1} {
                        $ns simplex-link $n($i) $n($j) $bw $delay $qtyp
                        $ns queue-limit $n($i) $n($j) $qlim
                }
        }
}

# Explicting the routes and calculating the average number of hops
#
$ns compute-routes
$ns get-prefrouterstnode1;
#Calculate network parameters and simulation time
#
set anh [$ns get-anh];
#set anh 3.7143;
puts "numero medio de hops:$anh"
set Cagr_f1 [expr 2*$numnode*$bw/$anh];
#set Cagr_f1 [expr 2*16*$bw/$anh];
puts "Capacidade total:$Cagr_f1"
set rate [expr 0.1*$lload*$Cagr_f1/$numus];
#set rate [expr 0.1*$lload*$Cagr_f1/15];
puts "Taxa:$rate"
set st [expr $qpkts/($lload*0.1*$Cagr_f1/($size*8))];
puts "Tempo de simulacao:$st"

#definning a finish procedure
#
proc finish {} {
        global ns f nf ptrf anhops crlinks
```

```
        $ns flush-trace
        #close the output files
        close $f
        exit 0
}

#Monitoring the buffers
#
proc monit {sour dest} {
        global ns qm fm st
        set now [$ns now]
        set currnow [expr $now/$st]
        $qm($sour,$dest) instvar pkts_
        if {$pkts_ < 0} {
          puts $fm($sour, $dest) "$currnow 0"
        }else{
         puts $fm($sour,$dest) "$currnow $pkts_"
        }
        flush $fm($sour, $dest)
        set interval [expr $st/30]
        set nexttime [expr $now +$interval]
        $ns at $nexttime "monit $sour $dest"
}

proc buffmaxsize {sour dest} {
        global ns qm st
        variable bufftime
        variable buffmax
        set now [$ns now]
        set currnow [expr $now/$st]
        if {$bufftime($sour,$dest)==0} {
          set bufftime($sour, $dest) $currnow
        }
        $qm($sour, $dest) instvar pkts_
        set currpsize $pkts_
        if {$currpsize > $buffmax($sour, $dest)} {
          set buffmax($sour, $dest) $currpsize
          set bufftime($sour,$dest) $currnow
        }
        set interval [expr $st/30]
        set nexttime [expr $now + $interval]
        $ns at nexttime "buffmaxsize $sour $dest"
}

proc compmaxbufsize {} {
        global buffmax bufftime numnode top fbuff
        for {set i 1} {$i <= $numnode} {incr i} {
```

```
                for {set j 1} {$j <= $numnode} {incr j} {
                        if {$top($i,$j) ==1} {
                                puts $fbuff "$i $j $buffmax($i,$j) $bufftime($i,$j)"
                        }
                }
        }
}

# Attaching constant UDP Traffic. noise = 0:SGP - noise = 1:AGP
#
proc attach-const-traffic {node sink size rate color noise prior flow_id maxttl} {
        global ns
        Agent/UDP set packetSize_ 6000
        set udp [new Agent/UDP]
        $udp set class_ $color
        $udp set prio_ $prior
        $udp set fid_ $flow_id
        $udp set ttl_ $maxttl;
        $ns attach-agent $node $udp
        set traffic [new Application/Traffic/CBR]
        $traffic set packetSize_ $size
        $traffic set rate_ $rate
        $traffic set random_ $noise
        $traffic attach-agent $udp
        $ns connect $udp $sink
        return $traffic
}

# Creating Traffic Sinks
#
for {set i 1} {$i <= $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                if {$i != $j} {
                        set sink($j,$i) [new Agent/Null]
                        $ns attach-agent $n($i) $sink($j,$i)
                }
        }
}

#Creating <numnode * (numnode -1)> traffic sources(users!!!)
#

for {set i 1} {$i <= $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                if {$i != $j} {
                        if {$vep($j,$i) != 1} {
```

```
                                        set source($aux1) [attach-const-traffic $n($j) $sink($j,$i)
$size $rate $aux1 $noise $normaltraff $aux1 $mttl]
                                        incr aux1
                                } else {
                                        set source($aux1) [attach-const-traffic $n($j) $sink($j,$i)
$size $rate $aux1 $noise $priotraff $aux1 $mttl]
                                        puts $ptrf "source: $sourc destination: $desti flowid: $aux1"
                                        incr aux1
                                }
                        }
                }
        }
}

#Monitor the links

for {set i 1} {$i <= $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                if {$top($i,$j) == 1} {
                }
        }
}

#Start the traffic sources
#

set tstart 0.0
for {set i 1} {$i < $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                set aux3 [expr $i + ($j-1) * $appnode]
                if {$aux3 <= $numus} {
                        $ns at [expr $t1 + $tstart] "$source($aux3) start"
                }
        }
        set tstart [expr $tstart + 2.0 * $tp]
}

#Stop the traffic sources
#
set tstop 0.0
for {set i 1} {$i < $numnode} {incr i} {
        for {set j 1} {$j <= $numnode} {incr j} {
                set aux4 [expr $i + ($j-1)*$appnode]
                if {$aux4 <= $numus} {
                        $ns at [expr $st + $tstop] "$source($aux4) stop"
                }
        }
        set tstop [expr $tstop + 2.0 *$tp]
```

```
}

$ns at [expr 3.5 * $st] "finish"
$ns run
```

Script utilizando a linguagem awk

```
BEGIN {
   highest_packet_id = 0;
} {

  action = $1;
  time = $2;
  link_src = $3;
  link_dest = $4;
  flow_id = $8;
  src_addr = $9;
  dest_addr = $10;
  seq_no = $11;
  packet_id = $12;
  ttl = $13;
  prio = $14;
  dfl = $15;


  if (maxTTL == 0) maxTTL = ttl;

  if ( packet_id > highest_packet_id ) highest_packet_id = packet_id;

  if ( start_time[packet_id] == 0 )  start_time[packet_id] = time;

  if ( action != "d" ) {
    if ( action == "r" ) {
      if ( link_dest == int(dest_addr) )  {
          Trc ++
          Ctrl[packet_id] = 1;
          delay[packet_id] = time - start_time[packet_id];
          Tdelay_r = Tdelay_r + delay[packet_id];
             hop[packet_id] = maxTTL - ttl;
          Thops_r = Thops_r + hop[packet_id];
          ndef[packet_id] = dfl;
          Tdef_r = Tdef_r + ndef[packet_id];

      }
    }
```

```
   } else {

        Tlost ++


        delay[packet_id] = time - start_time[packet_id];
        hop[packet_id] = maxTTL - ttl;
        hop_d[Tlost] = hop[packet_id];
        Thops_d = Thops_d + hop_d[Tlost];

        if ( hop[packet_id] == 0 )  {
                packet_lost_origem ++

        }

        delay_d[Tlost] = delay[packet_id];
        Tdelay_d = Tdelay_d + delay_d[Tlost];
        delay_d_src[Tlost] = delay[packet_id];
        Tdelay_d_src = Tdelay_d_src + delay_d_src[Tlost];


        ndef[packet_id] = dfl; #numero de deflexoes
        Tdef_d = Tdef_d + ndef[packet_id]; # total de deflexoes
        }
}

END {
   Tpkt_d = Tlost; #total de pacotes perdidos
   Tpkt_d_src = packet_lost_origem; #total de pacotes perdidos na origen
   Tpkt_d_consid = Tlost - packet_lost_origem; #total de pacotes perdidos considerados

   Tpkt_r = Trc; #total de pacotes recebidos
   Tpkt = Trc + Tlost; #total de pacotes gerados considerando perda de pacotes na entrada
   Tpkt_consid = Trc + Tpkt_d_consid; #total de pacotes gerados desconsiderando perda de
pacotes na entrada
   Tpckt_consid2 = Tpkt - Tpkt_d_src; #total de pacotes gerados so para confirmar linha de
cima
   #Tpckt_normaliz = Tpkt_r/Tpkt_consid # total de pacotes normalizados

   Tdelay_recebidos = Tdelay_r; #atraso total dos pacotes recebidos
   Tdelay_perdidos = Tdelay_d; # atraso total dos pacotes perdidos
   Tdelay = Tdelay_r + Tdelay_d;#atraso toal dos pacotes

   Thops = Thops_r + Thops_d; # total de hops
   Tdef = Tdef_r + Tdef_d;    # total de deflexoes
   #plf_consid = Tpkt_d_consid/Tpkt_normaliz; #fracao de perda de pacotes
desconsiderando perda no nó de origem
```

```
   #prf_consid = Tpkt_r/Tpkt_normaliz; #fracao de pacotes recebidos considerando qtidade
de pacotes total noramlizada
   plf = Tpkt_d_consid/Tpkt_consid;#fracao de perda de pacotes considerando perda no nó
de origem
   prf = Tpkt_r/Tpkt_consid; #fracao de recebimento de pacotes considerando qtidade de
pacotes total gerado

   Avhops = Thops/Tpkt_consid; #media hosps por pacote
   Avdelay = Tdelay/Tpkt_consid;#media de atraso por pacotes
   Avhops_r = Thops_r/Tpkt_r;#media de hops dos pacotes recebidos
   Avdelay_r = Tdelay_r/Tpkt_r; #media de atraso dos pacotes recebidos


        if (Tdef != 0) {
        pdf = Tdef/Thops;
        pdf_r = Tdef_r/Thops_r;
        if (Tdef_d != 0) {
                pdf_d = Tdef_d/Thops_d;
        }
   }

   if (Tpkt_d_consid != 0) {
        Avhops_d = Thops_d/Tpkt_d_consid;
        Avdelay_d = Tdelay_d/Tpkt_d_consid;
   } else {
        Avhops_d = 0;
        Avdelay_d = 0;
   }

   if(Tpkt_d_src != 0) {
        Avdelay_d_src = Tdelay_d_src/Tpkt_d_src;

   }else {
        Avdelay_d_src = 0 ;
   }

  if(Trc != 0 ){
        Vazao_pkts = Trc/Tdelay_r + Tdelay_d;
        Vazao_bits = (Trc*8)/Tdelay_r+tdelay_d;

   }else {
        Vazao_pkts = 0;
        Vazao_bits = 0;
   }

printf("%d %d %d %d %d %d %.8f %.8f %.8f %.8f %.8f %d %.8f %.8f %.8f %.8f %.8f
%.8f %.8f\n", Tpkt, Tpkt_r, Tpkt_d,
```

```
Tpkt_d_src, Tpkt_consid, Tpkt_consid2, plf, prf, Tdelay, Tdelay_recebidos,
Tdelay_perdidos, Thops, Avhops, Avhops_r,
Avdelay, Avdelay_r, Avdelay_d, Avdelay_d_src, Vazao_pkts)
}

# Desvio Padrão para o numero de hops e delay

#    for (i in hop) {
#         d1 = hop[i] - Avhops;
#         d2 = delay[1] - Avdelay;
#         sumhop = sumhop + d1*d1;
#         sumdelay = sumdelay + d2*d1;

# Procedimento auxiliar para o calculo de Parâmetros para
   # os pacotes perdidos e recebidos.

 #   if (Crtl[i] == 1) {
#         d1_r = hop[i] - Avhops_r;
#         d2_r = delay[i] - Avdelay_r;
#         sumhop_r = sumhop_r + d1_r*d1_r;
#         sumdelay_r = sumdelay_r + d2_r*d2_r;

  #   }else {
#         d1_d = hop[i] - Avhops_d;
#         d2_d = delay[i] - Avdelay_d;
#         sumhop_d = sumhop_d + d1_d*d1_d;
#         sumdelay_d = sumdelay_d + d2_d*d2_d;
#         }
#}
#Std_hop = sqrt(sumhop/Tpkt);
#Std_delay = sqrt(sumdelay/Tpkt);

#Std_hop_r = sqrt(sumhop_r/Tpkt_d);
#Std_delay_d = sqrt(sumdelay_d/Tpkt_d);

#         if (Tpkt_d!=0) {
#                   Std_delay_d = sqrt(sumhop_d/Tpkt_d);
#                   Std_delay_d = sqrt(sumdelay_d/Tpkt_d);
#         }else {
#           Std_hop = 0;
#           Std_delay_d = 0;
#         }
```

~~~~~~~~~
~~~~~~~~~