UNIVERSIDADE da MADEIRA

DEPARTAMENTO DE MATEMÁTICA E ENGENHARIAS

# ENCAMINHAMENTO ÓPTIMO DO TRÁFEGO EM REDES *TRIPLE PLAY*


**Sandy Carmo Relva Rodrigues**

Licenciada em Engenharia de Electrónica e Telecomunicações

Universidade da Madeira

**Orientador**

Professor Doutor Paulo Nazareno Maia Sampaio

Dissertação apresentada para a obtenção do grau de

Mestre em Engenharia de Telecomunicações e Redes

Madeira

2009

Departamento de Matemática e Engenharias

Universidade da Madeira

# ENCAMINHAMENTO ÓPTIMO DO TRÁFEGO EM REDES TRIPLE PLAY

**Sandy Carmo Relva Rodrigues**

Mestrado em Engenharia de Telecomunicações e Redes

2009

**Resumo**

A Internet é responsável pelo surgimento de um novo paradigma de televisão – IPTV (Televisão sobre IP). Este serviço distingue-se de outros modelos de televisão, pois permite aos utilizadores um elevado grau de interactividade, com um controlo personalizado sobre os conteúdos a que pretende assistir. Possibilita ainda a oferta de um número ilimitado de canais, bem como o acesso a conteúdos de *Vídeo on Demand* (VoD). O IPTV apresenta diversas funcionalidades suportadas por uma arquitectura complexa e uma rede convergente que serve de integração a serviços de voz, dados e vídeo. A tecnologia IPTV explora ao máximo as características da Internet, com a utilização de mecanismos de Qualidade de Serviço. Surge ainda como uma revolução dentro do panorama televisivo, abrindo portas a novos investimentos por parte das empresas de telecomunicações. A Internet também permite fazer chamadas telefónicas sobre a rede IP. Este serviço é denominado VoIP (Voz sobre IP) e encontra-se em funcionamento já há algum tempo.

Desta forma surge a oportunidade de poder oferecer ao consumidor final, um serviço que inclua os serviços de Internet, de VoIP e de IPTV denominado serviço *Triple Play*. O serviço *Triple Play* veio obrigar a revisão de toda a rede de transporte de forma a preparar a mesma para suportar este serviço de uma forma eficiente (QoS), resiliente (recuperação de falhas) e optimizado (Engenharia de tráfego).

Em redes de telecomunicações, tanto a quebra de uma ligação como a congestão nas redes pode interferir nos serviços oferecidos aos consumidores finais. Mecanismos de sobrevivência são aplicados de forma a garantir a continuidade do serviço mesmo na ocorrência de uma falha.

O objectivo desta dissertação é propor uma solução de uma arquitectura de rede capaz de suportar o serviço *Triple Play* de uma forma eficiente, resiliente e optimizada através de um encaminhamento óptimo ou quase óptimo. No âmbito deste trabalho, é realizada a análise do impacto das estratégias de encaminhamento que garantem a eficiência, sobrevivência e optimização das redes IP existentes, bem como é determinado o número limite de clientes permitido numa situação de pico de uma dada rede.

Neste trabalho foram abordados os conceitos de Serviços *Triple Play*, Redes de Acesso, Redes Núcleo, Qualidade de Serviço, MPLS (*Multi-Protocolo Label Switching*), Engenharia de Tráfego e Recuperação de falhas. As conclusões obtidas das simulações efectuadas através do simulador de rede NS-2.33 (*Network Simulator versão 2.33*) serviram para propor a solução da arquitectura de uma rede capaz de suportar o serviço *Triple Play* de uma forma eficiente, resiliente e optimizada.

**PALAVRAS-CHAVE:** VoIP, IPTV, *Triple Play*, VDSL2, MPLS, QoS, Engenharia de Tráfego, Recuperação de falhas, NS-2.33.

**Abstract**

The rapidly evolving Internet is responsible for the emergence of this new television paradigm called IPTV (Television over IP). This new technology distinguishes itself from all the other television models proposed over the years because the users have total control over what they see and when they see it. IPTV allows viewers to have an unlimited amount of TV channels and access to Video on Demand (VoD). IPTV presents a variety of functionalities supported by complex network architectures and a convergent network that integrates the data, voice and video services. The IPTV technology explores its true potential on the Internet with the assistance of Quality of Service mechanisms. This technology opens doors to a whole new era of investments for the telecommunication companies because these companies now have the opportunity to offer their clients the television service. Telephone calls can also be made through the Internet network. This service is called VoIP and has been around for quite some time.

These companies now have the opportunity to offer end users one pack of services that include Data, VoIP and IPTV, whilst also, cutting costs. This pack is known as the Triple Play service. This service made it mandatory to revise the existent transport network to prepare it so it could support this service efficiently (QoS), resiliently (fault proof network) and optimally (Traffic Engineering).

In telecommunication networks, faulty or congested links cause interference in the Triple Play services. Survivable mechanisms are used to ensure the continuity of the service even when faults occur.

The goal of this dissertation is to propose a network architecture that is capable of supporting the Triple Play service efficiently, resiliently, optimally and robustly as a solution, by routing the traffic in an optimal manner through the network. The impact of routing strategies in the existing IP networks to guaranty efficiency, resiliency and robustness in the network are analysed in this dissertation. The limit number of clients permitted simultaneously in a given congested network was also determined in this work.

In this dissertation, topics such as: concepts of the Triple Play service, Access networks, Core networks, Quality of Service mechanisms, MPLS (Multi-Protocol Label Switching) transport technology, Traffic Engineering and fault recuperation methods are discussed. The conclusions were achieved through the results obtained from the Network Simulator NS-2.33. This simulator was used to create simulations of the various scenarios, in order to propose a Final solution for a network architecture that makes an existing IP network able to support the Triple Play service.

**Key words:** Triple Play, IPTV, VDSL2, MPLS, QoS, Traffic Engineering, Fault Recuperation, NS-2.33.

**Agradecimentos**

A todos que de alguma forma me apoiaram ao longo da realização deste trabalho, quero agradecer a compreensão e o carinho que sempre me dedicaram.

Ao meu orientador Professor Doutor Paulo Nazareno Maia Sampaio pelo interesse e apoio na orientação, bem como, pela disponibilidade com que sempre me atendeu e orientou.

Ao Professor Eduardo Marques pelo apoio e orientação que prestou na elaboração da dissertação tanto na parte teórica como na parte prática.

Ao Milton Aguiar, pelo no esclarecimento de dúvidas relacionadas com as redes de Telecomunicações.

Ao meu noivo Marco Abreu, pela disponibilidade, força, compreensão e incentivo que me deu para completar a dissertação.

Ao meu irmão Kevin Rodrigues pelo carinho, pela força nos momentos mais difíceis e pelo apoio constante que me deu.

Aos meus pais, Ana Paula Rodrigues e João Santos, em especial, pela compreensão, força, apoio, incentivo e por me ajudarem no que fosse necessário e sempre sem hesitar.

Finalmente ao Centro de Ciência e Tecnologia da Madeira (CITMA) pelo apoio financeiro.

**ÍNDICE**

# Índice de Figuras

# Índice de Tabelas

# Glossário

AAL - *ATM Adaptation Layer*

ABR - *Available Bit Rate*

ADM - *Add Drop Multiplexer*

ADSL - *Asynchronous Digital Line Subscriber*

AF - *Assured Forwarding*

AON - *Active Optical Network*

ATM - *Assynchrounous Transfer Mode*

BB - *Bandwidth Broker*

CAPEX - *Capital Expenditures*

CAS - *Condition Access System*

CBR - *Constant Bit Rate*

CBR - *Constraint Based Routing*

CIDR - *Classes Inter-domain Routing*

CoS – *Class of Service*

CRC - *Cyclic Redundancy Check*

CR-LDP - *Constraint-based Routing Label Distribution Protocol*

CR-LSP - *Constraint Routing – Label Switching Path*

CS - *Convergence Sublayer*

CSMA/CD - *Carrier Sense Multiple Access with Collision Detection*

CSPF - *Constraint Shortest Path First*

DiffServ – *Differentiated Services*

DRM - *Digital Rights Management*

DS *Field - Differentiated Service Field*

DSL - *Digital Subscriber Line*

DSLAM - *Digital Subscriber Line Access Multiplexer*

DV - *Distance Vector*

EF - *Expedited Forwarding*

EIA - *Electronic Industries Association*

ER-LSP - *Explicit Routing – Label Switching Path*

FCS - *Frame check sequence*

FEC – *Forwarding Equivalence Class*

FIS – *Fault Indication Signal*

FLP - *Fast Link Pulses*

FRS - *Fault Repair Signal*

FTP - *Foil Twisted Pair*

FTTB - *Fiber To The*

FTTC - *Fiber To The*

FTTH - *Fiber To The*

FTTN - *Fiber To The Node*

GOP - *Group of Pictures*

HTTP - *Hypertext Transfer Protocol*.

IETF - *Internet Engineering Task Force*

*I-Frame - IntraFrame*

IGMP - *Internet Group Management Protocol*

IGP - *Internet Gateway Protocol*

IntServ – *Integrated Services*

IP - Protocolo Internet

IPTV - Televisão por IP

IS-IS - *Intermediate System – Intermediate System*

ISP - *Internet Service Provider*

ITU - *Recommendation* G.992.1

LBS – *Label Based Switching*

LDP - *Label Distribution Path*

LED - *Light Emitting Diode*

LSA – *Link State Advertisement*

LS - *Link State*

LSP – *Label Switching Path*

LSR - *Label Switch Router*

LSR - PSL – *Path Switch LSR*

MAC - *Media Access Control*

MF - *Multi-Field*

MOS - *Mean Opinion Score*

MPEG - *Moving Picture Experts Group*

MPLS - *Multiprotocol Label Switching*

MPLS-CR-LDP - *Constraint-based Routing Label Distribution Protocol*

MPLS-LDP - *Laber Distribution Protocol*

MSPP - *Multi-Service Provisioning Pack*

MSPP - *MultiService Provisioning Platform*

MTU - *Maximum Transmission Unit*

NDVR - *Network Digital Vídeo Recording*

NRT-VBR - *Non-Real Time Variable Bit Rate*

OLT - *Optical Line Terminal*

ONU - *Optical Network Unit*

OPEX - *Operational Expenditure*

OSPF - *Open Shortest Path First*

PBR - *Policy-Based Routing*

PCM - *Pulse-Code Modulation*

PDU - *Protocol Data Unit*

PHP - *Per Hop Behavior*

PM - *Physical Medium*

PON - *Passive Optical Network*

POR – *Point of Repair*

PSL - *Path Switch LSR*

PSTN - *Public Switching Telecommunications Network*

PT – Portugal Telecom

PTP - *Point To Point*

QBR - Qos-*Based Routing*

QoS – *Quality of Service*

RSVP - *Resource Reservation Protocol*

RSVP-TE - *Resource Reservation Protocol – Traffic Engineering*

RTCP - *Real Time Control Protocol*

RTP - Routing Transport Protocol

RTSP - *Real Time Stream Protocol*

RT-VBR - *Real Time Variable Bit Rate*

SAR.- *Segmentation and Reassembly Sublayer*

SDH - *Synchronous Digital Hierarchy*

SFD - *Start-of-Frame*

SFP - *Shortest Path First*

SHE - *Vídeo Headend*

SIP - *Session Initiation Protocol*

SLA - *Service Level Agreements*

SOH - *Section Overhead*

SPF - *Shortest Path First*

STB - *Set-Top-Box*

STM - *Synchronous Transport Module*

STP - *Shielded Twisted Pair*

TC - *Transmission Convergence*

TCP - *Transport Control Protocol*

TCP/IP - *Transport Control Protocol / Internet Protocol*

TDM - *Time Division Multiplexing*

TLV - *Type-Length-Value*

TOS - *Type of Service*

TTL - *Time To Live*

TV - *Televisão sobre a Internet*

UBR - *Unspecified Bit Rate*

UDP -*User Datagram Protocol*

UNI - *User-Network Interface*

UTP - *Unshielded Twisted Pair*

VC – *Virtual Channel*

VCI - *Virtual Channel Identifier*

VDSL - *Very High bit rate* DSL

VHO - *Vídeo Hub Office*

VLAN - (*Virtual Local Area Network*

VoD - *Vídeo on Demand*

VoIP – *Voice over IP*

VP - *Virtual Path*

VPI - *Virtual Path Identifier*

WFQ - *Weight Fair Queueing*)

xDLS - variantes da *Digital Line Subscriber*

xPON - variantes das redes *Passive Óptical Network*

# CAPÍTULO I

# INTRODUÇÃO

Neste primeiro capítulo, apresenta-se o problema da presente investigação, o seu objectivo geral e as questões que a orientaram na consecução desse objectivo. Sucedem-se a contextualização da investigação, a sua pertinência e, por fim, explicita-se a organização da dissertação.

## 1.1. CONTEXTUALIZAÇÃO

Os avanços tecnológicos relacionados às redes de telecomunicações, permitem surgir novas tecnologias e novos serviços. O serviço *Triple Play* é fruto destes avanços tecnológicos pois permite fornecer ao subscritor, num só pacote, os serviços de dados, voz e vídeo. Os serviços de dados e de voz existem no mercado português há alguns anos. O serviço de dados permite o acesso às páginas Web, ao correio electrónico e à transferência de arquivos pela rede IP (Protocolo Internet). O serviço de voz ou VoIP (voz sobre IP) permite efectuar chamadas telefónicas através da rede IP. A grande novidade é o fornecimento do serviço de conteúdo de vídeo através da rede IP denominado de serviço IPTV (Televisão por IP).

O aparecimento do serviço IPTV veio revolucionar o modo de ver televisão, onde o conteúdo de vídeo é transportado pela rede IP até à televisão do subscritor. O serviço IPTV permite fornecer ao subscritor o controlo total do conteúdo que pretende visualizar através do comando, pois este comunica bidireccionalmente com a rede IP. A comunicação bidireccional permite ao subscritor gravar, pausar, andar para a frente ou andar para trás com o conteúdo de vídeo que solicita para visualizar.

Os conteúdos de voz e de vídeo são intolerantes à perda de pacotes, uma vez que a emissão é efectuada em tempo real. A perda de pacotes afecta a percepção da voz no caso do conteúdo de voz e afecta a imagem no caso do conteúdo de vídeo. A disponibilidade da largura de banda na rede IP é um grande requisito para o conteúdo de vídeo, devido ao tamanho dos pacotes, e não tanto para o conteúdo de voz.

Estes problemas colocam muitas questões em termos de exigências requeridas pelo serviço *Triple Play* em relação à qualidade de serviço, à resiliência a falhas na rede e à eficiência na utilização dos recursos existentes na rede.

## 1.2. MOTIVAÇÃO E PRINCIPAIS CONTRIBUIÇÕES

A realização deste trabalho de mestrado foi motivada pelo aparecimento do conceito do serviço *Triple Play*, pois este é uma grande novidade para Portugal. Sabe-se que o serviço *Triple Play* inclui o fornecimento dos serviços de dados, voz e vídeo. A intolerância à perda de pacotes e a exigência da disponibilidade de grandes larguras de banda na rede IP são alguns dos factores existentes no serviço *Triple Play*. Estes factores despertaram interesse em analisar quais os requisitos necessários existir na rede IP, desde a rede núcleo até à casa do subscritor, para esta possuir a capacidade de suportar os requisitos de qualidade de serviço do serviço *Triple Play* bem como resistir a possíveis falhas de rede sem provocar grandes perdas de pacotes. Este estudo permite determinar quais as tecnologias de rede de acesso a utilizar, quais as tecnologias de rede núcleo a utilizar e quais as tecnologias ou arquitecturas a utilizar para fornecer qualidade de serviço na rede IP e resiliência contra falhas de rede. As opções tomadas determinam o tipo de qualidade de serviço oferecido ao subscritor.

Em redes de telecomunicações, a quebra de uma ligação pode interferir nos serviços oferecidos por várias conexões. Mecanismos de sobrevivência são aplicados de forma a garantir a continuidade do serviço mesmo na ocorrência de uma falha. Contudo, isto obriga a que sejam reservados recursos extra para o restauro.

O objectivo desta dissertação é propor uma solução de uma arquitectura de rede capaz de suportar o serviço *Triple Play* de uma forma eficiente, resiliente e optimizada através de um encaminhamento óptimo ou quase óptimo.

As principais contribuições realizadas no âmbito deste trabalho são:

- Optimizar a rede IP existente de modo a suportar o serviço *Triple Play*;
- Utilizar um simulador de rede para obter valores mais próximos da realidade e tirar conclusões mais concretas através de uma variedade de simulações e cenários;
- Determinar as diferenças entre as redes IP e MPLS através do simulador de rede;
- Determinar, através do simulador de rede, quais as configurações a atribuir a uma rede MPLS para esta suportar o serviço *Triple Play* de uma forma eficiente*;*
- Determinar, através do simulador de rede, as capacidades e os limites da ferramenta de Engenharia de Tráfego quando utilizada numa rede *Triple Play*;
- Determinar, através do simulador de rede, qual o método de recuperação de falhas mais eficiente a utilizar numa rede *Triple Play*;
- Propor uma solução de uma arquitectura de rede capaz de suportar o serviço *Triple Play* de forma eficiente, resiliente, optimizada e robusta. A arquitectura de rede inclui a

selecção do meio de transmissão, das tecnologias de transporte, da solução de Qualidade de Serviço e do método de recuperação de falhas, e;

- Determinar o número limite de clientes possíveis existir numa dada rede, capaz de suportar o serviço *Triple Play*, numa situação pico.

Uma rede em malha possui vários encaminhamentos possíveis. A quantidade de recursos excedentes para garantir a sobrevivência é dependente do encaminhamento. A análise do impacto das estratégias de encaminhamento para garantir a sobrevivência. Da mesma forma, são encontradas estratégias de encaminhamento óptimas ou quase óptimas para o caso proposto.

As soluções de encaminhamento são propostas através das seguintes tarefas:

a) Modelar uma rede de transporte;

b) Determinar os caminhos possíveis;

c) Proceder ao encaminhamento seguindo uma dada estratégia;

e) Repetir c) e d) considerando diversas estratégias de encaminhamento;

f) Definir uma estratégia de encaminhamento óptima ou quase óptima;

## 1.3. ORGANIZAÇÃO DA TESE

O restante desta dissertação está dividido em 5 Capítulos. O segundo capítulo apresenta o estado da arte do serviço *Triple Play.* Este capítulo apresenta uma introdução teórica aos conceitos relacionados com as Redes *Triple Play*. Está dividido em quatro secções: o Serviço *Triple Play*, o Meio de Transmissão de Dados, as Redes de Agregação e de Acesso e por fim as Redes Núcleo.

O Capítulo 3 apresenta uma introdução teórica aos conceitos relacionados com a Qualidade de Serviço nas redes e os métodos de Recuperação da Rede utilizados em caso de falha ou congestionamento da rede.

No Capítulo 4 são dados a conhecer alguns dos simuladores, existentes no mercado, que permitem efectuar as simulações de redes de transporte. Este estudo irá permitir determinar as características que nos levaram à escolha da ferramenta de simulação, no contexto deste projecto de mestrado.

No Capítulo 5 são apresentados os conceitos teóricos e o funcionamento experimental do simulador de rede NS-2.33 através das simulações de vários cenários. A análise dos resultados leva à criação do Cenário 4 que representa a arquitectura a ser utilizada numa rede eficiente, resiliente e robusta capaz de suportar o serviço *Triple Play.*

Por fim o Capítulo 6 apresenta as conclusões dos temas abordados na dissertação e sugere algumas perspectivas de continuação deste trabalho de mestrado como trabalhos futuros.

# CAPÍTULO II

# ESTADO DA ARTE: REDES *TRIPLE PLAY*

O Capítulo 2 apresenta uma introdução teórica aos conceitos relacionados com as Redes *Triple Play*. Este Capítulo está dividido em quatro secções: o Serviço *Triple Play*, o Meio de Transmissão de Dados, as Redes de Agregação e de Acesso e por fim as Redes Núcleo.

## 2.1 SERVIÇO *TRIPLE PLAY*

Nesta secção pretende-se dar a conhecer o conceito, o funcionamento, a arquitectura e os requisitos de cada serviço pertencente ao serviço *Triple Play*. Os serviços incluídos no serviço *Triple Play* são: o serviço de dados, o serviço VoIP (Voz sobre IP) e o serviço IPTV (Televisão sobre IP).

### 2.1.1 Serviço de Dados

A rede Internet foi concebida com o intuito de fornecer um meio de transferência de dados entre computadores remotos através da utilização do protocolo IP (*Internet Protocol*) com o apoio de vários serviços de dados. Os serviços de dados mais conhecidos incluem o serviço de correio electrónico, o serviço de transferência de ficheiros e o serviço de acesso às páginas Web. A rede Internet ou rede IP é muitas vezes referida como uma rede de "melhor-esforço". Este termo refere-se ao tipo de Qualidade de Serviço existente na rede IP, ou seja, numa rede de "melhor-esforço" é muito provável a existência de atrasos, de variações de atrasos e perda de pacotes.

**Arquitectura do Serviço de Dados**

A arquitectura de uma rede de dados consiste num servidor, numa rede de transporte (Internet) e num utilizador final, conforme pode ser visualizado na Figura 2.1. O utilizador final solicita informação aos servidores e estes fornecem o serviço pretendido (correio electrónico, acesso às páginas Web ou transferência de ficheiros). A rede Internet é constituída por elementos e tecnologias de rede que permitem encaminhar os dados até ao seu destino através de um endereço IP.

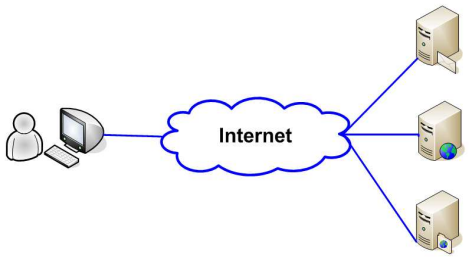



**Figura 2.1 – Arquitectura do Serviço de Dados.**

A rede IP é uma rede de comutação de pacotes. Esta particularidade permite que numa rede IP dois dispositivos troquem diferentes tipos de informação sem necessitarem de estar directamente conectados, nem de terem uma reserva de recursos. As tarefas de localização e de encaminhamento são da responsabilidade dos protocolos. Numa rede IP de "melhor esforço" todos os pacotes IP são tratados da mesma forma e entregues ao destino da forma mais rápida sem diferenciação do tráfego. O tráfego de "melhor esforço" atravessa a rede com uma taxa de transferência e uma variação do tempo de entrega variável, uma vez que depende da carga de tráfego carregado no momento. Desta forma, este tipo de tráfego não oferece garantias de entrega, de débito efectivo (*Throughput*), de atrasos fixos, de prioridade, nem de qualquer nível de qualidade e torna a recuperação dos dados perdidos numa operação muito difícil de efectuar. Por outro lado, as redes IP de "melhor esforço" oferecem eficiência na operação da rede e um baixo custo dos nós devido à sua reduzida complexidade.

A garantia da entrega do tráfego é oferecida pelo protocolo TCP (*Transport Control Protocol*) [Redbooks, 2006]. O protocolo TCP oferece um serviço orientado à conexão ou *unicast* (envio de dados ponto-a-ponto) pois verifica se toda informação transferida é recebida por inteiro no destino. Esta verificação é realizada através de uma mensagem de confirmação numa comunicação *Full duplex* (troca de dados em simultâneo e em ambos os sentidos). Este protocolo resolve os problemas de perdas, atrasos e duplicação. É um protocolo utilizado pelos serviços de dados na entrega de correio electrónico, na transferência de arquivos e no acesso às páginas Web. O protocolo TCP adapta-se à taxa de transferência existente na rede e tem como objectivo aumentar a sua taxa de transferência enquanto a rede trata de entregar todos os pacotes ao destino. O protocolo TCP interpreta a perda de pacotes como um sinal de congestionamento na rede e reage reduzindo a sua taxa de transferência de envio de forma a optimizar a utilização da rede. Assim, quando não existe muito tráfego na rede é de esperar um elevado débito efectivo e um baixo nível de variação de atrasos. Por outro lado, no caso de existir muito tráfego na rede é de esperar um baixo débito efectivo e níveis elevados de perda de pacotes e de variações de atraso [Stoica, 2004, Clark, 1998].

Os termos *upload* e *download* são utilizados para descrever o sentido da transferência dos dados. O termo *upload* refere-se aos dados que são transmitidos do utilizador final para o servidor, enquanto o termo *download* refere-se aos dados que são transmitidos do servidor para o utilizador

final. No caso do volume de dados recebidos ser maior do que a largura de banda existente na rede, os dados são transferidos através de gestores de *downloads*. Estes gestores de *downloads* são aplicações que permitem pausar, reiniciar ou efectuar *downloads* de dados em ligações de má qualidade [Stoica, 2004, Clark, 1998].

**Requisitos do Serviço de Dados**

Para a transmissão de grandes mensagens é necessário fragmentar as mensagens em pacotes mais pequenos, transmitir os mesmos na rede através de protocolos, reconstruir as mensagens e assegurar a chegada de todos os pacotes ao seu destino sem repetições e pela ordem correcta. Os serviços de dados apenas necessitam de receber os dados, independentemente de ser em tempo real, em sequência ou numa largura de banda constante. Estes serviços são afectados quando existe um grande atraso, uma grande variação de atraso ou uma cessão de largura de banda na rede. Estes factores provocam perdas de pacotes e consequentemente erros irreparáveis na mensagem transferida. Os pacotes de dados são igualmente perdidos na rede por motivos de falha de ligações ou de nós. Quanto maior for a taxa de transferência mais rapidamente os dados são transferidos pela rede IP. No entanto, os dados podem ser transferidos numa rede com largura de banda na ordem dos Kbps.

**Vantagens e Limitações do Serviço de Dados**

Os serviços de dados permitem a transferência de dados em tempo real entre computadores remotos e a redução do custo associado. O serviço de correio electrónico oferece a vantagem de enviar ficheiros de uma forma mais rápida, fácil, económica e ecológica do que o correio tradicional. O serviço de transferência de ficheiros permite uma troca mais facilitada e rápida de ficheiros entre computadores remotos. O serviço de acesso às páginas Web facilita o acesso à informação sem ser necessário, por exemplo, deslocar-se às bibliotecas. Os serviços de dados são tolerantes aos atrasos, às variações de atrasos, à escassez de largura de banda, e à desordenação da chegada de pacotes. Uma das maiores desvantagens que os serviços de dados proporcionam é a falta de garantia de privacidade dos dados transferidos entre os computadores. Outra desvantagem reside na intolerância à perda de pacotes que pode levar à impossibilidade de abertura do ficheiro. Este facto pode-se dever a erros irreparáveis que foram provocados na mensagem transferida [Stoica, 2004, Clark, 1998].

### 2.1.2 Serviço VoIP

O PSTN (*Public Switching Telecommunications Network*) é uma rede de telecomunicações pública projectada com o objectivo de transmitir a voz humana, ao contrário da Internet que tem o objectivo de transportar dados [Walker et al, 2002]. Actualmente, a rede PSTN transmite a voz humana através de uma técnica de comutação de circuitos.

O VoIP (Voz sobre IP) é um serviço que permite transmitir a voz humana em tempo real através de uma técnica de comutação de pacotes nas redes IP existentes.

De seguida é descrita a arquitectura do serviço VoIP, as suas características, os seus requisitos, as suas vantagens e suas limitações.

#### Arquitectura do Serviço VoIP

A transmissão do sinal da voz num sistema VoIP consiste na emissão e recepção do sinal da voz humana conforme ilustrado na Figura 2.2.

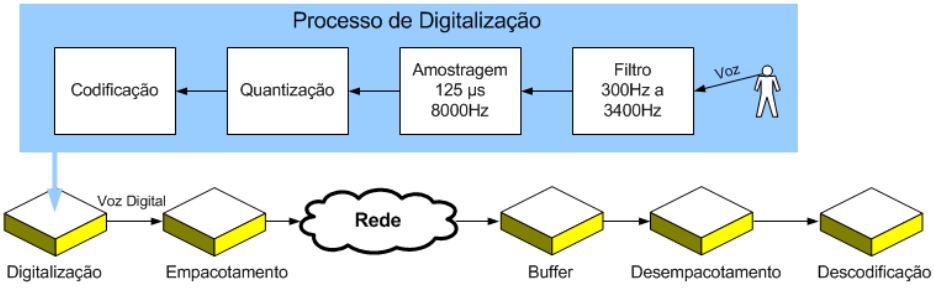



**Figura 2.2 – Tratamento dado ao som num sistema VoIP**

A emissão do sinal de voz consiste na digitalização, compressão, empacotamento e transmissão do sinal analógico da voz humana pela rede IP [ITU-T P.800, 1996, ITU-T P.830, 1996]. A digitalização do sinal consiste na amostragem, quantização e codificação do sinal analógico. A amostragem e quantização apresentam um atraso que foi estabelecido e fixado internacionalmente. A codificação permite comprimir o sinal de voz através de *codecs* (COmpressor/DECompressor) e consequentemente reduzir o tamanho da mensagem a transmitir na rede. Isto torna mais eficiente a utilização do espaço de memória da aplicação e da largura de banda necessária para a transmissão. A compressão provoca um aumento do atraso e a perda da qualidade do sinal devido ao processamento do algoritmo de codificação e descodificação. Os *codecs* possuem características que determinam a escolha da sua utilização tais como a taxa de transmissão, o atraso, a complexidade do algoritmo e a qualidade do sinal.

A Tabela 2.1 mostra os diferentes *codecs* e respectivas taxas de transferência, atraso de codificação e MOS (*Mean Opinion Score*). A avaliação da qualidade de serviço numa rede VoIP é

efectuada através de técnicas de metodologia tal como o MOS (*Mean Opinion Score*), entre outros. O MOS é um método subjectivo definido nas Recomendações ITU-T P.800 e ITU-T P.830, em que os avaliadores ouvintes atribuem uma pontuação de 1 (pobre) a 5 (excelente) à qualidade da fala reproduzida pelo sistema de comunicação em teste [ITU-T P.800, 1996, ITU-T P.830, 1996].

Da Tabela 2.1 observa-se que a técnica de compressão PCM (*Pulse-Code Modulation*) ou Modulação por Código de impulsos apresenta a maior taxa de transferência, o menor atraso de codificação e a maior pontuação MOS [Bakshi, 2006, Moura, 2005]. Sendo assim, o PCM é o *codec* mais propício para ser utilizado nas redes VoIP.

**Tabela 2.1 – *Codecs* do sistema VoIP e respectivas características.**

| *Codec* | Técnica de Compressão | Taxa de transferência (Kbps) | Atraso de codificação (ms) | MOS | Observações |
|---|---|---|---|---|---|
| G.711 | PCM | 64 | 0.125 | 4,5 | Uso Universal |
| G.726 | ADPCM | 16, 24, 32, 40 | 0.125 | 3,8 | Qualidade elevada e baixa complexidade |
| G.728 | LD-CELP | 16 | 3-5 | 3,6 | Recomendado para cabos |
| G.729 (A) | CS-ACELP | 8 | 10 | 3,7 | Uso geral |
| G.723.1 (6.3) | MPC-MLQ | 6.3 | 30 | 3.6 | Origem em videoconferência |
| G.723.1 (5.3) | ACELP | 5.3 | 30 | 3.1 | Origem em videoconferência |

Os protocolos de sinalização no sistema VoIP são utilizados para iniciar, gerir e terminar as sessões de voz. Entre os protocolos de sinalização mais utilizados no sistema VoIP estão o padrão H.323 e o protocolo SIP (SIP - *Session Initiation Protocol*) ou protocolo de iniciação de sessão. O padrão H.323 faz parte da família de recomendações ITU-T H.32x, que pertence à série H da ITU-T, e que trata de "Sistemas Audiovisuais e Multimédia". O padrão H.323 é na realidade um conjunto de protocolos que incorpora muitos protocolos individuais (H.263 (vídeo), G.711 (áudio), entre outros) desenvolvidos para aplicações específicas. O SIP foi desenvolvido especialmente para o serviço de voz sobre IP e tira vantagem dos protocolos já existentes para tratar dos processos de sinalização. Isto faz com que o cabeçalho do padrão H.323 seja maior do que o cabeçalho do protocolo SIP. Como a complexidade do sistema é reduzida no protocolo SIP, a implementação de novos serviços de voz é facilitada. Isto permite uma redução no tempo da implementação de novos serviços de voz e consequentemente uma redução no custo dos serviços oferecidos aos utilizadores finais [Nokia, 2003, Zultys, 2004]. O crescimento da *Internet* e a implementação de mecanismos de segurança (*firewall*) nas redes de acesso prejudicam os serviços e aplicações de voz sobre IP em termos de velocidade de transmissão das mensagens [Barbosa, 2006].

O empacotamento consiste em atribuir aos dados digitais um protocolo de transporte (UDP) para transferi-los através da rede. O protocolo de transporte UDP (*User Datagram Protocol*) fornece um serviço de uma comunicação não orientada à conexão (*conectionless-oriented*), utilizado pelas aplicações sensíveis ao tempo no qual a falta de dados é preferível à chegada tardia dos mesmos. Como o protocolo UDP não tem um cabeçalho para verificar a entrega dos dados no destino e a sua ordem de chegada, a transferência do tráfego torna-se mais rápida e eficiente. Ao

contrário do protocolo de transporte TCP, o protocolo de transporte UDP é compatível com o *broadcast* (envio de dados a toda a rede local), *multicast* (envio de dados a todos os subscritores) e *unicast* de pacotes [Stoica, 2004, Sardella, 2005]. As aplicações VoIP utilizam o protocolo RTP que define a fragmentação do fluxo de dados áudio, adicionando a cada fragmento informação de sequência e de tempo de entrega. O controlo é realizado pelo RTCP (*Real Time Control Protocol*). Ambos utilizam o protocolo UDP como protocolo de transporte, o qual não oferece qualquer garantia de entrega dos pacotes em um determinado intervalo [RFC 3550 et al, 2003].

A recepção do sinal de voz consiste no armazenamento do sinal digital recebido da rede num *buffer*, e no desempacotamento e descodificação do sinal digital da voz humana. O *buffer* é uma memória temporária que minimiza ou elimina os problemas da execução de áudio, no caso do VoIP, provocados pela variação do atraso [Markopoulou et al, 2002].

**Requisitos do Serviço VoIP**

Idealmente, uma rede VoIP seria capaz de fornecer uma transmissão de voz com uma qualidade equivalente à de uma rede PSTN. Um dos requisitos fundamentais para assegurar a qualidade do sinal da voz numa rede VoIP é a largura de banda. A qualidade de voz é assegurada pela existência de uma largura de banda suficiente na rede (idealmente superior a 64 Kbps) [Collins, 2001]. O grande interesse em utilizar o serviço VoIP, apesar de existir uma infra-estrutura pronta e fiável para a comunicação de voz denominada de PSTN, parte do facto de ser economicamente viável, uma vez que reduz os custos de telecomunicações, de telefones e de infra-estrutura.

Como a rede VoIP partilha o canal de comunicação com outras aplicações, que geram diferentes tipos de tráfego, há que manter uma qualidade de serviço (QoS – *Quality of Service*) adequada, de modo a que a qualidade perceptível pelo utilizador se mantenha. Existem vários factores que determinam a QoS de um serviço de voz. Entre todos os factores pode-se destacar o atraso, a variação do atraso e a perda de pacotes de dados.

O atraso é o tempo que um pacote de dados demora a chegar de um interlocutor ao outro. Para que uma conversa entre duas ou mais pessoas seja perceptível é necessário que o atraso não seja superior a 150 ms em cada sentido (de acordo com a recomendação da *International Telecommunication Union's Telecommunication branch's* - ITU-T's G.114). Para valores superiores a este intervalo de tempo, as vozes dos interlocutores acabam por se sobrepor, até a conversa se tornar impraticável. Numa rede de dados o atraso é obtido pela soma dos vários atrasos ao longo do trajecto que os pacotes de dados percorreram. É constituída por uma parte fixa, como o atraso da aplicação de VoIP e a propagação no meio físico, e por uma parte variável, como por exemplo a espera nas filas do equipamento activo de rede (ex. encaminhadores) e a disputa do meio com outro tráfego.

A variação do atraso é uma variação estatística do retardo na entrega de pacotes sucessivos de dados numa rede. Uma variação do atraso elevada produz uma recepção não regular de pacotes de dados e inviabiliza, neste caso, uma conversa normal que espera uma sucessão de pacotes a um ritmo constante. Idealmente, este ritmo deve ser igual àquele a que os pacotes são gerados no emissor. Embora na maioria das vezes o cenário ideal não possa ser obtido, a variação do atraso deve ter uma gama de variação limitada, de modo a permitir uma gestão controlada por parte das aplicações existentes nos extremos da comunicação. Uma das formas de minimizar o impacto da variação do atraso é utilizar um *buffer*. Este *buffer* armazena os pacotes de dados à medida que os mesmos chegam e envia-os para a aplicação/circuito descompressor a uma cadência fixa. Ao mesmo tempo, o *buffer* da variação do atraso pode proceder ao reordenamento de alguns dos pacotes, caso o protocolo utilizado o permita (ex. RTP). Devido ao facto deste *buffer* adicional implicar um atraso suplementar, deve ser especificado de modo a que a soma total de atrasos não ultrapasse os 150 ms referidos anteriormente, tendo muitas vezes um valor à volta dos 50 ms.

O número de pacotes de dados perdidos na rede, quer devido a erros motivados pelo meio físico, quer devido a políticas de eliminação de pacotes por excesso de tráfego na rede, influencia negativamente qualquer emissão de dados. No entanto, uma aplicação em tempo real como a proporcionada pela VoIP tem a desvantagem de não permitir o pacote ser reenviado em caso de erro, pois quando este finalmente chegasse ao seu destino o seu tempo certo já teria passado. Por outro lado, estas aplicações também não são tão sensíveis à perda de pacotes de dados como as aplicações de dados tradicionais (ex. transmissão de ficheiros), visto que a perda de 3% de pacotes de dados não afecta significativamente a qualidade da comunicação [Markopoulo et al, 2003].

O grande desafio das redes de voz sobre IP consiste em impedir que o tráfego de voz seja prejudicado pela congestão do tráfego de dados [Miras, 2002, Cisco, 2001].

**Vantagens e Limitações do Serviço VoIP**

A principal vantagem do serviço VoIP consiste na redução dos custos nas comunicações de voz, uma vez que este serviço utiliza a rede IP existente para transmitir os dados de voz. A desvantagem do serviço VoIP é a utilização do protocolo de transporte UDP pois este não fornece mecanismos de garantia de entrega de pacotes numa ordem sequencial nem fornece garantias de qualidade de serviço. Isto leva que o serviço VoIP tenha muitos problemas na existência de atrasos e variações de atrasos na rede IP. Estes factores provocam perdas de pacotes e consequentemente um fornecimento de um serviço de voz de má qualidade. O serviço VoIP também não oferece garantias de elevada privacidade.

### 2.1.3 Serviço IPTV

Os termos VoD (*Vídeo on Demand*), *Internet TV* (Televisão sobre a Internet) e IPTV (Televisão sobre IP) referem-se a serviços de vídeo em que os sinais de vídeo em cada um destes serviços são fornecidos ao utilizador final de uma forma diferente. O VoD consiste no serviço que fornece o conteúdo de vídeo armazenado em servidores (não em tempo real) sobre as redes IP até ao subscritor individual no momento em que o conteúdo de vídeo é solicitado pelo mesmo. Quando o conteúdo de vídeo é solicitado é fornecido em *unicast.* A QoS em tempo real não é um requisito necessário e o protocolo RTSP é utilizado nas opções de pausar, parar, *backward* e *forward*. O serviço VoD requer uma infraestrutura rica de *software* e *hardware* que interliga as componentes do VoD, também designado de *middleware*, como a subscrição VoD, um gravador de rede de vídeo e um gravador pessoal de vídeo.

Os termos *Internet TV* e IPTV são muitas vezes utilizados como sinónimos, uma vez que ambos são serviços que fornecem conteúdo de vídeo tanto em tempo real como em tempo não real, transmitem o conteúdo de vídeo em *multicast* e a rede IP é utilizada como meio de transporte do conteúdo de vídeo. Contudo, na realidade são termos que descrevem dois tipos de serviços diferentes. O que diferencia estes dois serviços é o facto do serviço *Internet TV* necessitar de um computador e uma aplicação de *media* para o utilizador final poder visualizar o conteúdo de vídeo enquanto que o serviço IPTV apenas requer um STB (*Set-Top-Box*) para descodificar o conteúdo media e permitir a visualização do conteúdo de vídeo directamente na televisão. Uma outra diferença encontra-se na qualidade da imagem pois o serviço IPTV oferece uma qualidade de imagem muito superior à do serviço *Internet TV*. [Altgeld et al, 2005, Taylor & Francis Group, 2007].

O termo IPTV é utilizado para descrever a funcionalidade e o fornecimento da qualidade de vídeo transportado sobre a rede IP. O IPTV é um serviço que permite fornecer ao utilizador uma interactividade bidireccional com a rede IP. Este serviço permite o utilizador controlar o conteúdo em tempo real (emissão em directo) através de pausas, *fast-forward* (puxar para frente) e *rewind* (puxar para trás). A natureza bidireccional do sistema IPTV também permite disponibilizar serviços como VoD (*Vídeo on Demand*) para requerer vídeos quando solicitados e NDVR (*Network Digital Vídeo Recording*) para gravar vídeos e visioná-los posteriormente. O serviço IPTV fornece um canal personalizado onde inclui apenas os programas seleccionados pelo cliente sem a perturbação dos intervalos publicitários.

Nas secções seguintes é descrita a arquitectura do serviço IPTV, as suas características, as tecnologias utilizadas, os requisitos necessários para manter a qualidade de serviço e por fim as vantagens e limitações do serviço IPTV.

**Arquitectura do Serviço IPTV**

Existem várias formas de implementar uma arquitectura IPTV. Apesar de poder haver diferenças entre arquitecturas, existem os elementos básicos que têm de existir em todas as arquitecturas. A arquitectura de rede do sistema IPTV é composta por 4 elementos: o *Vídeo Headend* (SHE) e *Vídeo Hub Office* (VHO), a rede núcleo, a rede de agregação/Acesso e a rede do subscritor, conforme ilustrado na Figura 2.3.

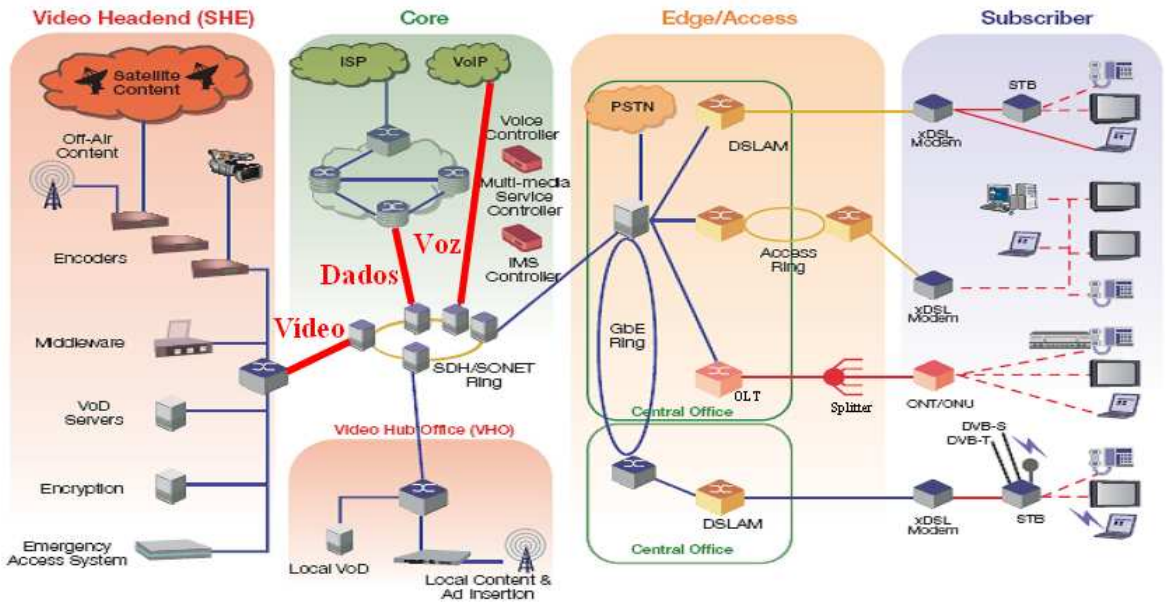



**Figura 2.3 – Arquitectura de rede do sistema IPTV [Tektronix, 2007].**

As componentes de uma rede IPTV são: o processador de vídeo, o *middleware*, os servidores de vídeo (VoD), o sistema de segurança do conteúdo CAS/DRM, os elementos e tecnologias utilizados na rede núcleo, os elementos e tecnologias utilizados na rede de agregação/acesso e o STB (*Set-Top-Box*).

O processador de vídeo é responsável pela compressão dos sinais de vídeo nos vários formatos que têm como alvo o STB do cliente. O *middleware* interliga as componentes da arquitectura do serviço IPTV e também inclui guias electrónicos de programas, o controle de aplicações, a facturação, entre outros. Os servidores VoD estão interligados aos grandes sistemas de armazenamento onde são armazenados filmes a partir do qual os utilizadores finais podem aceder e solicitar o conteúdo de vídeo pretendido. O CAS (*Condition Access System*) permite o fornecimento seguro do conteúdo e o DRM (*Digital Rights Management*) controla a utilização do subscritor do conteúdo fornecido, como por exemplo, a visita única ou a visita ilimitada durante um certo período [Tektronix, 2007]. A rede núcleo tem como tarefa dar prioridades e encaminhar o conteúdo de vídeo da melhor forma pela rede IP. A rede de agregação trata de distribuir os sinais de vídeo o mais próximo dos clientes para depois serem encaminhados na rede de acesso até ao *modem* na casa

do subscritor. Os sinais de vídeo passam do modem para o STB de onde é descodificado o formato do sinal de vídeo bem como o formato do sinal de voz para possibilitar a visualização do sinal de vídeo numa televisão.

O conteúdo de vídeo é injectado no *Vídeo Headend* (vídeo nacional) e/ou no *Vídeo Hub/Office* (vídeo local) numa variedade de formatos (comprimido e não comprimido) de uma variedade de mecanismos de transmissão, tais como satélites (estações nacionais) e transmissores terrestres (estações locais). Os dados são comprimidos através de *codecs* MPEG (*Moving Picture Experts Group*), conforme visualizado na Tabela 2.2, empacotados nos protocolos de transporte (UDP e RTP/RTCP) e enviados para a rede núcleo. A rede núcleo é utilizada para receber os serviços (Dados, VoIP e IPTV), tratar dos mesmos conforme as suas características, e encaminhá-los para a rede de agregação e depois para a rede de acesso. A rede de agregação, também denominada de rede de primeira milha, trata de distribuir o tráfego para os diferentes locais de distribuição perto dos subscritores. Por fim, o tráfego é encaminhado sobre a rede de acesso, também denominada de rede de última milha, até ao *modem* que existe na casa do subscritor.

O *modem* (modulador/demodulador) é um dispositivo electrónico que tem como funções fundamentais a modulação (através da qual os sinais digitais fornecidos pelo terminal são modificados de modo a poderem ser transmitidos pelo meio que se pretende), a transmissão (pela qual se implementam modos de compensação de distorções de amplitude e fase que tenham ocorrido, através de filtragens e eventuais igualizações) e a desmodulação (através da qual se recuperam os sinais digitais originalmente construídos). O *modem* é ligado ao dispositivo STB (*Set-Top-Box*) para ser possível a visualização do conteúdo de vídeo directamente da televisão. O STB recorre a um *buffer* para armazenar em primeiro o conteúdo a visualizar para então disponibilizar este conteúdo. O *buffer* comunica com os servidores de vídeo para verificar a existência de erros no conteúdo de vídeo provocados pela rede, de forma a melhorar a qualidade da imagem. A funcionalidade de recuperação de erros, oferecida pelos servidores de vídeo, baseia-se num mecanismo de UDP Fiável. Este mecanismo permite corrigir as falhas de entrega dos pacotes e a desordenação dos pacotes provocados pela utilização do protocolo de transporte UDP para transmitir o conteúdo de vídeo até ao utilizador final [Infante, 2008].

Os *codecs* utilizados para comprimir os sinais do serviço IPTV determinam a largura de banda a disponibilizar na rede de acesso. Os canais são fornecidos apenas quando é solicitado pelo subscritor e as mudanças de canais são efectuadas na rede e não no STB. Existem dois tipos de *codecs* de vídeo para comprimir o sinal de vídeo: o MPEG-2 [Pinnacle Systems, 2000] e o MPEG-4/H.264 [ATI Technologies, 2005], conforme se observa na Tabela 2.2. A definição do sinal de vídeo pode ser de padrão ou elevada. Da Tabela 2.2, observa-se ainda que a definição padrão requer uma largura de banda muito inferior à de alta definição. Nota-se também que o *codec* MPEG-

4/H.264 requer uma largura de banda muito inferior à do *codec* MPEG-2. Isto deve-se ao facto do *codec* MPEG-4/H.264 ter uma capacidade de compressão muito superior à do *codec* MPEG-2. Assim, a largura de banda a disponibilizar na rede de acesso é de 20 Mbps no caso de utilizar o *codec* MPEG-2 e de 10 Mbps no caso de utilizar o *codec* MPEG-4/H.264.

**Tabela 2.2 – *Codecs* do sistema IPTV e respectivas taxas de transferências [Flask, 2007].**

| *Codec* | Largura de Banda da Definição Padrão (*Standard Definition*) | Largura de Banda da Definição Elevada (*High Definition*) |
|---|---|---|
| MPEG-2 | 4-8 Mbps | 14-20 Mbps |
| MPEG-4 H.264 | 2-4 Mbps | 7-10 Mbps |

Os sinais de vídeo em *multicast* são encaminhados até ao início da rede de acesso e os sinais de vídeo em *unicast* são encaminhados na rede de acesso até ao STB do subscritor conforme é ilustrado na Figura 2.4.

Os protocolos RTP e RTCP são utilizados para controlar a qualidade da imagem do conteúdo em tempo real. O protocolo IGMP (*Internet Group Management Protocol*) é utilizado na mudança de canais de acesso para transferir os canais em *multicast*, enquanto o protocolo de sinalização RTSP (*Real Time Stream Protocol*) é utilizado para transferir os canais em *unicast.* Os canais de televisão tradicionais são transportados sobre a rede IP através do método *multicast* onde todos os utilizadores subscritos no mesmo grupo de programas recebem o mesmo sinal. O protocolo IGMP contém a informação de registo do cliente. É utilizado o método IGMP *Snooping* para encaminhar os pacotes *multicast* pela rede dentro de um domínio *broadcast.* Esta informação é analisada para criar listas de distribuição de forma a agrupar os subscritores registados com um determinado tipo de endereço *multicast*. A utilização do protocolo IGMP reduz a quantidade de largura de banda utilizada na rede e permite utilizar os recursos da rede de uma forma eficiente, uma vez que os utilizadores apenas solicitam ao encaminhador mais próximo o canal pretendido, em vez do encaminhador enviar todos os canais a todos os subscritores [O´Driscoll, 2007].

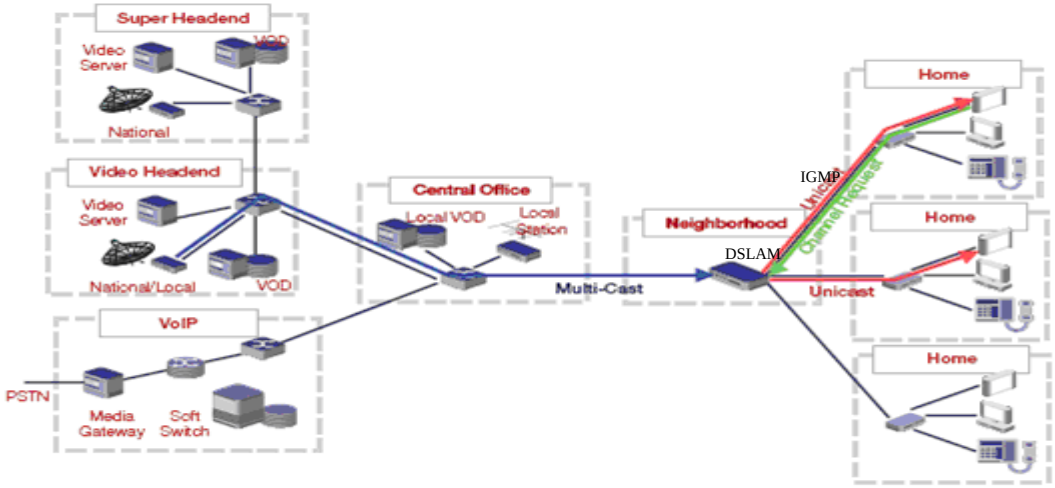



**Figura 2.4 – Cenário de Multicast/Unicast [Tektronix, 2007]**

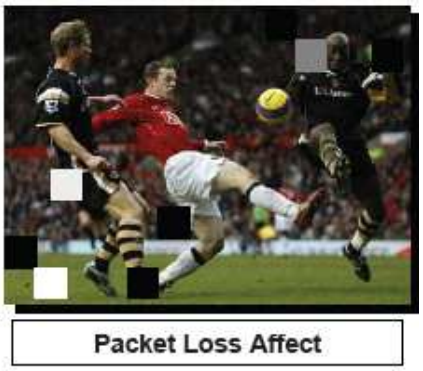
**Requisitos do Serviço IPTV**

Tal como foi referido anteriormente, a rede IP é uma rede de "Melhor Esforço" (*Best-Effort*). Estas redes são susceptíveis à perda de pacotes à medida que aumenta o atraso, a variação do atraso e a escassez da largura de banda. A perda de pacotes não tem grande impacto nos serviços de dados, pois os pacotes podem ser recebidos em tempos diferentes e por rotas diferentes. Já o vídeo é intolerante à perda de pacotes pois este factor causa um grande impacto na visualização do conteúdo. A rede utilizada para transportar os sinais de vídeo deve apresentar uma taxa de transferência conhecida e constante (no mínimo de 3 Mbps por canal) bem como um baixo atraso (menor que 150ms). A rede também deverá possuir uma baixa variação de atraso (menor que 30ms) e uma baixa taxa de perda de pacotes (menor que 1%). A taxa de transferência constante e conhecida e numa sequência correcta é esperada pelo STB, uma vez que alguns destes equipamentos não têm mecanismos para suportar erros de transmissão. O baixo atraso permite que a qualidade de experiência do subscritor e a resposta à mudança de canais não sejam afectados. A qualidade de experiência refere-se à qualidade da imagem visualizada na televisão do subscritor. A baixa variação do atraso permite que a chegada do conteúdo ao equipamento do subscritor não seja afectada e proporciona uma boa qualidade de experiência ao mesmo. A variação do atraso afecta o manuseamento dos pacotes de dados pelos elementos de rede. Quanto maior é a variação do atraso, maior é a perda de pacotes, pois as filas acumuladas nos elementos de rede não conseguem estabelecer um balanço no tráfego.

O atraso, a variação do atraso, e a escassez da largura de banda provocam a perda de pacotes e consequentemente condiciona a qualidade de experiência do subscritor, conforme mostra a Figura 2.5. A Figura 2.5 a) mostra uma linha sem imagem causada pela variação de atraso na rede. A Figura 2.5 b) mostra quadrados sem imagem causado pela perda de pacotes. A qualidade de experiência recebida pelo subscritor depende do número de erros de bloqueio de visibilidade provocados pela perda de pacotes. No caso de haver uma perda de *I-Frame* (*IntraFrame*), o impacto de bloqueio de visibilidade é muito pronunciado. O *I-Frame* é o nome dado ao conteúdo digital comprimido pelo método de compressão utilizado pelo padrão MPEG. Um *I-Frame* é um único quadro de conteúdo digital. Numa sequência de movimento os quadros individuais de *I-Frame* são agrupados e passam a ser denominados de GOP (*Group of Pictures*). Estes GOP dão ao subscritor a sensação de movimento moção espacial. O compressor examina cada um dos *I-Frame* individualmente e armazena a informação necessária para visualizar o *I-Frame* em questão. Quanto maior for o número de *I-Frame* contidas num GOP melhor é a qualidade do vídeo e, consequentemente, maior é o espaço ocupado no armazenamento. A utilização do *codec* MPEG-4 provoca um bloqueio na imagem mais significativo quando existe uma perda de *I-Frame*. Isto deve-

se ao facto de este *codec* carregar um maior número de GOP e consequentemente um maior número de informação [Tektronix, 2007].


(a)




(b)

**Figura 2.5 – Imagem de vídeo na presença de a) varição do atraso b) perda de pacotes [Gagnon, 2007].**

### Vantagens e Limitações do Serviço IPTV

O facto do serviço IPTV ser fornecido ao utilizador final através da rede IP traz muitas vantagens, pois possibilita a transferência de grandes quantidades de informação e a selecção do conteúdo solicitado. Estes factores permitem reduzir a largura de banda utilizada e optimizar a utilização dos recursos da rede. O subscritor tem o controlo total da visualização do conteúdo de vídeo, pois pode aceder, escolher, limitar e calendarizar o acesso ao conteúdo.

Uma das limitações do serviço IPTV é a perda de imagem das emissões em tempo real, que acontece quando ocorrem perdas esporádicas de pacotes de dados e atrasos na rede IP. A perda de qualidade da imagem pode ser provocada por conexões que não são suficientemente rápidas, pela distância física entre o operador e o utilizador final, pelo tipo de *codec* utilizado, por falhas ou por congestionamentos na rede.

Para que o serviço IPTV seja competitivo em relação ao serviço de televisão por cabo, há a necessidade de fornecer o sinal de vídeo em várias divisões da casa do utilizador (mais do que duas divisões). Isto só é possível caso haja uma grande largura de banda na ligação até ao subscritor.

## 2.1.4 Serviço *Triple Play*

O serviço *Triple Play* é o termo utilizado para descrever o fornecimento de três serviços ao subscritor num só pacote, nomeadamente, o serviço de dados, o serviço VoIP e o serviço IPTV. A rede *Triple Play* é uma rede convergente que serve de integração destes três serviços.

Seguem as características de uma rede *Triple Play*, a sua arquitectura, requisitos, vantagens e limitações.

**Arquitectura do Serviço *Triple Play***

A arquitectura de uma rede *Triple Play* é composta por cinco elementos [Tektronix, 2007, Cisco 1, 2008]:

- Os provedores de serviço;
- A rede núcleo*;*
- A rede de Agregação;
- A rede de Acesso, e;
- A rede do subscritor.

Os provedores de serviços (dados, voz e vídeo) injectam o seu conteúdo na rede núcleo, conforme pode ser observado na Figura 2.3. Depois, estes serviços são distribuídos para a rede de agregação e posteriormente para a rede de acesso. Por fim os serviços são distribuídos até à casa do subscritor. A partir do *modem*, que está localizado na casa do subscritor, são distribuídos os vários serviços aos seus respectivos equipamentos (computador, telefone e televisão).

Existem várias tecnologias que podem ser utilizadas na rede núcleo para o transporte dos três serviços até à rede de Agregação. De entre as várias tecnologias pode-se referir a tecnologia SDH (*Synchronous Digital Hierarchy*) [RAD 1, 2008, RAD 2, 2008] de camada 1 do modelo TCP/IP (*Transport Control Protocol / Internet Protocol*), a tecnologia *Ethernet* [IEEE 802.3, 2000**,** ChipCenter-QuestLink 1, 2002] de camada 2 do modelo TCP/IP, e a tecnologia MPLS (*Multiprotocol Label Switching*) [RFC 3031, 2001] de camada 2.5 (entre a camada 2 e a camada 3) do modelo TCP/IP. O elemento de rede que interliga a rede núcleo e a rede de Agregação é denominado de MSPP (*MultiService Provisioning Platform*).

A tecnologia mais utilizada na rede de Agregação é denominada de *Metro Ethernet* [IEEE 802.3, 2000**,** ChipCenter-QuestLink 1, 2002] com taxas de transmissão de 1 Gbps. Esta tecnologia é de camada 2 do modelo TCP/IP.

A rede de Acesso permite transportar os vários sinais até ao *modem* localizado na casa do cliente. As várias tecnologias e/ou infraestruturas que podem ser utilizadas nesta rede incluem as tecnologias xDSL (variantes da *Digital Subscriber Line*) [Nunes, 2006], as redes ópticas passivas xPON (variantes das redes *Passive Óptical Network*) [Allied Telesyn, 2004] e as redes ópticas FTTx (variantes da *Fiber To The x*) [Poe, 2005]. Caso a tecnologia utilizada para a interligação da rede de Agregação com a rede de Acesso seja a tecnologia xDSL, o elemento de interligação das redes denomina-se DSLAM (*Digital Subscriber Line Access Multiplexer*). No caso de se recorrer à infraestrutura de rede óptica passiva, o elemento de interligação entre as duas redes é chamado de OLT (*Óptical Line Terminal*).

No caso de ser utilizada a tecnologia xDSL, a rede do subscritor inclui um *modem* e um STB. O *modem* serve de interligação entre a rede de acesso e a rede do subscritor e é ligado directamente ao STB. O STB é ligado ao telefone VoIP e à televisão enquanto que o modem é ligado ao computador pessoal.

Caso a infraestrutura utilizada seja de redes ópticas passivas o dispositivo que interliga a rede de Acesso à rede de subscritor é denominado de ONU (*Óptical Network Unit*). Este ONU vai se ligar directamente aos equipamentos que permitem usufruir do serviço *Triple Play.*

Desde a rede núcleo até à rede do subscritor, cada serviço é transportado numa VLAN (*Virtual Local Area Network*) individual pela rede IP, conforme ilustra a Figura 2.6. Geralmente, são atribuídas prioridades aos diferentes serviços. A prioridade mais elevada é atribuída ao serviço de vídeo e a prioridade menor ao serviço de dados. A atribuição de prioridades permite encaminhar o conteúdo de forma a optimizar a utilização dos recursos da rede IP e de garantir QoS.

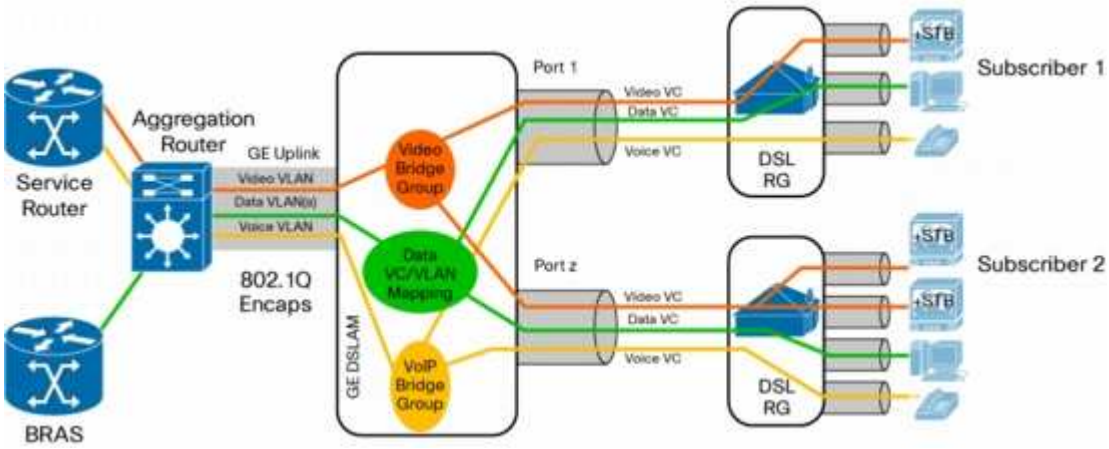



**Figura 2.6 – VLAN dos vários serviços nas redes de Agregação, de Acesso e de subscritor [Cisco 1, 2008].**

### Requisitos do Serviço *Triple Play*

Os requisitos da rede que suporta o serviço *Triple Play* abrangem os requisitos da QoS proporcionados pelas tecnologias e infraestruturas utilizadas na rede núcleo, na rede de Agregação, na rede de Acesso e na rede do subscritor.

A QoS é mantida quando os valores mínimos dos seus requisitos não são ultrapassados. Tal como referido anteriormente, os requisitos da QoS incluem a largura de banda, a perda de pacotes e os atrasos e variações dos atrasos existentes na rede IP.

Sabe-se que o serviço *Triple Play* fornece ao subscritor três tipos de serviços e que cada um destes serviços tem os seus próprios requisitos mínimos. Quando estes requisitos mínimos são atingidos, o serviço fornecido é de boa qualidade.

Os requisitos de QoS que os três serviços têm em comum são a necessidade de possuírem uma baixa perda de pacotes e a necessidade da disponibilidade de elevadas larguras de banda na

rede IP. Os serviços VoIP e IPTV requerem, para além dos requisitos referidos acima, a baixa variação de atrasos bem como baixos atrasos de forma a conseguirem fornecer os respectivos serviços com boa qualidade. Na Tabela 2.3 é apresentado um resumo dos valores mínimos dos requisitos de QoS requeridos por cada serviço. Analisando a tabela verifica-se que o serviço IPTV é o serviço mais exigente em termos de requisitos na rede IP. É de destacar ainda que o serviço IPTV requer a maior disponibilidade de largura de banda e a menor perda de pacotes na rede.

**Tabela 2.3 – Requisitos de cada serviço que pertence ao serviço *Triple Play*.**

| | Dados | VoIP | IPTV |
|---|---|---|---|
| **Largura de banda** | Ordem dos Kbps no mínimo | 64 Kbps constante no mínimo | 3 Mbps constantes no mínimo |
| **Tolerância à perda de pacotes** | Tolera uma perda de pacotes menor que 3% | Tolera uma perda de pacotes menor que 3% | Tolera uma perda de pacotes menor que 1% |
| **Tolerância a Atrasos** | Insensível | <150 ms | <150 ms |
| **Tolerância a variações de atrasos** | Insensível | <50 ms | <30 ms |
| **Considerações chave das redes** | Fiabilidade na rede sem perda de pacotes. | QoS (respeitar os mínimos);<br>Emissão em tempo real. | QoS (respeitar os mínimos);<br>Emissão em tempo real;<br>Fiabilidade;<br>Multicast e Unicast;<br>Desempenho elevado. |

Os serviços que constituem o serviço *Triple Play* estão dependentes de várias tecnologias, protocolos de telecomunicações, equipamentos e meios de transmissão de forma a conseguirem alcançar o seu destino. Consequentemente, pode-se concluir que a má qualidade do serviço pode ser provocada por uma variedade de factores. Em cada segmento da rede *Triple Play* existe uma série de factores a ter em consideração de forma a manter a QoS de cada serviço na rede IP, conforme ilustrado na Figura 2.7.

Posto isto, os factores a verificar na rede dos provedores de serviço são [Caballero, 2007]:

- A continuidade da conexão IP;
- A disponibilidade do serviço;
- As prioridades dadas ao tráfego de cada um dos serviços, e;
- O desempenho.

Na rede núcleo devem ser verificadas as perdas de pacotes, os atrasos, a gestão da QoS, o encaminhamento dos serviços, a resiliência a falhas, a congestão, a optimização da utilização dos recursos, a capacidade de restauro, implementação da engenharia de tráfego, a infraestrutura núcleo e o envio *multicast* do conteúdo.

Na rede de Acesso é de verificar as falhas existentes no meio de transmissão (cobre, coaxial ou fibra óptica), as expectativas das taxas de transmissão, a segurança e privacidade do conteúdo, o desempenho dos equipamentos de rede (DSLAM ou OLT) e o envio *unicast* do conteúdo.

Finalmente na rede do subscritor devem ser verificadas as configurações dos equipamentos (*modem*, STB ou ONU), a cablagem, o *hardware* e *software* auxiliar aos serviços, a qualidade de voz e de vídeo e o desempenho da transferência dos dados.

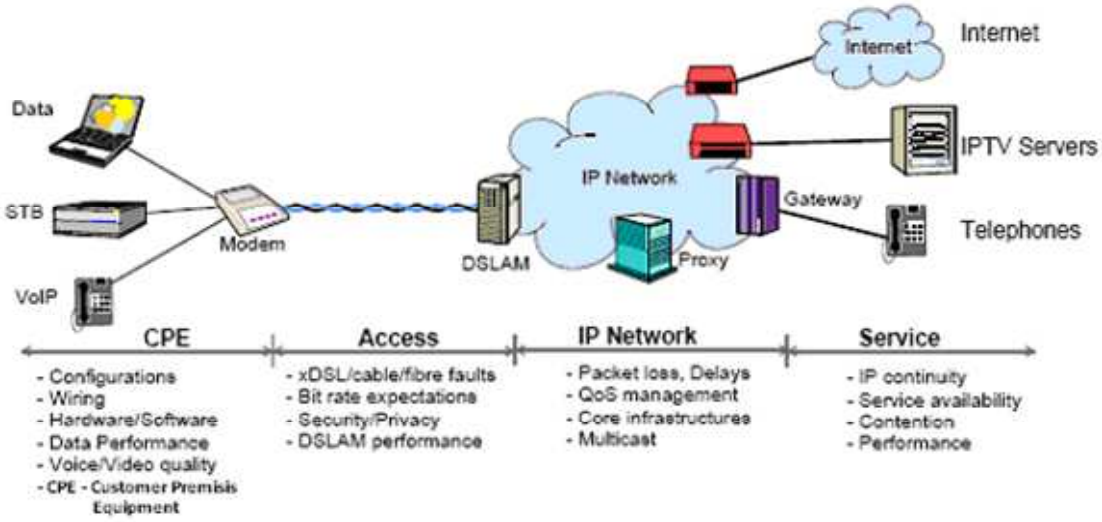



**Figura 2.7 – Factores em cada secção da rede *Triple Play* [Caballero, 2007].**

### Vantagens e Limitações do Serviço *Triple Play*

As vantagens que este tipo de tecnologia, baseada no IP, proporciona são várias. A principal vantagem consiste na variedade de serviços que podem ser integrados, entre os quais, a televisão (vários canais transmitidos em directo), personalização de multimédia (música, filmes, jogos), VoIP entre outros, através da ligação de internet (xDSL por exemplo). A integração destes serviços proporciona uma redução do custo da infraestrutura da rede convergente e dos custos dos serviços fornecidos ao subscritor. Os provedores de serviços que proporcionam o serviço *Triple Play* conseguem reduzir os custos dos serviços quando estes são fornecidos aos subscritores em pacotes em que são incluídos os três serviços (dados, voz e vídeo).

A desvantagem do serviço *Triple Play* consiste essencialmente no grande desafio de fornecer aos subscritores todos os serviços com uma QoS elevada. Disponibilidade de largura de banda elevada na rede IP elimina muitos dos problemas de congestionamento da rede e qualidade de experiência.

## 2.2 REDES DE ACESSO

Nesta secção é dado a conhecer as principais tecnologias e infraestruturas existentes em redes de acesso e em redes de agregação. As várias tecnologias incluem as variantes da tecnologia DSL (*Digital Subscriber Line*), as variantes das redes ópticas FTTx (*Fiber To The x*) e as várias infraestruturas das redes ópticas PON (*Passive Optical Network*). Descreve-se a seguir, o seu funcionamento, as suas arquitecturas, as suas características, as suas vantagens e limitações. Salienta-se que tem-se como objectivo analisar as várias tecnologias e infraestruturas de forma a suportar os requisitos do serviço *Triple Play.*

### 2.2.1 Redes de Acesso em cobre

O DSL (*Digital Subscriber Line*) é uma tecnologia da rede de acesso que fornece um meio de transmissão digital de dados até às residências onde aproveita a rede de telecomunicações em cobre existente [Nunes, 2006].

Existem vários tipos de DSL nomeadamente o ADSL (*Asymmetrical DSL*), o ADSL2 (*Asymmetrical DSL* 2), o ADSL2+ (*Asymmetrical DSL* 2+), o VDSL (*Very High bit rate* DSL) e o VDSL2 (*Very High bit rate* DSL - 2) [Nunes, 2006]. Estes diferem principalmente nos aspectos de velocidade (taxa de transferência), de codificação de linha, de número de linhas (1 par entrançado ou 2 pares entrançados) e de alcance. Os tipos de DSL são classificados como assimétricos quando as taxas no sentido descendente (da rede para o utilizador) e no sentido ascendente (do utilizador para a rede) são diferentes, e simétricos quando estas mesmas taxas são iguais.

O ADSL (*Asymmetrical DSL*), recomendação da ITU (*Recommendation* G.992.1), em que oferece taxas diferentes no sentido descendente e no sentido ascendente. As taxas de transferência no sentido descendente podem atingir os 8 Mbps e as taxas de transferência no sentido ascendente podem atingir os 1 Mbps. Esta tecnologia tem uma taxa de transferência suficiente para aceder à Internet e para suportar as aplicações em tempo real que necessitam de elevadas taxas de transferência no sentido descendente.

O ADSL2 (*Asymmetrical DSL2*), recomendação da ITU (*Recommendation* G.992.3) em 2002, fornece melhorias em relação ao ADSL no diagnóstico de linha, na gestão de energia, na reconfiguração *on-line,* na redução de energia e na redução de tramas. Tem uma taxa de transferência de 12 Mbps no sentido descendente e de 1,1 Mbps no sentido ascendente.

O ADSL2+ (*Asymmetrical DSL2+*), recomendação da ITU (*Recommendation* G.992.5) em 2004, tem uma taxa de transferência no sentido descendente de 24 Mbps e uma taxa de transferência no sentido ascendente de 2,2 Mbps em distâncias pequenas.

O VDSL, recomendação da ITU (*Recommendation* G.993.1) em 2004, surgiu para poder suportar os novos serviços em tempo real. O padrão VDSL oferece uma taxa de transferência no sentido descendente (*download*) de 52 Mbps e no sentido ascendente (*upload*) uma taxa de transferência de 2 Mbps em distâncias de 900m.

O VDSL2, recomendação da ITU (*Recommendation* G.993.2) em 2005, com transmissão simétrica máxima de 100 Mbps em *loops* (sinal enviado e recebido de volta para testar o correcto funcionamento do equipamento) máximos de 300 metros (utilizando uma banda de 30 MHz), transmissão simétrica de 10-30 Mbps em *loops* com uma distância intermediária (utilizando a banda de 12 MHz) e operação assimétrica com taxa no sentido descendente de 10-30 Mbps em *loops* de 1

a 3 km (utilizando uma banda de 8,5 MHz). O VDSL2 inclui a maioria das facilidades do ADSL2 e o seu desempenho é melhor do que a do VDSL [Nunes, 2006].

A qualidade de serviço é fundamental para a transferência contínua do conteúdo de vídeo e de áudio. O VDSL2 define um mecanismo que atribui elevadas prioridades ao conteúdo de vídeo e de áudio em contraste com as baixas prioridades atribuídas ao conteúdo de dados como o correio electrónico e páginas Web. Numa conexão de 100 Mbps não existe interferências de atraso entre os pacotes de voz de alta prioridade e os pacotes de dados de baixa prioridade. Ao contrário, numa ligação de velocidade de 1 Mbps, o atraso torna-se num factor capaz de provocar a variação de atraso no pacote de transferência da voz. O VDSL2 pára a transferência do conteúdo de pacotes com prioridade baixa até a missão da voz se completar [Wimoesterer, 2006].

A Tabela 2.4 mostra um resumo das características das variantes da tecnologia DSL tais como a taxa de transferência no sentido ascendente como descendente, a distância entre a residência e o comutador e a recomendação da ITU.

**Tabela 2.4 – Tabela Comparativa das Variantes da Tecnologia DSL [Nunes, 2006].**

| | ADSL | ADSL2 | ADSL2+ | VDSL | VDSL2 |
|---|---|---|---|---|---|
| Taxa de transferência dos dados no sentido descendente | Até 8 Mbps | Até 12 Mbps | Até 24 Mbps | Até 52 Mbps | Até 100 Mbps |
| Taxa de transferência dos dados no sentido ascendente | Até 1 Mbps | Até 1,1 Mbps | Até 2,2 Mbps | Até 2 Mbps | Até 100 Mbps |
| Distância entre a residência e o comutador | Até 5,5 km | Até 3,7 km | Até 2,7 km | Até 900 m | Até 500 m |
| Padrões ITU | G.992.1 | G.992.3 | G.992.5 | G.993.1 | G.993.2 |

A Figura 2.8 mostra a comparação de largura de banda entre as tecnologias DSL em função do comprimento do *loop*. Observa-se que quanto maior for a taxa de transferência da tecnologia menor é o comprimento do seu *loop*. Desta forma as residências que se encontram mais perto do comutador têm a possibilidade de visualizar um maior número de canais de televisão, por exemplo, em simultâneo do que as residências que se encontram mais afastadas do comutador.

O dispositivo que interliga a rede núcleo à rede de acesso é denominado DSLAM (*Digital Subscriber Line Access Multiplexer*) permite as linhas telefónicas fazerem conexões rápidas à Internet. O DSLAM é um dispositivo que suporta o serviço DSL e separa os sinais telefónicos dos sinais de dados através de técnicas de multiplexagem. Quanto mais afastado estiver o DSLAM menor é a taxa de transferência na residência, especialmente quando ultrapassa os 1,6 km de distância [Wikipedia 4, 2008].

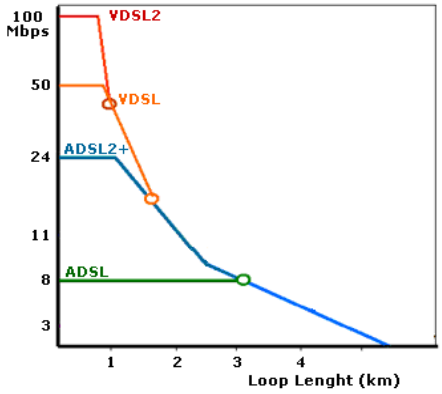



**Figura 2.8 – Taxa de Transferência em relação ao comprimento do *loop* [Foigel, 2007].**

As tecnologias DSL oferecem várias vantagens na comunicação de banda larga. A vantagem mais importante é o preço dado que o DSL é oferecido através da rede de cobre. Uma outra vantagem é que o tráfego de dados é transmitido simultaneamente com o tráfego de voz, enquanto o tráfego de dados é direccionado a uma rede de pacotes a voz é direccionada à rede PSTN (*Public Switched Telephone Network*).

### 2.2.2 Redes de Acesso em Fibra óptica

A rede de acesso é a parte da rede entre o utilizador e o ponto de interligação com a rede núcleo ou rede principal.

O factor de atracção em torno das redes de acesso de fibra óptica é a possibilidade de fornecer o serviço *Triple Play* com elevadas condições de qualidade de serviço, uma vez que a fibra óptica é o meio de transmissão que apresenta a maior taxa de transferência de dados e o menor tempo de atraso e variação de atraso dos pacotes na rede. O *Triple Play* é uma oportunidade de negócio crescente que não é apenas direccionado para as residências mas também para os negócios em prédios comerciais e locais de formação. A tendência dos provedores de serviço *Triple Play* é analisar a melhor maneira de aproximar a fibra óptica o mais perto do utilizador. A fibra óptica visa fornecer para além do *Triple Play* os serviços de ensino à distância, jogos interactivos e telemedicina.

A implementação da fibra óptica está fortemente relacionada com o débito efectivo da largura de banda de cada arquitectura definida e consequentemente à potencialidade de rentabilidade do serviço para o operador. Para a utilização da fibra óptica, o operador deve considerar que as exigências da largura de banda por parte dos utilizadores estão sempre a crescer. Os elementos que constituem a rede de acesso são o nó de acesso, a rede distribuição e o elemento terminal da rede de distribuição, conforme mostra a Figura 2.9. O nó de acesso é o elemento de rede responsável pela conexão entre a rede de acesso e a rede núcleo ou principal. A função do nó de

acesso é converter as velocidades de transferência de dados à conversão de protocolos. A rede de distribuição pode ser constituída por uma combinação de meios de transmissão ou por um único meio de transmissão. Os meios de transmissão podem ser de cobre ou de fibra óptica. O elemento terminal da rede de distribuição é o ponto de separação entre o domínio público e o domínio privado (residência). Este elemento pode ser passivo apenas com funções de conexão ou activo com funções de conversão de sinais e de protocolos.

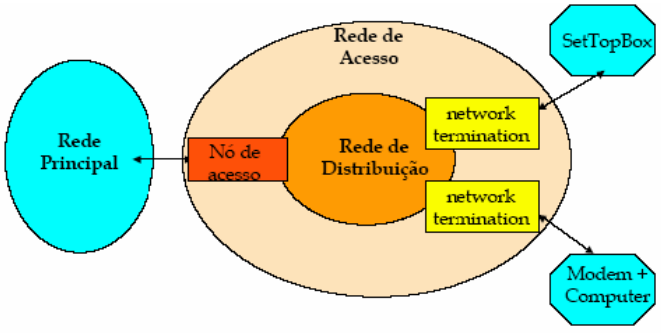



**Figura 2.9 – Elementos da Rede de Acesso.**

Como fora dito anteriormente, a rede de distribuição pode ser de cobre, de fibra óptica ou uma combinação destes dois. A arquitectura dos cabos de fibra óptica é classificada com base no local onde termina a ligação do cabo de fibra óptica. As classificações mais utilizadas são o FTTH (*Fiber To The* ), o FTTB (*Fiber To The* ), o FTTC (*Fiber To The* ) e o FTTN (*Fiber To The Node*) [FlexLight Networks, 2004]. No caso da ligação de fibra óptica terminar na residência do subscritor a distribuição da fibra óptica é classificada de FTTH, conforme mostra a Figura 2.10 a). No caso do FTTB, a ligação da fibra óptica termina no prédio e depois a ligação dentro do prédio até aos utilizadores finais é efectuado através do meio de transmissão de cobre, conforme mostra a Figura 2.10 b). A ligação da fibra óptica que vai até ao armário de distribuição perto de uma habitação é classificada como FTTC, conforme mostra a Figura 2.10 c). Por fim, a classificação da ligação da fibra óptica FTTN termina no nó que interliga a rede núcleo à rede de acesso onde a ligação de última milha até à residência do subscritor é em cobre, conforme mostra a Figura 2.10 d).

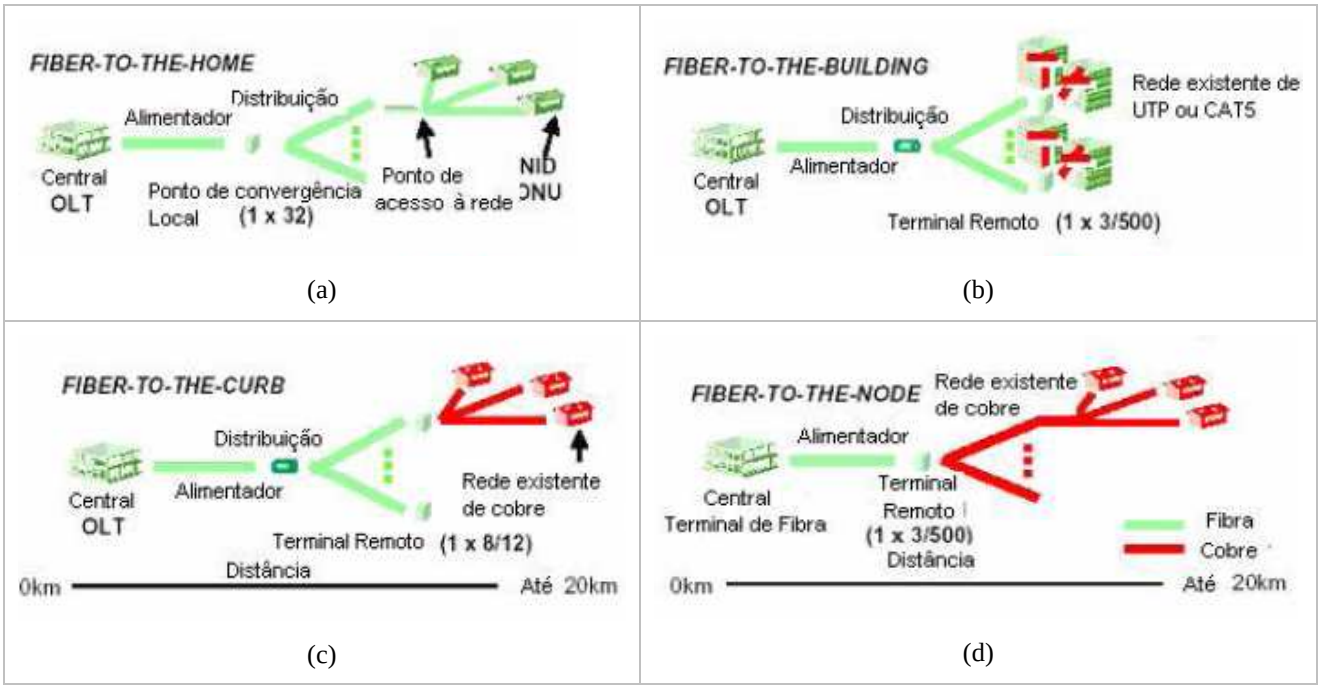



**Figura 2.10 – Classificações a) FTTH, b) FTTB, c) FTTC e d) FTTN.**

A rede FTTH permite reduzir os custos da rede de núcleo, nas operações da rede de acesso e no serviço ao cliente. A fiabilidade da rede aumenta com o fluxo constante proporcionada pela distribuição da fibra óptica FTTH [Poe, 2005]. Este tipo de rede é livre do cobre e fornece taxas de transferência entre os 30 Mbps e o 100 Mbps adequadas para suportar os serviços que necessitam de taxas de transferência elevadas.

As redes FTTH podem ser implementadas de duas formas, em ligações PTP (*Point To Point*) ou ponto-a-ponto e em ligações efectuadas através de redes PON (*Passive Optical Networks*). Nas ligações PTP a fibra é dedicada a cada utilizador na rede de acesso e nas ligações PON a fibra óptica é partilhada entre um número específico de utilizadores (16 e 32 utilizadores) através da utilização de um divisor de potência (*splitter*).

O FTTB utiliza tipicamente a arquitectura PTP e fornece uma fibra óptica dedicada a cada edifício ou bloco de edifícios. A fibra óptica termina num terminal remoto (dispositivo activo), que requer potência e segurança no armário de distribuição. Se o edifício for equipado com cabo CAT5 a cada unidade da moradia, significa que existe uma rede local de Ethernet e é fornecida uma largura de banda partilhada entre os 10 Mbps e os 100 Mbps. Se apenas o par entrançado estiver disponível, o terminal remoto é ligado ao utilizador final através de uma linha digital multiplexada e ao elemento de rede de acesso através da fibra óptica.

As redes FTTC levam a fibra óptica até 305 m do utilizador final com a terminação num terminal remoto a servir entre oito a doze utilizadores.

As redes FTTN são muito parecidas às redes FTTC quanto à arquitectura. No entanto, nas redes FTTN, o terminal remoto é posicionado acima dos 1524 m dos utilizadores finais e servem

entre três a 500 utilizadores. Ambas as redes utilizam um par entrançado para conectar ao utilizador final. A escolha do tipo de tecnologia DSL a utilizar nas redes é baseada no comprimento do par entrançado de cobre e na largura de banda pretendida para suportar certos serviços. Tanto o ADSL2 quanto o ADSL2+ funcionam melhor com maiores comprimentos de par entrançado e são predominantemente utilizados nas redes FTTN. Os sinais transferidos sobre o cobre degradam significativamente em longas distâncias, afectando directamente a potencialidade da largura de banda.

**Redes Ópticas**

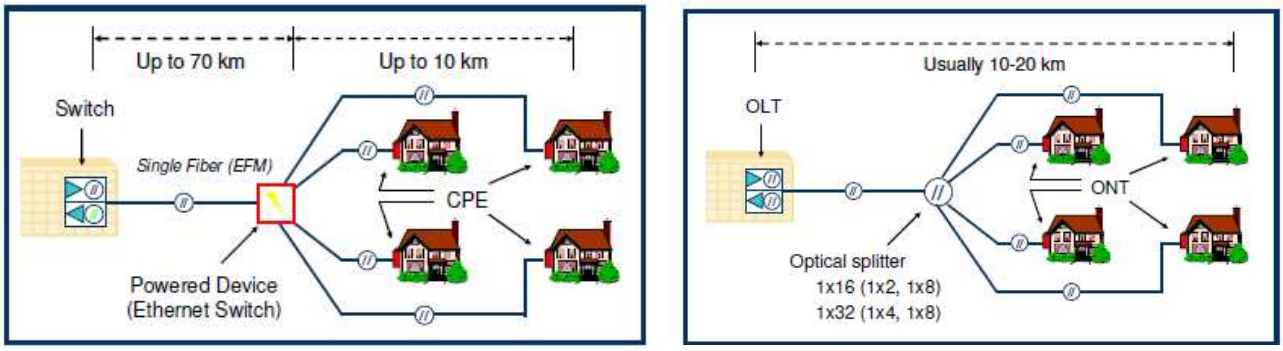
Existem dois tipos de arquitecturas de redes de fibra óptica nomeadamente a arquitectura AON (*Active Optical Network*) e a arquitectura PON (*Passive Optical Network*).

A arquitectura AON apresenta uma topologia ponto-a-ponto onde a cada utilizador final é ligada a uma fibra óptica com largura de banda bidireccional dedicada. Desta forma, o cliente pode ter uma largura de banda que pode atingir 1 Gbps. Na AON são utilizados comutadores, encaminhadores ou multiplexadores ou equipamentos de conversão de sinais e de protocolos. Esta é uma solução cara em que a agregação é efectuada através da tecnologia Ethernet de baixo custo. A AON tem um alcance com o limite de 80 km independentemente do número de clientes que estão a ser servidos, conforme mostra a Figura 2.11 a). O número limite de clientes imposto deve-se aos comutadores instalados e não à infraestrutura como acontece no PON: A arquitectura AON facilita a adição de novos clientes à rede e é uma solução que suporta a tecnologia *Gigabit* Ethernet.

A arquitectura PON utiliza divisores e acopladores para dividir a largura de banda entre os utilizadores. A largura de banda é dividida tipicamente entre 32 utilizadores sobre uma distância máxima de 10 a 20km, conforme mostra a Figura 2.11 b). Como a rede é partilhada, a conexão PON é ponto-a-multiponto e a adição de novos utilizadores é complexa.

A rede PON é formada por equipamentos passivos como o OLT (*Optical Line Terminal*) localizados junto à rede núcleo, os divisores ópticos nos armários de distribuição e os ONT (*Optical Network Terminal*) localizados na casa dos utilizadores finais. Os equipamentos passivos não necessitam de electricidade para funcionar, mas dividem a largura de banda pelos utilizadores através de divisores ópticos (*splitters*). Estes equipamentos reduzem o custo de investimento e o custo operacional, uma vez que os equipamentos são baratos e não utilizam electricidade. Como a largura de banda é dividida, o número de cabo é reduzido, o tamanho dos armários é reduzido e o manuseamento dos equipamentos é facilitado. Por vezes são utilizados equipamentos activos (ONU (*Optical Network Units*)) no sistema PON para interligar o meio óptico ao meio de cobre. O ONU é utilizado quando é reaproveitado o cobre até à casa do utilizador final para transportar o tráfego e é localizado nos armários de distribuição perto das casas dos utilizadores finais. Numa rede PON o

cliente não pode estar mais do que 20 km afastado do CO (*Central Office*) onde está localizado o OLT.

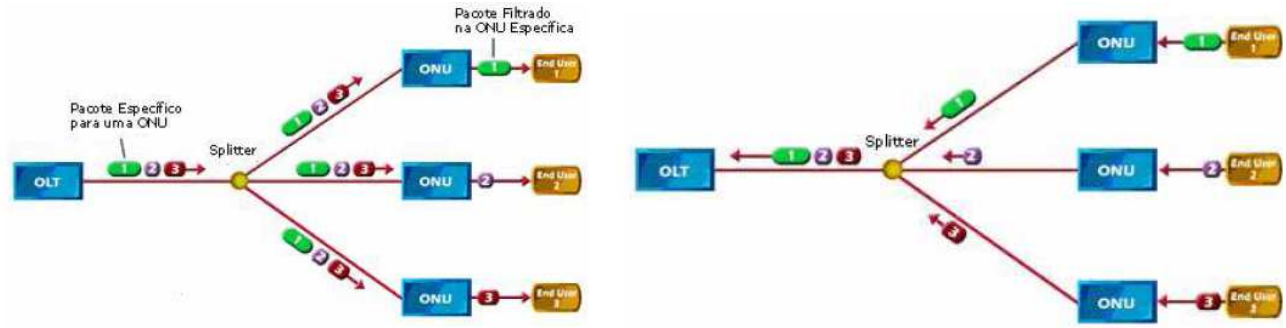



(a) (b)

**Figura 2.11 – Arquitectura a) AON b) PON [Allied Telesyn, 2004].**

O OLT fornece os serviços ao utilizador, controla a qualidade de serviço (QoS) e controla o SLA (*Service-Level Agreement*). O SLA é um contracto informal entre o provedor de serviços e o cliente onde são definidos os termos de responsabilidade do portador ao cliente e o tipo de extensão de remuneração no caso do não comprimento das responsabilidades. O OLT também trata da multiplexagem dos vários utilizadores.

A ONU é o equipamento utilizado para converter o sinal óptico num sinal eléctrico e encaminhá-lo até ao equipamento do utilizador final, conforme mostra a Figura 2.12.



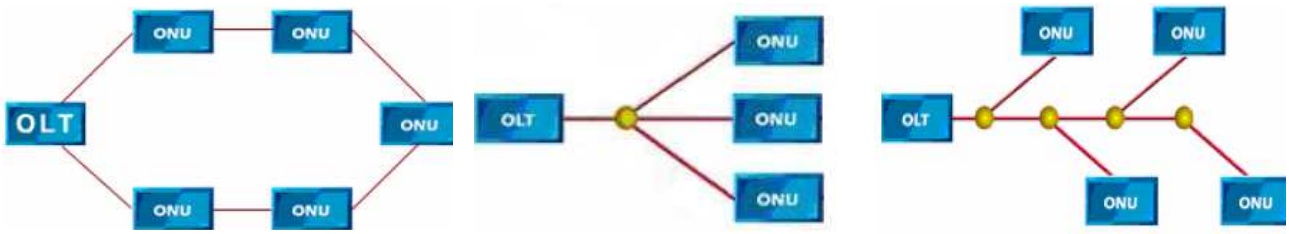

(a) (b)

**Figura 2.12 – Funções do equipamento a) OLT e b) ONU**

O sinal óptico da fibra óptica é enviado a um ou mais divisores de potência passivos, e depois retransmitido para os vários equipamentos ONU. Cada ONU recebe e transmite sinais num canal próprio com a largura de banda dinamicamente alojada com QoS e SLA individuais. Os sinais transmitidos e recebidos operam com comprimentos de onda diferentes permitindo a operação ocorrer numa única fibra. A OLT avalia os QoS e SLA bem como a disponibilidade do segmento PON. Posteriormente, o alojamento dinâmico é aplicado. Este processo fornece uma taxa de transmissão entre 1 Mbps e 10 Gbps aos utilizadores.

A tecnologia PON apresenta algumas vantagens tais como o baixo custo devido a inexistência de elementos activos (economia de energia, de espaço e manutenção), a partilha da capacidade da fibra óptica e a demanda dos utilizadores por elevadas larguras de banda é superada. A utilização da fibra óptica é flexível e óptima devido ao alojamento dinâmico da banda larga e por fim as redes PON são capazes de fornecer uma diversidade de serviços aos utilizadores finais incluindo o serviço *Triple Play.*

Entre as opções de topologias utilizadas na PON, tem-se o anel, a árvore e a barramento, conforme mostra Figura 2.13.




(a) (b) (c)

**Figura 2.13 – Topologias em a) anel, b) árvore e c) barramento**

Uma PON típica é composta por uma variedade de topologias de acordo com a estratégia de implementação e com a grande flexibilidade da arquitectura.

Existem vários padrões da tecnologia PON. Actualmente, entre os mais utilizados estão o PON/GEPON (Ethernet PON/Gigabit Ethernet PON) [IEC a, 2007] e o GPON (Gigabit PON) [FlexLight Networks, 2004]. A tecnologia Ethernet para os subscritores da rede de acesso, também referido como “Ethernet na última milha”, pode ser utilizada nas redes de par de cobre ou nas redes de fibra óptica. O conceito de EPON utiliza a Ethernet em fibra óptica numa conexão ponto-a-multiponto através de divisores ópticos passivos. O mecanismo OAM (*Operation, Administration and Maintenance*) facilita a operação da rede e também facilita as operações de recuperação de falhas de rede, no entanto o mesmo é limitado. A EPON tem uma baixa eficiência e não tem a capacidade de suportar qualquer serviço senão a Ethernet sobre o PON. Isto introduz factores negativos relativamente ao fornecimento de qualidade de serviço aos serviços de vídeo e de voz. A EPON favorece o provedor de serviços mais do que o cliente.

A GPON permite taxas de transferências elevadas e maior eficiência ao carregar múltiplos serviços sobre a PON. A estrutura da trama é escalável, 622Mbps até 2,5Gbps, e suporta taxas de transferência assimétricas. A relação utilização/eficiência é elevada para qualquer tipo de serviço. O método de encapsulação utilizado em qualquer tipo de serviço é a encapsulação em tramas periódicas de 125 µs. Elevada eficiência sem o cabeçalho de transporte. Permite a alocação

dinâmica da largura de banda *upstream* através dos apontadores de largura de banda para cada ONT/ONU.

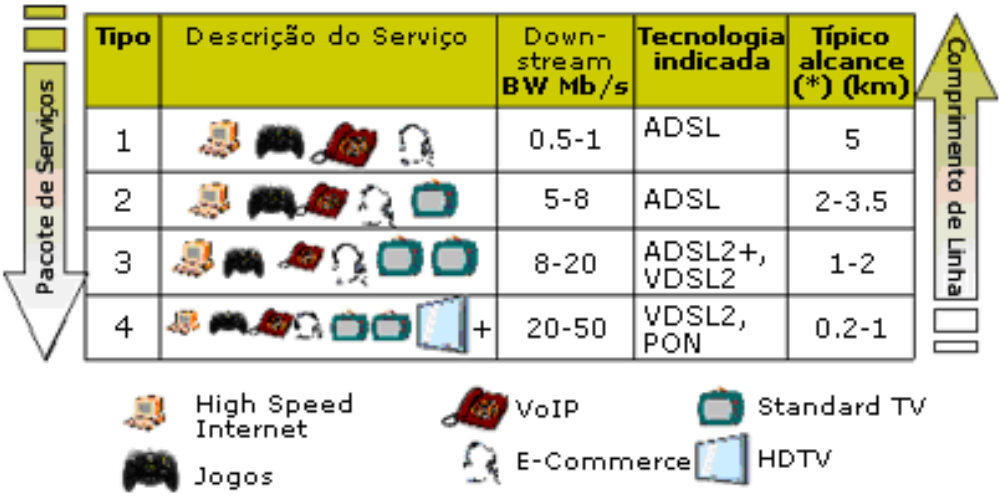
Comparando o EPON (1 Gbps) e o GPON (1,2 Gbps), este último é o protocolo PON mais avançado e oferece o suporte de múltiplos serviços com o maior número de conjuntos de factores de OAM. A eficiência é o factor que determina o custo do sistema. Uma rede com eficiência de 100% fornece um débito efectivo de 1,2 Gbps, enquanto uma rede de 50% de eficiência fornece um débito efectivo de 622 Mbps. Para produzir o 1,2 Gbps numa rede de eficiência de 50% são necessários dois equipamentos e consequentemente o aumento do custo do sistema. Quanto maior a eficiência do equipamento maior é o rendimento de receita por bit (diminui o tempo do retorno do investimento) e mais barato é o sistema de equipamentos. Segundo [FlexLight Networks, 2004] a eficiência da EPON é de 49% e a eficiência da GPON é de 93%. Isto mostra uma grande diferença entre a tecnologia EPON e a tecnologia GPON. Esta última tecnologia assegura a simplicidade e escalabilidade quando se trata de novos serviços. É fornecido um caminho de uma migração clara aos serviços novos sem qualquer disrupção ao equipamento GPON existente e sem quaisquer alterações à camada de transporte [FlexLight Networks, 2004].

### 2.2.3 Comparações entre as Redes de Acesso

As redes de acesso em cobre apresentam limites de largura de banda e atrasos em comparação com as redes de acesso em fibra óptica. A solução óptima é a implementação de redes em fibra óptica em toda rede de acesso. No entanto, o seu custo elevado condiciona a sua implementação. A alternativa é utilizar o cobre da rede de acesso existente para transferir os dados a taxas de transferência de 100 Mbps através da tecnologia VDSL2. Esta solução tem um custo reduzido em comparação com a rede de acesso em fibra óptica. A única limitação desta tecnologia é o reduzido comprimento do segmento entre o dispositivo de rede VDSL2 e o utilizador final. Quanto mais afastado estiver o utilizador final do dispositivo de rede VDSL2 menor é a sua taxa de transferência.

A Tabela 2.5 representa uma correlação entre os serviços *Triple Play* e as tecnologias da rede de acesso. Sabe-se que quanto maior é o comprimento do segmento de cobre menor é a sua taxa de transferência. Verifica-se que com a utilização do ADSL2+ ou VDSL2 é permitido haver pelo menos dois canais de qualidade normal a correr em simultâneo. Observa-se também que as soluções VDSL2 e PON são as mais adequadas para suportar o serviço de televisão de alta definição e ainda dois canais de televisão de qualidade normal.

**Tabela 2.5 – Correlação entre os serviços *Triple Play* e as tecnologias da rede de acesso [Foigel, 2008].**




A Figura 2.14 mostra um gráfico que indica que as redes PON oferecem o maior número de canais de alta definição em simultâneo em comparação com a tecnologia VDSL2. Observa-se também que quando é utilizado o método de compressão MPEG-4 o número de canais aumenta em comparação com o método de compressão MPEG-2. Posto isto, as redes de fibra óptica correspondem a uma solução óptima em comparação com as redes em cobre.

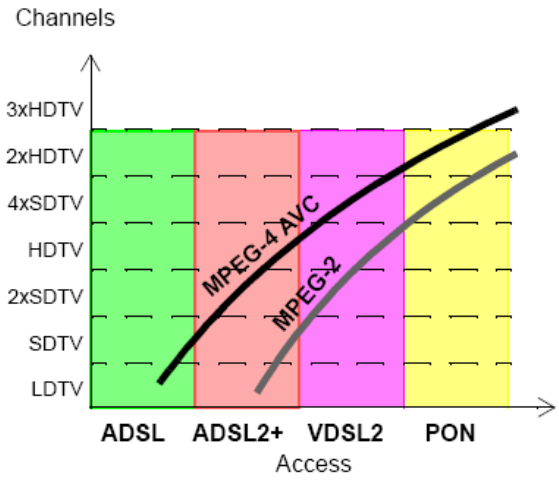



**Figura 2.14 – Relação entre a tecnologia da rede de acesso e o número de canais a visualizar [Caballero 1, 2007]**

A Figura 2.15 mostra a localização dos dispositivos das várias tecnologias da rede de acesso e suas distâncias do utilizador final. Observa-se que a fibra óptica permite ter os dispositivos de rede, o mais afastado do utilizador final sem provocar atrasos. De todas as tecnologias da rede de acesso em cobre o VDSL2 deve estar o mais próximo do utilizador final para fornecer elevadas larguras de banda e reduzir os atrasos.

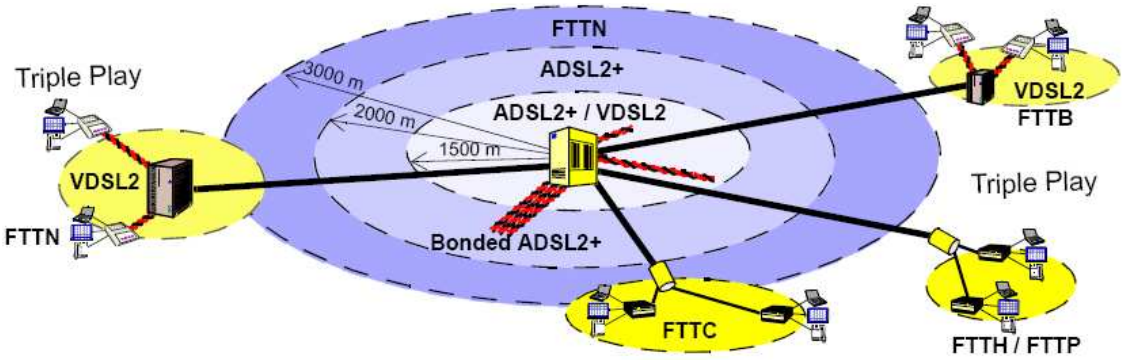



**Figura 2.15 – As diferentes tecnologias da rede de acesso e suas distâncias do utilizador final [Caballero 1, 2007]**

A Tabela 2.6 mostra uma comparação entre as características das várias tecnologias da rede de acesso. De todas as tecnologias DSL, a tecnologia VDSL2 apresenta as melhores taxas de transmissão. Esta tecnologia é utilizada na ligação entre o equipamento da rede de acesso e o equipamento do cliente. Para aumentar a taxa de transferência nesta ligação é necessário colocar o equipamento da rede de acesso perto do equipamento do cliente. Isto é uma desvantagem, uma vez que implica um custo para colocar os equipamentos da rede de acesso perto dos clientes. Quanto mais afastado estiver o cliente do equipamento de rede de acesso menor é a taxa de transferência. Posto isto, é muito raro o cliente receber 100 Mbps através da tecnologia VDSL2 mas certamente deve receber taxas de transferências mais elevadas do que aquelas fornecidas pelas restantes tecnologias DSL.

Observa-se na Tabela 2.6 que as características das soluções em fibra óptica são mais atraentes dos que as soluções em cobre de par entrançado em termos de alcance e também em termos de taxas de transferência por utilizador. Entre a tecnologia EPON e a tecnologia GPON, esta última apresenta as melhores características. Posto isto, no caso do provedor de rede querer aproveitar o cobre de par entrançado deve escolher a tecnologia VDSL2 para transportar os dados na rede de acesso, já que a mesma suporta o serviço *Triple Play*. No caso do provedor de serviços estar disposto a investir numa estrutura em fibra óptica para prevenir futuras demandas de largura de banda, a melhor solução para suportar qualquer serviço é o GPON.

**Tabela 2.6 – Comparação entre as tecnologias de rede de acesso [Cisco, 2008].**

| Tecnologia | Meio de transmissão | Taxa de transferência por utilizador | Alcance |
|---|---|---|---|
| ADSL | Par entrançado | 8 Mbps | Até 5,5 km |
| ADSL2 | Par entrançado | 12 Mbps | Até 3,7 km |
| ADSL2+ | Par entrançado | 24 Mbps | Até 2,7 km |
| VDSL | Par entrançado | 52 Mbps | Até 900 m |
| VDSL2 | Par entrançado | 100 Mbps | Até 300 m |
| EPON | Fibra óptica | 1 Gbps dividido por 32 utilizadores dá. 30 Mbps | Até 20 km |
| GPON | Fibra óptica | 1,2 Gbps dividido por 32 utilizadores dá. 38 Mbps | Até 20 km |

## 2.3 REDES NÚCLEO

Nesta secção apresenta-se os conceitos relacionados com as duas tecnologias de transporte mais utilizadas nas redes núcleo: a tecnologia de transporte SDH (*Synchronous Digital Hierarchy*) e a tecnologia *Ethernet.* Também são apresentados, nesta secção, os métodos de recuperação de falhas utilizados nas redes núcleo.

### 2.3.1 A Tecnologia SDH

A rede de telecomunicações é constituída por largos quilómetros de fibra óptica que operam em SDH (*Synchronous Digital Hierarchy*) [RAD 1, 2008, RAD 2, 2008].

O SDH é uma tecnologia de trama repetitiva onde uma trama, designada STM (*Synchronous Transport Module*), é transmitida 8000 vezes por segundo, ou seja, uma trama é enviada cada 125µs. A trama STM-1, conforme mostra a Figura 2.16, é a unidade primária de transmissão do SDH e é representada por uma matriz de 9 filas por 270 colunas de *bytes* a que corresponde o débito binário de: 9 (filas) x 270 (colunas) x 8 (*bits*) x 8000 (tramas/s) = 155,52 Mbps.

Na trama SDH, a sinalização e a supervisão encontram-se numa zona especial separada da informação a transferir. A zona reservada para a gestão do SDH é designada por SOH (*Section Overhead*), enquanto que a zona de Carga útil (*Payload*) destina-se à informação a ser transferida pela rede. Cada *byte* da trama corresponde a um canal de 8 *bits* x 8000 (tramas/s) = 64 Kbps. A zona SOH inclui canais de sinalização para configurar dinamicamente e monitorizar o desempenho, diagnostica falhas de linha ou de equipamento e por fim inclui funções de administração.

A carga útil (*Payload*) constitui a zona onde é inserida e extraída a informação transportada pelo sistema. É constituída por 9 filas e 261 colunas de *bytes* com uma capacidade de transporte de: 9 (filas) x 261 (colunas) x 8 (*bits*) x 8000 (tramas/s) = 150,336 Mbps.

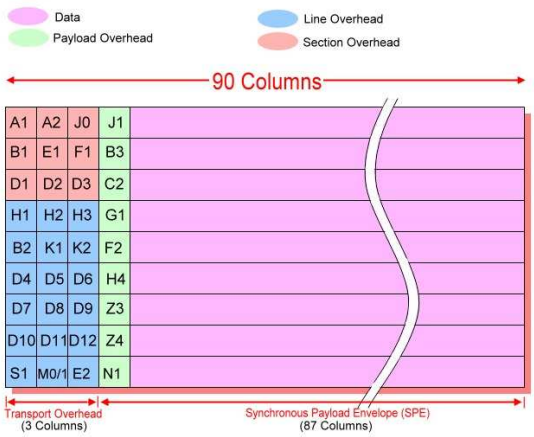



**Figura 2.16 – Estrutura da Trama STM-1 [Prakash, 2005].**

O SDH é sincronizado a todos os níveis da hierarquia, o que significa que as velocidades dos níveis superiores são múltiplas exactas da velocidade do primeiro nível, ou seja, STM-N = N x 155,53 Mbps. As velocidades da hierarquia foram seleccionadas para permitir o transporte dos dados desde a origem até ao destino.

Os transportes de nível superior são conseguidos por entrelaçamento dos *bytes* das tramas tributárias. N tramas individuais STM-1 são multiplexadas, por entrelaçamento de *bytes*, para formar a trama STM-N. Pode-se observar na Figura 2.17 uma trama STM-4 constituída por entrelaçamento de 4 tramas STM-1. A trama exibe uma estrutura regular normalmente visualizada num formato rectangular – a transmissão é em série, os bits dos octetos são enviados sucessivamente da esquerda para a direita em cada linha e percorre as linhas de cima para baixo (tal como se lê um texto).

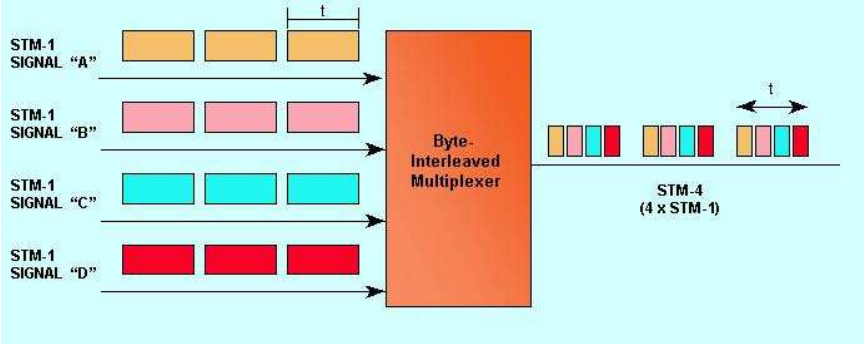



**Figura 2.17 – Trama STM-4 com Entrelaçamento de Tramas STM-1 [RAD 1, 2008].**

A taxa de transmissão básica para SDH foi definida em 155.52 Mbps, velocidade denominada STM-1 definindo assim, o primeiro nível da hierarquia SDH. As taxas de transmissão dos níveis superiores são múltiplas de STM-1. A Tabela 2.7 mostra os demais níveis hierárquicos. Os vários tributários de baixa ordem (2 Mbps, 34 Mbps e 144 Mbps) são multiplexados para formarem uma trama SDH denominada de STM-1 com uma taxa de transferência de 155 Mbps. Actualmente é possível transportar 64 tramas SDH numa só fibra fornecendo uma taxa de transferência de aproximadamente 10 Gbps e está em estudo a possibilidade de transportar 256 tramas SDH que permite fornecer uma taxa de transferência de aproximadamente 40 Gbps [RAD 1, 2008].

**Tabela 2.7 – Hierarquias SDH.**

| STM-N | Taxa de Transferência |
|---|---|
| STM-1 | 155,52 Mbps |
| STM-4 | 622,08 Mbps |
| STM-16 | 2488,32 Mpbs |
| STM-64 | 9953,28 Mbps |
| STM-256 | 39813,12 Mbps |

O SDH apresenta uma forma simplificada de fazer a inserção e extracção de tributários de baixa ordem nos elementos de rede devido à sincronização da rede. O cabeçalho da trama SDH permite gerir a rede de uma forma centralizada para facilitar a rapidez e optimização dos recursos da rede. Existe uma padronização das interfaces existentes nos equipamentos o que leva a um mercado mais competitivo para reduzir o custo total da rede. Os equipamentos possuem mecanismos de protecção e é possível utilizar a largura de banda de forma flexível e dinâmica.

Os elementos de rede da tecnologia SDH são denominados ADM (*Add Drop Multiplexer*). Estes permitem a inserção e extracção de taxas de transferência de ordem baixa de uma taxa de transferência de ordem elevada existente na rede, de forma a encaminhar as taxas de transferência para outras redes. Ultimamente foram desenvolvidos equipamentos MSPP (*Multi-Service Provisioning Pack*) que actuam como ADM da rede SDH mas também têm a capacidade de interligar tecnologias como a Ethernet, entre outras, à rede núcleo SDH do provedor de serviços.

O projecto, a instalação e a operação da rede SDH são complexos e devem ser efectuados com um planeamento criterioso e detalhado. A tecnologia SDH permite haver sistema de gestão, que possibilita a monitorização dos equipamentos de diferentes fabricantes num único sistema [RAD 2, 2008].

### 2.3.2 A Tecnologia Ethernet

A Ethernet é um protocolo que controla a forma como é transferida os dados pela rede. A tecnologia Ethernet opera na camada 2 do modelo TCP/IP e suporta qualquer protocolo de camadas superiores, principalmente o IP. A Ethernet tradicional suporta transferências a uma taxa de 10 Mbps. À medida que a demanda por largura de banda foi aumentando foram criadas as especificações para a *Fast* Ethernet e a *Gigabit* Ethernet. A *Fast* Ethernet e a *Gigabit* Ethernet são extensões da Ethernet tradicional e têm uma taxa de transferência máxima de 100 Mbps e de 1000 Mbps respectivamente [IEEE 802.3, 2000].

A Figura 2.18 mostra a estrutura básica da trama Ethernet 802.3. A trama está dividida em 7 secções nomeadamente a *Preamble*, o delimitador SFD (*Start-of-Frame*), o endereço de destino, o endereço da origem, o comprimento/tipo, a carga útil de dados e a FCS (*Frame check sequence*).

O campo *Preamble* de 7 *bytes* é um padrão de uns e zeros que informa as estações receptoras da chegada da trama e também proporciona um meio de sincronização na recepção da trama. O campo SFD de 1 *byte* é também um padrão de uns e zeros que indica o local onde inicia a trama. O campo endereço de destino de 6 *bytes* identifica qual a estação que deve receber a trama. O campo endereço de origem de 6 *bytes* indica qual a estação de envio. O campo comprimento/tipo de 2 *bytes* indica o número de *bytes* de clientes MAC (*Media Access Control*) contidos no campo de dados da trama ou a identificação do tipo de trama no caso da trama utilizar um formato opcional.

Cada dispositivo Ethernet contém um endereço MAC único atribuído pelo fabricante. O campo de dados tem uma sequência de n *bytes* (46 <= n <= 1500) de qualquer valor em que o número mínimo total de *bytes* é 64. O MTU (*Maximum Transmission Unit*) é a sigla utilizada para indicar o número máximo de *bytes* a transferir pela trama Ethernet. O campo FSC de 4 *bytes* é uma sequência que contém um valor CRC (*Cyclic Redundancy Check*) de 32 bits criado pelo MAC de envio e recalculado pelo MAC de recepção para verificar as tramas corrompidas. Assim os tamanhos mínimos e máximos da trama Ethernet são 72 e 1526 *bytes* respectivamente. A trama Ethernet mais pequena é de 64 *bytes* e a trama Ethernet maior é de 1518 bytes.

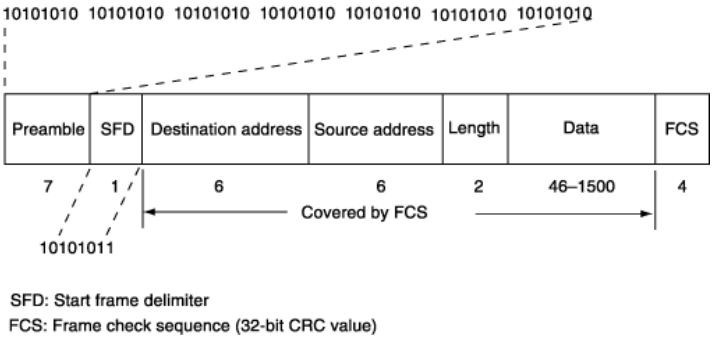



**Figura 2.18 – A estrutura da Trama Ethernet [ChipCenter-QuestLink 1, 2002].**

A transportadora CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) é a técnica utilizada para partilhar o acesso à largura de banda disponível. Entre duas estações existem ligações entre numerosos elementos de rede, todos a competir pela largura de banda através da utilização da mesma técnica CSMA/CD [ChipCenter-QuestLink 2, 2002]. Colectivamente, todos os elementos de rede operam num domínio de colisão. O domínio de colisão é a porção da rede onde dois ou mais elementos de rede que transferem dados ao mesmo tempo interagem uns com os outros. Cada elemento de rede espera um sinal do meio de transmissão para poder transferir uma trama pela rede. A colisão ocorre quando de repente um elemento de rede começa a transferir dados sem esperar pelo sinal do meio de transmissão a indicar que pode transferir os seus dados pela rede. Os sinais dos vários elementos de rede colidam onde é causado uma distorção no sinal. Esta distorção no sinal é identificada pelo elemento de rede que o recebe e envia uma mensagem de congestionamento pela rede. Todos elementos de rede que recebem esta mensagem iniciam um tempo de espera aleatório antes de iniciar a sua transferência. O tempo aleatório é utilizado para prevenir que os mesmos elementos de rede colidem de novo uns com os outros e consequentemente aumentar as colisões sucessivas para a mesma trama.

Os erros nas redes podem ser provocados por razões relacionadas com o tamanho da trama, com o meio de transmissão ou com o excesso de perda de largura de banda devido às colisões. Quando a trama a transferir é muito pequena, as tramas maiores são fragmentadas em duas ou mais tramas. Isto contribui para a utilização em excesso da largura de banda e contribui também para o

aumento de colisões. O meio de transmissão pode causar erros quando não é utilizada a categoria correcta ou quando não utilizado o conector correcto. A instalação imprópria do meio de transmissão também causa erros na transferência de dados. A tecnologia Ethernet exibe um desempenho mau quando a sua utilização da largura de banda é de 60% ou superior. O excesso de utilização que inclui a perda de largura de banda devido às colisões é tipicamente o resultado de muitos elementos de rede a operar num mesmo domínio de colisão. A substituição de *hubs* (dispositivo que permite conectar os vários elementos de rede entre si) por comutadores ou encaminhadores permite a partição da rede em múltiplos domínio de colisão, cada um com um número inferior de elementos de rede. Isto contribui para melhorar significativamente o desempenho da rede.

### *Fast* Ethernet

A *Fast* Ethernet está implementada em diversas maneiras diferentes, todas referidas colectivamente como a tecnologia 100BaseT. Como referido anteriormente, é uma tecnologia que permite taxas de transferência de 100 Mbps. A desvantagem desta tecnologia é o seu reduzido diâmetro de rede de 200m, cerca de 1 décimo da rede Ethernet tradicional. Esta redução é necessário para manter os parâmetros de CSMA/CD a uma taxa mais rápida. Os sinais movimentam-se à mesma velocidade no meio de transmissão mas os tempos de trama são mais curtos por um factor de 10. Os dados são transferidos em grupos de 4 *bits* e não *bit* a *bit* como acontece na tecnologia Ethernet.

### *Gigabit* Ethernet

Mais uma vez o aumento da taxa de transferência implicou a redução do diâmetro da rede para manter o CSMA/CD. O diâmetro de rede *Gigabit* Ethernet é de 25m. São utilizadas duas técnicas para aumentar a taxa de transferência dos dados de 100 Mbps para 1000 Mbps e manter o diâmetro da rede nomeadamente a extensão da transportadora (*carrier extension*) e a *frame bursting*. A Figura 2.19 mostra o campo da extensão da transportadora de 0 a 448 *bytes* adicionada à trama Ethernet.

A extensão da transportadora é utilizada para manter a trama mínima de 512 *bytes* (não inclui nem o *preamble* nem o SFD). Desta forma, uma trama Ethernet de 10/100 Mbps que contém apenas 100 *bytes* requer um campo de extensão da transportadora de 412 *bytes* para ser utilizada sobre o *Gigabit* Ethernet [IEEE 802.3, 2000**,** ChipCenter-QuestLink 2, 2002].

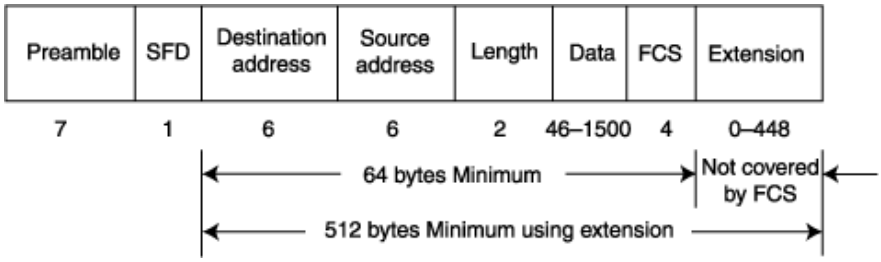



**Figura 2.19 – A estrutura da Trama Ethernet [ChipCenter-QuestLink 2, 2002].**

A frame *bursting* envolve o envio de múltiplas tramas num só *burst* (envio explosivo) de transferência. A primeira trama no *burst* deve ser preencher o campo da extensão da transportador no caso do seu comprimento ser inferior a 512 *bytes*. Tramas adicionais dentro do *burst* não requerem preenchimento do campo de extensão da transportadora mas é requerido um *interframe gap* de 0,096 µs entre as tramas. O emissor continua a transferir dados durante o *interframe gap* para manter a sua prioridade no meio de transmissão da rede. O tempo de *burst* inicia quando a primeira trama é enviada onde limita o comprimento do *burst* a um máximo de 65536 *bits* [IEEE 802.3, 2000**,** ChipCenter-QuestLink 2, 2002].

### 2.3.3 Recuperação nas Redes Núcleo

Esta secção descreve o desempenho da recuperação de falhas de uma rede. As falhas comuns de rede, as formas de detectar as falhas e as soluções de recuperação de redes são explicadas a seguir.

As técnicas de recuperação podem ser utilizadas nas redes de comutação de circuitos bem como nas redes de comutação de pacotes. No caso de falhar a ligação ou o nó, o tráfego é comutado para o caminho alternativo. É importante a rapidez do desempenho da operação de recuperação de forma a prevenir a perda de pacotes no local da falha. Se a recuperação é rápida a falha é mal percebida pelos utilizadores finais. A comutação é efectuada pelos encaminhadores adjacentes à falha e estes actualizam as suas tabelas de encaminhamento para encaminhar os pacotes num caminho diferente e evitar a componente de falha. O caminho utilizado pelo tráfego antes da falha é denominado de caminho primário ou o caminho de trabalho e o novo caminho é denominado de caminho de protecção [Schupke, 2005].

As técnicas de recuperação consistem em quatro tarefas: Primeiro, a rede deve ser capaz de detectar a falha; Segundo, os nós que detectam a falha notificam os nós restantes da ocorrência da falha; Terceiro, o caminho de protecção é calculado, e; Quarto, o nó de Comutação de Caminhos encaminha o tráfego para o caminho de protecção. Esta última tarefa é denominada de *switchover*.

No caso de uma ligação *unicast* falhar entre o emissor e o receptor, o utilizador final experimenta uma falha de serviço antes de finalizar as quatro tarefas. A duração do tempo de falha

calcula-se através da soma do tempo da detecção da falha, do tempo da notificação da falha a todos os nós da rede, do tempo do cálculo de um novo caminho de protecção e o tempo que leva para fazer a comutação.

Qualquer recurso dentro de uma rede tem a possibilidade de falhar. O factor humano pode muitas vezes ser a causa de falha ao desligar uma ligação sem intenção. Também podem surgir falhas devido ao processo de envelhecimento do equipamento ou suas componentes.

A detecção de falhas em redes ópticas é geralmente assistida por protocolos de camada 2 que podem desempenhar a notificação no sentido da fonte. Isto requer uma comunicação bidireccional entre os nós. Tal solução existe nas redes SDH. Nestes casos a detecção é assistida por notificações e aumenta o tempo de recuperação.

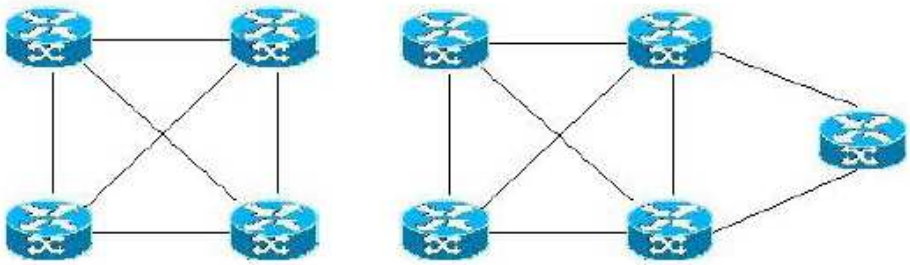
**Topologias das redes núcleo e seus métodos de recuperação**

Existem três tipos de topologias de rede utilizadas para recuperar o tráfego em caso de falha da rede: topologia em anel, topologia em malha e topologia híbrida anel/malha.

A topologia em anel é a forma mais comum de recuperação na camada física. As redes de topologia em anel são denominadas de anéis auto recuperáveis. Nestas redes, cada nó é conectado aos seus nós vizinhos através de duas ligações. No caso de falha o tráfego é comutado para a ligação de protecção.

Existem dois tipos de topologias em malha nomeadamente malha completa e malha parcial. Numa topologia em malha completa todos os nós são conectados a todos os restantes nós da rede, conforme mostra a Figura 2.20 a). A malha completa tem um elevado custo de implementação mas oferece redundância e no caso de um dos nós ou ligações falharem o tráfego da rede é reencaminhado para qualquer nó da rede. A topologia em malha parcial apresenta um custo de implementação mais barato mas oferece menos redundância comparada com a topologia em malha completa. Numa malha parcial nem todos os nós são conectados a todos os nós restantes, conforme mostra a Figura 2.20 b).

A topologia em malha é fiável e oferece redundância. No caso de falha os nós continuam a comunicar uns com os outros directamente ou através de nós intermediários. A grande desvantagem das topologias em malha é o elevado custo devido ao número de conexões e cabos requeridos [Rajagopal, 2008].



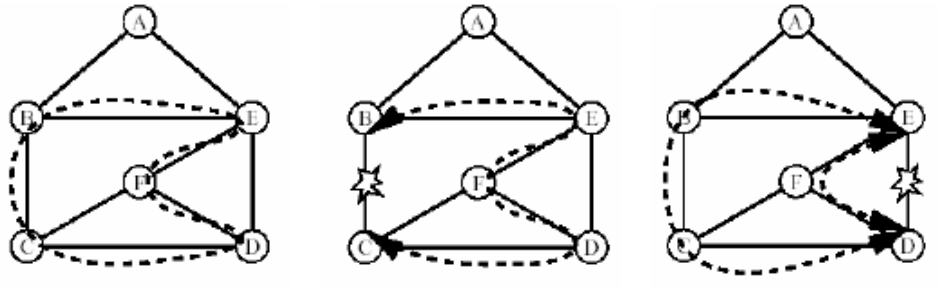
(a) (b)

**Figura 2.20 – Topologia em malha a) completa b) parcial.**

A rede com topologia híbrida anel/malha consiste numa rede com uma mistura das duas topologias. A recuperação através de mecanismos de anéis auto recuperáveis oferece tempos muito rápidos de recuperação (aproximadamente 50 ms), mas o número de recursos reservados para caminho de trabalho e para o caminho de protecção é elevado. Os mecanismos de protecção nas topologias em malha reservam um menor número de recursos. Como a recuperação nas redes em malha envolve uma sinalização complexa, a recuperação nas redes em malha é geralmente mais lenta comparada com as redes em anel.

De forma a combinar as melhores características de ambas as topologias considera-se um novo conceito denominado *p-cycles* [Schupke, 2005]. O método *p-cycles* é baseado na formação de caminhos fechados. Estes caminhos são criados antes da ocorrência da falha. A Figura 2.21 ilustra o princípio de recuperação do método *p-cycles* para a protecção de ligações. A topologia ilustrada na Figura 2.21 a) é configurada antes da ocorrência da falha através de uma conexão fechada no ciclo B-C-D-F-E-B. O *p-cycle* protege o caminho de trabalho com as suas próprias ligações, conforme mostra a Figura 2.22 b). No caso de falha na ligação B-C, o *p-cycle* oferece protecção através da comutação do tráfego para os caminhos restantes do ciclo (C-D-F-E-B). A capacidade de protecção é de uma unidade. Ao contrário da topologia em anel, o método *p-cycle* também protege as ligações que não pertencem ao caminho *p-cycle.* As ligações que têm ambas as terminações no *p-cycle* também podem ser protegidas. Estas ligações são denominadas de ligações *straddling.* A Figura 2.21 c) ilustra a protecção de tal ligação (E-D). Existem dois caminhos de protecção para as ligações *straddling,* no exemplo tem-se E-B-C-D e E-F-D. Desta forma, protege-se duas unidades de capacidade das ligações *straddling.*

Ao contrário dos anéis convencionais SDH, no caso de falha numa ligação apenas um caminho de protecção é disponibilizado onde apenas as ligações que pertencem ao anel são protegidas. Nos *p-cycles* a capacidade de recuperação ocupa a mesma capacidade de uma rede em malha e a operação de recuperação utilizada numa rede com *p-cycles* é denominada de recuperação por comutação 1:n utilizada nas redes de topologia em anel como é utilizada nas redes SDH através dos anéis MSPRing [Schupke, 2005].




(a) (b) (c)

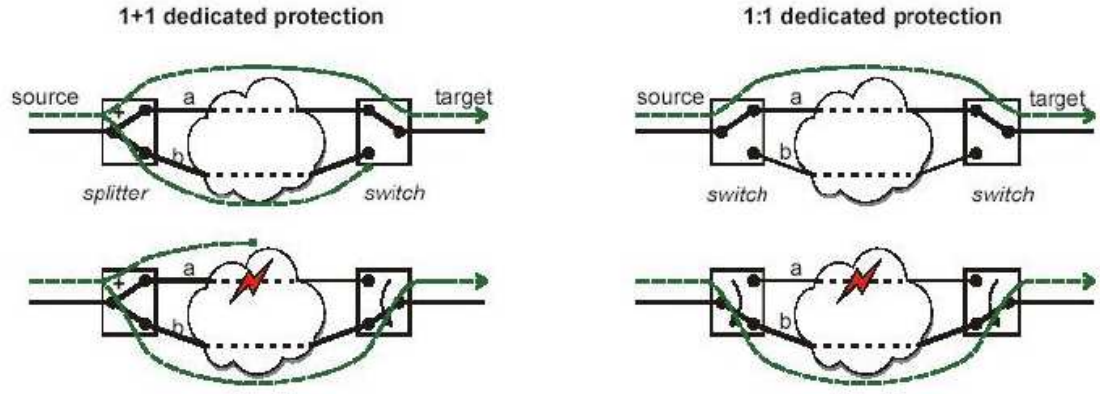
**Figura 2.21 – O princípio de recuperação do método *p-cycles* para a protecção de ligações [Schupke, 2005].**

## Recuperação na Camada Física

A recuperação na camada física é efectuada sem notificar os nós da rede. Apenas os nós adjacentes à falha actuam de forma a recuperar a falha [Optical Network, 2006]. Isto permite a recuperação de falhas ser mais rápida. Na camada física pode ser utilizada a protecção por comutação 1+1 ou a protecção por comutação 1:1.

Nas redes que utilizam a protecção por comutação 1+1, é utilizado um divisor (*splitter*) para replicar o sinal e encaminhá-lo por dois caminhos diferentes, conforme mostra a Figura 2.22 a). O comutador receptor compara os dois sinais recebidos e escolhe o melhor sinal para ser encaminhado no caminho de trabalho, enquanto o tráfego com sinal mais fraco é descartado. No caso de ocorrer uma falha num dos caminhos, o comutador recebe sempre um sinal. Sempre que é criado um caminho de trabalho tem que ser criado um caminho de protecção. Esta redundância torna-se cara.

Nas redes que utilizam a protecção por comutação 1:1 (um por um), o tráfego é encaminhado na ligação de protecção apenas depois de detectada a falha no caminho de trabalho, conforme ilustrado na Figura 2.22 b). Quando ocorre uma falha, a fonte começa a encaminhar o tráfego sobre o caminho de protecção. Nalguns casos o nó do destino informa o nó fonte sobre a falha antes deste comutar o tráfego para o caminho de protecção [Optical Network, 2006].




(a) (b)

**Figura 2.22 – Protecção por comutação a) 1+1 e b) 1:n.**

Na protecção por comutação 1:N os recursos de protecção não são dedicados à recuperação de uma conexão específica, mas sim partilhada por N conexões para atender a diferentes cenários de falha. Isto significa que N caminhos de trabalho podem ser protegidos por um único caminho de protecção, assim uma única ligação pode fornecer protecção a qualquer um dos N caminhos de trabalho. Na maioria das implementações o número limite de N está configurado para 14. Devido à partilha dos recursos de protecção, a protecção por comutação 1:N é mais eficiente em termos de utilização dos recursos na rede do que as protecções por comutação 1:1 e 1+1. Este tipo de protecção também requer um mecanismo de sinalização para activar a comutação para o caminho de protecção. Este esquema pode se estender a um esquema mais generalizado para M:N onde N conexões de trabalho são protegidas por M conexões de protecção. A Figura 2.23 ilustra uma situação de falha numa rede com protecção por comutação 1:N [Goff, 2005].

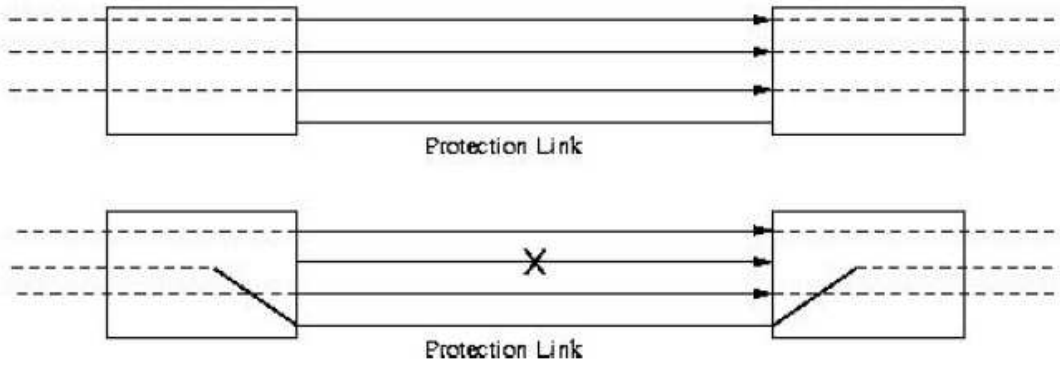



**Figura 2.23 – Protecção por comutação 1:N.**

**SDH**

Na camada física geralmente é utilizada a tecnologia SDH (*Synchronous Optical Networks*). Nas redes SDH são utilizados equipamentos de rede denominados ADM (*Add-Drop Multiplexers*) que permitem comutar o tráfego de um caminho para outro. É utilizada a topologia em anel e o meio de transmissão utilizado é em fibra óptica. A protecção com anéis auto recuperáveis é denominada de APS (*Automatic Protection Switching*). Existem duas versões de anéis APS denominadas de SNCP (*Subnetwork Connection Protection*) e MS-SPRing (*Multiplex Section – Shared Protection Ring*). Nas redes SDH a recuperação do tráfego é efectuado atraves de dois anéis de fibra óptica. O tempo de comutação do tráfego na rede SDH é aproximadamente 50 ms, isto torna estas redes aptas para transportar e recuperar o tráfego sensível ao atraso.

No SDH SNCP é utilizado a protecção por comutação 1+1. Com este tipo de protecção, o tráfego é rapidamente recuperado e cumpre o objectivo da recuperação em 50 ms, próprio para recuperar o tráfego de voz e de vídeo. A desvantagem da recuperação SDH SNCP é a reserva de um elevado número de recursos dedicados e necessários para a protecção na ligação de protecção. A

Figura 2.24 ilustra o funcionamento de uma topologia em anel que utiliza a técnica SDH SNCP. Observa-se que é encaminhado o tráfego a partir do encaminhador 1 até ao encaminhador 4 através do caminho ou fibra óptica de trabalho e através do caminho ou fibra óptica de protecção. No modo normal o caminho de trabalho é o caminho (1-2-3-4) mas no caso de ocorrer uma falha no mesmo caminho, o encaminhador 4 começa a utilizar o tráfego recebido do caminho de protecção (1-8-7-6-5-4) vindo do encaminhador 5.

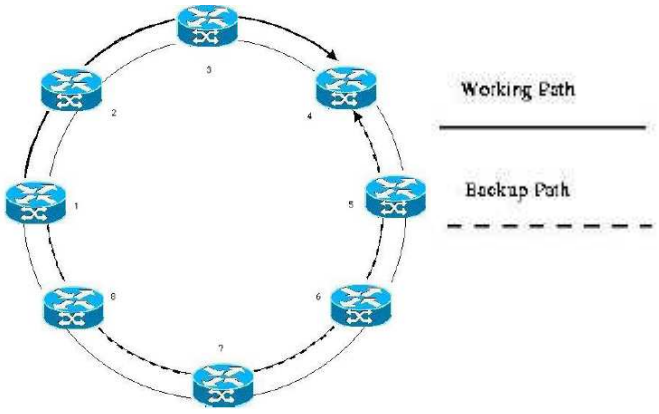



**Figura 2.24 – Rede SDH com técnica SNCP.**

No SDH MS-SPRing é utilizada a protecção por comutação 1:1 no qual todas as ligações podem carregar tanto tráfego regular como tráfego de recuperação e desta forma não são requeridas ligações de protecção dedicadas. No caso de ocorrer uma falha, o nó mais perto da fonte comuta o tráfego de um anel para outro e encaminha-o até ao nó destino ou no sentido inverso. No MS-SPRing não são utilizados tantos recursos como no SNCP.

Na Figura 2.25 observa-se que o encaminhador 1 encaminha o tráfego até ao encaminhador 4 através do caminho de trabalho (1-2-3-4). No caso da falha ocorrer entre a ligação do encaminhador 2 e 3, o encaminhador 2 comuta o tráfego do caminho de trabalho para o caminho de protecção no sentido inverso. O tráfego é encaminhado a partir do encaminhador 1 até ao encaminhador 4 e atravessa a rede pelos encaminhadores (1-2-1-8-7-6-5-4) [Cisco 2, 2008].

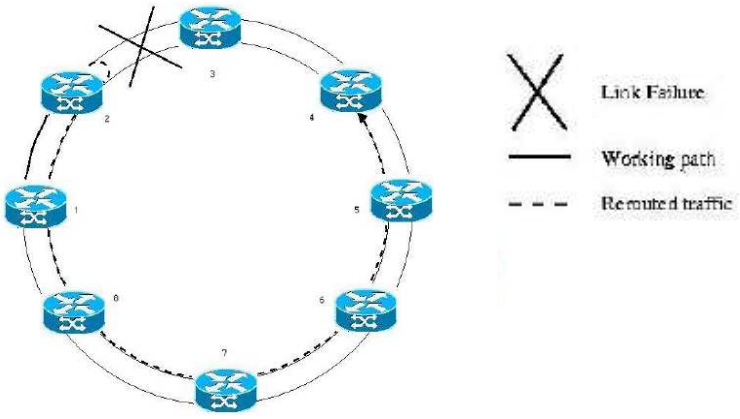



**Figura 2.25 – Rede SDH em topologia em anel com técnica MS-SPRing.**

**Recuperação na camada de rede.**

Nas redes de comutação por pacotes (Internet), os mecanismos de recuperação dependem das competências dos protocolos de encaminhamento. No caso de ocorrer uma falha, todos os nós da rede são informados e as suas tabelas de encaminhamento são actualizadas para encaminhar o tráfego de forma a contornar a falha através do caminho mais curto até ao destino.

Os protocolos de encaminhamento fazem com que sobrevivem os dados que atravessem as ligações ou nós de falha, mas não garantem que o tempo de recuperação seja menor que 50 ms. O tempo de recuperação depende das dimensões da rede e do protocolo de encaminhamento utilizado. A camada IP depende da camada física que fornece o transporte de pacotes IP entre dois pontos na rede. Não existe um mecanismo padrão na troca de informação de estado na rede entre a camada IP e as camadas inferiores.

Os protocolos de encaminhamento utilizam temporizadores para obter informação temporal sobre o acontecimento da falha das mensagens "*hello*". Estas mensagens são recebidas e enviadas periodicamente pelos nós da rede. O nó que detecta a falha envia a todos os nós da rede uma mensagem LSA (*Link State Advertisement*).

Como as configurações por defeito nos protocolos de encaminhamento são no modo OSPF (*Open Shortest Path First*), a rede leva várias décimas de segundos antes de recuperar a falha devido ao elevado tempo de detecção da falha [Goyal et al, 2003]. Existem propostas para reduzir o tempo de recuperação através da redução do valor do intervalo da mensagem "*hello*". Mas demonstram que a redução do intervalo pode causar problemas. No caso do intervalo ser muito pequeno a rede corre o risco de congestionar mais vezes e perder várias mensagens "*hello*" e consequentemente fazer o nó pensar que existe uma falha de ligação onde na realidade existe uma congestão na ligação. Ao fazer o nó pensar que existe uma falha na ligação, a rede é enchida com LSA e todos os nós calculam novos caminhos. Ao receber as mensagens "*hello*" de novo os nós pensam que as ligações voltam a funcionar e consequentemente a rede enche de novo com novas mensagens LSA. Isto não apenas provoca mudanças desnecessárias de encaminhamento como aumenta a carga de processamento nos nós [Alaettinoglu et al, 2000].

### 2.3.4 Comparações entre as Redes Núcleo

A rede IP pode oferecer uma qualidade superior à da rede da camada física num ambiente controlado, pois é menos sujeita a ruídos. As redes de convergência dos serviços (dados, voz e vídeo), também conhecidas por Redes de Próxima Geração ou simplesmente NGN (*Next Generation Networks*), apresentam a melhor solução para suportar o serviço *Triple Play*. A NGN associa uma forte redução nos custos operacionais da rede e viabiliza o aumento de novas fontes de

receita, pois provê uma grande diversidade de serviços multimédia de próxima geração [Leroux et al, 2006].

A omnipresença da Internet é real, tanto no segmento corporativo, onde o aumento da produtividade é resultante da transformação gerada pelo *e-business*, como no segmento residencial com a crescente demanda por serviços diferenciados, em particular os relacionados ao entretenimento. São serviços que requerem elevadas larguras de banda e taxas de transmissão que garantem a qualidade e o desempenho esperados pelo utilizador.

Torna-se essencial disponibilizar uma solução de rede que seja flexível para prover serviços diferenciados e sob demanda, que associa o desempenho, a fiabilidade e resiliência da infra-estrutura das redes de telecomunicações de forma poder suportar o crescimento de novas demandas.

A tecnologia IP é o ambiente utilizado para o transporte de serviços por pacotes, porque possibilita maior flexibilidade no provimento de novos serviços multimédia e de banda larga. Desta forma, a migração de plataformas de telecomunicações para um ambiente em que associa as vantagens tecnológicas do protocolo IP (flexibilidade e rapidez) às vantagens das tecnologias tradicionais (fiabilidade, desempenho e protecção de rede) é um factor crucial para o sucesso futuro de empreendimentos nos segmentos para operação das Redes de Próxima Geração. O ambiente IP permite às operadoras oferecer novos serviços, aplicações e comodidade ao seu cliente de uma forma eficiente e de baixo custo em comparação com aquilo que oferecem as redes de serviços baseados em circuitos.

A implementação de uma infraestrutura de rede convergente para fornecer serviços de dados, voz e vídeo integrados, em contraste com as plataformas independentes, representa um enorme potencial de redução de custos de operação e manutenção de rede. Verifica-se que quanto maior a diversidade de serviços associados, maior é a quantidade de elementos e a complexidade da rede. Mas as NGN, possibilitam uma redução de até 80% dos elementos de rede de comutação, resultando em 40% de redução nos custos operacionais e de manutenção da rede.

Expandindo o horizonte com IP sobre SDH permite obter de custo reduzido e baseia-se na migração da actual rede óptica SDH, de perfil puramente estático, para um modelo mais flexível em direcção ao modelo dinâmico e eficiente, planeado com soluções de Redes Ópticas de Próxima Geração. Aqui são introduzidas novas funcionalidades aos sistemas SDH existentes, viabilizando a implementação de serviços Ethernet / *Fast* Ethernet / *Gigabit* Ethernet, providos por interfaces de baixo custo integradas aos sistemas SDH. Esta solução protege os investimentos realizados na planta SDH existente e cria novas oportunidades de negócios para a extensão de soluções VPN ou LAN-to-LAN, de custo muito mais competitivo do que as soluções tradicionais [Leroux et al, 2006].

A Tabela 2.8 mostra a diferença entre as capacidades das tecnologias SDH e Ethernet. A tecnologia SDH foi desenvolvida para transmitir o tráfego através de circuitos (entrega de pacotes garantida), enquanto a tecnologia Ethernet foi desenvolvida para transmitir o tráfego através de pacotes (entrega de pacotes não garantida). A tecnologia SDH melhou a sua eficiência ao longo dos anos mas continua a ser inflexível e cara. Actualmente a tecnologia Ethernet oferece largura de banda suficiente para suportar qualquer serviço mas não oferece o elevado desempenho oferecido pela tecnologia SDH. A tecnologia Ethernet não tem mecanismos de recuperação, não monitoriza os serviços e não oferece qualidade de serviço, ao contrário das redes SDH. Estes factores podem ser adicionados à rede Ethernet para melhorar o seu desempenho pelo administrador de rede mas devem ser monitorizados e testados para fornecer o nível de serviço desejado na rede. A recuperação de falhas é o factor mais importante a considerar.

**Tabela 2.8 – Comparação entre o SDH e a Ethernet [Leroux et al, 2006].**

| Tecnologia / Critérios | SDH | Ethernet |
|---|---|---|
| **Protecção redundante** | Capacidade automática de protecção por comutação (50ms); Esquema com capacidade de ajuste (LCAS – *Link Capacity Adjustment Scheme*) para a concatenação virtual | Agregação de ligações; Anel resiliente de pacotes (< 50ms); Reencaminhamento rápido através do MPLS (*Multi-Protocol Label Switching*) (< 50ms); |
| **Operações, Administração e manutenção (OAM)** | Estrutura SDH com OAM. | As ligações ponto-a-ponto através do IEEE 802.3ah e ITU Y.17 padrões ethoam; serviços fim-a-fim através do IEEE 802.1ag; Serviço OAM de Metro Ethernet. |
| **Detecção de falhas** | Monitorização de erros por secções e indicações remostas; Monitorização do desempenho. | Monitorização remoto com limites exclusivos. |
| **Manutenção** | Testes através da capacidade de *loops*. | Não tem capacidade de efectuar *loops*; A informação do comutador ou do encaminhador é obtido através da monitorização remota. |
| **Engenharia de Tráfego** | Concatenação Virtual (VC). | Caminhos LSP (*Label Switching Path*) através do MPLS; Criação de VLAN (*Virtual Local Area Network*) |
| **Escalabilidade** | Taxa de transferência até 40 Gbps; Granularidade até ao nível VC (2 Mbps). | Taxa de transferência até 10 Gbps. Granularidade até qualquer taxa. |
| **QoS** | Predizível | Qualidade de Serviço próprio; Dificuldades de interoperabilidade |
| **Robustez** | 99,9999% do tempo está a funcionar; O BER (*Bit Error Rate*) é de $10^{-12}$ | A duração do funcionamento da rede depende do serviço de redundância/protecção que o administrador implementa na rede; O BER é de $10^{-12}$ |
| **Custo** | Elevado | Baixo |

Entre as duas tecnologias de transporte a Ethernet é a tecnologia que apresenta as melhores condições, uma vez que podem ser adicionados e implementados os factores necessários na rede para esta assegurar o bom funcionamento da rede *Triple Play* e suportar os serviços *Triple Play* de forma eficiente e com qualidade de serviço.

# CAPÍTULO III

# QUALIDADE DE SERVIÇO

O Capítulo 3 apresenta uma introdução teórica aos conceitos relacionados com a Qualidade de Serviço nas redes e os métodos de Recuperação da Rede em caso de falha ou congestionamento.

## 3.1 INTRODUÇÃO

A Internet funciona com o protocolo IP. Este protocolo trabalha com a filosofia do "melhor esforço", onde cada utilizador de rede envia os seus dados e partilha a largura de banda com todos os fluxos de dados de outros utilizadores. Numa rede de "melhor esforço" os pacotes são analisados rapidamente sem proporcionar qualquer tipo de garantia sobre a Qualidade de Serviço. Os encaminhadores tratam de encaminhar o tráfego de dados pelo caminho mais rápido até ao destino, conforme as rotas da sua tabela de encaminhamento e a largura de banda que estiver disponível. No caso de haver congestionamento, os pacotes são descartados. Desta forma a rede de "melhor esforço" não oferece qualquer garantia sobre o sucesso do funcionamento do serviço. As aplicações que funcionam em tempo real, como o tráfego IPTV e VoIP, necessitam de uma rede que forneça garantias de um correcto funcionamento do serviço.

A Qualidade de Serviço (QoS) permite oferecer garantias de funcionamento a qualquer aplicação da Internet. A atribuição de prioridades ao tráfego é o mecanismo utilizado para oferecer Qualidade de Serviço. No caso de existir congestionamento apenas o tráfego de menor prioridade é descartado. De uma forma geral, a QoS especifica o grau de satisfação ou visão do utilizador em relação à garantia da prestação de um serviço em termos de certos parâmetros tais como a taxa de perda, o atraso, a variação do atraso, o débito efectivo, entre outros.

O desafio coloca-se em obter QoS nas redes IP onde o encaminhamento convencional do tipo SPF (*Shortest Path First*) [RFC 1131, 1989] é fonte de dois problemas: o atraso de propagação dos pacotes e o congestionamento da rede IP. A comutação IP resolve o problema do atraso de propagação, pois torna mais ágil o encaminhamento de pacotes. A Engenharia de Tráfego é a solução para o problema do congestionamento, pois trata da avaliação e optimização do desempenho de redes através de caminhos alternativos.

A IETF (*Internet Engineering Task Force*) tomou a iniciativa de criar um grupo de trabalho para propor uma arquitectura de suporte ao encaminhamento de pacotes baseados em etiquetas (LBS – *Label Based Switching*) numa plataforma aberta e inter-operável em vários tipos de redes e

de protocolos. Esta plataforma é denominada de MPLS (*Multiprotocol Label Switching*) [RFC 3031, 2001] e tem como objectivo proporcionar o encaminhamento orientado à conexão. Este Capítulo está organizado nas seguintes secções: Secção 3.2 – Qualidade de Serviço (QoS), Secção 3.3 – Soluções para a QoS e Secção 3.3 – Recuperação nas Redes MPLS.

## 3.2 QUALIDADE DE SERVIÇO

A QoS pode ser definida através de um certo número de parâmetros, pois a noção de "serviço" pode variar consoante as necessidades de cada utilizador. A camada de transporte pode permitir ao utilizador determinar os valores preferenciais, os valores aceitáveis e os valores mínimos para vários parâmetros de serviço, no momento em que a conexão é estabelecida. Nesse momento, essa camada trata de examinar estes parâmetros e determinar a possibilidade de realizar o serviço solicitado, com base nos tipos de serviços de rede disponíveis.

Os parâmetros típicos da Qualidade de Serviço na camada de transporte são: a probabilidade de falha no estabelecimento da conexão, o débito efectivo (*Throughput*), o atraso, o atraso de estabelecimento da conexão, a variação de atraso (*jitter*), a perda de pacotes, a taxa de erros residuais, a protecção, a prioridade e a resiliência [Tanembaum, 2003].

A probabilidade de falha ao estabelecer a conexão é a possibilidade da conexão não se estabelecer dentro de um período máximo estabelecido. Isto é provocado pelo congestionamento existente na rede.

O débito efectivo, contrariamente à largura de banda, calcula o número de *bytes* transferidos, por segundo, durante um determinado intervalo de tempo [Tanembaum, 2003, Amaro et al, 2000].

O atraso diz respeito ao tempo que um pacote demora a ser enviado desde a origem até ao seu destino. O tempo que um pacote deve demorar a atravessar a rede deve ser inferior a 150 ms como referido no Capítulo II. O termo atraso é usado como referência às ligações enquanto o termo latência é usado para referir o atraso dos equipamentos.

O atraso de estabelecimento da conexão é o tempo que decorre entre a conexão de transporte solicitada e a recepção da sua confirmação pelo utilizador do serviço de transporte. Aqui também está incluído o atraso de processamento na entidade de transporte remota. Quanto menor for o atraso melhor é o serviço.

A variação de tempo é a diferença dos atrasos consecutivos. Os *buffers* resolvem o problema da variação de atraso ao suavizar os tempos de chegada. Este parâmetro é importante para as aplicações (voz ou vídeo) que necessitam de garantir a chegada da informação em períodos de tempo bem definidos para serem processados. O efeito da variação de atraso provoca a entrega dos pacotes com periodicidade variável e também provoca a entrega desordenada dos mesmos.

A perda de pacotes totaliza-se pela percentagem de pacotes descartados. Pode ocorrer rejeição de pacotes nos encaminhadores devido às suas limitações de armazenamento ou por causa de erros ocorridos nas tramas durante o transporte.

A taxa de erros residuais calcula o número de mensagens perdidas numa percentagem do total enviado.

O parâmetro protecção oferece ao utilizador protecção contra a leitura ou alteração de dados por parte de terceiros.

O parâmetro prioridade fornece ao utilizador a possibilidade de indicar quais as conexões mais importantes para proteger as mesmas da perda de pacotes no caso de congestionamento.

Por fim, a resiliência permite a camada de transporte finalizar uma conexão na presença do congestionamento ou falha.

Os parâmetros de QoS são especificados pelo administrador de rede quando é solicitada uma conexão. Os valores mínimos e máximo aceitáveis podem ser fornecidos. Por vezes, quando são conhecidos os valores de QoS, a camada de transporte detecta que alguns deles não podem ser alcançados. Neste caso, a falha da tentativa de conexão é informada. Noutros casos, a camada de transporte tem conhecimento que não pode alcançar o objectivo desejado (por exemplo, um débito efectivo de 600 Mbps), mas pode atingir uma taxa mais baixa, porém aceitável (por exemplo, 150 Mbps). De seguida, a camada de transporte envia a taxa mais baixa à máquina remota e envia uma mensagem a solicitar o estabelecimento de uma conexão. Se a máquina remota não puder administrar o valor sugerido mas conseguir administrar qualquer valor acima do mínimo, a camada de transporte faz uma contraproposta. Se a máquina remota não aceitar qualquer valor acima do mínimo, é rejeitada a tentativa de conexão. Por fim, o utilizador da máquina de origem é informado da conexão estabelecida ou rejeitada. No caso de a conexão ser estabelecida, o utilizador é informado sobre os valores dos parâmetros acordados. Este procedimento é denominado de negociação de opção (*option negotiation*). Uma vez negociadas as opções, estas são mantidas durante toda a conexão [Tanembaum, 2003].

A QoS também envolve dar prioridades ao tráfego na rede. O sistema de monitorização da rede permite a provisão do QoS, de forma a assegurar o bom desempenho da rede no nível desejado. A QoS na Internet permite assegurar os pacotes de maior importância, em caso de congestionamento e descartar os pacotes de menor importância. Dar prioridades aos pacotes consiste em distinguir os tipos de aplicações/serviços. Os encaminhadores são configurados para criar filas distintas para cada aplicação de acordo com as prioridades das mesmas [Santos, 2004].

Fornecer a QoS é fundamental em diversas áreas de aplicação (por exemplo, a telemedicina) e aplicações em tempo real. É de salientar que os núcleos tecnológicos da Internet, tais como a

*Ethernet*, não foram desenvolvidos para suportar prioridades no tráfego nem dar garantidas de níveis de desempenho. Isto torna mais difícil implementar as soluções de QoS.

## 3.3 SOLUÇÕES PARA A QoS

O desenvolvimento do suporte à QoS nas redes IP proporcionou a proposta de alguns métodos, nomeadamente: os Serviços Integrados (IntServ – *Integrated Services*) [RFC 1633, 1994], os Serviços Diferenciados (DiffServ – *Differentiated Services*) [RFC 2475, 1998], o MPLS (*Multiprotocol Label Switching*) [RFC 3031, 2001] e a Engenharia de Tráfego [RFC 3272, 2002].

O IntServ através da reserva de recursos baseada no protocolo RSVP (*Resource Reservation Protocol*) [RFC 2205, 1997] permite ao emissor reservar um canal na rede para garantir a largura de banda e especificar exigências de atraso e variação de atraso. O DiffServ permite tratar cada classe de tráfego de forma diferente. Por exemplo, uma classe de tráfego em tempo real pode atravessar a rede mais rapidamente do que a transferência de um ficheiro (*best effort*). O MPLS é utilizado para evitar o congestionamento no núcleo da rede através de uma técnica de encaminhamento mais rápida e eficaz em comparação à rede IP. Por fim, a Engenharia de Tráfego é uma ferramenta que permite utilizar todos os recursos existentes na rede de forma a balancear o fluxo de dados na mesma.

### 3.3.1 Serviços Integrados

O modelo de Serviços Integrados é caracterizado pela reserva de recursos. As aplicações devem configurar os caminhos e reservar os recursos antes da transmissão de dados. O RSVP (*Resource Reservation Protocol*) é um protocolo de sinalização que permite configurar os caminhos e reserva os recursos [RFC 2205, 1997, Tanembaum, 2003].

O processo de sinalização está ilustrado na Figura 3.1. O emissor envia uma mensagem PATH (caminho) ao receptor com as especificações do tráfego (1). Cada encaminhador intermediário passa a mensagem PATH para o próximo salto determinado pelo protocolo de encaminhamento (2). Ao receber uma mensagem PATH (3), o receptor responde com uma mensagem RESV (reserva de caminho) para requisitar recursos para o fluxo (4). Cada encaminhador intermediário, ao longo do caminho, pode rejeitar ou aceitar as requisições da mensagem RESV (5), (6). No caso de a mensagem ser rejeitada, o encaminhador envia uma mensagem de erro para o receptor e o processo de sinalização termina. Se a sinalização é aceite, a largura de banda e o espaço dos *buffers* são alocados para cada fluxo, e as informações de estado do fluxo são instaladas no encaminhador [Santos, 2004]. Neste período de tempo, o emissor do serviço tem uma faixa da largura de banda disponível para transmitir os seus dados.

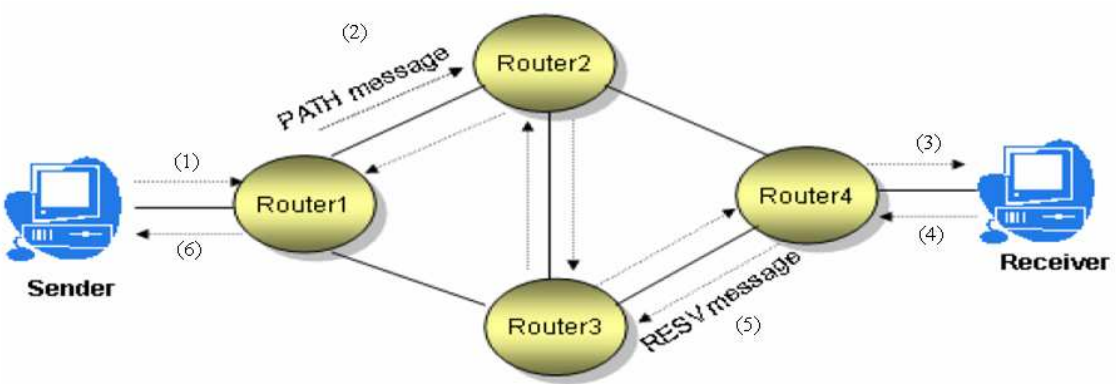



**Figura 3.1 – Configurações básicas de operações de reserva de recursos do protocolo de sinalização RSVP [LEE, 2006].**

O modelo de Serviços Integrados, conforme mostra a Figura 3.2 consiste em cinco componentes: o Classificador e Calendarizador de pacotes (*Scheduling*), o Controle de Admissão de recursos, o Protocolo de sinalização RSVP e o Policiamento.

Quando o encaminhador recebe um pacote o classificador realiza uma classificação MF (*Multi-Field*) e coloca o pacote numa fila específica baseada no resultado da classificação. A calendarização gere o encaminhamento dos vários pacotes através da utilização de uma disciplina de filas.

O Controlo de Admissão de recursos implementa o algoritmo que o encaminhador utiliza para verificar se o novo fluxo tem o seu pedido de QoS, sem interferir nas garantias feitas anteriormente para os fluxos existentes no encaminhador.

O protocolo RSVP é utilizado por uma aplicação para informar à rede os seus requisitos de QoS e efectuar a reserva de recursos ao longo do caminho que o pacote percorrerá.

O Policiamento verifica se o fluxo está de acordo com as especificações negociadas na fase de estabelecimento da conexão.

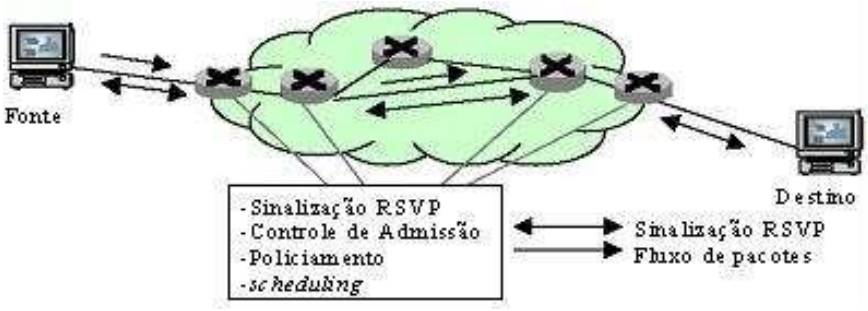



**Figura 3.2 – Modelo IntServ.**

O *IntServ* fornece duas classes de serviço: o *Serviço Garantido*, para as aplicações que requerem um atraso fixo, e o *Serviço de Carga Controlada* para aplicações que requerem um

serviço “melhor esforço” mais fiável e melhorado. Na Figura 3.3 são ilustradas as diferentes classes existentes na arquitectura IntServ [Tanembaum, 2003].

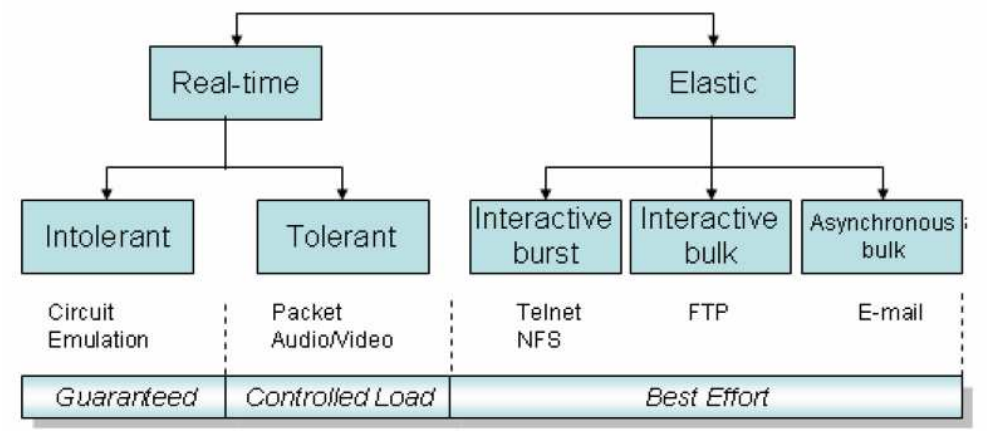



**Figura 3.3 – Fontes de tráfego para a arquitectura IntServ [LEE, 2006].**

O *Serviço Garantido* foi definido para fornecer um nível assegurado de largura de banda, um limite de atraso ponto-a-ponto e nenhuma perda nas filas. É utilizado nas aplicações que correm em tempo real.

A definição do *Serviço de Carga Controlada* não inclui qualquer garantia quantitativa mas sim “a aparência de uma rede menos carregada”. Suporta uma classe ampla de aplicações desenvolvidas originalmente para a Internet actual, mas é altamente sensível à sobrecarga da rede. É apropriada para ser utilizada por aplicações que podem tolerar uma quantia limitada de perdas e atrasos, bem como aplicações adaptativas que correm em tempo real. Visa aproximar o seu comportamento ao das aplicações que recebem o serviço “melhor esforço” durante as condições não sobrecarregadas.

Existem duas grandes limitações na arquitectura dos Serviços Integrados nomeadamente a grande quantidade de informação de estado e a quantidade de componentes que constituem os Serviços Integrados. A quantidade de informação de estado aumenta proporcionalmente com o número de fluxos. Isto exige um enorme espaço de armazenamento e gera sobrecarga de processamento nos encaminhadores. Por esta razão, esta arquitectura não é escalável para o núcleo da Internet. As exigências nos encaminhadores são altas. Todos os encaminhadores devem implementar RSVP, controle de admissão, classificação MF e a calendarização de pacotes. Posto isto, o modelo IntServ é implementado apenas num número limitado de redes. Consequentemente o IETF procedeu ao desenvolvimento do DiffServ como uma alternativa à aproximação do QoS com menor complexidade [LEE, 2006].

### 3.3.2 DiffServ

Devido aos problemas de escalabilidade e por dificuldades na implementação dos Serviços Integrados e do protocolo RSVP, foram introduzidos os Serviços Diferenciados (DiffServ) [RFC 2474, 1998].

O modelo DiffServ implementa QoS com base na definição de tipos de classes. No cabeçalho do pacote IP, existe um campo denominado de TOS (*Type of Service*) que pode identificar o tipo de serviço. No entanto, os serviços diferenciados ampliam a representação de serviços e o tratamento que pode ser dado para encaminhar um pacote através da definição de um novo *layout* para o TOS. Este *layout* é denominado de DS *Field* (*Differentiated Service Field*) e encontra-se ilustrado na Figura 3.4. No DS *Field*, são codificadas as classes para serviços diferenciados. Cada campo DS corresponde a um tratamento diferente de encaminhamento chamado PHP (*Per Hop Behavior*) em cada nó ou encaminhador.

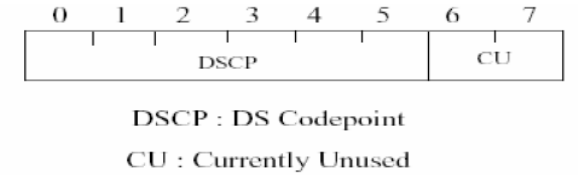



**Figura 3.4 –O campo DS [LEE, 2006]**

A arquitectura DiffServ parte do princípio que os domínios adjacentes têm um acordo sobre os serviços que são disponibilizados entre eles. Este acordo denomina-se SLA (*Service Level Agreement*). Um SLA determina, de uma forma simples, as classes de serviços suportados e a quantidade de tráfego entre os domínios. Os domínios podem definir um SLA estático (renovação agendada) ou dinâmico. Para este último é necessário um protocolo de sinalização e controle para gerir a banda.

Dois novos tipos de classes de serviços especiais surgem juntamente com os modelos de serviços diferenciados: AF (*Assured Forwarding*) e EF (*Expedited Forwarding*).

Os serviços Assegurados (AF) são:

- Serviços para clientes que precisam de segurança dos seus provedores para os serviços no momento em que haja um congestionamento;
- Serviços que emulam o comportamento de uma rede com pouca carga mesmo durante a ocorrência de congestionamento;
- Serviços onde a latência negociada é garantida com um alto grau de probabilidade;
- Responsáveis pela definição de níveis de prioridade de tráfego (Ouro, Prata, Bronze e “melhor esforço”), e;

- Serviços nos quais para cada nível de prioridade são definidos 3 preferências de rejeição de pacotes.

Os serviços *Expedited Forwarding* – Premium (EF) são:

- Para aplicações que necessitam de baixo atraso e de baixa variação de atraso;
- Para fornecer o melhor nível de qualidade de serviço;
- Serviços que emulam uma linha dedicada convencional minimizando os atrasos, probabilidade de perda e variação de atraso para os pacotes, e;
- Serviços que utilizam mecanismos de *traffic shapping*, *buffering* e prioridades de filas.

Existem alguns tipos de serviços que não podem conviver sem garantias de QoS. Consequentemente, é inserido um componente mediador no modelo para gerir os recursos no domínio QoS. Este componente é denominado de BB (*Bandwidth Broker*). O BB trabalha como um gestor de recursos do domínio que tem como função básica controlar a largura de banda, as políticas e prioridades dentro e entre as organizações. Aquando uma solicitação de um fluxo, o BB é o componente que verifica a disponibilidade de recursos e a autorização do cliente para a conexão dentro do domínio QoS. O BB também se encarrega de fazer as alocações necessárias para a comunicação dentro do seu domínio. Caso o pedido de conexão seja fora do domínio, o BB pede ao BB do domínio adjacente para fazer o mesmo. O processo de solicitação de alocação de recursos é realizado continuamente entre BBs adjacentes até chegar ao BB do domínio do receptor. O protocolo de sinalização para a alocação de recursos entre os BBs pode ser o RSVP.

O tráfego que passa pelos encaminhadores DiffServ é tratado de forma agregada. A diferenciação de serviços é obtida através do campo DS que dita o tratamento que o pacote deve obter num determinado encaminhador (PHB – *Per Hop Behavior*). A complexidade é deixada para os encaminhadores de borda, enquanto os encaminhadores do núcleo mantêm-se simples. Na Figura 3.5 é esquematizada a filosofia DiffServ.

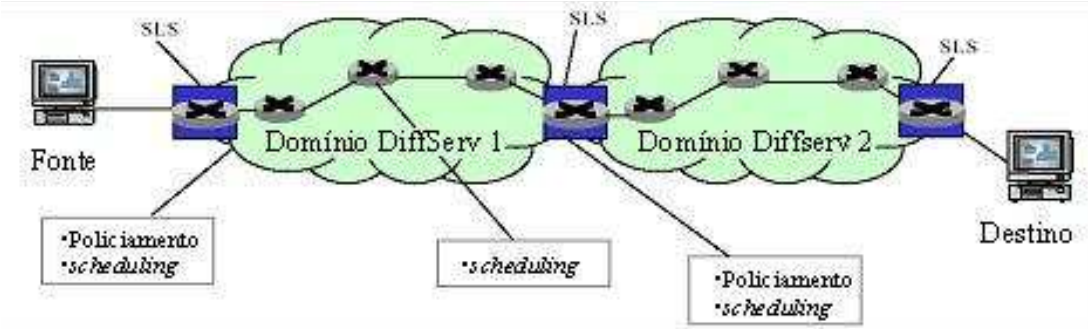



**Figura 3.5 – Modelo DiffServ**

Os Serviços Diferenciados têm sido o modelo mais utilizado para a implementação de QoS. O DiffServ necessita de menos encaminhadores, de pouca actualização de software para fornecer bons métodos de classificação, policiamento, montagem e remarcação de pacotes.

As vantagens de utilizar a arquitectura de serviços diferenciados são:

- A simples forma de diferenciação das classes de serviços para um ISP (*Internet Service Provider*) que tem como base uma tarifa diferenciada;
- A gestão de classes de tráfego aplicada aos fluxos agregados que não requer a utilização explícita de nenhum protocolo de sinalização, e;
- Resolução dos problemas de escalabilidade do IntServ em relação aos encaminhadores do núcleo da rede e em relação às funções complexas que são realizadas apenas na borda da rede.

Os problemas com a arquitectura de serviços diferenciados são:

- A complexidade crescente das técnicas de configuração e do dimensionamento do núcleo da rede;
- Falta de maturidade destas técnicas;
- Importância da Engenharia de Tráfego tomar conhecimento com precisão dos perfis do tráfego e os volumes que transitam nos nós da rede bem como a topologia da rede e os diferentes encaminhamentos. Esta informação nem sem é disponibilizada, e;
- As garantias de QoS são relativas a uma classe de tráfego agregada e não a um fluxo de dados [LEE, 2006].

### 3.3.3 *Multiprotocol Label Switching*

O *Multiprotocol Label Switching* (MPLS) é mecanismo especificado pela *Internet Engineering Task Force* (IETF) que fornece eficiência no encaminhamento de fluxos de tráfego na rede através do *forwarding* (procedimento de envio de pacotes para o próximo encaminhador) e da comutação. O MPLS proporciona orientação à conexão para as tecnologias não orientadas à conexão, como é o caso do IP e *Ethernet*, pois oferece uma maior garantia de funcionamento às aplicações. Localiza-se entre as camadas 2 e 3 do modelo TCP/IP e permite uma melhor interacção entre elas, pois acelera o processo de comunicação entre as camadas 2 e 3. A rápida expansão da Internet e o aumento de procura da largura de banda por parte dos clientes dos ISPs (*Internet Service Providers*) estimularam o desenvolvimento desta tecnologia de forma a suportar o crescimento das redes (escalabilidade). A crescente busca por largura de banda provoca um aumento no número de nós da rede, de tabelas de encaminhamento e de fluxos que passam por cada nó da rede. Outro factor importante que contribuiu para o desenvolvimento desta tecnologia foi a necessidade de propagar a funcionalidade de encaminhamento da Internet e das redes IP em geral.

Alterar o encaminhamento IP tem um custo elevado, pois é necessário alterar o plano de controlo e o algoritmo de encaminhamento, que geralmente é implementado no *hardware.* Uma das vantagens de atribuir etiquetas aos pacotes é a alteração do plano de controlo sem a necessidade de se alterar o algoritmo de encaminhamento [RFC 3031, 2001].

A componente principal das redes IP é o encaminhador, cuja tarefa é o encaminhamento de pacotes. Esta tarefa é complexa pois os encaminhadores efectuam uma gama de serviços e suportam diversos protocolos. Por outro lado, os comutadores são mais simples, pois suportam poucos protocolos e tipos de interface. Isto faz com que a relação custo/desempenho dos comutadores seja melhor que a dos encaminhadores. O principal desafio do MPLS é construir dispositivos que inclua a maioria das funcionalidades dos encaminhadores e que possuam hardware semelhante ao do comutador. Portanto, foram adicionadas funcionalidades extras nos encaminhadores de forma a suportar a Engenharia de Tráfego e a QoS [IEC b, 2007].

O encaminhamento IP convencional – SPF (*Shortest Path First*) – é fonte de dois problemas: o atraso de propagação dos pacotes na rede e o congestionamento da rede. A comutação IP é a solução do problema do atraso de propagação enquanto a Engenharia de Tráfego é a solução do problema do congestionamento. O MPLS integra ambas as soluções, ou seja, o encaminhamento no nível da camada de rede é integrado, comuta por etiquetas e suporta a Engenharia de Tráfego. O objectivo da implementação do MPLS é reduzir os custos, melhorar o desempenho do encaminhamento e permitir a flexibilidade na introdução de novos serviços e novos elementos na rede.

**Encaminhamento IP Convencional**

Quando recebe um datagrama, o encaminhador efectua uma procura na sua tabela de encaminhamento para determinar o próximo salto do percurso. Nos *backbones* IP, o número de entradas na tabela de encaminhamento está na ordem dos milhares. Como consequência a procura é demorada, o que provoca atrasos na propagação dos pacotes na rede. Para além do tamanho da tabela, existe o problema da forma de como são guardados os registos na tabela. Na agregação de endereços proporcionada pelo CIDR (*Classes Inter-domain Routing*) onde o prefixo de rede possui um tamanho variável, os protocolos de encaminhamento propagam tais prefixos para serem armazenados nas tabelas de encaminhamento.

O encaminhador recebe um datagrama IP e procura na tabela de encaminhamento o prefixo mais longo que coincida com o endereço de destino encontrado no cabeçalho do datagrama. Como consequências tem-se a elevada variação de atraso capaz de inviabilizar os serviços, o problema do tráfego se concentrar em determinadas ligações enquanto outras permanecem sem uso e o problema do congestionamento (provocado pelo tráfego concentrado em certas ligações) [Rexford, 2006].

**Componentes da Rede MPLS**

De seguida são apresentados os componentes da rede MPLS de forma a compreender-se a criação do encaminhamento dos pacotes e o funcionamento desta rede.

Os encaminhadores de comutação de etiquetas (LSR - *Label Switch Router*) são os equipamentos responsáveis pela comutação do protocolo MPLS. Isto proporciona um aumento da velocidade de encaminhamento no núcleo da rede MPLS. Quando um LSR se localiza na periferia da rede MPLS denomina-se LSR de ingresso ou egresso, enquanto os situados no núcleo da rede denominam-se LSR de núcleo, conforme ilustra a Figura 3.6. O LSR de ingresso tem a função de inserir a etiqueta e associá-la a uma classe de equivalências (FEC – *Forwarding Equivalence Class*) e encaminhá-la num caminho de comutação de etiquetas (LSP – *Label Switching Path*). O LSR de egresso é responsável por retirar a etiqueta e entregar o pacote à rede não MPLS. O LSR de núcleo tem a função de encaminhar os pacotes de acordo com a informação contida na etiqueta. Ao receber o pacote, cada LSR de núcleo troca a etiqueta existente por uma sua e envia para o próximo LSR. O conjunto dos vários LSR é denominado de nuvem MPLS [Andrade, 2003].

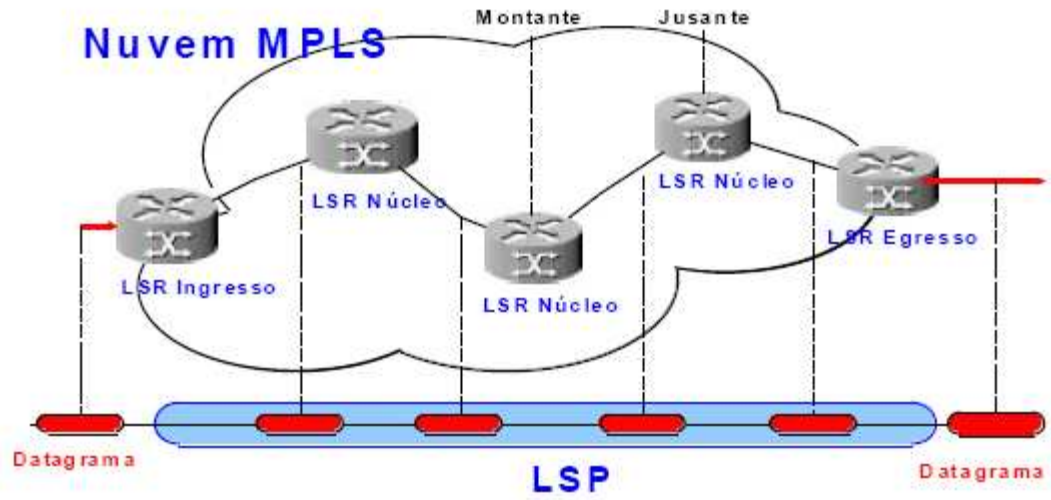



**Figura 3.6 – Principais elementos MPLS [Andrade, 2003].**

As etiquetas são de tamanho fixo e são colocadas nos pacotes durante o seu percurso na rede MPLS. As etiquetas são inseridas pelo LSR de ingresso e são removidas pelo LSR de egresso. Desta maneira, a etiqueta não é identificada fora da rede MPLS. Para um LSR associar uma etiqueta a um pacote é necessário conhecer quais as etiquetas estipuladas pelos LSR adjacentes. Isto deve-se ao facto da etiqueta de saída, que pertence a uma posição na tabela de um LSR, ser determinada pelo LSR que recebe o pacote com a etiqueta em questão. Logo, é necessário existir um protocolo de distribuição de etiquetas. Existem vários protocolos de distribuição de etiquetas. Dois exemplos comuns destes protocolos são o MPLS-LDP (*Laber Distribution Protocol*) e o MPLS-CR-LDP (*Constraint-based Routing Label Distribution Protocol*) [Stephen, 2001].

O cabeçalho MPLS é posicionado depois do cabeçalho da camada 2 e antes do cabeçalho da camada 3 e é conhecido como *Shim Header*. Nas redes MPLS baseadas no protocolo IP, alguns bytes são inseridos antes do cabeçalho IP com o objectivo de fazer o papel da etiqueta. A etiqueta está representada na Figura 3.7.

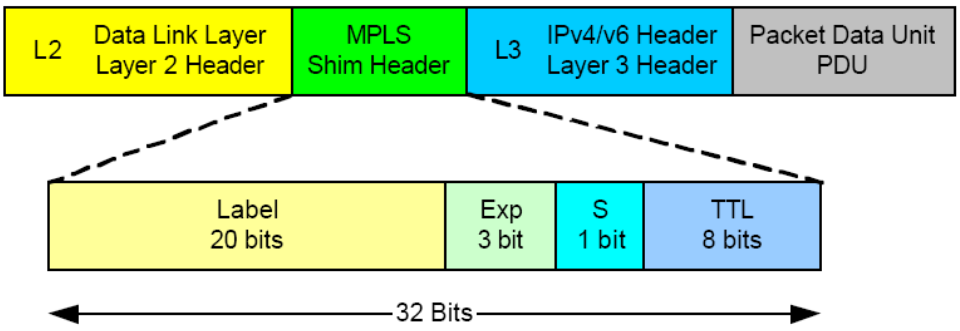



**Figura 3.7 – A etiqueta *Shim Header* do MPLS [Yip, 2002].**

Os primeiros 20 bits da etiqueta representam a identificação da etiqueta. Os 3 bits de EXP (*Experimental*) e a classe de serviço (CoS – *Class of Service*) ao qual o pacote pertence, são utilizados para alterar os algoritmos de fila e de rejeição de pacotes. Com isto, é possível dar prioridades a certos pacotes. O bit S (*Stack*) permite a criação de uma pilha hierárquica de etiquetas, para o caso de o pacote receber mais do que uma etiqueta. O campo TTL (*Time To Live*) tem o mesmo papel que no IP, ou seja, conta o número de encaminhadores por onde passa o pacote, num total de 255. No caso do pacote percorrer a rede por mais de 255 encaminhadores, este é descartado para evitar possíveis *loops* [Stephen, 2001, Rexford, 2006, Brodkin, 2007].

### FEC (*Forwarding Equivalency Class*)

Uma FEC consiste numa classe de equivalência, ou seja, um grupo que contém um conjunto de parâmetros que determinam o caminho para os pacotes. Os pacotes associados a uma mesma FEC são encaminhados pelo mesmo caminho. A FEC é representada por uma etiqueta e cada LSP é associada a uma FEC. Ao receber um pacote o LSR de ingresso da rede MPLS verifica a FEC ao qual o pacote pertence e encaminha-o para a LSP correspondente. A união entre o pacote e a FEC acontece apenas ao entrar na rede MPLS. Isto proporciona uma grande flexibilidade e escalabilidade a este tipo de rede.

A FEC pode ser determinada por um ou mais parâmetros, especificados pelo gestor de rede. Alguns destes parâmetros são nomeadamente o endereço IP (da fonte, destino ou rede), o número da porta (da fonte ou do destino), a identificação (ID) do protocolo IP e a QoS [LEE, 2006].

**LSP (*Label Switch Path*)**

O LSP (*Label Switching Path*) é um percurso por onde passam os pacotes na rede MPLS. Quando o pacote entra na rede MPLS, é associado a uma classe de equivalências (FEC – *Forwarding Equivalence Class*) onde é criado uma LSP para esta FEC. Como a criação da LSP ocorre apenas na entrada da rede MPLS os restantes encaminhadores apenas verificam os rótulos e encaminham o pacote de acordo com a LSP pré-determinada, sem precisar de fazer encaminhamentos adicionais aos pacotes. As etiquetas são distribuídas no momento em que são estabelecidas as LSP. Existem dois modelos de estabelecimento de LSP: o modelo orientado aos dados e o modelo orientado ao controlo. No modelo orientado aos dados, as etiquetas são alocadas em resposta à chegada dos fluxos de pacotes de dados dos utilizadores de rede. No modelo orientado ao controlo, as associações são estabelecidas em resposta ao controlo de tráfego. Isto inclui a utilização do protocolo IP, a alteração do encaminhamento ou a alteração da topologia da rede.

Existem duas opções para activar o LSP: o CR-LSP (*Constraint Routing – Label Switching Path*) e o ER-LSP (*Explicit Routing – Label Switching Path*) [Stephen, 2001, Rexford, 2006]. No encaminhamento CR-LSP o próximo salto de uma FEC é seleccionado em cada LSR. A selecção do salto baseia-se nos parâmetros de congestionamento de tráfego ou do tamanho do *buffer*. Esta selecção é efectuada de uma forma dinâmica. No encaminhamento ER-LSP o LSR de ingresso específica a lista de nós pelo qual o tráfego passará. Este tipo de encaminhamento baseia-se nas informações pré-definidas pelo administrador da rede. Apesar de ser o mais adequado, pode não ser o mais eficiente. Assim o encaminhamento ER-LSP é um processo manual que requer algum planeamento e análise da rede de forma a ser determinado. Consequentemente, o encaminhamento ER-LSP não é efectuado dinamicamente. Estas duas opções de activação de LSP também podem ser utilizadas em simultâneo, segundo [Yip, 2002]. Uma LSP é unidireccional, logo é necessário ter duas LSP para uma comunicação entre duas entidades.

O LIB (*Label Information Base*) contém uma tabela de encaminhamento que contem informações que correlacionam as etiquetas às interfaces do encaminhador. Uma vez criada a LSP, a relação da etiqueta com a interface é armazenada no LIB. Quando o pacote entra no LSR, este verifica a interface para qual o pacote deve ser encaminhado, para que o mesmo alcance o próximo nó. Desta forma, o LIB contém uma tabela que é utilizada para adicionar ou remover a etiqueta a um pacote, enquanto determina a interface de saída pela qual o pacote deve ser enviado [LEE, 2006].

**Protocolos de Sinalização do MPLS**

Os protocolos de sinalização mais comuns do MPLS são o LDP (*Label Distribution Path*), o CR-LDP (*Constraint-based Routing Label Distribution Protocol*) e o RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) [Yip, 2002]. Estes protocolos têm como objectivo distribuir as etiquetas e estabelecer os caminhos LSP.

O LDP é um protocolo que permite a distribuição de etiquetas entre os LSR de forma a criar as LSP. Para isto, o LDP disponibiliza um mecanismo de "descoberta" de LSR que permite aos LSR se encontrarem uns aos outros e estabelecer a comunicação. O LDP é transferido pela rede sobre o TCP para garantir a entrega das mensagens. O LDP possui um sistema de serviço de mensagens, com o intuito de autenticar as LSPs [Yip, 2002]. A Tabela 3.1 explica a utilização de cada mensagem.

**Tabela 3.1 – Utilização das Mensagens LDP.**

| | |
|---|---|
| ***Request*** | Solicitar uma LSP através do envio da mensagem de Requisição que circula entre o nó de ingresso e o nó de egresso. |
| ***Mapping*** | Mapear a autenticação da requisição através da mensagem *Mapping* entre o nó de egresso e o nó de ingresso. |
| ***Withdraw*** | Mensagem para desfazer um caminho |
| ***Release*** | Mensagem para libertar a LSP feita previamente |
| ***Notification*** | Mensagem de notificação (pode ser de falha) |

O CR-LDP [Yip, 2002] é um protocolo de sinalização que permite o estabelecimento de caminhos explícitos com parâmetros de QoS associados aos mesmos. Estes caminhos, denominados CR-LSP, são semelhantes aos LSP do LDP. A diferença é que, enquanto os LSPs estabelecidos pelo LDP são baseados nas informações da tabela de encaminhamento, os CR-LSP são calculados a partir de um ponto na borda da rede de acordo com vários critérios. Desta forma, podem-se atribuir características especiais às CR-LSP, tais como a garantia de uma certa largura de banda ou forçar caminhos físicos diferentes dentro da rede. Assim, o LDP e o CR-LDP possuem um esquema de codificação denominado TLV (*Type-Length-Value*) ou Tipo-Comprimento-Valor. Trata-se de mensagens passadas pela rede, que estão divididas em três campos básicos. O campo Tipo define o tipo de mensagem, o campo Comprimento específica o campo seguinte em bytes e o campo Valor codifica a informação interpretada de acordo com o campo Tipo. O CR-LDP descreve uma série de TLV de modo a suportar características como o encaminhamento explícito, a especificação de parâmetros de tráfego, a fixação do caminho, a preempção do caminho através de prioridades, a gestão de falhas, o LSPID (identificador Único de uma CR-LSP dentro da rede MPLS) e a classe de recursos.

O protocolo RSVP pode ser utilizado numa rede MPLS para a distribuição de etiquetas entre os LSR. O protocolo RSVP-TE padrão adiciona algumas características ao protocolo RSVP, para

permitir o estabelecimento de túneis LSP nas redes MPLS. Isto permite manter o nível de qualidade de serviço da engenharia de tráfego solicitada por uma aplicação. O RSVP-TE funciona como um protocolo de sinalização de uma rede MPLS. O protocolo RSVP-TE estabelece um caminho para o fluxo de dados entre o equipamento de origem e o equipamento de destino do cliente. A sua característica principal é de poder fazer reservas de recursos para cada fluxo de dados, de acordo com a qualidade de serviço desejada. O conceito de fluxo de dados fica mais caracterizado com a utilização da arquitectura MPLS e o estabelecimento de túneis LSP. Assim como o RSVP, o RSVP-TE também utiliza os conceitos definidos na arquitectura IntServ, para fornecer os níveis de qualidade de serviço para cada túnel LSP (o Controlo Carregado, a Garantia de Serviço e o "melhor esforço") [Iselt, 2004].

**Funcionamento da rede MPLS**

Quando um pacote é enviado de um encaminhador para outro, através de um protocolo de rede sem conexão, cada encaminhador analisa o pacote e toma decisões independentes sobre o caminho para onde enviar o pacote. Isto significa que cada encaminhador analisa o cabeçalho e corre o seu próprio algoritmo de encaminhamento. Porém, o cabeçalho dos pacotes contém informação adicional para determinar o próximo salto. A tarefa de encaminhar um pacote pela rede pode ser dividida em duas operações distintas. A primeira operação consiste em determinar as FEC, que são todas as possibilidades de encaminhamento de um pacote através da rede. A segunda operação consiste em correlacionar cada FEC a um próximo salto.

Cada FEC está relacionada a um LSP. Os LSPs são caminhos determinados dentro da nuvem MPLS. Uma FEC pode ser associada a mais de um LSP, porém, todos apresentam a mesma origem e o mesmo destino. No encaminhamento convencional, cada encaminhador da rede associa dois pacotes à mesma FEC. No MPLS a associação do pacote a uma determinada FEC é efectuada apenas uma vez, que é quando o pacote entra na rede através do LSR de ingresso. A FEC, à qual o pacote está associado, é codificada através de uma etiqueta de tamanho fixo inserida entre a camada de ligação e a camada de rede.

Nos saltos subsequentes não existe nenhuma análise do cabeçalho da camada de rede ao pacote. Em cada encaminhador comutador de etiquetas que o pacote passa, as etiquetas são trocadas, pois a etiqueta representa um índice na tabela de encaminhamento do próximo encaminhador. Assim, quando o pacote com etiqueta entra na LSR, o encaminhador procura na sua tabela o índice representado pela etiqueta. Ao encontrar este índice, o encaminhador substitui a etiqueta de entrada pela etiqueta de saída associada à FEC ao qual pertence o pacote. Depois de completar a operação de troca de etiquetas o pacote é encaminhado pela interface especificada na tabela de encaminhamento. Quando o pacote chega ao LSR de egresso da rede MPLS, a etiqueta é

removida e o pacote é encaminhado pela interface associada à FEC ao qual pertence o pacote [Cheung, 2003].

**Vantagens do MPLS**

A primeira vantagem do MPLS é que o encaminhamento poder ser feito apenas com comutadores que desempenham o papel de encaminhadores. Geralmente, os comutadores realizam as tarefas de pesquisa e troca de etiquetas, mas não analisam o cabeçalho da camada de rede, ou não o fazem rapidamente. A utilização de comutadores no lugar dos encaminhadores é vantajosa, uma vez que são mais baratos e operam a velocidades superiores à dos encaminhadores. Outra vantagem introduzida pelo MPLS é o facto de os pacotes serem analisados apenas uma vez, quando entram na rede MPLS. Desta forma, o encaminhador de ingresso pode utilizar a informação sobre o pacote, que não está presente no cabeçalho da camada de rede, para determinar a FEC ao qual pertence o pacote. Como a parte pesada do processamento dos pacotes é efectuada nas bordas da rede, o núcleo da rede pode operar mais folgadamente. Isto é uma grande vantagem para as redes núcleo, uma vez que a taxa de pacotes por segundo no núcleo da rede é maior do que a taxa de pacotes nas bordas.

Devido a estes aspectos, é possível criar classes de serviços para a diferenciação dos pacotes e aplicar a engenharia de tráfego para não sobrecarregar os caminhos congestionados. Desta forma é possível escolher os caminhos mais rápidos, porém com custo mais elevado, para pacotes de maior prioridade.

### 3.3.4 Engenharia de Tráfego

A Engenharia de Tráfego permite determinar os melhores caminhos para o encaminhamento dinâmico na rede consoante as características dos tráfegos e as suas necessidades de QoS de forma a evitar o congestionamento. De facto, a engenharia de tráfego favorisa a QoS, pois permite dar prioridades às aplicações e alterar o seu caminho de encaminhamento por outro com melhores condições de desempenho de tráfego. A Engenharia de Tráfego optimiza a rede, pois balanceia o tráfego nas possíveis ligações e consequentemente evita deixar os caminhos ociosos.

A Engenharia de Tráfego é definida como um aspecto da Engenharia de Redes que trata da avaliação e optimização do desempenho de redes [LEE, 2006]. Para isto, são utilizados princípios científicos e tecnológicos que possibilitam a medição, a caracterização, a modelação e o controlo do tráfego da rede. Os principais objectivos de desempenho podem ser classificados como:

- Orientados aos recursos: dizem respeito à optimização da utilização dos recursos da rede, de maneira que não haja congestionamento e sobrecarga de certas partes da rede,

bem como pontos onde haja pouca utilização. A principal função da Engenharia de Tráfego é gerir a largura de banda da rede de maneira eficiente, e;

- Orientados ao tráfego: engloba aspectos relacionados com a QoS do tráfego. Melhora as medidas de desempenho tais como a variação de atraso, o atraso, a perda de pacotes e o débito efectivo. Aqui a minimização da perda de pacotes é possível.

Um dos principais objectivos de desempenho, do ponto de vista do tráfego e dos recursos, é minimizar o congestionamento. O congestionamento ocorre sobre dois cenários [LEE, 2006]:

- Os recursos de rede são insuficientes ou inadequados para atender à demanda. Neste caso, pode-se expandir a capacidade da rede, aplicar mecanismos clássicos de controlo de congestionamento (que regulam a demanda ao delimitar o tráfego) ou ambos, e;
- O tráfego é encaminhado de maneira eficiente nos recursos disponíveis. Neste caso, a Engenharia de Tráfego é útil por conseguir encaminhar o tráfego de maneira diferente ao encaminhamento produzido por protocolos de encaminhamento baseados em SFP (*Shortest Path First*) e por realizar um melhor balanceamento de carga.

Historicamente, tem sido difícil efectuar a Engenharia de Tráfego nas redes IP de maneira satisfatória [LEE, 2006]. Tal constatação deve-se às limitações das funcionalidades das tecnologias IP convencionais. As limitações das funções de controlo de encaminhamento interno são outro problema nos sistemas IP. Os protocolos de encaminhamento interno IGP (*Internet Gateway Protocol*) baseados no algoritmo SPF, como o IS-IS (*Intermediate System – Intermediate System*) e o OSPF (*Open Shortest Path First*), são encaminhados de acordo com as decisões de encaminhamento efectuadas recorrendo à instância local de uma tabela de estados. A selecção de encaminhamento é baseada na selecção do menor caminho (menor número de saltos) [LEE, 2006]. Esta abordagem é largamente escalável e distribuída, mas contém falhas. As falhas são que estes protocolos não consideram características do tráfego e as restrições de capacidades da rede ao fazer as decisões. Isto resulta no congestionamento em certas ligações, enquanto outros caminhos permanecem subutilizados. A Engenharia de Tráfego através do encaminhamento CBR (*Constraint Based Routing*) procura corrigir este tipo de problema, pois é exercida uma pressão sobre o fluxo de dados (restrições) com o objectivo de optimizar a eficiência da rede [LEE, 2006].

Os protocolos de encaminhamento IGP utilizam o algoritmo SPF baseado na selecção do caminho com o número menor de saltos. Desta forma, o processo de Engenharia de Tráfego é aperfeiçoado com a utilização do CBR. Com o CBR é possível seleccionar caminhos diferentes dos obtidos pelo SPF baseando-se nas restrições definidas aos parâmetros QoS (atraso, largura de banda, entre outros). O CBR considera fluxos agregados, também conhecido por “fluxos macro”, e não os fluxos individuais ou “micro-fluxos” tal como o fluxo HTTP (*Hypertext transfer protocol*). A função do CBR é seleccionar o caminho de acordo com os critérios de encaminhamento. Existem

dois critérios de encaminhamento: o QBR (Qos-*Based Routing*) e o PBR (*Policy-Based Routing*) [Younis, 2007]. O QBR consiste em realizar encaminhamentos com base na restrição de Qualidade de Serviço (atraso, largura de banda, perda de pacotes ou variação de atraso) solicitada, onde requer a classificação de fluxos e escolhas de caminhos distintos para cada classe. O PBR consiste em escolher caminhos com base em decisões administrativas e dos SLA (*Service Level Agreements*) onde é possível, por exemplo, proibir o tráfego comercial de utilizar certos troços da rede. Os encaminhamentos que satisfazem as restrições têm como objectivo reduzir os custos, balancear a carga da rede e aumentar a segurança.

As estratégias de encaminhamento são classificadas de acordo com os mecanismos que accionam a procura de caminhos que satisfazem o constrangimento solicitado e com o valor do estado mantido. O mecanismo que acciona a procura de caminhos, denominado de encaminhamento DV (*Distance Vector*), distribui o seu cálculo do caminho entre os nós da rede. Cada nó troca, periodicamente, informações dos vectores de distância com os seus vizinhos. Cada nó utiliza a informação dos vectores de distância para calcular os caminhos. A limitação desta abordagem é a falta de conhecimento global da rede que provoca uma convergência lenta e *loops* de encaminhamento. O mecanismo que acciona a procura de caminhos, denominado de encaminhamento LS (*Link State*), distribui periodicamente o estado de todas as ligações locais a todos os nós da rede. Baseado neste estado, o caminho pretendido é determinado localmente. Este tipo de encaminhamento tem as vantagens da simplicidade, da exactidão e evita *loops.* Em contrapartida este encaminhamento tem três limitações que consistem no elevado armazenamento no cabeçalho, na elevada computação exercida no cabeçalho e na elevada actualização do estado no cabeçalho. O encaminhamento DV é proactivo e o encaminhamento LS é reactivo. Segundo [Younis, 2007], o encaminhamento reactivo é o menos popular devido ao seu elevado custo em termos de atraso e valor do estado mantido.

### 3.3.5 Engenharia de Tráfego e o MPLS

A Engenharia de Tráfego pode ser efectuada manualmente ou através de uma técnica automatizada, como o MPLS, que utiliza a QoS para procurar e estabelecer os caminhos mais adequados a determinados conjuntos de fluxos de rede.

O MPLS é largamente utilizado como forma de integrar a Engenharia de Tráfego ao plano de controlo do IP. Desta forma, podem-se destacar os componentes da Engenharia de Tráfego associados ao MPLS [LEE, 2006]: o encaminhamento de pacotes, a distribuição das informações, a selecção do caminho e a selecção da sinalização.

O encaminhamento do pacote ocorre da mesma forma do que no MPLS. A questão essencial fica por conta da escolha de uma LSP que escolheria o caminho mais curto para alcançar o destino.

A componente representada pela distribuição das informações é fundamental na estrutura da Engenharia de Tráfego baseada no MPLS. Isto porque é necessário um conhecimento sobre a topologia da rede, assim como informações dinâmicas sobre a carga da rede. A implementação deste elemento dá-se através das extensões ao IGP de modo que os atributos das ligações sejam incluídos nas mensagens de anúncio distribuídas nos encaminhadores.

A selecção do caminho a ser tomado pelos LSP é baseada num algoritmo denominado CSPF (*Constraint Shortest Path First*) [LEE, 2006] utilizado pelo CBR. Este algoritmo baseia-se em restrições que são atribuídas aos elementos da rede, para determinar um caminho para o LSP. Para isto, é necessário que os atributos associados ao LSP sejam atendidos. A componente sinalização é responsável pelo estabelecimento dos LSP e pela distribuição dos rótulos no MPLS. Estes são, nomeadamente, o LDP e o RSVP.

## 3.4 RECUPERAÇÃO NAS REDES MPLS

A resiliência é a capacidade de reagir perante uma falha através de estratégias de encaminhamentos, enquanto a fiabilidade trata de minimizar as falhas através da redundância dos elementos de rede. Proporcionar resiliência nas redes de dados é muito importante pois assegura o funcionamento e disponibilidade fim-a-fim do serviço.

A implementação da recuperação de falhas no domínio MPLS é efectuada através de mecanismos e modelos de recuperação. No [RFC 3469, 2003] existe a terminologia definida para a recuperação no domínio MPLS. Seguem as explicações dos termos que serão utilizadas nesta dissertação.

O *caminho de trabalho* refere-se ao caminho que carrega o tráfego antes de ocorrer a falha. O *caminho de recuperação* é o caminho para o qual o caminho de trabalho comuta na ocorrência de uma falha. No *caminho de comutação LSR* (PSL – *Path Switch LSR*), o LSR *upstream* da falha é responsável pela comutação do tráfego entre o caminho de trabalho e o caminho de recuperação. No *ponto de reparação* (POR – *Point of Repair*) o LSR é configurado para desempenhar a recuperação MPLS, ou seja, é responsável pela reparação do LSP. O *sinal de indicação de falha* (FIS – *Fault Indication Signal*) é a mensagem que indica a existência da falha no caminho. Esta mensagem é enviada por cada LSR para o seu vizinho *upstream* ou *downstream*, até chegar ao LSR configurado para desempenhar a recuperação MPLS no POR. O FIS é enviado periodicamente, pelo nó ou pelos nós mais próximos, ao ponto de falha durante um limite de tempo configurável. O FRS (*Fault Repair Signal*) é a mensagem que indica se a falha no caminho de trabalho está ou não reparada. O FRS tem o mesmo comportamento que o FIS em termos de distribuir a sua informação.

### 3.4.1 Detecção e Notificação de Falhas no MPLS

Como citado anteriormente, o MPLS introduz uma nova camada no modelo da rede (entre a camada 2 e a camada 3) independente das restantes camadas existentes na rede. Desta forma, é necessário que o MPLS tenha os seus próprios mecanismos de detecção e de notificação de falhas. Mesmo que as camadas inferiores tenham mecanismos de detecção e de notificação de falhas mais rápidas, nada pode ser assumido nessas mesmas camadas, uma vez que o MPLS funciona com muitos tipos de redes diferentes.

A extensão RSVP-TE *Hello* (*Resource Reservation Protocol – Traffic Extention*) […] permite que os LSR detectem quando um nó adjacente não é alcançável. A extensão é composta por uma mensagem *Hello,* um objecto HELLO REQUEST e um objecto HELLO ACK. No caso de o LSR não receber nenhuma mensagem *Hello* dentro de um intervalo de tempo configurado (3,5ms ou 5ms), o nó presume uma possível falha e notifica a rede. O RSVP-TE é utilizado para verificar se o plano de controlo (*control plane*) encontra-se a funcionar e se o LSR é alcançável. Este mecanismo não é utilizado para verificar o plano de dados (*data plane*).

O protocolo RSVP-TE é um protocolo *soft state.* Isto significa que os LSP sinalizados juntamente com o RSVP-TE são actualizados constantemente com as mensagens PATH e RESV. No caso das mensagens PATH ou RESV não actualizarem o LSP, a mensagem PathErr ou ResvErr é enviada desde o ponto de falha até ao LSR de ingresso do LSP. O valor do intervalo *refresh* é muitas vezes configurado para 30s. Isto torna as mensagens *refresh* da detecção de falhas pelo *soft state* impróprias para os mecanismos de *fast reroute* (reencaminhamento rápido).

O mecanismo modelado pelo paradigma *Ping/Traceroute* verifica o plano de dados do LSR no LSP. Com este modelo, é possível verificar se os pacotes que pertencem a um dado FEC, chegam ao fim do seu LSP através dos LSR pretendidos e vão em direcção ao LSR de egresso correcto. O modo *ping* verifica se a FEC chega ao LSR de egresso correcto e o modo *traceroute* verifica se o FEC percorre todos os LSR pretendidos até chegar ao LSR egresso. No caso de falhar a recepção do *ping,* é accionado o *traceroute* para localizar a falha. As falhas, tanto no plano de dados como no plano de controlo, não são detectadas rapidamente. Isto sobrecarrega os LSR de trânsito.

As falhas também podem ser detectadas pelos mecanismos das camadas mais inferiores e reportadas à camada MPLS. Neste caso, a recuperação é desempenhada na camada inferior bem como nas camadas MPLS. Isto significa que o MPLS actua no acto da detecção da falha. Quando a operação de recuperação é finalizada pelo MPLS, a recuperação da camada inferior finaliza o seu próprio mecanismo de recuperação e a ligação volta de novo a funcionar. Depois, o MPLS reconhece que a componente de falha recomeçou a funcionar e que o LSP pode ser reencaminhado

de volta para o caminho de trabalho. Os mecanismos de detecção nas camadas inferiores são muitas vezes mais rápidos do que o mecanismo de detecção de falhas associadas ao MPLS. Assim, é preferível utilizar este tipo de mecanismo de detecção e notificação de falhas se estiver disponível [Rozycki et al, 2008].

### 3.4.2 Mecanismos de recuperação no MPLS

Tal como o mecanismo de recuperação nas outras camadas, a recuperação do MPLS opera através do *forwarding* (envio) de tráfego num novo caminho à volta do ponto de falha na rede. O posicionamento deste lugar, quando calculado e configurado, depende do mecanismo de recuperação utilizado. No caso de não ser utilizado nenhum mecanismo de recuperação no domínio MPLS, a recuperação é desempenhada pelo protocolo utilizado para configurar e manter o LSP. O tempo de recuperação deste esquema é tipicamente longo e é apenas aceitável para o tipo de tráfego "melhor esforço". No caso de querer desempenhar a recuperação de uma forma mais rápida, há necessidade de serem utilizados outros mecanismos de MPLS para minimizar o tempo de notificação de falha ou diminuir o tempo de cálculo do caminho de recuperação.

Os mecanismos de configuração dos caminhos de recuperação são classificados de acordo com dois critérios: recuperação local versus recuperação global e reencaminhamento versus protecção por comutação.

#### Métodos e Modelos de Recuperação de falhas no MPLS

Existem três métodos de recuperação de falhas no MPLS [Calle et al, 2004]: o caminho de recuperação global, o caminho de recuperação reverso e o caminho de recuperação local.

Na recuperação global, também conhecida por modelo *Makam*, o LSR de ingresso é responsável pelo caminho de recuperação quando recebe uma mensagem FIS. Isto requer um caminho de recuperação não conectado, para cada caminho de trabalho. É no LSR de ingresso que o processo de protecção é iniciado, independentemente do local da falha no LSP. Se não houver um caminho de recuperação atribuído a cada um dos caminhos de trabalho na rede, quando é utilizada a recuperação global, não é causado qualquer tipo de problema. A protecção é iniciada no LSR de ingresso, conforme mostra a Figura 3.8. A vantagem deste método é que apenas é necessário configurar um caminho de recuperação. Como este método de protecção é centralizado, apenas um LSR deve ter as funções de PSL (*Path Switch LSR*). Por outro lado, este método tem um elevado custo (em termos de tempo), uma vez que o FIS é enviado até ao LSR de ingresso. Este método provoca uma elevada taxa de perda de pacotes durante o tempo de comutação. Os caminhos de

recuperação preestabelecidos consomem menos tempo de recuperação do que os caminhos estabelecidos de forma reactiva ou *on demand*.

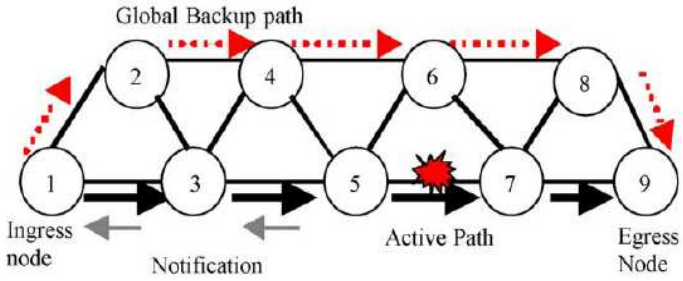



**Figura 3.8 – Recuperação Global [Calle et al, 2004]**

O factor principal do método do caminho de recuperação *Reverse* é o facto de o tráfego voltar no sentido contrário no ponto de falha. Depois percorre o caminho até chegar ao LSR de ingresso para de seguida percorrer o caminho de recuperação global, conforme ilustra a Figura 3.9. O LSP é denominado de *Reverse Backup* LSP. O modelo *Haskin* propõe o mesmo método, mas com o caminho de recuperação preestabelecido, poupando no consumo de tempo de recuperação. A vantagem deste método é a redução da taxa de perda de pacotes, factor crucial para os serviços em tempo real. Outra vantagem deste método é a simplificação da indicação de falha, uma vez que o LSP de recuperação *Reverse* envia uma mensagem FIS ao LSR de ingresso e para o caminho de recuperação ao mesmo tempo. As desvantagens são a má utilização de recursos, o longo comprimento do percurso entre o ponto de falha e o ponto de saída e o tempo de recuperação mais elevado. Os caminhos de recuperação preestabelecidos consomem menos tempo de recuperação do que os caminhos estabelecidos de forma reactiva ou *on demand* [Calle et al, 2004].

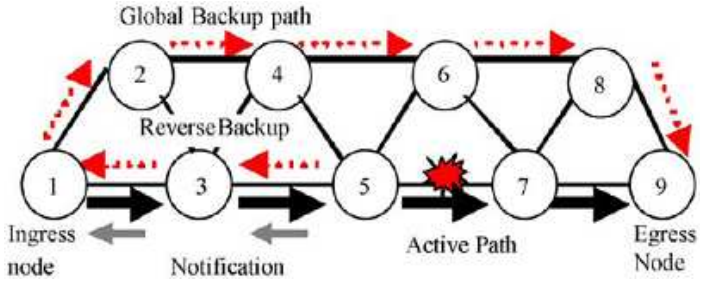



**Figura 3.9 – Recuperação *Reverse* [Calle et al, 2004]**

No método de recuperação local, também conhecido por *fast reroute*, a recuperação inicia-se no LSR mais próximo da falha onde o tráfego contorna e depois o tráfego regressa novamente ao caminho de trabalho, conforme mostra a Figura 3.10. Este método oferece a vantagem do rápido tempo de recuperação em comparação com o método de recuperação global. Outra vantagem da recuperação local é a redução da taxa de perda de pacotes. A desvantagem deste método é a quantidade de caminhos de recuperação que são necessários criar para atender a todo o tipo de falha

que pode acontecer na rede. Consequentemente, ocorre uma utilização baixa de recursos e é aumentada a complexidade da rede [Calle et al, 2004].

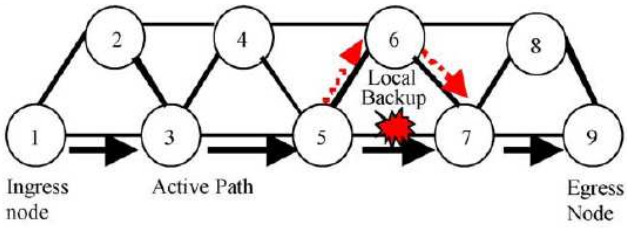



**Figura 3.10 – Recuperação Local [Calle et al, 2004]**

Em ambientes dinâmicos a recuperação local, também conhecida por recuperação regional, actua de forma que o tráfego, em caso de falha, seja comutado no local. No entanto, não volta ao caminho do trabalho mas percorre o caminho de recuperação até ao LSR de egresso, conforme pode ser observado na Figura 3.11 [Calle et al, 2004].

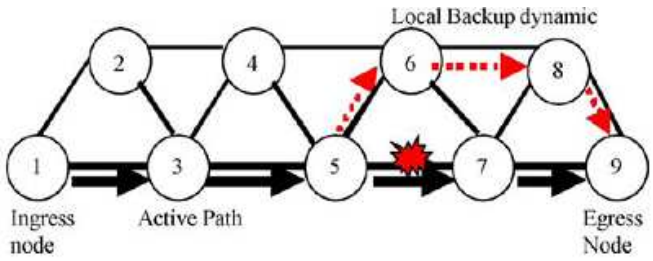



**Figura 3.11 – Recuperação Local em ambientes Dinâmicos [Calle et al, 2004]**

### 3.4.3 Comparação entre a recuperação na camada IP e na camada MPLS

As várias tecnologias que operar em diferentes camadas fornecem capacidades de protecção e de recuperação em escalas diferentes. Estas escalas podem ser referentes a tempos de recuperação (desde a ordem das dezenas de milissegundos aos minutos) à granularidade de diferentes larguras de banda (desde os Kbps aos Gbps) ou à granularidade de diferentes tipos de QoS (desde o tráfego agregado ao fluxo de tráfego individual) [Owens et al, 2002].

Existem 3 tipos de recuperação na rede IP: a recuperação na camada física, a recuperação na camada IP e a recuperação na camada MPLS.

A camada física utiliza a tecnologia de transporte SDH. A recuperação na rede SDH é efectuada através de topologias de rede em anel duplo. Esta topologia tem dois caminhos: o caminho de trabalho e o caminho de protecção. A inutilização do caminho de protecção torna ineficiente a utilização da largura de banda na rede. A recuperação na camada física é rápida, pois a detecção da falha é efectuada no equipamento de rede sem a necessidade do envio de mensagens e a comutação do tráfego para o caminho de protecção é automática. A desvantagem da rede SDH é o elevado custo dos equipamentos de rede.

A recuperação na camada IP é lenta, uma vez que os caminhos de recuperação são seleccionados baseados na prioridade e requisitos do tráfego e exige uma troca de mensagens entre os nós da rede, causando atrasos e reduções da largura de banda da rede. Os elevados atrasos na rede causam a desconexão dos serviços. Isto não tem impacto no tráfego de dados de "melhor-esforço" mas tem um impacto negativo no tráfego de voz e de vídeo.

A tecnologia MPLS é implementada nas redes IP e encontra-se entre as camadas 2 e 3. A tecnologia MPLS permite reestruturar a rede numa topologia em malha. Este tipo de topologia de rede tem a vantagem de oferecer muitas alternativas de encaminhamento ao tráfego na presença de falhas devido à existência de múltiplos caminhos. Nas redes em malha existem mais do que um caminho de protecção para cada caminho de trabalho. Desta forma, é utilizada a recuperação partilhada, onde todos os nós da rede tomem conhecimento das falhas através da troca de mensagens. Como os cabeçalhos dos pacotes são de fácil e rápida leitura na camada MPLS o elevado número de mensagens dentro da rede não provoca grandes atrasos, como acontece na camada IP. A tecnologia MPLS permite aplicar à rede uma variedade de métodos de recuperação de falhas que apresentam valores de tempo de recuperação muito mais rápidos do que aqueles da camada IP.

Posto isto, o reencaminhamento do tráfego nas camadas inferiores é rápido mas requer equipamento de rede dedicado. O reencaminhamento IP é lento mas não depende de uma topologia específica e está implementado em todos os equipamentos da rede. O MPLS é implementado entre a camada 2 e a camada 3, e é possível implementar mecanismos de recuperação que fornecem uma solução de rápida recuperação e de custo reduzido.

A seguir descreve-se a razão pela qual a recuperação deve ser implementada pela camada MPLS e não por outras camadas. A camada IP não tem capacidade de fornecer recuperação de largura de banda, onde requer a capacidade de fornecer um caminho alternativo para o tráfego bem como um caminho onde a largura de banda é equivalente ao do caminho original. Isto é necessário nas redes QoS, pois os utilizadores pagam pela elevada qualidade de serviço. A utilização da recuperação na camada MPLS deve ser motivada, pois a camada IP oferece limitações nos melhoramentos dos tempos de recuperação provocados pelos algoritmos de encaminhamento. Estes algoritmos de encaminhamento requerem o seguimento do processo da detecção da falha, da notificação da falha e dos cálculos do caminho mais curto antes de reencaminhar o tráfego. Nas camadas inferiores o reencaminhamento é efectuado logo após a detecção da falha. A camada MPLS permite a alocação do tráfego IP sobre canais ópticos WDM (*Wavelength Division Multiplexing*) e fornece a opção de recuperação sem a intervenção da camada SDH. Os mecanismos de recuperação nas camadas inferiores não têm a percepção das operações das camadas superiores. Posto isto, é apenas possível a recuperação de uma ligação e não a recuperação de nós nem a

recuperação do tráfego transportado na camada 3. O MPLS oferece à rede, tempos de recuperação de falhas muito reduzidos.

### 3.4.4 *Ethernet* sobre MPLS

Segundo discutido em [RAD, 2008] é possível transportar os pacotes *Ethernet* sobre vários tipos de tecnologias de rede, uma vez que existem dispositivos com interfaces de conversão. É possível transportar o tráfego *Ethernet* sobre a fibra óptica, a tecnologia SDH (*Synchronous Digital Hierarchy*) e o MPLS (*Multiprotocol Label Switching*).

A tecnologia *Ethernet* é considerada barata relativamente a qualquer outro meio, fácil de utilizar através do conceito "*plug-and-play*", ubíquo e tem um plano de controlo simples. Os factores negativos desta tecnologia são [OST, 2006]:

- A ausência dos factores OAM (*Operation, Administration and Maintenance*) resulta numa lenta recuperação de falhas e consequentemente num tempo elevado de convergência. Salienta-se que segundo existe os factores OAM apenas na rede de acesso. Os factores OAM tornam a rede mais fiável;
- Gasto de largura de banda ao descobrir os endereços dos *hosts*;
- A inexistência de mecanismos de prevenção de *loops*, e;
- A ausência do estado da topologia no plano de controlo, a inexistência do balanceamento de carga entre os portos e consequentemente o bloqueio das ligações.

Apesar dos factores negativos acima referidos, existem factores positivos da *Ethernet* que é útil para o transporte de dados, tais como:

- A interface ubíqua;
- A forma como é criada a trama (*Framing*), e;
- A necessidade de separar o plano de dados e o plano de controlo no meio de transmissão para tornar a *Ethernet* uma tecnologia transportadora WAN (*Wide Area Network*).

Os critérios da tecnologia *Ethernet* incluem a escalabilidade, a fiabilidade através da rápida convergência e recuperação dos serviços e a QoS. Para manter e melhorar estes critérios é utilizado o MPLS devido à sua natureza multi-protocolo. Esta natureza é utilizada no transporte, nos serviços e na virtualização e segmentação dos recursos. Sabe-se que as vantagens do MPLS incluem:

- A robustez do plano de controlo de dados;
- A descoberta dos endereços e da topologia no plano de controlo;
- A possibilidade de aplicar a Engenharia de Tráfego;
- A possibilidade de escolher entre os vários métodos de recuperação de falhas;
- A escolha da estrutura da rede e o grau de convergência, e;

- A capacidade de fornecer escalabilidade, fiabilidade e QoS.

A solução *Ethernet over* MPLS, também conhecida por EoMPLS [Juniper, 2007, RFC 4448, 2006], fornece uma infraestrutura convergente baseada nos pacotes *Ethernet*, um plano de controlo IP/MPLS robusto, um plano de dados MPLS escalável e o sistema de "*plug-and-play*" para a rede MPLS. A Figura 3.12 ilustra a arquitectura da rede EoMPLS. Esta arquitectura mostra como a rede núcleo MPLS recebe os dados vindos dos provedores de serviços através da tecnologia *Ethernet* para depois serem entregues à rede de acesso através da tecnologia *Ethernet*. Esta tecnologia é compatível com um número variado de meios de transmissão, conforme mostra a Figura 3.12. A aplicação da tecnologia EoMPLS permite os provedores de serviços criarem circuitos ponto-a-ponto sobre a rede núcleo MPLS através da sinalização LDP. Os provedores primeiro provêm os túneis LSP, depois estabelecem um circuito virtual por cliente. Os dados são transferidos na camada 2 e encapsulados na trama MPLS. As pilhas de etiquetas permitem a agregação sobre um único LSP e fornece escalabilidade.

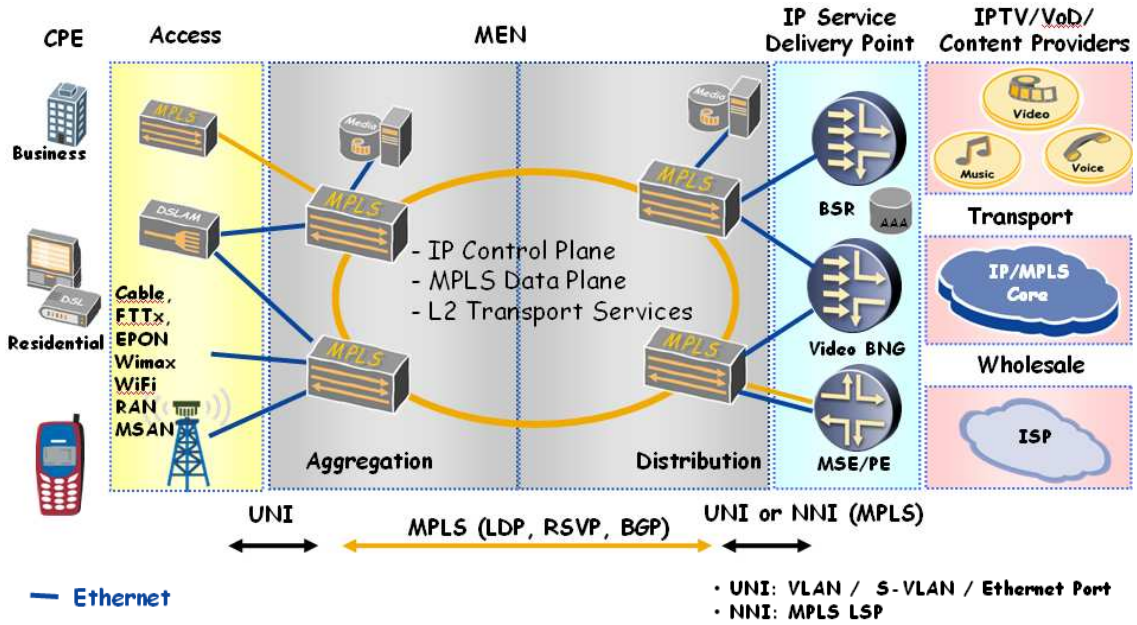
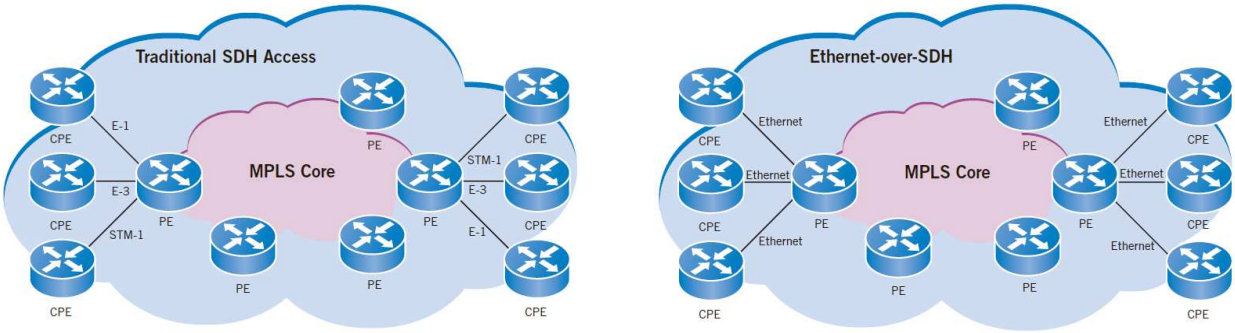



**Figura 3.12 – Arquitectura da rede EoMPLS [Juniper, 2007]**

A tecnologia SDH também pode ser utilizada para interligar a rede núcleo à rede de acesso, conforme mostra a Figura 3.13. A solução *Ethernet over* SDH, também conhecido por EoSDH [Tellabs, 2007], consiste em utilizar a tecnologia *Ethernet* através das interfaces *Ethernet* nos equipamentos de rede SDH. Esta solução permite reduzir os custos dos equipamentos de rede, uma vez que é possível através de uma interface *Ethernet* servir vários clientes ao contrário das interfaces SDH em que cada interface serve apenas um único cliente. O número reduzido de interfaces reduz o custo dos equipamentos de rede. A tecnologia *Ethernet* permite alterar remotamente a largura de banda de um determinado sítio sem ser necessário a intervenção no local,

enquanto que quando é utilizado a tecnologia SDH é necessária a intervenção no local para modificar a carta de interfaces ou equipamento terminal.




(a) (b)

**Figura 3.13 – Interligação entre a rede núcleo e a rede de acesso através do a) SDH b) EoSDH [**Tellabs, 2007**]**

A rede núcleo ideal para suportar os serviços *Triple Play* seria uma que tivesse o MPLS como tecnologia de transporte devido às suas vantagens. Existem outras tecnologias ainda em uso nas redes de agregação e na rede de acesso. Para reduzir os custos os provedores de serviços reaproveitam os recursos e tecnologias que interligam as redes núcleo e as redes de acesso. Posto isto, seria interessante verificar quais os efeitos combinados das várias tecnologias ao serem injectadas na rede núcleo MPLS. Em [Kankkunen, 2004] existe um estudo que mostra os resultados destes efeitos combinados e a seguir são explicados os resultados.

A Tabela 3.3 mostra as possíveis tecnologias de transporte que podem ser injectadas na rede núcleo MPLS, as suas respectivas características, desvantagens, vantagens e efeitos combinados. A sinergia define a interacção de dois ou mais agentes de modo que o efeito combinado seja maior que os efeitos individuais. Observa-se que a tecnologia SDH apresenta as desvantagens de inflexibilidade e falta de multiplexagem estatística. O SDH tem a vantagem de ser uma tecnologia madura e ubíqua. A *Ethernet* é limitada na gestão do tráfego mas é uma tecnologia simples e de custo reduzido. A EoMPLS é uma tecnologia nova e requer novas infraestruturas mas fornece QoS, gestão de tráfego e adapta-se facilmente à tecnologia IP/*Ethernet*. A tecnologia EoSDH não oferece optimização para o tráfego de pacotes mas é uma tecnologia muito utilizada. Verifica-se que a melhor tecnologia a utilizar para interligar a rede núcleo MPLS à rede de acesso IP/*Ethernet* é a EoMPLS e a pior tecnologia a utilizar é o SDH. A tecnologia *Ethernet* e a tecnologia EoSDH apresentam resultados iguais, quando utilizada para interligar a rede núcleo MPLS à rede de acesso IP/*Ethernet*. A tecnologia que melhor suporta o protocolo IP na rede de acesso é mais uma vez o EoMPLS e a pior mais uma vez a SDH. A tecnologia *Ethernet* e a EoSDH apresentam resultados iguais em relação ao suporte ao protocolo IP que fornecem na rede de acesso. Posto isto, a tecnologia que fornece os melhores resultados é a EoMPLS.

**Tabela 3.2 – Tecnologias de Trasporte que podem injectar dados na rede núcleo MPLS [Kankkunen, 2004]**

| Properties / Technology (Implementation details) | Typically supported service bit rates | Synergy with IP over Ethernet end user networks and MPLS core networks | Major weaknesses | Major strengths | Support for "IP Enabling" the access and regional network |
|---|---|---|---|---|---|
| **SDH** (TDM LL over SDH over Fiber) | 2M, 34M, 155M, 622M | ☆ | Inflexibility and lack of statistical multiplexing. | Mature technology with wide availability. | ☆ |
| **Metro Ethernet** (Ethernet over Fiber) | 2M - 1G | ☆☆☆ | Limited traffic management support. | Simple and low cost. | ☆☆ |
| **Metro Ethernet + MPLS** (Ethernet over MPLS over Fiber) | 2M - 1G | ☆☆☆☆ | Requires new network infrastructure. | IP/Ethernet friendliness, QoS and traffic mgmt. | ☆☆☆☆ |
| **NG-SDH / EoSDH** (Ethernet over SDH) | 2M - 1G | ☆☆☆ | TDM core is not optimal for packet dominated traffic. | SDH is widely available. TDM LL support. | ☆☆ |

O objectivo deste trabalho é encontrar um encaminhamento óptimo ou quase óptimo para o tráfego de serviços *Triple Play*. Para isto, é necessário aplicar a QoS nestas redes para assegurar o correcto funcionamento dos serviços *Triple Play* em caso de falha ou congestionamento. Nas redes não orientadas à conexão, os pacotes de dados são descartados em caso de falha ou congestionamento. O MPLS surge como uma solução apropriada para resolver este problema pois proporciona orientação à conexão às tecnologias não orientadas à conexão, como é o caso das redes IP e *Ethernet* (mais utilizadas). O MPLS é uma arquitectura de múltiplos protocolos que procuram estabelecer um caminho para um determinado fluxo, no caso de falha ou congestionamento, de uma forma mais rápida do que as redes IP convencionais. Ao aumentar a velocidade de recuperação da rede na ocorrência de falha ou congestionamento, o número de pacotes descartados é menor. Existem vários métodos de recuperação de redes que podem ser utilizados nas redes MPLS tais como a recuperação Global ou *Makam*, a recuperação *Reverse*, a recuperação *Haskin*, a recuperação Local e a recuperação Local em ambientes dinâmicos. Todos estes métodos de recuperação devem ser analisados para determinar qual o método que proporciona a menor número de pacotes descartados.

A Engenharia de tráfego também é uma solução com muitas vantagens pois permite encaminhar os fluxos de dados pelos caminhos desejados tanto na presença de falhas como na ausência das mesmas. Isto permite balancear o fluxo de dados pela rede e optimizar a utilização de todos os recursos existentes na mesma.

Neste trabalho será utilizado a junção do EoMPLS e a Engenharia de Tráfego pois, como fora visto, proporciona as vantagens de obter uma rede capaz de:

- Recuperar rapidamente em caso de falha ou congestionamento, e;
- Balançar os fluxos de dados por toda a rede de forma a optimizar o funcionamento da mesma.

# CAPÍTULO IV

# SIMULAÇÃO DE REDES

As simulações ajudam a prever as reacções das redes perante interacções complexas e mais realistas do que os modelos matemáticos, que recorrem a médias e probabilidades. As simulações permitem planear e analisar a rede de forma a testar a sua escalabilidade no caso de se querer aumentar a sua capacidade e fazer a rede suportar um maior número de utilizadores. As simulações possibilitam, igualmente, prever a reacção da rede perante falhas que podem surgir na mesma e analisar alternativas para a sua recuperação.

Neste Capítulo são dados a conhecer alguns dos simuladores, existentes no mercado, que permitem efectuar as simulações de redes de transporte. Este estudo irá permitir determinar as características que nos levaram à escolha da ferramenta de simulação, no contexto deste projecto de mestrado.

## 4.1 SIMULADORES DE REDE

Nesta secção são apresentados os principais simuladores de rede com base na sua capacidade de implementar a tecnologia MPLS, a Engenharia de Tráfego e a recuperação de falhas. Salienta-se, entre os vários disponíveis na Internet, os simuladores que são mais utilizados para redes de transporte fixas: J-Sim (*Java Simulator*) [Miller et al, 2003], OPNet (*Optimized Network Engineering Tool*) [Alicart, 2005, Lucio et al, 2003] e NS-2 (*Network Simulator 2*) [Chung et al, 1999].

### 4.1.1 J-SIM

O J-Sim é um simulador de redes que proporciona ao utilizador a simulação através de um ambiente de animação. Neste ambiente são construídos e executados os modelos de simulação, é visualizada a animação estática, são adicionados *ícones* de animação e são geradas as estatísticas. O J-Sim foi desenvolvido em Java e visa simplificar o trabalho de quem cria os simuladores e de quem os utiliza. Através da componente *graphical designer*, que gera código ao construir o modelo estático, é simplificado o código ao construtor de modelos. Ao utilizador é fornecido uma animação fácil de compreender e que mostra as actividades de simulação. O construtor de modelos cria uma representação estática do modelo de simulação. O J-Sim fornece a animação a partir da representação estática com incorporação de animações dentro de cada componente de simulação.

O J-Sim utiliza o conceito de *Query Driven Simulation* (QDS). Este conceito permite comparar os resultados da simulação com os valores de simulações anteriores, no caso de estas existirem alocadas na base de dados. O J-Sim suporta linguagens de script tais como o Perl, o Tcl e o Python para configurar as componentes que correm as simulações. É também um ambiente que integra as componentes Tcl/Java. Tais características simplificam a criação dos cenários de simulação e os seus diagnósticos. O J-Sim tem um GUI (*Grafic User Interface*) que pode ser ser executado sobre o *Windows* ou o *Linux/Unix*. É requerido o JVM (*Java Virtual Machine*) e a versão mais recente JDK (*Java SE Development Kit*) fornecido pela *Sun* para executar o J-Sim [Miller et al, 2003].

### 4.1.2 OPNET

O OPNET (*Optimized Network Engineering Tool*) *Modeler* é um simulador de rede que permite criar e estudar as redes de comunicação, dispositivos de rede, protocolos e aplicações. O OPNET oferece uma interface gráfica ao utilizador (GUI – *Graphical User Interface*) que permite editar e construir os modelos de várias entidades de redes, desde a camada física até à camada da aplicação, sem recorrer à linguagem de programação. No OPNET também é permitido a manipulação do código de programação.

O OPNET *Modeler* tem três componentes, o *software*, os modelos e a documentação. Este *software* pode funcionar tanto em máquinas com o sistema operativo *Windows* ou com o sistema operativo *Solaris*. Deve ser instalado o compilador C++ para a simulação e construção de modelos. O OPNET *Modeler* pode modelar protocolos, dispositivos de rede e comportamentos através de 400 funções.

O OPNET suporta a especificação de modelos através de várias ferramentas denominadas de editores. Estes editores tratam da informação necessária para modelar a rede em paralelo com a estrutura de um sistema de rede real. Desta forma, os editores das especificações de modelos estão organizados hierarquicamente para simplificar os vários níveis da construção do modelo de rede. As especificações desempenhadas no editor de projecto dependem dos elementos especificados no editor de nós. Os restantes editores são utilizados para definir e especificar de forma personalizada os vários modelos de dados, as novas ligações e os novos nós.

Depois de criados os modelos de rede, são escolhidos os parâmetros das estatísticas pretendidas. Posteriormente é executada a simulação e por fim são visualizados e analisados os resultados. [Alicart, 2005, Lucio et al, 2003].

### 4.1.3 NS-2.33

O *Network Simulator* versão 2 é um simulador baseado num projecto iniciado em 1989 denominado de *Real Network Simulator*. Actualmente é suportado através do *Defense Advanced Research Projects Agency* (DARPA) juntamente com o *Simulation Augmented* pelo *Measurement and Analysis for Networks* (SAMAN) e através do *National Science Foundation* (NSF) com a *Collaborative Simulation for Education and research* (CONSER). Ambos em colaboração com outros investigadores onde se inclui o *The ICSI Center for Internet Research* (ICIR).

Para melhorar a eficiência do tempo de simulação, este simulador utiliza a linguagem de programação C++ para implementar os modelos de objectos e a calendarização de eventos. O utilizador define e configura os detalhes da rede tais como a topologia, as aplicações, os tipos de tráfego, os pontos de início e fim das simulações e outros parâmetros. Utiliza também a linguagem MIT *Object* Tcl (OTcl) que não necessita de ser compilada. Assim, são utilizadas duas linguagens, a linguagem C++ que permite criar e personalizar a arquitectura do protocolo e a linguagem OTcl que é utilizada para variar os parâmetros e configurações da simulação de uma forma fácil.

A simulação do NS-2 cria um ficheiro *trace* que contém a informação da topologia e o trajecto dos pacotes para depois ser ilustrado no NAM. O NAM (*Network Animator*) [Chung et al, 1999] é uma ferramenta de animação para visualizar os *traces* da simulação. Desta forma a visualização em tempo real não é possível. O pacote de *software* NS-2 contém uma componente opcional chamada *xgraph*. Este componente é um programa utilizado para criar representações gráficas dos resultados de simulação. A análise do ficheiro *trace* pode ser efectuada através da linguagem Perl ou da linguagem AWK.

O NS-2 é executado no ambiente Linux/Unix, mas também é possível ser executado no ambiente Windows através da utilização da aplicação *Cygwin*. O componente *xgraph* corre na plataforma Unix com o XWindows, no entanto, o suporte para esta componente no Windows não está disponível. Este simulador é muito utilizado nas pesquisas e está disponível em versões gratuitas. A versão mais recente do NS-2 é a versão 2.33.

O NS-2 é um simulador de eventos direccionado para a investigação na área das redes onde permite a simulação do TCP, do UDP, de geradores de tráfego personalizados, de encaminhamento de pacotes e de protocolos *unicast* e *multicast* sobre redes fixas e redes móveis [Wikipedia 5, 2008]. Segundo [Gaeil, 2000] é possível implementar o MPLS e a Engenharia de tráfego no NS-2 através do módulo MNS-2.0 (MPLS NS-2) [Calle et al, 2004]. A recuperação de falhas também é possível através do NS-2.

### 4.1.4 Estudo comparativo entre as ferramentas de simulação

Segundo [J-Sim 1, 2003] os tempos de simulação do J-SIM são muito mais rápidos e a utilização do CPU é mais leve do que no simulador NS-2.

Em [Lúcio et al, 2003], pode-se analisar a comparação entre o simulador OPNET e o simulador NS-2. É utilizado o gerador de dados CBR (*Constant Bit Rate*) e o gerador de transferência de ficheiros FTP. É concluído que as simulações do NS-2 e do OPNET apresentam resultados muito próximos dos obtidos na realidade. O factor mais atractivo do simulador NS-2 é o facto de este simulador ser gratuito. Segundo [Fahmy, 2006] o NS-2 não simula camadas tal como são na realidade e os pacotes são tratados como mensagens, enquanto o OPNET simula camadas reais a partir da camada 2. Outra observação em [Fahmy, 2006] é que os modelos dos dispositivos no NS-2 são gerais e simples e no OPNET são modelos de dispositivos personalizados.

Actualmente, tanto o OPNET como o NS-2 suportam o MPLS e a Engenharia de Tráfego [Boucadair et al, 2004]. De acordo com [J-Sim 2, 2003], o J-Sim suporta a tecnologia MPLS mas não suporta a Engenharia de Tráfego e a recuperação de falhas ainda está em desenvolvimento. No NS-2 é possível simular a recuperação de falhas em redes MPLS [Calle, 2004]. O mesmo se pode afirmar em relação ao OPNET, segundo [Huang, 2003].

As simulações devem ser implementadas de forma a representar a realidade. Quanto mais fino for a granularidade da implementação da simulação mais próximo os resultados estão da realidade. Desta forma, o impacto da granularidade na implementação das simulações tem grande influência nos resultados das simulações. Segundo [Hogie et al, 2006] o NS-2 apresenta uma implementação mais fina do que o OPNET e o J-SIM. Por fim, verifica-se em [Hogie et al, 2006] que a popularidade do J-Sim é de 0,45%, a popularidade do OPNET é de 2,61% e a popularidade do NS-2 é de 88,8%. Os restantes 8,14% pertencem a vários outros simuladores de rede recentemente desenvolvidos. Desta forma, o NS-2 é o simulador mais popular e mais utilizado nas simulações de redes e consequentemente o que tem mais informação disponível. A Tabela 4.1 apresenta as características de cada simulador.

**Tabela 4.1 – Tabela Comparativa entre o J-SIM, o OPNET e NS-2.**

| | J-Sim | OPNET | NS-2 |
|---|---|---|---|
| Programa Gratuito | Sim | Não | Sim |
| Ano Desenvolvido | 2001 | 2000 | 1989 |
| Linguagem de implementação | Java | C++ | C++/OTCL |
| Suporta tecnologia MPLS | Sim | Sim | Sim |
| Suporta implementar a ferramenta Engenharia de Tráfego | Não | Sim | Sim |
| Popularidade | Muito Baixa | Baixa | Elevada |
| Granularidade | Fino | Fino | Muito fino |

### 4.1.5 Conclusões

O simulador OPNET parece ser um simulador de fácil utilização, uma vez que os modelos de rede são criados através de uma interface gráfica que permite, através de editores, modelar a rede pretendida. O OPNET suporta todas as funcionalidades actualizadas da tecnologia MPLS mas tem a grande desvantagem de não ser um simulador gratuito.

Resta comparar os simuladores gratuitos J-Sim e NS-2. Sabe-se que ambos os simuladores suportam a tecnologia MPLS. O simulador NS-2 suporta a tecnologia MPLS desde 2000, segundo [NS-2, 2000] enquanto o simulador J-Sim apenas suporta a tecnologia MPLS desde 2003 [J-Sim, 2003]. Como o NS-2 foi desenvolvido há mais tempo e a sua popularidade é grande, existe mais informação e código relativo à tecnologia MPLS disponível na Internet. Desta forma, é utilizado neste trabalho de dissertação o simulador NS-2 para a implementação das simulações dos vários cenários.

O simulador NS-2 é utilizado neste trabalho para analisar os resultados das simulações dos vários cenários propostos. Estas simulações têm o objectivo de verificar qual o melhor encaminhamento a atribuir ao tráfego *Triple Play* sem provocar uma taxa de perda de pacotes elevada. O simulador de rede permite verificar, de forma quase realista, os condicionantes existentes na rede e analisar qual a melhor maneira de contornar os condicionantes de forma a optimizar a eficiência de uma dada rede.

# CAPÍTULO V

# SIMULAÇÃO DE QOS COM NS-2.33

Neste Capítulo são apresentados os conceitos teóricos e o funcionamento experimental do simulador de rede NS-2 através das simulações de vários cenários. A análise dos resultados leva à criação do Cenário 4 que representa a arquitectura a ser utilizada numa rede resiliente capaz de suportar o serviço *Triple Play.*

## 5.1 O SIMULADOR NS-2

Neste trabalho é utilizado o simulador NS-2 (*Network Simulator 2*), uma vez que este é o mais popular e o que possui muita informação disponível na Internet de forma a proporcionar a atingirmos o objectivo final deste trabalho. O simulador foi instalado no sistema operativo *Open Suse* 10.1. O NS-2 utiliza duas linguagens de programação orientadas a objectos para efectuar as simulações: o OTcl (*Object Tool Command Language*) e o C++. O Tcl é uma linguagem *script* que permite um acesso simples às funções das livrarias do NS-2. A única alternativa ao acesso a estas livrarias é através da linguagem C++. Como a sintaxe da linguagem Tcl é de fácil compreensão e manipulação, o acesso às funcionalidades das livrarias do NS-2 é rápido. O OTcl é utilizado na simulação da topologia (acção periódica - Controlo) e o C++ é utilizado para programar cada objecto na topologia da simulação (acção por pacote - Dados).

O objecto de controlo (OTcl) permite configurar as simulações, atribuir acções periódicas à simulação, manipular os objectos C++ existentes e facilitar a escrita e manipulação do código. No entanto, a sua execução é lenta. O objecto de dados (C++) trata de implementar o *kernel* (parte central do sistema operativo) para o simulador NS-2 funcionar. A escrita e manipulação da linguagem de programação do objecto de dados é lenta mas a sua execução é rápida. O NS-2 é um simulador "*Text-based*", ou seja, tudo o que é necessário para realizar a simulação tem que ser efectuado através da linguagem de código. A Figura 5.1 mostra a separação dos objectos de controlo (OTcl) e dos objectos de dados (C++) e a interacção entre as duas linguagens. Os objectos de dados compilados são disponibilizados ao interpretador OTcl através de uma ligação que cria um objecto OTcl para cada objecto C++. Desta forma, os controlos dos objectos C++ são dados ao OTcl. A interface gráfica GUI (*Graphical User Interface*) não é suportada pelo simulador NS-2 para a criação da topologia e a simulação dos modelos de rede.

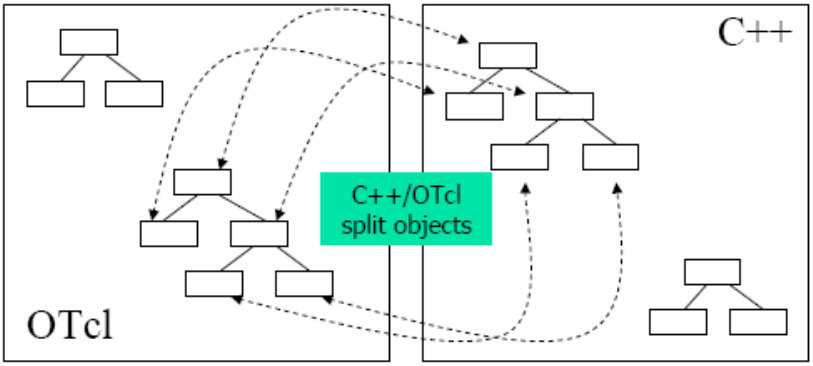



**Figura 5.1 – Arquitectura do NS-2 [**Heidemann et al, 2006**]**

O simulador NS-2 é constituído por quatro componentes: o próprio simulador, o NAM (*Network Animator*), o pré-processamento e o pós-processamento. O simulador utilizado neste trabalho é o NS-2.33 (*Network Simulator 2 versão 2.33*). O NAM é a ferramenta que permite visualizar a simulação através do ficheiro ".nam" criado pelo NS-2. A componente de pré-processamento inclui os geradores de tráfego utilizados nos cenários de simulação. Por fim, a componente de pós-processamento utilizada neste trabalho inclui o ficheiro ".awk" e o xgraph [Heidemann et al, 2006]. O ficheiro ".awk" contém código que permite calcular os parâmetros de QoS a partir do processamento do ficheiro ".tr" criado pelo NS-2. Os resultados dos cálculos dos parâmetros QoS são apresentados na janela de comandos. O xgraph processa os dados contidos nos ficheiros ".r" criados pelo NS-2 e fornece ao utilizador um gráfico que mostra as variações de determinado parâmetro QoS ao longo da simulação.

A Figura 5.2 mostra o processo da simulação no NS-2. Primeiro é criado o ficheiro OTcl para a simulação. Depois o ficheiro OTcl é executado pelo interpretador OTcl que tem o acesso à livraria do simulador NS. Em terceiro lugar é criado um ficheiro ".tr" com os resultados da simulação. Por fim, são analisados os resultados através da janela de comandos, do NAM e/ou do Xgraph.

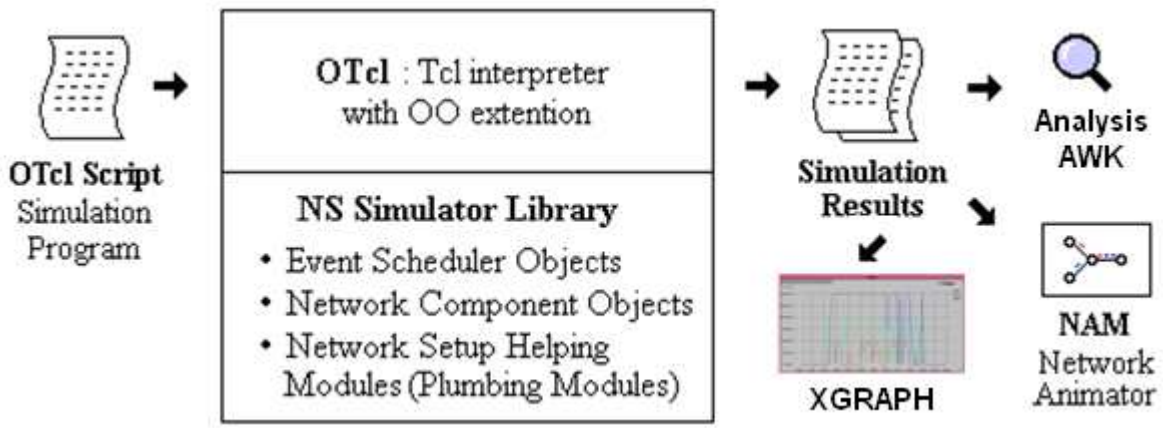



**Figura 5.2 – O processo de simulação no NS-2 [**Chung et al, 1999**].**

### 5.1.1 Funcionamento do MPLS no NS-2

Esta secção descreve a implementação do protocolo MPLS no simulador NS-2 [Ganchev, 2003]. Este simulador suporta as duas funções principais do MPLS, nomeadamente o LDP e a comutação de etiquetas MPLS [Ganchev, 2003]. Vários exemplos da modelação MPLS estão disponíveis na pasta do simulador de rede NS-2 (…/tcl/test/test-suite-mpls.tcl).

O NS-2 é um simulador baseado no protocolo IP onde cada nó consiste em classificadores e agentes. Um agente é um objecto que recebe e envia pacotes. O classificador é o objecto responsável pela classificação dos pacotes recebidos para depois encaminhar os mesmos ao nó desejado. Também poderá entregar os mesmos ao agente local no caso do nó que receber os pacotes ser o nó de destino. Desta forma, para construir um nó MPLS, deve ser criado o classificador MPLS, denominado *MPLS classifier*, para permitir a classificação dos pacotes recebidos e determinar se os mesmos contêm a etiqueta do MPLS. Posteriormente deverá tratar dos mesmos, conforme a informação contida dentro do pacote. Deve ser inserido, igualmente, um novo agente LDP no nó IP para ser possível a distribuição de etiquetas entre os nós MPLS e construir os caminhos LSP.

A arquitectura de um nó MPLS, que inclui o classificador MPLS e o agente LDP, é ilustrada na Figura 5.3.

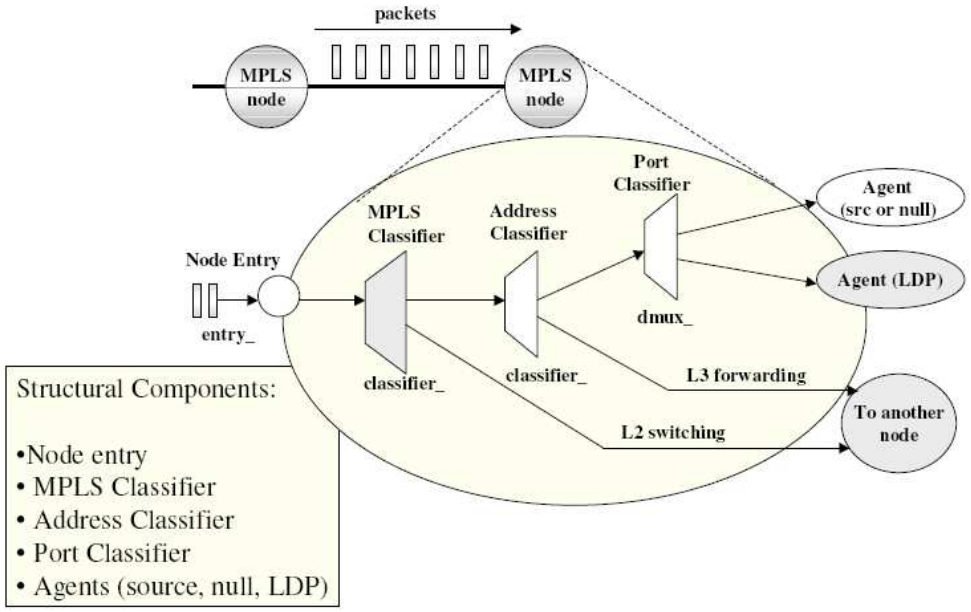



**Figura 5.3 – Arquitectura do nó MPLS no NS-2 [Ganchev, 2003]**

Quando o nó recebe o pacote, o seu classificador MPLS determina se o pacote recebido contém ou não uma etiqueta. No caso do pacote recebido conter a etiqueta, o classificador executa a comutação da camada 2 (L2 *Switchin*g). O nó substitui a etiqueta presente no cabeçalho MPLS do pacote pela etiqueta correspondente ao destino do pacote (FEC). Depois, o nó transmite o pacote para o nó seguinte. No caso de o pacote não conter a etiqueta MPLS e existir um LSP para o destino

do pacote (FEC), o classificador cria um cabeçalho MPLS, inclui uma etiqueta no cabeçalho do pacote e transmite o pacote para o próximo salto correspondente.

No caso do pacote recebido não conter uma etiqueta e não existir nenhum LSP, o nó MPLS entrega o pacote ao classificador de endereços que executa o *forwarding* (envio) da camada 3 examinando o endereço de destino do pacote. O pacote é entregue ao classificador de portos quando o nó receptor é o destino do pacote. Este classificador entrega o pacote ao agente conveniente. O agente LDP é utilizado para distribuir e iniciar os LSP baseado no protocolo de distribuição LDP.

O nó MPLS tem três tabelas para gerir a informação relacionada com o LSP e a distribuição de etiquetas: a tabela LIB (*Label Information Base*), a tabela PFT (*Partial Forwarding PFT*) e a tabela ERB (*Explicit Routing Information Base*).

A tabela PFT é um subconjunto da tabela *Forwarding* e consiste nos campos FEC, PHB (*Per-Hop-Behavior*) e no apontador LIBptr. A tabela LIB tem informação para o LSP e a tabela ERB tem informação para o ER-LSP. A Figura 5.4 mostra a estrutura das tabelas e o algoritmo para o *forwarding* dos pacotes. Em cada tabela, o apontador LIBptr é um apontador que aponta para uma entrada LIB.

A procura na tabela PFT/LIB é iniciada quando o nó MPLS recebe um pacote com ou sem etiqueta. No caso do pacote não conter uma etiqueta, o nó MPLS procura por uma entrada na tabela PFT com o FEC (endereço de destino do pacote) do pacote. Se o LIBptr da entrada encontrada na tabela PFT indicar NULL, o nó MPLS reencaminha (*forward)* o pacote através do esquema *forwarding* da camada 3. Caso contrário, o nó MPLS desempenha a operação de imposição da etiqueta no pacote, ou seja, não empurra para dentro do pacote a etiqueta de saída da entrada da tabela LIB. Pode haver sucessivamente uma operação de pilha de etiquetas para o pacote onde a operação de empurrar a etiqueta é repetida até o apontador LIBptr da entrada LIB indicar NULL. Depois de finalizadas as operações de etiqueta, o pacote é encaminhado directamente para o próximo salto indicado pela interface de saída da entrada LIB.

Caso o pacote contenha uma etiqueta, o nó MPLS identifica facilmente uma entrada LIB para o pacote, através da utilização da etiqueta inserida como um índice da tabela LIB. De seguida, o nó MPLS desempenha uma operação de troca de etiquetas que substitui a etiqueta do pacote por uma etiqueta de saída da entrada da tabela LIB. No caso da etiqueta de saída ser uma etiqueta NULL, o nó MPLS desempenha uma operação de salto da pilha em vez da operação de troca de etiquetas. Depois, o nó MPLS desempenha a operação da pilha de etiquetas para o pacote, no caso do LIBptr da entrada LIB não ser NULL. Finalmente, o pacote é encaminhado directamente ao próximo nó indicado pela interface de saída da entrada da tabela LIB.

A tabela ERB é utilizada para armazenar apenas a informação do ER-LSP. Desta forma, a tabela ERB não participa no *forwarding* de pacotes. No caso de ser necessário mapear um fluxo

num ER-LSP previamente estabelecido, deve ser inserida na tabela PFT uma nova entrada com o mesmo apontador LIBptr da tabela ERB [Gaeil, 2000].

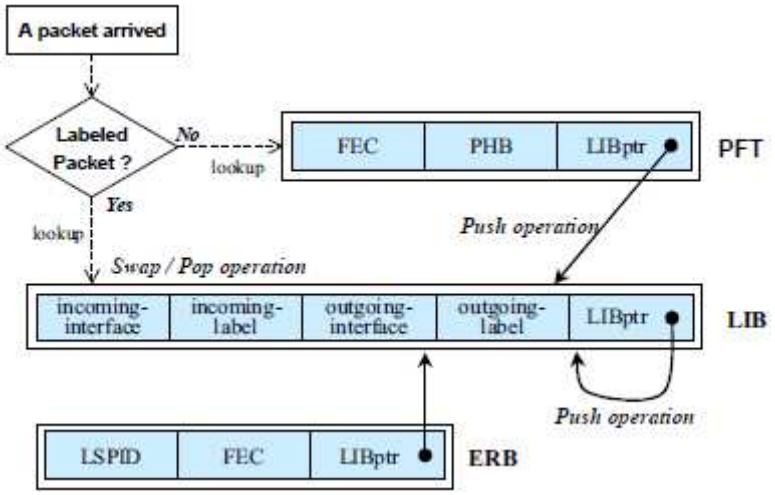



**Figura 5.4 – Estrutura das tabelas para a comutação de pacotes MPLS [**Gaeil, 2000**]**

## O Encaminhamento de Protocolos

Existem dois protocolos de encaminhamento que podem ser utilizados no NS-2: o DV (*Distance Vector*) e o LS (*Link State*). O *"Distance Vector"* e o *"Link State"* são termos que descrevem os protocolos de encaminhamento utilizados pelos encaminhadores para enviar *(forward)* os pacotes entre redes. O objectivo de qualquer protocolo de encaminhamento é de comunicar, de forma dinâmica, a informação sobre todos os caminhos existentes na rede. Este procedimento vai facilitar a escolha do melhor caminho para os pacotes chegarem ao destino. Estes dois protocolos de encaminhamento são utilizados para agrupar os protocolos em duas categorias:

- Baseado na distância entre a fonte e o destino e escolher o caminho com menor distância, e;
- Baseado no estado de cada ligação, no caminho até ao destino, e escolher o caminho com menor congestionamento.

O protocolo de encaminhamento DV utiliza os cálculos de distância em conjunto com uma interface, de forma a escolher o melhor caminho até ao destino. Os protocolos de rede (IP, entre outros) enviam os dados através dos melhores caminhos seleccionados.

Os protocolos de encaminhamento LS conhecem o estado e tipo de conexão de cada ligação. Produzem uma métrica calculada, tendo como base estes factores. O protocolo LS reconhece se existe, ou não, uma falha na ligação e a velocidade da ligação. Também calcula o custo do percurso para chegar ao destino. Estes protocolos são capazes de escolher caminhos com maiores distâncias mas com meios de transmissão rápidos em vez de caminhos com menores distâncias e meios de transmissão mais lentos. Como consequência, o protocolo LS requer mais energia de processamento

e mais memória do que o protocolo DV. Como os protocolos DV têm algoritmos mais simples requerem equipamentos mais simples do que os requeridos pelo protocolo LS.

Existem dois modos de distribuição de etiquetas: a distribuição *Data-Driven* e a distribuição *Control-Driven.* As junções *(binding) Data-Driven* ocorrem quando o tráfego inicia o seu fluxo, onde é recebido pelo LSR e reconhecido como um candidato para a comutação de etiquetas. As junções de etiquetas são estabelecidas apenas quando necessário, o que resulta em menores entradas na tabela de envios *(Forwarding Table).* As etiquetas são atribuídas individualmente a cada fluxo de tráfego IP e não a cada pacote. Esta distribuição é utilizada na camada 2 do modelo OSI (*Open Systems Interconnection*). As junções *Control-Driven* são estabelecidas como resultado da actividade do plano de controlo e são independentes das junções do plano de dados. As junções de etiquetas podem ser estabelecidas em resposta às actualizações de encaminhamento. Por outro lado, as junções *Control-Driven* de etiquetas são mais eficientes do que a distribuição *Data-Driven* e por isso são utilizadas no MPLS. Esta distribuição é utilizada na camada 3.

**A Distribuição de Etiquetas através do Protocolo LDP**

A distribuição de etiquetas e a construção dos LSP é efectuada através da troca de mensagens LDP entre os agentes LDP e os nós LSR. A arquitectura das redes MPLS oferece três modos de distribuição de etiquetas: o *Control-Driven*, o *Data-Driven* e o *Explicit Routing Labeling*.

O modo de *Control-Driven* conta com a distribuição das mensagens LDP entre todos os agentes LDP, mesmo no caso de não haver dados para transmitir. Os LSP são associados a cada FEC, e isto é efectuado através do envio de mensagens de mapeamento de cada agente LDP para as restantes LDP que contêm a FEC ao longo do trajecto. A etiqueta é utilizada mais tarde para a transmissão dos dados. No fim, todas as tabelas LIB de todos os nós MPLS são preenchidas. Os LSP são associados a todos os FEC, mesmo no caso de não haver dados para ser transferidos.

O modo *Data-Driven* distribui as mensagens LDP e constrói os LSP apenas para os FEC de destino dos agentes que pretendem transmitir dados. Desta forma, quando um nó pretende transmitir dados, envia uma mensagem de pedido, juntamente com os dados, até ao FEC *upstream.* Quando o FEC recebe a mensagem de pedido, envia uma mensagem de mapeamento, no sentido *downstream*, até à fonte. Cada encaminhador, pelo caminho, recebe a mensagem de mapeamento. Os encaminhadores tratam estas mensagens e criam uma nova mensagem LDP e transmitem para o próximo salto. Desta forma, um LSP é construído desde a fonte até ao destino. Os primeiros pacotes transmitidos são encaminhados como pacotes de camada 3, até construir o LSP no qual a comutação da camada 2 pode ser efectuada.

No modo *Explicit Routing Labeling*, os LSP são construídos de uma forma simplificada. O utilizador necessita de inserir os nós sucessivos do encaminhamento explícito por onde os dados

devem ser transmitidos. Desta maneira, as mensagens de mapeamento são distribuídas ao longo do caminho e ao mesmo tempo é construído o LSP até ao FEC.

**A Recuperação de Falhas**

Quando o pacote é recebido por um nó, é tratado pelo classificador MPLS. Este classificador processa e encaminha o pacote para o agente local ou para um outro nó. A Figura 5.5 ilustra o algoritmo utilizado para processar o pacote.

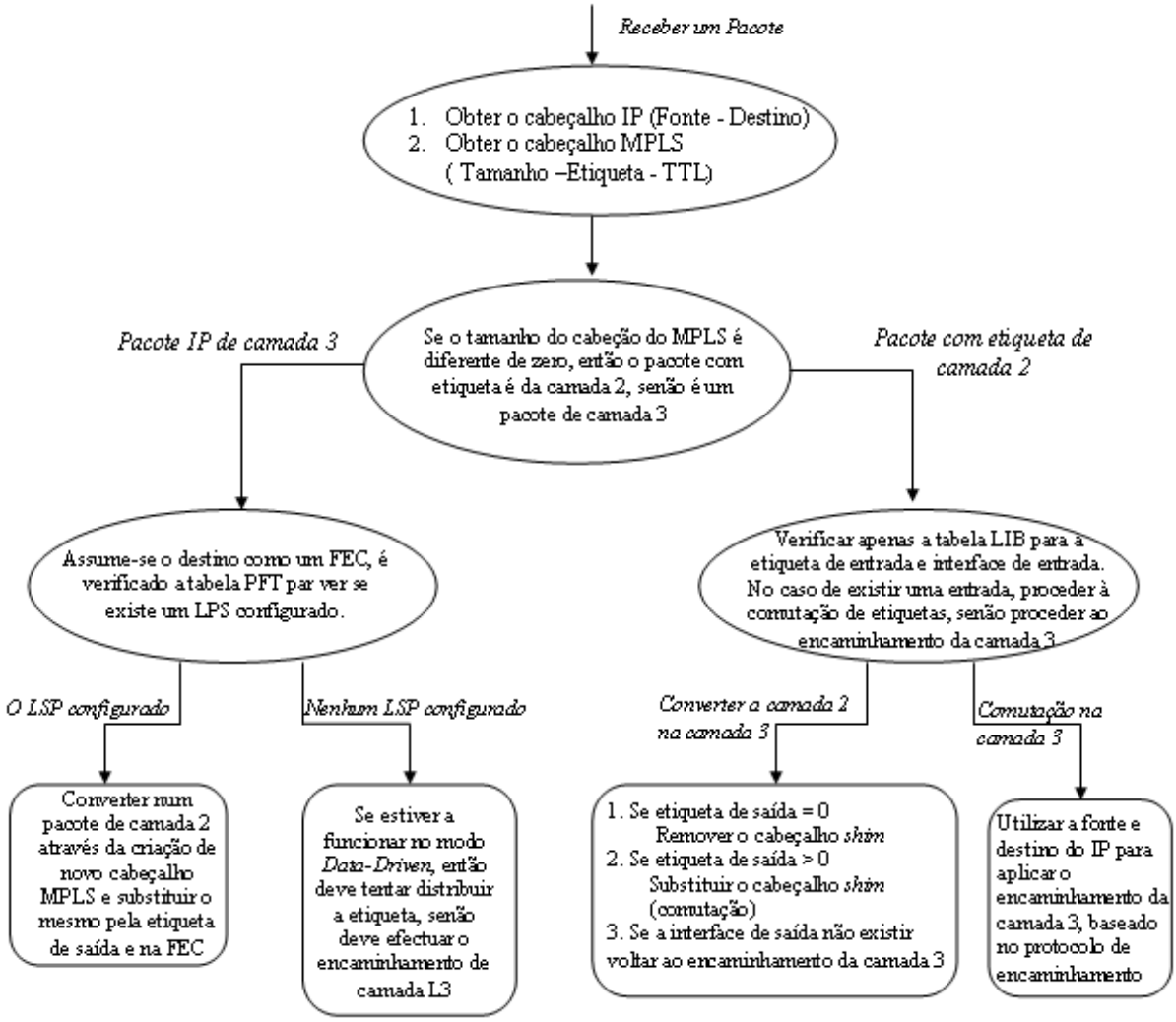



**Figura 5.5 – O processo da comutação no nó MPLS no NS-2 [Boudani, 2002]**

O mecanismo de comutação que ocorre no nó MPLS, quando existe uma falha na ligação, está ilustrado na Figura 5.6. No exemplo abaixo, em caso de falha é utilizada a tabela ERB de forma a ser determinado qual o caminho a seguir.

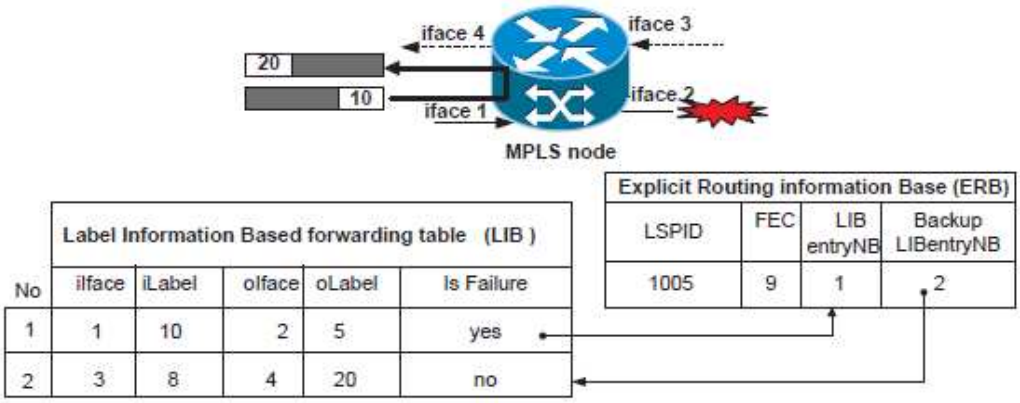



**Figura 5.6 – Recuperação do LSP ao utilizar o LSP de protecção através da comutação [Calle et al, 2004]**

## 5.2 TRÁFEGO UTILIZADO NAS SIMULAÇÕES

O NS-2 possui objectos geradores de tráfego que se utiliza durante as simulações: o gerador *Pareto*, o gerador *Exponencial* e o gerador *PackMime* [Weigle et al, 2004]. O gerador *Pareto* é utilizado para simular a geração de tráfego VoIP. O gerador *Exponencial* para simular a geração de tráfego IPTV e de Dados e o gerador *PackMime* para simular a geração de tráfego associado ao acesso a páginas Web entre o cliente e o servidor.

**Tráfego VoIP**

O *codec* G.711 (também conhecido por *Pulse-Code Modulation*) é o mais utilizado na transferência de voz sobre a rede IP. A carga útil do conteúdo de voz no pacote IP é de 160 *bytes* e a taxa de transferência do *codec* é de 64 Kbps [Cisco, 2005]. Na simulação será utilizado o pacote *Ethernet* para transferir o conteúdo de voz. Desta forma, considera-se o tamanho do cabeçalho *Ethernet* (18 *bytes*) bem como os tamanhos dos cabeçalhos IP (20 *bytes*), RTP (12 *bytes*) e UDP (8 *bytes*). O *payload* do VoIP é de 160 *bytes*. Em [Cisco, 2005] encontra-se as fórmulas para calcular o tráfego por chamada de voz. Calcula-se primeiro o tamanho total do pacote (VoIP + *Ethernet* + IP + RTP + UDP = 160 + 18 + 20 + 12 + 8 = 218 *bytes*) depois calcula-se os pacotes por segundo (taxa de transferência do *codec* / VoIP = 64/160 =0,400 pacotes/s) e por fim calcula-se a largura de banda (tamanho total do pacote * pacote/s = 218 * 0,400 = 87,2 Kbps). Posto isto, o tamanho do pacote a utilizar na simulação é de 218 *bytes* e a taxa de transferência a utilizar na simulação é de 87,2 Kbps. O NS-2 oferece vários geradores de tráfego que ajudam a simular a realidade.

É utilizado o gerador de tráfego *Pareto* neste trabalho para o conteúdo de VoIP. O tráfego *Pareto* é accionado e desligado (*Pareto* ON/OFF) em intervalos de tempo estipulados. A Figura 5.7 a) mostra a curva da distribuição do *Pareto*. Durante o período de "ON", os pacotes são enviados numa taxa de transferência fixa enquanto durante o período "OFF" nenhum pacote é enviado. São exigidas variáveis para o objecto *Pareto*, nomeadamente o tamanho do pacote, o tempo "ON", o

tempo “OFF”, a taxa de transferência e a forma (*shape*) da distribuição. No caso de escolher uma forma menor ou igual a 1, o valor esperado do *Pareto* é infinito ou não definido. No caso da forma ser menor ou igual a 2, a variância é infinita ou não definida. A escolha da distribuição e das variáveis para a geração do tráfego VoIP foi efectuada com base em [Mauthe, 2008]. O Tráfego utilizado para simular o VoIP é criado a partir das seguintes variáveis:

| | |
|---|---|
| PacketSize_ 218 | (gerado pacotes constantes do mesmo tamanho) |
| burst_time_ 500ms | (tempo médio para o envio de pacotes) |
| idle_time_ 50ms | (tempo médio em que não são enviados pacotes) |
| rate_ 87k | (taxa de transferência durante o tempo que está activo) |
| shape_ 1.5 | (o parâmetro de forma utilizado pela distribuição pareto) |

Observa-se que o “burst_time” está a 500ms e o “idle_time” está a 50ms. Isto permite simular uma chamada de voz em que existe o envio da voz (*burst_time*) ao falar e o silêncio (*idle-_time*) ao ouvir. O agente utilizado em todos os tráfegos é o UDP, pois permite simular as rajadas existentes na rede IP segundo [Perreira et al, 2004]. Também permite monitorizar os pacotes recebidos pelo utilizador final através da linha de código de agente (new Agent/LossMonitor).

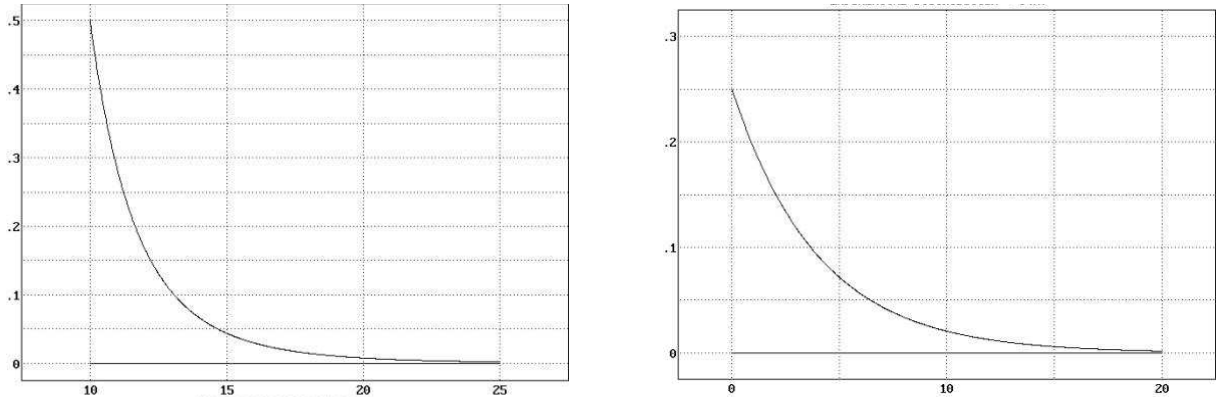
**Tráfego IPTV**

O *codec* H.264 é o mais utilizado na transferência de vídeo sobre a rede IP. A sua taxa de transferência é de 384 Kbps num *stream* de vídeo de 30 *frames/s*. Apresentado em [Salah et al, 2006] um *stream* de vídeo tem uma carga útil de 1344 *bytes*. Na simulação será utilizado o pacote *Ethernet* para transferir o conteúdo de vídeo. Desta forma, e segundo os cálculos efectuados para o VoIP, o tamanho total do pacote (IPTV + *Ethernet* + IP + RTP + UDP = 1344 + 18 + 20 + 12 + 8 = 1402 *bytes*), os pacotes por segundo (taxa de transferência do *codec* / IPTV = 384/1344 = 0,286 pacotes/s) e por fim a taxa de transferência (tamanho total do pacote * pacote/s = 1402 * 0,286 = 4907 Kbps). Posto isto, o tamanho do pacote a utilizar na simulação é de 1402 *bytes* e a taxa de transferência do pacote é de 4907 Kbps.

É utilizado o gerador de tráfego *Exponencial* ON/OFF para o conteúdo de IPTV. O tráfego *Exponencial* é accionado e desligado (*Exponencial* ON/OFF) em intervalos de tempo estipulados. A Figura 5.7 b) mostra a curva da distribuição *Exponencial*. Durante o período de “ON”, os pacotes são enviados numa taxa de transferência fixa e durante o período “OFF” nenhum pacote é enviado. São exigidas variáveis para o objecto *Exponencial* tais como o tamanho do pacote, o tempo “ON”, o tempo “OFF” e a taxa de transferência. O Tráfego utilizado para simular o IPTV é criado a partir das seguintes variáveis:

| | |
|---|---|
| PacketSize_ 1402 | (gerado pacotes constantes do mesmo tamanho) |
| burst_time_ 0ms | (tempo médio em que são enviados pacotes) |
| idle_time_ 0ms | (tempo médio em que não são enviados pacotes) |
| rate_ 4907k | (taxa de transferência durante o tempo em que está activo) |

O tamanho do pacote "PacketSize_" é dado em *bytes*, os tempos em milissegundos e a taxa de transferência em Kbps. Observa-se que o "burst_time" e o "idle_time" estão ambos a zero. Isto faz com que o gerador *Exponencial* gere fluxos de tráfego constantes.




(a) (b)

**Figura 5.7 – Distribuição a) Pareto b) *Exponencial* [Borghers et al, 2008]**

**Tráfego de Dados**

São utilizados dois tipos de tráfego de dados em dois cenários diferentes. Num dos cenários é utilizado o tráfego de dados cuja aplicação é o CBR (*Constante Bit Rate*). No outro é utilizado o tráfego de dados cuja aplicação é o *Exponencial*. A aplicação CBR gera pacotes a uma taxa de transferência fixa. As variáveis exigidas por esta aplicação são:

| | |
|---|---|
| $tv set packetSize_ 3000 | (gerado pacotes constantes do mesmo tamanho). |
| $tv set interval_ 0.008 | (intervalo de envio de cada pacote) |

O tamanho do pacote é dado em *bytes* e o intervalo de envio de cada pacote é dado em segundos. Neste caso, se um pacote de 3000 *bytes* é enviado a cada 0,008 segundos, são enviados 125 pacotes num segundo (1/0,008). Logo, a taxa de transferência é de 3 Mbps (125*3000*8*bits*/1000000).

A diferença entre o tráfego IPTV e o tráfego de dados *Exponencial* está nos tempos "burst_time" e "idle_time". No caso do tráfego de dados *Exponencial* o objectivo é simular o envio de ficheiros FTP. A aplicação FTP do NS-2 é conectada ao agente TCP. Não é possível monitorizar a rede através do comando "new Agent/LossMonitor" quando é utilizado o agente TCP. Desta forma, a única alternativa é utilizar a Aplicação *Exponencial* de forma a simular a transferência de

ficheiros. Como discutido em [Uzmi, 2006] a distribuição *Poisson* pode representar a transferência de ficheiros FTP aleatória. A distribuição *Poisson* está representada na Figura 5.8. Durante as simulações não foi possível utilizar, no simulador de rede NS-2.33 (*Network Simulator-2 versão 2.33*), a aplicação *Poisson*. Posto isto, e segundo [SFR Fresh, 2007] configurou-se a aplicação *Exponencial* de forma a ter o comportamento da aplicação *Poisson* através do parâmetro "burst_time" igual a zero e do parâmetro tempo "idle_time" a um valor muito elevado. Desta forma, utiliza-se a aplicação *Exponencial* para simular a transferência de ficheiros FTP com os seguintes parâmetros:

| | |
|---|---|
| PacketSize_ 1500 | (gerado pacotes constantes do mesmo tamanho) |
| burst_time_ 0ms | (tempo médio para o envio de pacotes) |
| idle_time_ 200ms | (tempo médio em que não são enviados pacotes) |
| rate_ 10000k | (taxa de transferência durante o tempo que está activo) |

O tamanho do pacote é dado em *bytes* e salienta-se que tem o tamanho máximo do MTU da tecnologia *Ethernet*. O envio de pacotes de 1500 *bytes* a uma taxa de transferência de 10 Mbps dá um envio total de 80 M*Bytes/s* (10*8*bits*). No entanto, como existe um tempo "OFF" muito longo, este envio de 80 MB*ytes/s* não se realiza em um segundo mas sim ao longo da simulação.

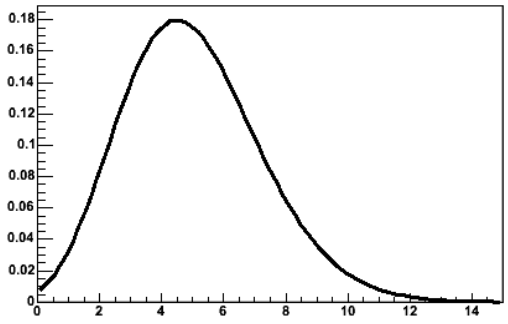



**Figura 5.8 – Distribuição Poisson [**Brun, 2004**]**

**Tráfego Web**

O gerador *PackMime* simula a actividade entre o cliente e o servidor durante o acesso a uma página Web. É possível, através da variável "rate", configurar o número de acessos simultâneos a páginas Web por segundo. Sabe-se que, no NS-2 existe o objecto "*Applications*" que controla a transferência de dados durante a simulação. Estas aplicações comunicam através de "*Agents*" que representam a camada de transporte da rede. O *PackMimeHTTP* é o objecto ns que executa a geração do tráfego http. Cada objecto *PackMimeHTTP* controla a operação de dois tipos de aplicações: a aplicação do servidor *PackMimeHTTP* e a aplicação do cliente *PackMimeHTTP*. Cada

uma destas aplicações está conectada a um agente TCP (*Full-TCP*). O modelo de tráfego Web denominado *PackMime* está representado na Figura 5.9.

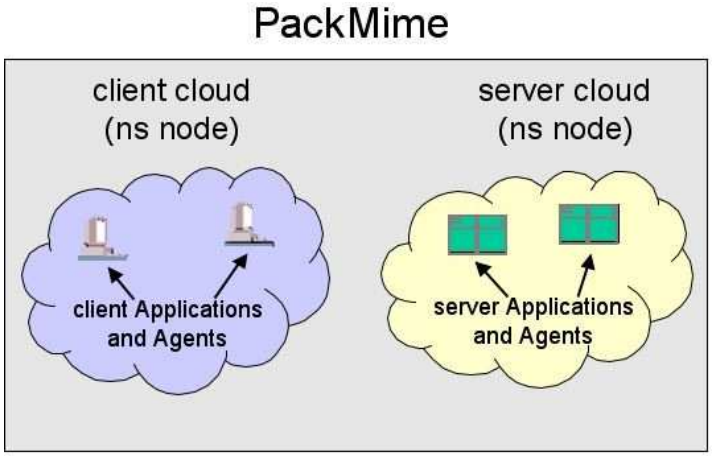



**Figura 5.9 – Modelo de Tráfego Web denominado PackMime [**Weigle et al, 2004**]**

Cada objecto PackMimeHTTP controla entre 1 a 10 nuvens de servidores e de clientes. Cada nuvem pode representar múltiplas aplicações de clientes ou de servidores. Cada aplicação representa um único servidor Web ou um único cliente Web. Cada nuvem de servidor ou de cliente é representada por um nó *ns* que pode produzir e consumir múltiplas conexões HTTP de uma só vez. Para cada conexão http, o PackMimeHTTP cria aplicações de servidor e de cliente e seus agentes TCP. Depois de configurar e iniciar cada conexão, o PackMimeHTTP configura o temporizador para terminar quando a nova conexão for iniciada. Os tempos entre as conexões são governados pelo parâmetro taxa de conexão "rate" configurado pelo utilizador. As novas conexões são iniciadas de acordo com os tempos de chegada sem o conhecimento de pedidos prévios. Por outro lado, um novo pedido entre o par cliente e servidor, como acontece no http 1.1, inicia-se após a resposta ao pedido entre o par se ter completado.

O *PackMime* trata da reutilização das aplicações e agentes que completem a sua transferência de dados. Cada cliente *PackMimeHTTP* controla o tamanho dos pedidos que são transferidos. O cliente e servidor Web iniciam no momento em que a conexão TCP é estabelecida.

A implementação do *PackMimeHTTP* fornece vários objectos *"RandomVariable"* para especificar as distribuições das variáveis de conexão do PackMimeHTTP. Isto permite que as variáveis conexão sejam especificadas de uma forma aleatória [Weigle et al, 2004].

## 5.3 CENÁRIOS E SIMULAÇÕES

O objectivo do trabalho de simulação nesta dissertação é apresentar uma solução para o encaminhamento óptimo, ou quase óptimo, do tráfego existente em redes *Triple Play*. Em contexto com as redes *Triple Play*, o encaminhamento óptimo ou quase óptimo é aquele que permite reduzir a taxa de perda de pacotes e a latência nas redes que suportam o serviço *Triple Play*. Os serviços VoIP e IPTV pertencentes ao serviço *Triple Play* são intolerantes à perda de pacotes. Posto isto, os cenários e respectivas simulações que se seguem ajudam a compreender o funcionamento da rede *Triple Play*, as suas exigências e seus limites. Os cenários apresentados também ajudam a perceber como o MPLS, a Engenharia de Tráfego e os métodos de recuperação de falhas da rede podem melhorar o desempenho e a eficiência da rede IP existente.

A arquitectura MPLS é utilizada nas simulações para obter a QoS para os clientes em redes *Triple Play*, e através da análise do seu funcionamento, é possível explicar os factores, o desempenho, os problemas relacionados com a qualidade de serviço, as vantagens e limitações. Desta forma, as simulações permitem prever situações futuras de escalonamento de acordo com o aumento de adesões ao serviço *Triple Play.* As simulações foram efectuadas através da ferramenta NS-2.33 onde são utilizados ficheiros ".tcl" para programar a simulação, os ficheiros ".awk" para processar/analisar os dados dos ficheiros ".tr" criados pela ferramenta NS-2.33 para depois ser possível a geração de relatórios sobre os parâmetros QoS para analisar as simulações.

Para determinar o encaminhamento óptimo são apresentados quatro cenários. O cenário 1 permite observar e verificar o comportamento dos diferentes protocolos de encaminhamento, dos vários modos de distribuição de protocolos, da rede IP e da rede MPLS. O cenário 2 permite conhecer o funcionamento da Engenharia de Tráfego bem como a sua aplicação numa rede com elevadas taxas de perdas, devido ao congestionamento. O cenário 3 permite observar e analisar o comportamento dos vários métodos de recuperação de falhas. O cenário 4 apresenta uma rede *Triple Play* que inclui as componentes mais eficientes do cenário 1, a aplicação da Engenharia de tráfego para reduzir a taxa de perda de pacotes e o melhor método de recuperação de falhas do cenário 3. O Anexo C contém os quatro ficheiros ".tcl" referentes aos quatro cenários propostos. O Anexo D contém os ficheiros ".awk" que contêm o código que permite processar os dados de uma dada simulação para depois mostrar os resultados dos parâmetros de QoS na janela de comandos.

Os cenários com as soluções de encaminhamento são propostos através das seguintes tarefas:

a) Modelação de uma rede de transporte;

b) Determinação dos caminhos possíveis;

c) Proceder ao encaminhamento seguindo uma dada estratégia;

e) Repetir c) e d) considerar diversas estratégias de encaminhamento, e;

f) Definir uma estratégia de encaminhamento óptima ou quase óptima de forma a reduzir a taxa de perda de pacotes.

### 5.3.1 Cenário 1 – Diferenças Entre a Rede IP e a Rede MPLS

Este cenário permite conhecer os diferentes protocolos de encaminhamento, os diferentes modos de distribuição de protocolos e a distinguir a diferença entre a rede IP e a rede MPLS.

O cenário 1 tem 3 objectivos para cumprir. O primeiro objectivo é verificar qual o protocolo de encaminhamento (DV ou LS) que possibilita o encaminhamento dos pacotes mais rápido pela rede. O segundo objectivo é verificar qual o modo de distribuição de protocolos (*Data-Driven* ou *Control-Driven*) que torna a distribuição dos pacotes mais rápida pela rede. Por fim, o terceiro objectivo é verificar a diferença entre uma rede IP e uma rede MPLS.

A topologia de rede utilizada neste trabalho foi modelada para ser uma rede simples com poucos nós de forma a visualizar e compreender facilmente os resultados obtidos das simulações. As redes complexas simuladas nos simuladores de rede sobrecarregam o sistema operativo e aumenta o tempo de simulação. Foi fundamental haver pelo menos dois caminhos para encaminhar o tráfego de dados. Os dois caminhos diferem um do outro pelo número de nós. Desta forma, a topologia de rede deste trabalho apresenta dois caminhos distintos, sete nós que representam encaminhadores de rede, um gerador de tráfego e um cliente.

A Figura 5.10 mostra a topologia de rede em anel utilizada na simulação do Cenário 1. Esta topologia consiste em sete nós, um gerador de tráfego IPTV e um Cliente. Existe a possibilidade do tráfego percorrer dois caminhos (0-1-2-3-4-7-8 ou 0-1-5-6-7-8). Um caminho apresenta um menor número de saltos até ao destino do que o outro.

Nas simulações da rede MPLS os nós 2, 3, 4, 5 e 6 representam os LSRs. O nó 1 representa o LSR de ingresso numa rede MPLS e o nó 7 representa o LSR de egresso.

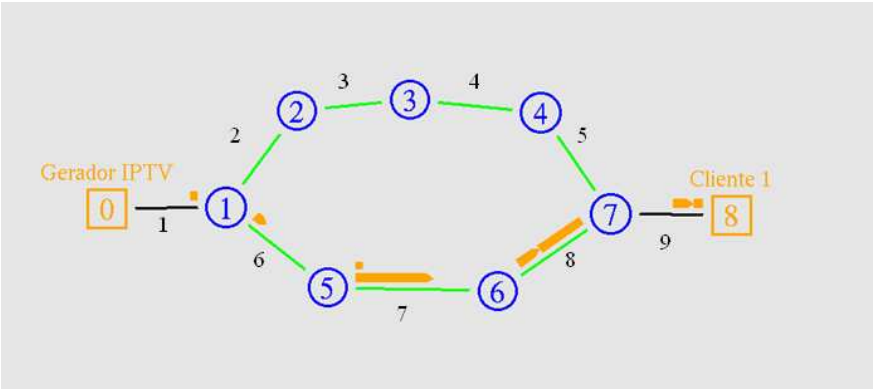



**Figura 5.10 – Topologia de rede do Cenário 1.**

A Tabela 5.1 contém todos os parâmetros atribuídos à topologia de simulação para o cenário 1. Todas as ligações entre os nós têm uma largura de banda de 10 Mbps e um atraso de 1 ms. O gerador de tráfego IPTV (tráfego *Exponential*) envia pacotes de 1402 *Bytes* a uma taxa de transferência de 4907 Kbps. O gerador de tráfego IPTV inicia o envio de pacotes no instante 0,1s e termina no instante 1,8s. A simulação termina ao fim de 2s.

**Tabela 5.1 – Parâmetros atribuídos à topologia de rede do Cenário 1.**

| | | | |
|---|---|---|---|
| Topologia de rede e configurações utilizado em todos os casos de simulação | Caminho 1 | 0-1-5-6-7-8 | |
| | Ligação 1 | 10 Mb | 1 ms |
| | Ligação 2 | 10 Mb | 1 ms |
| | Ligação 3 | 10 Mb | 1 ms |
| | Ligação 4 | 10 Mb | 1 ms |
| | Ligação 5 | 10 Mb | 1 ms |
| | Ligação 6 | 10 Mb | 1 ms |
| | Ligação 7 | 10 Mb | 1 ms |
| | Ligação 8 | 10 Mb | 1 ms |
| | Ligação 9 | 10 Mb | 1 ms |
| | Tráfego | *Exponential* | |
| | Tamanho do Pacote | 1402 | Bytes |
| | Taxa de Transferência | 4907 | Kbps |
| | Gerador IPTV inicia | 0,1 | s |
| | Gerador IPTV termina | 1,8 | s |
| | Fim da Simulação | 2 | s |

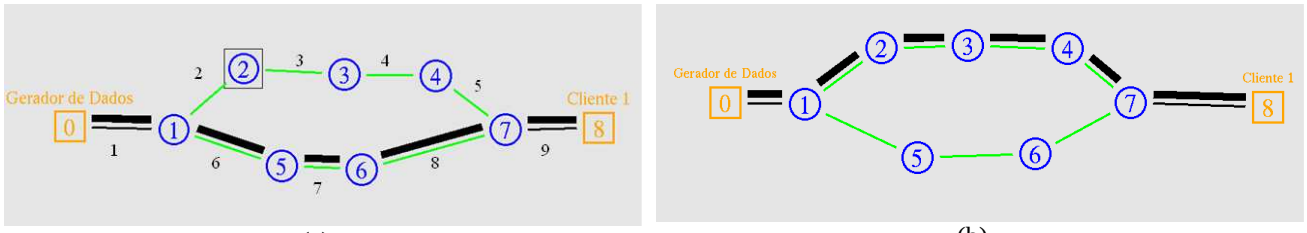
Os parâmetros acima referidos representam uma rede IP e são mantidos em todas as simulações do Cenário 1. De forma a cumprir os objectivos propostos para este cenário, as linhas de código relacionadas com a tecnologia MPLS, o protocolo de encaminhamento do pacote e o protocolo de distribuição do pacote são alteradas. As linhas de código referentes a cada tipo de simulação deste cenário encontram-se no Anexo B. Os ficheiros de código utilizados no simulador de rede NS-2.33 para cada simulação do Cenário 1 encontram-se nos Anexos C e D. Os resultados de cada simulação deste cenário estão representados e analisados na secção 5.4.

### 5.3.2 Cenário 2 – Funcionamento da Engenharia de Tráfego

Este cenário tem o objectivo de fazer perceber o funcionamento da Engenharia de Tráfego bem como identificar os casos onde a sua aplicação contribui para a eficiência da rede. O factor que mais afecta os serviços VoIP e IPTV é a perda de pacotes. Desta forma, na rede *Triple Play* a Engenharia de Tráfego será utilizada com o objectivo de reduzir a taxa de perda de pacotes provocada pelo congestionamento da rede. A Engenharia de Tráfego permite encaminhar o fluxo de dados num caminho diferente daquele que é utilizado na rede por defeito. Este procedimento tem o objectivo de reduzir o congestionamento da ligação que apresenta perdas.

O Cenário 2 é idêntico ao Cenário 1, apenas difere no tipo de gerador de tráfego e está representado na Figura 5.11. A Figura 5.11 a) ilustra o caminho escolhido pela rede quando não é aplicado a Engenharia de Tráfego. A rede, por defeito, escolhe o caminho com o menor número de saltos. Na Figura 5.11 b) pode ser visualizado o caminho que o fluxo de tráfego percorre quando é

aplicada a Engenharia de Tráfego. A Engenharia de Tráfego é uma ferramenta que permite o administrador de rede estipular o caminho por onde são encaminhados os pacotes pela rede.




(a) (b)

**Figura 5.11 – Cenário da simulação a) sem Engenharia de Tráfego b) com Engenharia de Tráfego**

As configurações da simulação da rede IP estão representadas na Tabela 5.2. Posto isto, foram simulados em primeiro lugar os três tipos de redes com o fluxo de 1000 *bytes*, depois as três redes com o fluxo de 2000 *bytes* e por fim foram simuladas as três redes com o fluxo de 3000 *bytes*. É de salientar que à medida que o fluxo aumenta no número de *bytes*, a largura de banda das ligações (1, 2, 6 e 9) também aumentam para suportar o fluxo de dados na entrada e saída da rede e prevenir o congestionamento na rede.

**Tabela 5.2 – Parâmetros atribuídos à topologia de rede do Cenário 2**

| | | | | | |
|---|---|---|---|---|---|
| Topologia de rede e configurações utilizado em todos os casos de simulação | Caminho 1 | 0-1-5-6-7-8 | | | |
| | Caminho 2 | 0-1-2-3-4-7-8 | | | |
| | Ligação 1 | 1 Mb | 2 Mb | 3 Mb | 1 ms |
| | Ligação 2 | 1 Mb | 2 Mb | 3 Mb | 1 ms |
| | Ligação 3 | 1 Mb | 1 ms | | |
| | Ligação 4 | 1 Mb | 1 ms | | |
| | Ligação 5 | 1 Mb | 1 ms | | |
| | Ligação 6 | 1 Mb | 2 Mb | 3 Mb | 1 ms |
| | Ligação 7 | 1 Mb | 1 ms | | |
| | Ligação 8 | 1 Mb | 1 ms | | |
| | Ligação 9 | 1 Mb | 2 Mb | 3 Mb | 1 ms |
| | Tráfego | *Exponential* | | | |
| | Tamanho do Pacote | 1000 | 2000 | 3000 | Bytes |
| | Taxa de Transferência | 1000 | kbps | | |
| | Gerador de Dados inicia | 0,1 | S | | |
| | Gerador de Dados termina | 1,8 | S | | |
| | Fim da Simulação | 2 | S | | |

Para demonstrar a perda de pacotes na rede são utilizados fluxos de tráfego de 1000 *bytes*, de 2000 *bytes* e de 3000 *bytes*. Este tráfego não corresponde a nenhum tráfego estipulado para o serviço *Triple Play*, porque o objectivo deste cenário é verificar a perda de pacotes e agir de forma a reduzir a perda de pacotes através da ferramenta Engenharia de Tráfego. A diferença de comportamento entre as redes IP, MPLS e MPLS-TE de acordo com o fluxo é demonstrada nestas simulações. As linhas de código referentes a cada tipo de simulação deste cenário encontram-se no Anexo B. Os ficheiros de código utilizados no simulador de rede NS-2.33 para cada simulação do Cenário 2 encontram-se nos Anexos C e D. Os resultados de cada simulação deste cenário estão representados e analisados na secção 5.4.

### 5.3.3 Cenário 3 – Métodos de Recuperação de Falhas

O objectivo deste cenário é mostrar as diferenças entre os vários métodos de recuperação de falhas nas ligações da rede. O factor mais importante a considerar é a taxa de perda de pacotes, uma vez que os serviços VoIP e IPTV são intolerantes ao mesmo. Posto isto, o método que apresentar a menor taxa de perda de pacotes será o método adoptado no cenário final.

Existem quatro métodos de recuperação de falhas: a Recuperação Global *Makam*, a Recuperação Global *Haskin*, a Recuperação Regional e a Recuperação Local. A topologia a ser utilizada neste cenário está ilustrada na Figura 5.12. O número de ligações existentes numa rede deve ser ponderada quando é considerada a recuperação de falhas. Em comparação com os cenários anteriores, nesta topologia existem mais duas ligações. Estas duas ligações são denominadas de ligações de protecção e tornam a rede resiliente a falhas. Uma ligação de protecção entre os nós LSR3 e LSR5 e outra entre os nós LSR4 e o LSR6. Isto permite facilitar o processo de recuperação de falhas, uma vez que o fluxo de tráfego pode contornar a falha e percorrer um caminho mais curto até ao destino. Adicionar mais uma ligação entre os nós LSR2 e LSR5 foi considerado, mas deu erro no simulador de rede NS-2.33.

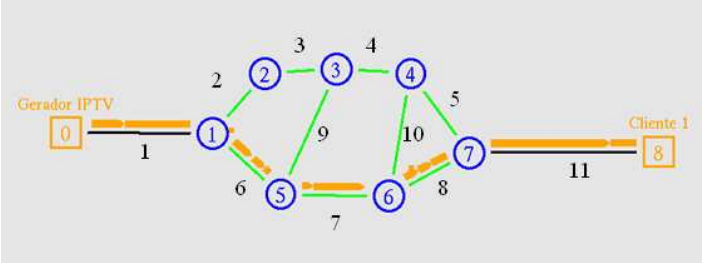



**Figura 5.12 – Topologia de rede do Cenário 3.**

Neste cenário, as configurações comuns a todas as simulações estão representadas na Tabela 5.3. É de destacar que o comando “rtmodel” provoca as falhas. Quando este comando é configurado como “down” é provocada a falha na ligação entre os nós LSR5 e LSR6, no instante indicado. Quando é configurado como “up” a ligação de falha é recuperada no instante indicado.

**Tabela 5.3 – Parâmetros atribuídos à topologia de rede do Cenário 3**

| | | | |
|---|---|---|---|
| Topologia de rede e configurações utilizado em todos os casos de simulação | Caminho 1 | 0-1-5-6-7-8 | |
| | Caminho 2 | 0-1-2-3-4-7-8 | |
| | Ligação 1 | 10 Mb | 1 ms |
| | Ligação 2 | 10 Mb | 1 ms |
| | Ligação 3 | 10 Mb | 1 ms |
| | Ligação 4 | 10 Mb | 1 ms |
| | Ligação 5 | 10 Mb | 1 ms |
| | Ligação 6 | 10 Mb | 1 ms |
| | Ligação 7 | 10 Mb | 1 ms |
| | Ligação 8 | 10 Mb | 1 ms |
| | Ligação 9 | 10 Mb | 1 ms |
| | Tráfego | *Exponential* | |
| | Tamanho do Pacote | 1402 | Bytes |
| | Taxa de Transferência | 4907 | Kbps |
| | $ns rtmodel-at 0.5 down $LSR5 $LSR6 | | |
| | $ns rtmodel-at 1.5 up $LSR5 $LSR6 | | |
| | Gerador de Dados inicia | 0,1 | s |
| | Gerador de Dados termina | 1,8 | s |
| | Fim da Simulação | 2 | s |

Para determinar qual o método de recuperação de rede mais eficaz são simulados os quatro métodos em cada tipo de rede (IP e MPLS e MPLS-TE) tanto na existência de falhas como na sua ausência. A implementação de cada método de recuperação de rede é distinta e as linhas de código encontram-se no Anexo B. Os ficheiros de código utilizados no simulador de rede NS-2.33 para cada simulação do Cenário 3 encontram-se nos Anexos C e D. Os resultados de cada simulação deste cenário estão representados e analisados na secção 5.4.

### 5.3.4 Cenário 4 – Limites da Rede *Triple Play*

O objectivo deste cenário é conhecer os limites da rede *Ethernet* (10/100/1000 Mbps) ao suportar o serviço *Triple Play* dentro dos limites dos requisitos de QoS de cada serviço. A topologia deste cenário está ilustrada na Figura 5.13. Observa-se que existem quatro Geradores de tráfego: um Gerador de Dados, um Gerador VoIP, um Gerador IPTV e um Gerador Web. O Gerador de Dados envia num tempo *Poisson/Exponencial* pacotes de 1500 *bytes* cada. O Gerador VoIP envia num tempo *Pareto* pacotes de 218 *bytes* cada. O Gerador IPTV envia num tempo *Exponencial* constante, pacotes de 1402 *bytes* cada. Por fim, o Gerador Web envia um fluxo de pacotes por segundo, nos dois sentidos da rede, em que simula o acesso a uma página Web. O Gerador Web envia, por vezes, rajadas de tráfego que condicionam o funcionamento e a eficiência da rede. O Gerador Web permite fazer com que esta rede tenha comportamentos muito próximos da realidade.

A topologia é semelhante à do Cenário 3 de modo a ser possível a recuperação na rede. Considera-se neste cenário um canal IPTV, um canal VoIP, uma transferência de ficheiros de dados e um acesso por segundo ao servidor HTTP correspondente a um cliente *Triple Play*. Analisa-se neste cenário o comportamento da rede com os 3 serviços (Dados, VoIP e IPTV) a funcionar em simultâneo, para cada cliente. É de salientar que este comportamento nem sempre se aplica na realidade, embora devem existir certos momentos, durante o dia, em que se verificam os 3 serviços

a funcionar em simultâneo. Para efeitos de simulação e de forma a verificar os limites da rede em questão, são simulados os 3 serviços a operar em simultâneo para todos os clientes existentes na rede *Triple Play*.

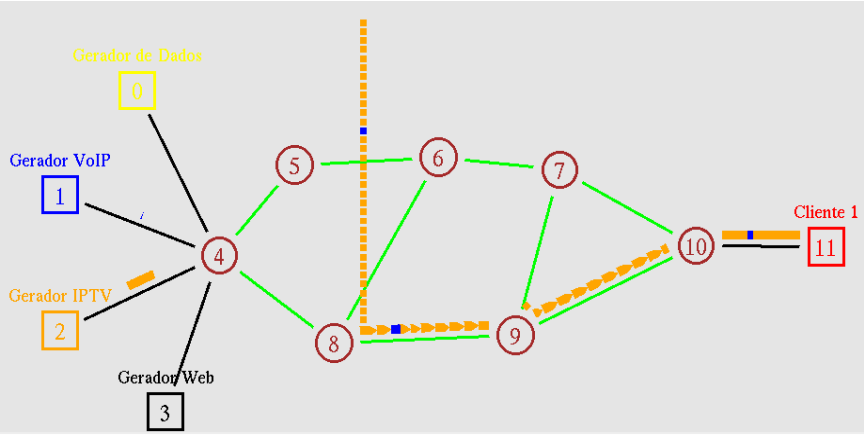



**Figura 5.13 – Topologia de rede do Cenário 4.**

Neste cenário são verificadas 5 situações baseadas nos resultados obtidos nos 3 cenários anteriores:

1. Apenas são utilizadas redes MPLS e MPLS-TE, uma vez que estas são as mais eficientes no encaminhamento de tráfego;
2. As configurações que são comuns a todas as redes e simulações deste cenário incluem o tráfego *PackMime* (Gerador Web) e todos os parâmetros da Tabela 5.4, de forma a aproximar a simulação de rede da realidade;
3. As configurações das redes sem falhas utilizam o protocolo de distribuição de etiquetas *Control-Driven*, uma vez que torna a rede mais eficiente;
4. As configurações das redes com falhas utilizam o protocolo de distribuição de etiquetas *Data-Driven*, o método de recuperação Global *Haskin* e o modelo "Deterministic" nas ligações entre os nós LSR4, LSR8, LSR9 e LSR10. O método de recuperação Global *Haskin* é o que apresenta a menor taxa de perda de pacotes de todos os métodos de recuperação e para ser configurado necessita do protocolo de distribuição de etiquetas *Data-Driven* para funcionar. O modelo "Deterministic" aplicado nas ligações permite causar falhas nas mesmas num tempo indeterminado de forma a aproximar a simulação de rede à realidade.
5. O Atraso nas ligações é de 1ms, pois estipulou-se que a fibra óptica seria utilizada como meio de transmissão em toda a rede.

**Tabela 5.4 – Parâmetros atribuídos à topologia de rede do Cenário 4**

| | | | | | |
|---|---|---|---|---|---|
| Topologia de rede e configurações utilizado em todos os casos de simulação | Caminho 1 | 4-5-6-7-10 | | | |
| | Caminho 2 | 4-5-6-7-9-10 | | | |
| | Caminho 3 | 4-5-6-8-9-10 | | | |
| | Caminho 4 | 4-5-6-8-9-7-10 | | | |
| | Caminho 5 | 4-8-9-10 | | | |
| | Caminho 6 | 4-8-9-7-10 | | | |
| | Caminho 7 | 4-8-6-7-10 | | | |
| | Caminho 8 | 4-8-6-7-9-10 | | | |
| | Ligação 1 | 1000 Mb | 1 ms | | |
| | Ligação 2 | 1000 Mb | 1 ms | | |
| | Ligação 3 | 1000 Mb | 1 ms | | |
| | Ligação 4 | 1000 Mb | 1 ms | | |
| | Ligação 5 | 1000 Mb | 1 ms | | |
| | Ligação 6 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 7 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 8 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 9 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 10 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 11 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 12 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 13 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Ligação 14 | 10 Mb | 100 Mb | 1000 Mb | 1 ms |
| | Tráfego | Poisson/Exponential | 1500 0s 200ms | | |
| | Tamanho do Pacote de Dados | 1500 | Bytes | | |
| | Taxa de Transferência do envio de Dados | 10000 | kbps | | |
| | Tempo em que não são Enviados Dados | 200 | ms | | |
| | Tráfego | Pareto | 218 500ms 50ms | | |
| | Tamanho do Pacote VoIP | 218 | Bytes | | |
| | Tempo em que são Enviados Pacotes VoIP | 500 | ms | | |
| | Tempo em que não são Enviados Pacotes VoIP | 50 | ms | | |
| | Taxa de Transferência do envio de VoIP | 87 | kbps | | |
| | Forma do Pareto VoIP | 1,5 | | | |
| | Tráfego | Exponential | 1402 0ms 0ms | | |
| | Tamanho do Pacote IPTV | 1402 | Bytes | | |
| | Taxa de Transferência do envio de IPTV | 4907 | kbps | | |
| | Iniciar o Tráfego | | | | |
| | | 10 Mb | 100 Mb | 1000 Mb | |
| | Tráfego de Páginas Web | 2 | 20 | 26 | 0,1s |
| | Inciar o Tráfego de Dados | 2 | 20 | 26 | 0,1s |
| | Inciar o Tráfego de VoIP | 2 | 20 | 26 | 0,1s |
| | Inciar o Tráfego de IPTV | 2 | 20 | 26 | 0,1s |
| | Terminar o Tráfego de Dados | 2 | 20 | 26 | 4,2s |
| | Terminar o Tráfego de VoIP | 2 | 20 | 26 | 4,2s |
| | Terminar o Tráfego de IPTV | 2 | 20 | 26 | 4,2s |
| | Terminar o Tráfego de Páginas Web | 2 | 20 | 26 | 4,2s |
| | Terminar Simulação | 5s | 5s | 5s | |

A perda de pacotes é o factor que mais afecta a qualidade de experiência do utilizador final. Posto isto, utiliza-se este factor como limitador das simulações. Tem-se como critério principal manter os limites das taxas de perdas dos serviços, particularmente os do serviço IPTV. Este é o serviço que envia a maior fluxo de tráfego na rede. Para mostrar as perdas de pacotes dentro do domínio MPLS é necessário forçar as perdas de pacotes nos nós LSR5 e LSR8. Efectua-se isto através da atribuição da largura de banda de 1 Gbps nas ligações 1,2,3,4,5 e 9 de forma a verificar perdas nos vários caminhos. Caso contrário, as perdas todas dar-se-ão no nó LSR4 de ingresso e não poderá ser utilizada a ferramenta da Engenharia de Tráfego, tal como foi concluído no cenário 2.Variaram-se as velocidades da Tecnologia *Ethernet* 10/100/1000 Mbps para verificar qual o limite de clientes que a rede suporta.

A implementação das linhas de código de cada simulação de rede utilizada neste cenário encontram-se no Anexo B. Os ficheiros de código utilizados no simulador de rede NS-2.33 para cada simulação do Cenário 4 encontram-se nos Anexos C e D. Os resultados de cada simulação deste cenário estão representados e analisados na secção 5.4.

## 5.4 RESULTADOS E ANÁLISES

Neste subcapítulo é apresentado e analisado os resultados obtidos das várias simulações e dos vários cenários propostos no subcapítulo 5.3. As conclusões tiradas dos três primeiros cenários são utilizadas para criar a topologia do Cenário 4. O objectivo do Cenário 4 é indicar qual o limite do número de clientes admitido numa dada rede (*Ethernet* 10/100/1000 Mbps) que utiliza as componentes mais eficientes dos cenários 1, 2 e 3.

### 5.4.1 Cenário 1 – Diferenças Entre a Rede IP e a Rede MPLS

Antes de determinar qual o melhor protocolo de encaminhamento de pacotes a utilizar numa rede MPLS é necessário ver o comportamento de dois modos de funcionando do protocolo DV. O protocolo DV funciona numa rede em que os encaminhamentos explícitos estão ou não presentes. Posto isto, verifica-se qual o modo mais eficiente de funcionamento do protocolo DV. Durante as simulações verificou-se um atraso no instante em que é efectuado o caminho explícito, nos casos em que não são previamente explícitos os encaminhamentos na rede. Assim, quanto mais cedo forem estipulados os caminhos explícitos, menor é o atraso dos pacotes na rede. Isto contribui para a optimização da eficiência da rede. Segundo os resultados obtidos, representados na Tabela 5.5, o modo de funcionamento do protocolo DV na presença do encaminhamento explícito é o mais eficiente, uma vez que apresenta o maior número de pacotes enviados, o menor atraso e o maior débito efectivo em comparação com o modo de funcionamento do protocolo DV na ausência do encaminhamento explícito. Nas simulações a seguir é utilizado o protocolo de encaminhamento de pacotes DV com os encaminhamentos explícitos.

A tabela 5.5 permite também verificar as diferenças entre os protocolos de encaminhamento DV e LS. Verifica-se que o protocolo DV apresenta uma menor variação de atraso e um maior débito efectivo do que o protocolo LS apesar de este último apresentar um menor número de pacotes enviados. O protocolo de encaminhamento LS demora muito tempo a analisar a rede para depois escolher o melhor caminho, enquanto o protocolo de encaminhamento DV escolhe o caminho com o menor número de saltos, tal como acontece na rede IP. Desta forma o protocolo de encaminhamento DV é mais eficiente do que o LS.

A comparação entre a rede IP e a rede MPLS também é possível através da Tabela 5.5. Observa-se que a rede MPLS apresenta um maior número de pacotes enviados com um menor atraso em comparação com a rede IP.

**Tabela 5.5 – Resultados obtidos para o modo de funcionamento do protocolo de encaminhamento de pacotes DV**

| | IP | MPLS | | |
|---|---|---|---|---|
| | | DV sem make-explicit-route | DV com make-explicit-route | LS |
| **Pacotes Enviados** | 7430 | 7521 | 7537 | 6266 |
| **Pacotes Recebidos** | 7430 | 7521 | 7537 | 6266 |
| **Pacotes Perdidos** | - | - | - | - |
| **Pacotes Perdidos (%)** | - | - | - | - |
| **Atraso Fim-a-Fim (ms)** | 9,161 | 8,691 | 8,614 | 8,033 |
| **Variação de Atraso Fim-a-Fim (ms)** | 0,321 | 0,374 | 0,411 | 0,288 |
| **Variação de Atraso Fim-a-Fim (ms)** | 1,640 | 1,950 | 1,967 | 2,003 |
| **Débito Effectivo Fim-a-Fim (Mbps)** | 23,051 | 21,005 | 21,009 | 18,883 |

É possível melhorar o desempenho do protocolo de distribuição de etiquetas *Data-Driven* no NS-2.33 através do modo "on demand", do modo "ordered control" e do modo "on demand - ordered control". Antes de proceder à comparação entre os protocolos de distribuição de etiquetas *Data-Driven* e *Control-Driven* é necessário verificar qual o tipo de protocolo *Data-Driven* que apresenta os melhores resultados.

Observa-se na Tabela 5.6 que as redes com o protocolo *Data-Driven* sem melhoramentos apresentam valores de qualidade de serviço inferiores aos das redes com o protocolo *Data-Driven* com melhoramentos. Verifica-se que o protocolo *Data-Driven* e o protocolo *Data-Driven-ordered control* apresentam os mesmos valores de qualidade de serviço em todos os tipos de redes. Observa-se também, que o protocolo *Data-Driven* e o protocolo *Data-Driven-ordered control* apresentam valores de QoS mais baixos do que o protocolo *Data-Driven-on demand*. Verifica-se que o protocolo *Data-Driven - on demand - ordered control* apresenta os melhores valores de QoS, em comparação com todas as combinações do protocolo *Data-Driven*. Nas simulações a seguir é utilizado o protocolo de distribuição de etiquetas *Data-Driven - on demand - ordered control*.

**Tabela 5.6 – Resultados obtidos para verificar qual o melhor modo de funcionamento do protocolo *Data-Driven***

| | Data Driven | | | Data Driven - on demand | | | Data Driven - order control | | | Data Driven – on demand – order control | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IP | MPLS | | IP | MPLS | | IP | MPLS | | IP | MPLS | |
| | | DV | LS | | DV | LS | | DV | LS | | DV | LS |
| **Pacotes Enviados** | 7438 | 7559 | 6284 | 7448 | 7575 | 6300 | 7438 | 7559 | 6284 | 7451 | 7578 | 6303 |
| **Pacotes Recebidos** | 7438 | 7559 | 6284 | 7448 | 7575 | 6300 | 7438 | 7559 | 6284 | 7451 | 7578 | 6303 |
| **Pacotes Perdidos** | - | - | - | - | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos (%)** | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso Fim-a-Fim (ms)** | 9,12 | 8,51 | 7,95 | 9,06 | 8,44 | 7,87 | 9,12 | 8,51 | 7,95 | 9,05 | 8,43 | 7,85 |
| **Variação de Atraso Fim-a-Fim (ms)** | 0,35 | 0,44 | 0,32 | 0,35 | 0,43 | 0,32 | 0,35 | 0,44 | 0,32 | 0,36 | 0,44 | 0,33 |
| **Variação de Atraso Fim-a-Fim (ms)** | 1,66 | 1,97 | 2,01 | 1,65 | 1,95 | 1,99 | 1,66 | 1,97 | 2,01 | 1,66 | 1,96 | 1,99 |
| **Débito Effectivo Fim-a-Fim (Mbps)** | 23,05 | 21,01 | 18,89 | 23,05 | 21,01 | 18,89 | 23,05 | 21,01 | 18,89 | 23,06 | 21,02 | 18,89 |

Esta próxima simulação tem como objectivo determinar quais as configurações a utilizar no Cenário 4. Foi verificado, durante as simulações, que os modos "on demand" e "ordered control" não têm qualquer influência na rede quando aplicados no protocolo de distribuição de etiquetas *Control-Driven*. A Tabela 5.7 mostra que o protocolo *Control-Driven* apresenta valores de QoS

melhores do que o protocolo *Data-Driven-on demand-ordered control*, uma vez que regra geral é enviado um maior número de pacotes com um atraso menor. De acordo com estes resultados, será utilizado o protocolo de distribuição de etiquetas *Control-Driven* na solução final.

Resta comparar as redes IP e MPLS que utilizam o protocolo *Control-Driven*. Observa-se que a rede MPLS permite enviar um maior número de pacotes pela rede e com menor atraso do que a rede IP. Isto deve-se ao facto de que o processo de leitura do cabeçalho do pacote, realizado pelos encaminhadores localizados dentro da rede MPLS através do processo de distribuição de etiquetas, é mais rápido do que o processo de leitura do cabeçalho do pacote pelos encaminhadores da rede IP.

Em suma, a simulação do Cenário 4 será efectuada numa rede MPLS com o protocolo de encaminhamento DV com explicitação de encaminhamentos e com o protocolo de distribuição de etiquetas *Control-Driven*.

**Tabela 5.7 – Resultados obtidos para verificar qual o melhor protocolo de distribuição de etiquetas.**

| | Data Driven – on demand – order control | | | Control Driven | | |
|---|---|---|---|---|---|---|
| | IP | MPLS | | IP | MPLS | |
| | | DV | LS | | DV | LS |
| **Pacotes Enviados** | 7451 | 7578 | 6303 | 7502 | 7615 | 6303 |
| **Pacotes Recebidos** | 7451 | 7578 | 6303 | 7502 | 7615 | 6303 |
| **Pacotes Perdidos** | - | - | - | - | - | - |
| **Pacotes Perdidos (%)** | - | - | - | - | - | - |
| **Atraso Fim-a-Fim (ms)** | 9,048 | 8,425 | 7,854 | 8,786 | 8,261 | 7,855 |
| **Variação de Atraso Fim-a-Fim (ms)** | 0,360 | 0,440 | 0,326 | 0,312 | 0,402 | 0,292 |
| **Variação de Atraso Fim-a-Fim (ms)** | 1,659 | 1,955 | 1,994 | 1,706 | 1,886 | 1,960 |
| **Débito Effectivo Fim-a-Fim (Mbps)** | 23,055 | 21,015 | 18,890 | 23,066 | 21,023 | 18,891 |

### 5.4.2 Cenário 2 – Funcionamento da Engenharia de Tráfego

A Engenharia de Tráfego é uma ferramenta utilizada na rede MPLS para balancear o tráfego pelos vários caminhos existentes na rede e reduzir o congestionamento da mesma e consequentemente reduzir a perda de pacotes. Na Tabela 5.8 pode ser observado que nas simulações efectuadas com o fluxo de 1000 *bytes* não provocaram congestionamento nem perdas de pacotes. Neste caso não é necessária a aplicação da Engenharia de Tráfego. Por curiosidade aplicou-se a Engenharia de Tráfego para verificar o comportamento da rede. O encaminhamento do tráfego através da Engenharia de Tráfego é efectuado no NS-2.33 através do comando "flow-erlsp-install". Este comando força o tráfego a ser encaminhado no caminho configurado. A cada caminho explícito é atribuído um número, que neste caso são o 1000 e o 1001. Neste caso foi utilizado o caminho explícito 1000 para encaminhar o tráfego através da Engenharia de Tráfego. Observa-se que, ao aplicar a Engenharia de Tráfego numa rede sem perda de pacotes, o número de pacotes enviados aumenta sem provocar congestionamento na rede. Isto deve-se ao facto do caminho 2 ter uma maior largura de banda do que o caminho 1. O atraso da rede MPLS é menor do que o atraso da rede MPLS-TE, uma vez que neste caso o fluxo percorre um caminho mais longo até chegar ao seu destino. Apesar da aplicação da Engenharia de Tráfego na rede obrigar o fluxo percorrer um

caminho mais longo, o atraso é menor do que o da rede IP e a quantidade de pacotes enviados é superior. As aplicações de serviços (Dados, VoIP e IPTV) funcionam melhor quanto maior for o número de pacotes recebidos e quanto menor for o atraso da chegada dos pacotes. Esta simulação demonstra que o balanceamento do tráfego na rede contribui para a eficiência do funcionamento das aplicações que recebem os pacotes.

As simulações efectuadas com o fluxo de tráfego de 2000 *bytes* apresentam alguma perda de pacotes. Nesta simulação a rede IP apresenta uma taxa de perda de pacotes e um atraso superior à da rede MPLS. Posto isto, a rede MPLS é mais eficiente do que a rede IP. É verificado na Tabela 5.8 que a aplicação da Engenharia de Tráfego contribui para a eliminação total da perda de pacotes. O processo da aplicação da Engenharia de Tráfego consiste em:

1. Identificar o nó que está a descartar os pacotes e o respectivo caminho (através do NAM);
2. Verificar o tempo de início da rejeição dos pacotes (através do NAM);
3. Encaminhar o tráfego para o caminho alternativo, no instante antes do início da rejeição de pacotes;
4. Verificar a existência da perda de pacotes. No caso da perda de pacotes continuar a ocorrer na rede é necessário repetir os pontos 1), 2), 3) e 4) até não ocorrer rejeição de pacotes ou até a perda de pacotes ser reduzida para um número inferior ao limite de QoS do serviço (VoIP ou IPTV) em questão.

Ao realizar a repetição dos 4 pontos acima referidos foi possível uma redução total da perda de pacotes, conforme pode ser observado na Tabela 5.8.

Por fim as simulações efectuadas com o fluxo de tráfego de 3000 *bytes* apresentam uma perda de pacotes significativa (na rede IP ~15,3% e na rede MPLS ~14,7%). Ao aplicar a ferramenta da Engenharia de Tráfego verificou-se que a taxa de perda era muito elevada para ser reduzida. Mesmo assim, tentou-se reduzir a perda de pacotes através da atribuição de múltiplos encaminhamentos, mas não foi o suficiente. Isto faz com que exista um número elevado de mudanças de encaminhamento. Observa-se através da Tabela 5.8 que a redução da taxa de perda de pacotes não é significativa. O elevado número de mudanças de encaminhamento provoca um aumento significativo no atraso fim-a-fim dos pacotes. Nestes casos, a única solução para o problema do congestionamento e consequente perda de pacotes é o aumento da largura de banda na rede de forma a suportar o fluxo em questão.

Em suma, a Engenharia de Tráfego aumenta a eficiência da rede mesmo quando não existe perda de pacotes. A Engenharia de Tráfego serve para reduzir totalmente a perda de pacotes no caso de esta não ser muito elevada. Para o caso da taxa de perda de pacotes e do número de mudanças de encaminhamento serem muito elevados, a solução é aumentar a largura de banda da rede ou reduzir

o fluxo existente na rede. Isto pode ser efectuado através da redução do número de clientes a aceder à rede. No entanto, não é viável a adopção desta segunda solução, uma vez que o número de adesões ao serviço *Triple Play* aumenta diariamente. No Cenário 4 será utilizada a ferramenta de Engenharia de Tráfego para reduzir a taxa de perda de pacotes na rede.

**Tabela 5.8 – Resultados obtidos para verificar o comportamento do funcionamento da Engenharia de Tráfego**

| | 1000 Bytes | | | 2000 Bytes | | | 3000 Bytes | | |
|---|---|---|---|---|---|---|---|---|---|
| | IP | MPLS | MPLS-TE | IP | MPLS | MPLS-TE | IP | MPLS | MPLS-TE |
| **Pacotes Enviados** | 1137 | 1250 | 1408 | 1820 | 1933 | 2486 | 2460 | 2573 | 3047 |
| **Pacotes Recebidos** | 1137 | 1250 | 1408 | 1627 | 1740 | 2475 | 2055 | 2167 | 2767 |
| **Pacotes Perdidos** | - | - | - | 164 | 164 | - | 377 | 378 | 249 |
| **Pacotes Perdidos (%)** | - | - | - | 9,011 | 8,484 | - | 15,325 | 14,691 | 8,172 |
| **Pacotes Perdidos LSR2** | - | - | - | - | - | - | - | - | 249 |
| **Pacotes Perdidos LSR2 (%)** | - | - | - | - | - | - | - | - | 8,172 |
| **Pacotes Perdidos LSR5** | - | - | - | 164 | 164 | - | 377 | 378 | - |
| **Pacotes Perdidos LSR5 (%)** | - | - | - | 9,011 | 8,484 | - | 15,325 | 14,691 | - |
| **Atraso Fim-a-Fim (ms)** | 33,987 | 25,097 | 28,859 | 169,973 | 138,496 | 150,003 | 127,541 | 110,323 | 135,690 |
| **Variação de Atraso Fim-a-Fim (ms)** | 0,098 | 3,760 | 3,281 | 233,113 | 196,647 | 5,134 | 192,288 | 169,179 | 127,001 |
| **Débito Effectivo Fim-a-Fim (Mbps)** | 4,643 | 4,316 | 4,976 | 6,237 | 6,243 | 9,156 | 7,952 | 7,957 | 10,328 |

### 5.4.3 Cenário 3 – Métodos de recuperação de falhas

As recuperações Global *Makam*, Regional e Local são configuradas no NS-2.33 através da ferramenta de Engenharia de Tráfego.

A recuperação Global *Haskin* tem a particularidade de utilizar o protocolo de distribuição de pacotes “Data-Driven” em conjunto com o comando “$m enable-reroute "new" ” e o comando “reroute-binding” para ser simulada no NS-2.33. Quando não é utilizado o comando “$m enable-reroute "new" ” a eficiência da rede diminui, ou seja, são enviados menos pacotes até ao destino. Os tempos dos encaminhamentos explícitos e das junções, através do comando “reroute-binding”, devem ser respeitadas, caso contrário a simulação não funciona no modo de recuperação Global *Haskin*.

A simulação da recuperação nas redes IP ou de “melhor esforço” é efectuada no NS-2 através do comando da Engenharia de tráfego “flow-erlsp-install” e sem o modo de encaminhamento de protocolos DV. A simulação dos vários métodos das recuperações de falhas é efectuada através do comando da Engenharia de tráfego “flow-erlsp-install”.

O aspecto da recuperação de cada método está representado na Figura 5.14. Pode-se verificar que os resultados estão de acordo com os fundamentos teóricos. No método Global *Makam* (Figura 5.14 a)), a recuperação da falha é efectuada pela comutação do fluxo de tráfego com o caminho alternativo no LSR de ingresso. Por outro lado, no método Global *Haskin* (Figura 5.14 b)), a recuperação da falha é efectuada através da comutação do fluxo de tráfego até ao LSR de ingresso, no sentido contrário a partir do ponto de falha. Depois é encaminhado pelo caminho alternativo até ao utilizador final. No método Regional (Figura 5.14 c)) a comutação do fluxo de tráfego é efectuada pelo LSR que detecta a falha. Este encaminha o fluxo em direcção ao caminho

alternativo através da ligação mais próxima da falha. Finalmente, no método Local (Figura 5.14 d)) a comutação é efectuada, localmente, pelo LSR que detecta a falha onde o fluxo de tráfego contorna a falha. Depois retorna ao caminho de trabalho.

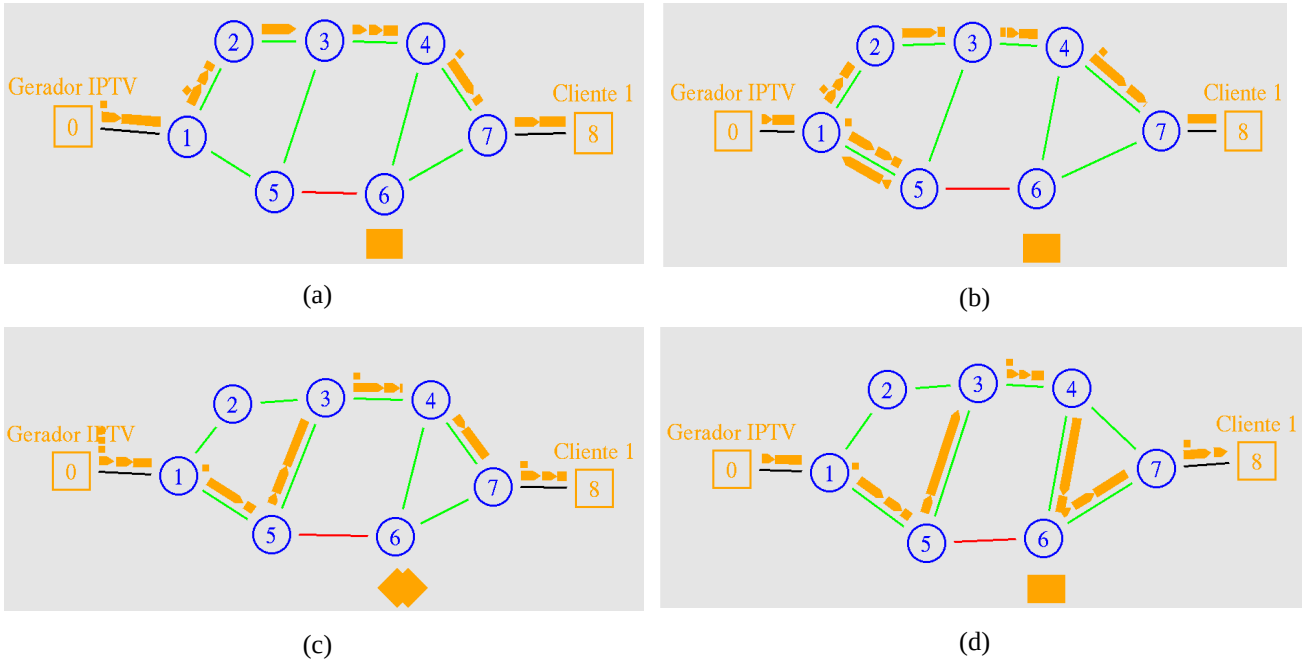



**Figura 5.14 – Método de Recuperação a) Global Makam b) Global Haskin c) Regional d) Local**

Os resultados das simulações encontram-se na Tabela 5.9. Observa-se que a rede IP utiliza o método de recuperação cujo encaminhamento é igual ao método de recuperação global *Makam*, ou seja, os dados são encaminhadas pelo caminho de recuperação, independentemente da localização da falha. O número de pacotes enviados são mais elevados quando existem falhas. Isto porque além de ser utilizado o caminho de trabalho, também é utilizado o caminho alternativo (com mais saltos do que o caminho de trabalho). Quanto maior o número de saltos, maior é a largura de banda. Quanto maior a largura de banda, maior é a quantidade de tráfego que passa pela rede e consequentemente maior é número de pacotes enviados até ao destino.

Como fora dito anteriormente, o factor mais importante numa rede *Triple Play* é a perda de pacotes. No entanto, é de salientar a importância do factor da reserva de recursos e do factor do tempo de interrupção do serviço.

Observa-se que o método Global *Makam* e o método Regional apresentam o mesmo número de taxa de perda de pacotes. O *Makam* e o Regional apresentam uma taxa de perdas mais elevada, em comparação com o método Global *Haskin* e o método Local, porque a FIS (*Fault Indication Signal*) é enviada ao LSR de ingresso antes do tráfego ser comutado para o caminho de recuperação. Quanto mais afastado estiver a falha do LSR de ingresso, mais lento é o processo de detecção da falha e maior é o número de perda de pacotes. A perda de pacotes é provocada pelo atraso da detecção, notificação, cálculo do caminho alternativo e recuperação da rede perante uma

falha. Durante o tempo em que não é conhecida a falha e não é reencaminhado o tráfego para um caminho alternativo, existe perda de pacotes.

Os métodos Global *Haskin* e Local são os que apresentam a menor taxa de perda de pacotes. Isto porque, qualquer LSR detecta falhas e comuta o tráfego para o caminho de recuperação de forma imediata. Quanto mais perto estiver a falha do LSR de egresso menor é o número de pacotes descartados. Isto deve-se ao facto de que quanto mais perto estiver a falha do LSR de egresso, mais pequeno é o caminho de recuperação.

Destaca-se que o método de recuperação que apresenta menor taxa de perda é o método de recuperação Global *Haskin*.

A recuperação de falhas implica, em alguns casos, a reserva de recursos antes da ocorrência da falha. Noutros casos são exigidos recursos adicionais para que a falha seja recuperada (*on demand*) no instante em que ocorre a falha. A reserva prévia dos recursos implica a existência na rede de recursos extra para serem utilizados em caso de falha. Trata-se de uma desvantagem em termos de custo para os provedores de serviços. No entanto, tem a vantagem de assegurar qualquer falha que ocorra na rede. Esta vantagem supera a desvantagem do custo, uma vez que a perda de dados e a indisponibilidade do serviço de transferência de dados causam grandes prejuízos à imagem das empresas dependentes da Internet. Uma má imagem da empresa que presta o serviço pode ser causada devido à indisponibilidade do mesmo.

A presença ou ausência de recursos adicionais na rede depende do método de recuperação utilizado na rede. O método Regional é o único método que não necessita de reservar recursos antes da ocorrência de uma falha, pois o caminho alternativo é calculado pelo protocolo de encaminhamento DV. Este cálculo é efectuado na altura da ocorrência da falha (*on demand*) com base no menor número de saltos até ao destino.

O método *Makam* e o método Local necessitam apenas de reservar quatro recursos. O método *Haskin* reserva os quatro recursos que pertencem ao caminho de recuperação juntamente com os recursos incluídos no caminho onde o tráfego toma o sentido contrário (no nosso caso são mais dois). Depois é seguido o caminho de recuperação. O número de reserva de recursos depende da topologia da rede. Quanto maior for o número de ligações na topologia, maior é o número de reserva de recursos.

O tempo de interrupção do serviço é o tempo em que o utilizador final não recebe quaisquer dados devido a uma falha na rede. O tempo em que o utilizador final não recebe pacotes (a) é dado por:

$$\mathbf{a = b - c - d}$$

em que (b) refere-se ao tempo em que o pacote demora a contornar a ligação de falha e a chegar ao cliente. A variável (c) corresponde ao instante em que ocorreu a falha enquanto que o parâmetro (d) diz respeito ao tempo de detecção e recuperação da falha.

Observa-se que a recuperação *Makam* tem um tempo de detecção e recuperação da falha mais lento do que os restantes métodos. Nos métodos *Haskin* e *Makam*, quanto mais afastada estiver a falha do LSR de ingresso, maior é o tempo de interrupção do serviço. No método Local, quanto mais afastada estiver a falha do LSR de egresso, maior é o tempo de interrupção do serviço. O tempo de detecção da falha é de 1,314 ms para os métodos *Haskin*, Regional e Local e de 1,800 ms para os métodos *Makam* e *Makam* sem DV.

Em suma, o método *Haskin* apresenta a menor taxa de perda de pacotes, o maior número de recursos reservados na rede e o maior tempo de interrupção do serviço.

Como conclusão, numa rede *Triple Play* deve ser utilizado o método de recuperação *Haskin*, pois este método reduz a taxa de perda de pacotes na rede. Sabe-se que o método *Haskin* apresenta o maior tempo de interrupção do serviço mas é mais compensatório esperar um certo intervalo de tempo do que perder os pacotes. Os *buffers* das aplicações tratam do atraso dos pacotes, no entanto não tratam de recuperar pacotes perdidos. Desta forma, será utilizado no Cenário 4 o método de recuperação Global *Haskin*.

**Tabela 5.9 – Resultados obtidos para verificar qual o melhor método de recuperação de falhas**

| | Redes Sem Falhas | | Redes Com Falhas | | | | | |
|---|---|---|---|---|---|---|---|---|
| | IP | MPLS | Global Makam sem DV | Regional – Local Dinâmico | Global Makam | Global Haskin | Regional – Local Dinâmico | Local – Fast Reroute |
| | | | IP/MPLS-TE | MPLS | MPLS-TE | MPLS-TE | MPLS-TE | MPLS-TE |
| **Pacotes Enviados** | 7538 | 7664 | 8692 | 8705 | 8977 | 10269 | 8989 | 10131 |
| **Pacotes Recebidos** | 7538 | 7664 | 8690 | 8703 | 8975 | 10267 | 8987 | 10129 |
| **Pacotes Perdidos** | - | - | 2 | 2 | 2 | 2 | 2 | 2 |
| **Pacotes Perdidos (%)** | - | - | 0,023 | 0,023 | 0,022 | 0,019 | 0,022 | 0,020 |
| **Pacotes Perdidos LSR1** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR1 (%)** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR2** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR2 (%)** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR3** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR3 (%)** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR4** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR4 (%)** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR5** | - | - | 2 | 2 | 2 | 2 | 2 | 2 |
| **Pacotes Perdidos LSR5 (%)** | - | - | 0,023 | 0,023 | 0,022 | 0,019 | 0,022 | 0,020 |
| **Pacotes Perdidos LSR6** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR6 (%)** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR7** | - | - | - | - | - | - | - | - |
| **Pacotes Perdidos LSR7 (%)** | - | - | - | - | - | - | - | - |
| **Atraso Fim-a-Fim (ms)** | 8,611 | 8,055 | 9,741 | 8,314 | 8,534 | 10,869 | 8,498 | 9,576 |
| **Variação de Atraso Fim-a-Fim (ms)** | 1,668 | 1,807 | 1,676 | 1,719 | 1,725 | 1,930 | 1,724 | 1,747 |
| **Débito Efectivo Fim-a-Fim (Mbps)** | 23,074 | 21,029 | 26,546 | 23,510 | 24,258 | 28,414 | 24,260 | 27,483 |
| **Recursos Reservados** | - | - | 4 | - | 4 | 6 | - | 4 |
| **Tempo de detecção e recuperação da falha (ms)** | - | - | 1,800 | 1,314 | 1,800 | 1,314 | 1,314 | 1,314 |
| **Tempo de interrupção do serviço** | - | - | 7,200 | 5,400 | 7,200 | 9,000 | 6,741 | 8,514 |

### 5.4.4 Cenário 4 – Limites da Rede *Triple Play*

Para determinar qual o número limite de clientes para uma dada rede, recorre-se às limitações dos parâmetros de QoS de cada serviço do *Triple Play*, estipuladas na Tabela 5.10. Os resultados obtidos nas simulações do Cenário 4 que ultrapassam os parâmetros de QoS abaixo citados não são aceites. O parâmetro de QoS que nenhum dos serviços tolera, é a taxa de perda de pacotes logo este parâmetro será o principal condicionador das simulações. No caso dos resultados

obtidos da taxa de perda de pacotes apresentarem valores superiores a 3% para os serviços Dados e VoIP a simulação não será aceite. Também não serão aceites as simulações cujos resultados obtidos da taxa de perda de pacotes sejam superiores a 1% para o serviço IPTV.

**Tabela 5.10 – Requisitos de cada serviço que pertence ao serviço *Triple Play*.**

| | Dados | VoIP | IPTV |
|---|---|---|---|
| **Largura de banda** | Ordem dos Kbps no mínimo | 64 Kbps constante no mínimo | 3 Mbps constantes no mínimo |
| **Tolerância à perda de pacotes** | Tolera uma perda de pacotes menor que 3% | Tolera uma perda de pacotes menor que 3% | Tolera uma perda de pacotes menor que 1% |
| **Tolerância a Atrasos** | Insensível | <150 ms | <150 ms |
| **Tolerância a variações de atrasos** | Insensível | <50 ms | <30 ms |
| **Considerações chave das redes** | Fiabilidade na rede sem perda de pacotes. | QoS (respeitar os mínimos);<br>Emissão em tempo real. | QoS (respeitar os mínimos);<br>Emissão em tempo real;<br>Fiabilidade;<br>Multicast e Unicast;<br>Desempenho elevado. |

Neste cenário existem dois grupos de simulações: grupo A e grupo B. As simulações do grupo A, determinam o número limite de clientes de uma dada rede (*Ethernet* 10/100/1000 Mbps) na ausência de falhas. As simulações do grupo B, determinam o comportamento de uma dada rede (*Ethernet* 10/100/1000 Mbps) na existência de falhas nas ligações.

Para simplificar o processo da obtenção dos resultados das simulações efectuadas para este cenário, foi delineado uma série de passos a seguir. O procedimento indicado abaixo foi seguido de forma a simular as 3 diferentes redes (10/100/1000 Mbps) para determinar o número limite de clientes para uma dada rede:

**Grupo A**

1. Fazer simulações onde são adicionados clientes *Triple Play* até a rede apresentar uma taxa de perda de pacotes não superior a 1% no tráfego de IPTV.
2. Aplicar a ferramenta da Engenharia de Tráfego na última simulação do ponto 1 de forma a encaminhar o tráfego *Triple Play* para o caminho 2 no instante 2.1s (comutar o tráfego a metade do tempo da simulação).
3. Adicionar mais um cliente para além do limite de clientes no ponto 1 e simular sem a ferramenta da Engenharia de Tráfego.
4. Aplicar a ferramenta da Engenharia de Tráfego à simulação do ponto 3 em vários caminhos da rede até reduzir a perda de pacotes para um valor inferior a 1%, no tráfego de IPTV.

Através do ponto 1 do procedimento do Grupo A, constata-se que na rede *Ethernet* de 10 Mbps é apenas possível a existência simultânea de 2 clientes *Triple Play* na rede. A taxa de perda de pacotes de todos os serviços estão dentro dos parâmetros de QoS apresentados na Tabela 5.10. Verifica-se através da Tabela 5.11 que a taxa de perda de pacotes dos serviços *Triple Play* desceu quando aplicado a ferramenta da Engenharia de Tráfego (exemplo: IPTV = 0,282% desceu para

IPTV = 0,076%) mencionado no ponto 2 do procedimento do Grupo A. Neste caso, a Engenharia de Tráfego serviu para balancear o tráfego pela rede.

Simular a rede com 3 clientes (ponto 3) provocou um aumento na taxa de perda de pacotes dos serviços *Triple Play*, para valores superiores aos limites dos parâmetros de QoS. A aplicação da ferramenta da Engenharia de Tráfego (ponto 4) melhorou apenas os valores da taxa de perda de pacotes do serviço VoIP. Os valores da taxa de perda de pacotes dos serviços de Dados e IPTV são demasiado elevados para a realização do ponto 4 (caso semelhante ao cenário 2 de tráfego de 3000 *bytes)*. Desta forma, a rede *Ethernet* de 10 Mbps não suporta o serviço *Triple Play* com mais de 2 clientes em simultâneo. A solução para aumentar o número de clientes numa rede é aumentar a largura de banda da rede.

Da Tabela 5.11 observa-se que os valores do atraso são mantidos abaixo dos limites dos estipulados na Tabela 5.10 em todos os serviços do serviço *Triple Play*. O mesmo acontece para os valores da variação de atraso.

Verifica-se através da Tabela 5.11 que os nós de congestionamento em que são perdidos os pacotes são os LSR5 e LSR8. Estes nós encontram-se no início da rede onde existe o maior fluxo de dados. Os pacotes são descartados nos nós, uma vez que a largura de banda das ligações localizadas à frente dos nós não suporta o fluxo de tráfego.

**Tabela 5.11 – Resultados obtidos para verificar o limite de clientes numa rede *Ethernet* 10 Mbps.**

| | 10Mb | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Simulações Sem Falhas | | | | | | | | | | | |
| | Dados | | | | VoIP | | | | IPTV | | | |
| | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE |
| | | | | | | | | | PackMime = 2 | | PackMime = 3 | |
| | Nº canais = 2 | | Nº canais =3 | | Nº canais = 2 | | Nº canais =3 | | Nº canais = 2 | | Nº canais =3 | |
| **Pacotes Enviados** | 353 | 344 | 594 | 726 | 1865 | 2070 | 2656 | 3177 | 37654 | 39334 | 45559 | 52279 |
| **Pacotes Recebidos** | 350 | 344 | 561 | 678 | 1859 | 2069 | 2564 | 3103 | 37548 | 39304 | 41541 | 48313 |
| **Pacotes Perdidos** | 3 | - | 33 | 48 | 6 | 1 | 92 | 74 | 106 | 30 | 4018 | 3966 |
| **Pacotes Perdidos (%)** | 0,850 | - | 5,556 | 6,612 | 0,322 | 0,048 | 3,464 | 2,329 | 0,282 | 0,076 | 8,819 | 7,586 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR5** | - | - | - | 48 | - | 1 | - | 74 | - | 22 | - | 3966 |
| Pacotes Perdidos LSR5 (%) | - | - | - | 6,612 | - | 0,048 | - | 2,329 | - | 0,05 | - | 7,586 |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - | | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - | | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - | | - | - |
| Pacotes Perdidos **LSR8** | 3 | - | 33 | - | 6 | - | 92 | - | 106 | 8 | 4018 | - |
| Pacotes Perdidos LSR8 (%) | 0,850 | - | 5,556 | - | 0,322 | - | 3,464 | - | 0,282 | 0,020 | 8,819 | - |
| Pacotes Perdidos **LSR9** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR9 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR10** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR10 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 17,129 | 27,324 | 24,392 | 36,591 | 19,642 | 31,624 | 27,457 | 47,314 | 20,995 | 32,284 | 21,478 | 35,399 |
| **Variação de Atraso** Fim-a-Fim (ms) | 116,813 | 126,267 | 64,801 | 69,721 | 12,300 | 13,387 | 16,032 | 20,562 | 0,560 | 0,859 | 10,911 | 18,023 |
| **Débito Efectivo** Fim-a-Fim (Mbps) | 0,428 | 0,436 | 0,761 | 0,935 | 0,759 | 0,839 | 1,047 | 1,259 | 49,660 | 51,544 | 55,963 | 64,860 |

Através do ponto 1 do procedimento do Grupo A, verifica-se que na rede *Ethernet* de 100 Mbps é apenas possível existirem 20 clientes *Triple Play* em simultâneo. A taxa de perda de pacotes

de todos os serviços estão dentro dos parâmetros de QoS apresentados na Tabela 5.10. Verifica-se através da Tabela 5.12 que a taxa de perda de pacotes dos serviços Dados e VoIP aumentou quando aplicado a ferramenta da Engenharia de Tráfego enquanto que a taxa de perda de pacotes do serviço IPTV desceu. O aumento da taxa de perda de pacotes dos serviços Dados e VoIP deve-se ao elevado número de pacotes enviados quando aplicado a ferramenta da Engenharia de Tráfego. Por outro lado, a aplicação da ferramenta da Engenharia de Tráfego revelou-se positiva para o serviço IPTV.

Simular a rede com 21 clientes (ponto 3) provocou um aumento na taxa de perda de pacotes dos serviços *Triple Play*. Apenas o serviço IPTV apresentou valores superiores aos limites dos parâmetros de QoS. A aplicação da ferramenta da Engenharia de Tráfego (ponto 4) melhorou os valores da taxa de perda de pacotes do serviço IPTV mas não foi o suficiente, uma vez que foi apenas possível baixar o valor para 1,025%, conforme ilustrado na Tabela 5.12, apesar das inúmeras tentativas. Desta forma, a rede *Ethernet* de 100 Mbps não suporta o serviço *Triple Play* com mais de 21 clientes em simultâneo. A solução para aumentar o número de clientes numa rede é aumentar a largura de banda da rede.

Da Tabela 5.12 observa-se que os valores do atraso são mantidos abaixo dos limites dos estipulados na Tabela 5.10 em todos os serviços do serviço *Triple Play*. O mesmo acontece para os valores da variação de atraso. Verifica-se através da Tabela 5.12 que os nós de congestionamento em que são perdidos os pacotes são os LSR5 e LSR8.

**Tabela 5.12 – Resultados obtidos para verificar o limite de clientes numa rede *Ethernet* 100 Mbps.**

| | 100Mb | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Simulações Sem Falhas | | | | | | | | | | | |
| | Dados | | | | VoIP | | | | IPTV | | | |
| | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE | MPLS | MPLS-TE |
| | | | | | | | | | PackMime = 20 | | PackMime = 21 | |
| | Nº canais = 20 | | Nº canais =21 | | Nº canais = 20 | | Nº canais =21 | | Nº canais = 20 | | Nº canais =21 | |
| **Pacotes Enviados** | 4443 | 4810 | 4103 | 6876 | 18243 | 20249 | 19249 | 29296 | 351987 | 387455 | 362797 | 567159 |
| **Pacotes Recebidos** | 4422 | 4781 | 4067 | 6843 | 18207 | 20204 | 19166 | 29203 | 349643 | 385153 | 356933 | 561344 |
| **Pacotes Perdidos** | 21 | 29 | 36 | 33 | 36 | 45 | 83 | 93 | 2344 | 2302 | 5864 | 5815 |
| **Pacotes Perdidos (%)** | 0,473 | 0,603 | 0,877 | 0,480 | 0,197 | 0,222 | 0,431 | 0,317 | 0,666 | 0,594 | 1,616 | 1,025 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR5** | - | 17 | - | 33 | - | 34 | - | 91 | - | 1376 | - | 5765 |
| Pacotes Perdidos LSR5 (%) | - | 0,353 | - | 0,48 | - | 0,168 | - | 0,311 | - | 0,355 | - | 1,016 |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR8** | 21 | 12 | 36 | - | 36 | 11 | 83 | 2 | 2344 | 926 | 5864 | 50 |
| Pacotes Perdidos LSR8 (%) | 0,473 | 0,249 | 0,877 | - | 0,197 | 0,054 | 0,431 | 0,007 | 0,666 | 0,239 | 1,616 | 0,009 |
| Pacotes Perdidos **LSR9** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR9 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR10** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR10 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 6,762 | 7,245 | 6,735 | 9,839 | 6,755 | 7,304 | 6,767 | 9,895 | 6,793 | 7,333 | 6,644 | 9,612 |
| **Variação de Atraso** Fim-a-Fim (ms) | 9,119 | 9,267 | 9,817 | 9,317 | 1,629 | 1,646 | 1,574 | 1,884 | 0,188 | 0,201 | 0,356 | 0,529 |
| **Débito Effectivo** Fim-a-Fim (Mbps) | 6,244 | 6,784 | 5,777 | 9,707 | 7,515 | 8,338 | 7,911 | 12,054 | 465,013 | 512,241 | 475,593 | 748,297 |

Através do ponto 1, verifica-se que na rede *Ethernet* de 1000 Mbps é apenas possível a existência de 26 clientes *Triple Play* em simultâneo na rede, uma vez que o valor da taxa de perda de pacotes do serviço IPTV ultrapassou o limite do valor de 1%. Os serviços de Dados e VoIP não apresentaram perdas de pacotes ao adicionar mais um cliente aos 26 numa rede *Ethernet* 1000 Mbps. Isto deve-se ao facto dos pacotes dos serviços referidos por último são muito pequenos em comparação com o tamanho dos pacotes do serviço IPTV. A taxa de perda de pacotes do serviço IPTV é de 0,794%. Com o ponto 2 do procedimento do Grupo A, conseguiu-se que este valor baixasse para 0,720%, conforme mostra a Tabela 5.13.

Simular a rede com 27 clientes (ponto 3) provocou um aumento na taxa de perda de pacotes do serviço IPTV para 1,575%, conforme ilustrado na Tabela 5.13. Este valor está relativamente próximo do limite de 1%. No caso anterior verificou-se que apesar de se aplicar a Engenharia de Tráfego a taxa de perda de pacotes ultrapassava os 1%. Isto também se aplica ao presente caso. Desta forma, não foi aplicada a Engenharia de Tráfego para reduzir a taxa de perda de pacotes.

**Tabela 5.13 – Resultados obtidos para verificar o limite de clientes numa rede *Ethernet* 1000 Mbps.**

| | 1000Mb | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Simulações Sem Falhas | | | | | | | | |
| | Dados | | | VoIP | | | IPTV | | |
| | MPLS | MPLS-TE | MPLS | MPLS | MPLS-TE | MPLS | MPLS | MPLS-TE | MPLS |
| | | | | | | | PackMime = 26 | | PackMime = 27 |
| | Nº canais = 26 | | Nº canais =27 | Nº canais = 26 | | Nº canais =27 | Nº canais = 26 | | Nº canais =27 |
| **Pacotes Enviados** | 5530 | 6006 | 5420 | 24215 | 25967 | 24660 | 449396 | 495346 | 452962 |
| **Pacotes Recebidos** | 5530 | 6006 | 5420 | 24215 | 25967 | 24660 | 445830 | 491780 | 445830 |
| **Pacotes Perdidos** | - | - | - | - | - | - | 3566 | 3566 | 7132 |
| **Pacotes Perdidos (%)** | - | - | - | - | - | - | 0,794 | 0,720 | 1,575 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | 3566 | 3566 | 7132 |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | 0,794 | 0,72 | 1,575 |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR5** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR5 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR8** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR8 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR9** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR9 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR10** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR10 (%) | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 5,043 | 5,537 | 5,043 | 5,012 | 5,512 | 5,012 | 5,177 | 5,696 | 5,177 |
| **Variação de Atraso** Fim-a-Fim (ms) | 7,340 | 7,420 | 7,488 | 0,828 | 0,891 | 0,795 | 0,085 | 0,085 | 0,085 |
| **Débito Effectivo** Fim-a-Fim (Mbps) | 7,814 | 8,491 | 7,658 | 10,000 | 10,728 | 10,186 | 592,372 | 653,283 | 592,377 |

**Grupo B**

Simular a rede (*Ethernet* 10/100/1000 Mbps) com o número limite de clientes já estipulado nas simulações do Grupo A com uma falha "Deterministic":

1. Na ligação entre o LSR4 e LSR8;
2. Na ligação entre o LSR8 e LSR9;
3. Na ligação entre o LSR9 e LSR10.

Nas simulações a seguir verifica-se se os parâmetros de QoS não ultrapassam os limites estipulados na Tabela 5.10, numa dada rede (*Ethernet* 10/100/1000 Mbps) com o número limite de clientes estipulados nas simulações do Grupo A nas piores das hipóteses que é numa rede MPLS com falhas nas ligações e sem o uso da ferramenta da Engenharia de Tráfego.

Verifica-se, através da Tabela 5.14, que a presença das falhas de ligações na rede *Ethernet* 10 Mbps não fazem com que os valores dos parâmetros de QoS ultrapassam os limites em nenhum dos serviços do *Triple Play.* Os resultados obtidos a seguir são em função da utilização do método de recuperação Global *Haskin.* Estes resultados devem-se ao facto do método de recuperação Global *Haskin* obrigar a comutação do fluxo de dados até ao LSR de ingresso, no sentido contrário a partir do ponto de falha para depois ser encaminhado pelo caminho alternativo até ao utilizador final, conforme ilustra a Figura 15.4 b). Este processo é demorado mas faz com que a perda de pacotes seja mínima.

A falha de ligação entre os nós LSR4 e LSR8 e a falha de ligação entre os nós LSR8 e LSR9 contribuem para a diminuição do valor da taxa de perda de pacotes dos serviços de Dados e VoIP. Enquanto que a falha de ligação entre os nós LSR9 e LSR10 aumenta o valor da taxa de perda de pacotes para os mesmos serviços.

A falha de ligação entre os nós LSR4 e LSR8 e a falha de ligação entre os nós LSR9 e LSR10 contribuem para a diminuição do valor da taxa de perda de pacotes do serviço IPTV. Da mesma forma, a falha de ligação entre os nós LSR8 e LSR9 aumenta o valor da taxa de perda de pacotes para o mesmo serviço. A taxa de perda de pacotes depende do número de pacotes enviados. A presença de falhas geralmente influencia negativamente o número de pacotes enviados, uma vez que as falhas fazem com que haja um maior número de protocolos de sinalização a serem transferidos na rede e a ocupar a largura de banda. O nó LSR8 apresenta um número elevado de perda de pacotes em comparação com o resto dos nós existentes na rede. Este nó encontra-se no início da rede e tem uma concentração de fluxos de dados muito elevada que por vezes é estrangulada pela largura de banda neste ponto levando os nós a descartarem o excesso de pacotes.

A presença de falhas causam um maior atraso na rede em todos os serviços do *Triple Play*, uma vez que a rede demora a se adaptar aos novos encaminhamentos de tráfego de forma a contornar a falha. O menor atraso no serviço de Dados acontece na presença de falha na ligação entre os nós LSR9 e LSR10. Nos serviços de VoIP e IPTV o menor atraso acontece na presença de falha na ligação entre os nós LSR8 e LSR9. O maior atraso em todos os serviços do *Triple Play* acontece na presença de falha de ligação entre os nós LSR4 e LSR8.

**Tabela 5.14 – Resultados obtidos para verificar o comportamento da rede *Ethernet* 10 Mbps em caso de falha.**

| | 10Mb | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Nº canais = 2 | | | | | | | | | | | |
| | Dados | | | | VoIP | | | | IPTV | | | |
| | | | | | | | | | PackMime = 2 | | | |
| | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | |
| | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 |
| **Pacotes Enviados** | 353 | 345 | 510 | 351 | 1865 | 1967 | 2189 | 1991 | 37654 | 37544 | 41755 | 37102 |
| **Pacotes Recebidos** | 350 | 343 | 506 | 345 | 1859 | 1964 | 2185 | 1977 | 37548 | 37487 | 41621 | 37001 |
| **Pacotes Perdidos** | 3 | 2 | 4 | 6 | 6 | 3 | 4 | 14 | 106 | 57 | 134 | 101 |
| **Pacotes Perdidos (%)** | 0,850 | 0,580 | 0,784 | 1,709 | 0,322 | 0,153 | 0,183 | 0,703 | 0,282 | 0,152 | 0,321 | 0,272 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | - | - | - | - | 4 | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | - | - | - | - | 0,011 | - | - |
| Pacotes Perdidos **LSR5** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR5 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR8** | 3 | - | 4 | 6 | 6 | 1 | 4 | 14 | 106 | 8 | 134 | 91 |
| Pacotes Perdidos LSR8 (%) | 0,850 | - | 0,784 | 1,709 | 0,322 | 0,051 | 0,183 | 0,703 | 0,282 | 0,021 | 0,321 | 0,245 |
| Pacotes Perdidos **LSR9** | - | - | - | - | - | - | - | - | - | - | - | 10 |
| Pacotes Perdidos LSR9 (%) | - | - | - | - | - | - | - | - | - | - | - | 0,027 |
| Pacotes Perdidos **LSR10** | - | 2 | - | - | - | 2 | - | - | - | 45 | - | - |
| Pacotes Perdidos LSR10 (%) | - | 0,580 | - | - | - | 0,102 | - | - | - | 0,120 | - | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 17,129 | 24,149 | 22,395 | 21,481 | 19,642 | 26,940 | 21,430 | 24,522 | 20,995 | 28,072 | 21,614 | 25,856 |
| **Variação de Atraso** Fim-a-Fim (ms) | 116,813 | 117,963 | 87,419 | 120,093 | 12,300 | 12,750 | 10,876 | 13,804 | 0,560 | 0,883 | 0,780 | 1,282 |
| **Débito Effectivo** Fim-a-Fim (Mbps) | 0,428 | 0,439 | 0,644 | 0,441 | 0,759 | 0,799 | 0,894 | 0,806 | 49,660 | 49,362 | 54,980 | 48,867 |

Verifica-se, através da Tabela 5.15, que a presença das falhas de ligações na rede *Ethernet* 100 Mbps não fazem com que os valores dos parâmetros de QoS ultrapassam os limites em nenhum dos serviços do *Triple Play*. Os resultados obtidos a seguir são em função da utilização do método de recuperação Global *Haskin.*

Todas as falhas de ligação dos serviços de Dados e IPTV contribuem para a diminuição do valor da taxa de perda de pacotes. De forma semelhante, a falha de ligação entre todas as ligações no serviço VoIP aumenta o valor da taxa de perda de pacotes para os mesmos serviços. Os nós LSR5 e LSR8 apresentam um número elevado de perda de pacotes em comparação com o resto dos nós existentes na rede. Estes nós encontram-se no início da rede e têm uma concentração de fluxos de dados muito elevada que por vezes é estrangulada pela largura de banda nestes pontos e os nós descartam o excesso de pacotes.

A presença de falhas causam um maior atraso na rede em todos os serviços do *Triple Play*, uma vez que a rede demora a se adaptar aos novos encaminhamentos de tráfego de forma a contornar a falha. O menor atraso em todos os serviços do serviço *Triple Play* acontece na presença de falha na ligação entre os nós LSR9 e LSR10. O maior atraso em todos os serviços do *Triple Play* acontece na presença de falha de ligação entre os nós LSR8 e LSR9.

**Tabela 5.15 – Resultados obtidos para verificar o comportamento da rede *Ethernet* 100 Mbps em caso de falha.**

| | 100Mb | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Nº canais = 20 | | | | | | | | | | | |
| | Dados | | | | VoIP | | | | IPTV | | | |
| | | | | | | | | | PackMime = 20 | | | |
| | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | |
| | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 |
| **Pacotes Enviados** | 4443 | 4451 | 4692 | 4322 | 18243 | 18997 | 21547 | 19472 | 351987 | 372130 | 414585 | 372289 |
| **Pacotes Recebidos** | 4422 | 4436 | 4672 | 4305 | 18207 | 18931 | 21454 | 19415 | 349643 | 370111 | 412367 | 369981 |
| **Pacotes Perdidos** | 21 | 15 | 20 | 17 | 36 | 66 | 93 | 57 | 2344 | 2019 | 2218 | 2308 |
| **Pacotes Perdidos (%)** | 0,473 | 0,337 | 0,426 | 0,393 | 0,197 | 0,347 | 0,432 | 0,293 | 0,666 | 0,543 | 0,535 | 0,620 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | 3 | - | - | - | 40 | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | 0,016 | - | - | - | 0,011 | - | - |
| Pacotes Perdidos **LSR5** | - | 4,000 | 3,000 | - | - | 16,000 | 16,000 | - | - | 483,000 | 510,000 | - |
| Pacotes Perdidos LSR5 (%) | - | 0,09 | 0,064 | - | - | 0,084 | 0,074 | - | - | 0,13 | 0,123 | - |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR8** | 21 | 11 | 17 | 15 | 36 | 30 | 41 | 55 | 2344 | 1488 | 1660 | 2255 |
| Pacotes Perdidos LSR8 (%) | 0,473 | 0,247 | 0,362 | 0,347 | 0,197 | 0,158 | 0,190 | 0,282 | 0,666 | 0,400 | 0,400 | 0,606 |
| Pacotes Perdidos **LSR9** | - | - | - | 2 | - | - | - | 2 | - | - | - | 53 |
| Pacotes Perdidos LSR9 (%) | - | - | - | 0,046 | - | - | - | 0,01 | - | - | - | 0,014 |
| Pacotes Perdidos **LSR10** | - | - | - | - | - | 17 | 36 | - | - | 8 | 48 | - |
| Pacotes Perdidos LSR10 (%) | - | - | - | - | - | 0,089 | 0,167 | - | - | 0,002 | 0,012 | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 6,762 | 8,068 | 8,556 | 7,509 | 6,755 | 7,992 | 8,563 | 7,517 | 6,793 | 8,072 | 8,655 | 7,555 |
| **Variação de Atraso** Fim-a-Fim (ms) | 9,119 | 9,557 | 10,005 | 9,868 | 1,629 | 1,719 | 1,739 | 1,673 | 0,188 | 0,205 | 0,204 | 0,202 |
| **Débito Effectivo** Fim-a-Fim (Mbps) | 6,244 | 6,257 | 6,613 | 6,068 | 7,515 | 7,812 | 8,853 | 8,012 | 465,013 | 492,063 | 547,895 | 491,926 |

Verifica-se, através da Tabela 5.16, que a presença das falhas de ligações na rede *Ethernet* 1000 Mbps não fazem com que os valores dos parâmetros de QoS ultrapassam os limites em nenhum dos serviços do *Triple Play*. Os resultados obtidos a seguir são obtidos em função da utilização do método de recuperação Global *Haskin.*

Observa-se através da Tabela 5.16 que os serviços de Dados e VoIP são minimamente afectados pelas falhas de ligação nesta rede *Ethernet* 1000 Mbps. Todas as falhas de ligação no serviço IPTV contribuem para a diminuição do valor da taxa de perda de pacotes. Os nós Gerador IPTV e LSR8 apresentam um número elevado de perda de pacotes em comparação com o resto dos nós existentes na rede. Estes nós encontram-se no início da rede e têm uma concentração de fluxos de dados muito elevada que por vezes é estrangulada pela largura de banda nestes pontos e os nós descartam o excesso de pacotes.

A presença de falhas causam um maior atraso na rede em todos os serviços do *Triple Play*, uma vez que a rede demora a se adaptar aos novos encaminhamentos de tráfego de forma a contornar a falha através do método de recuperação Global *Haskin*. O menor atraso em todos os serviços do serviço *Triple Play* acontece na presença de falha na ligação entre os nós LSR4 e LSR8. O maior atraso em todos os serviços do *Triple Play* acontece na presença de falha de ligação entre os nós LSR8 e LSR9 tal como na rede *Ethernet* 100 Mbps.

**Tabela 5.16 – Resultados obtidos para verificar o comportamento da rede *Ethernet* 100 Mbps em caso de falha.**

| | 1000Mb | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Nº canais = 26 | | | | | | | | | | | |
| | Dados | | | | VoIP | | | | IPTV | | | |
| | | | | | | | | | PackMime = 26 | | | |
| | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | | MPLS sem falhas | MPLS com falhas entre | | |
| | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 | | LSR4 e LSR8 | LSR8 e LSR9 | LSR9 e LSR10 |
| **Pacotes Enviados** | 5530 | 5874 | 6252 | 5902 | 24215 | 25720 | 28729 | 25306 | 449396 | 474243 | 527663 | 475596 |
| **Pacotes Recebidos** | 5530 | 5874 | 6250 | 5902 | 24215 | 25716 | 28723 | 25304 | 445830 | 470626 | 524001 | 471980 |
| **Pacotes Perdidos** | - | - | 2 | - | - | 4 | 6 | 2 | 3566 | 3617 | 3662 | 3616 |
| **Pacotes Perdidos (%)** | - | - | 0,032 | - | - | 0,016 | 0,021 | 0,008 | 0,794 | 0,763 | 0,694 | 0,760 |
| Pacotes Perdidos no **Gerador** | - | - | - | - | - | - | - | - | 3566 | 3566 | 3566 | 356 |
| Pacotes Perdidos no Gerador (%) | - | - | - | - | - | - | - | - | 0,794 | 0,752 | 0,676 | 0,75 |
| Pacotes Perdidos **LSR4** | - | - | - | - | - | 4 | - | - | - | 51 | - | - |
| Pacotes Perdidos LSR4 (%) | - | - | - | - | - | 0,016 | - | - | - | 0,011 | - | - |
| Pacotes Perdidos **LSR5** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR5 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR6** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR6 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR7** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR7 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos **LSR8** | - | - | 2 | - | - | - | 6 | - | - | - | 96 | - |
| Pacotes Perdidos LSR8 (%) | - | - | 0,032 | - | - | - | 0,021 | - | - | - | 0,018 | - |
| Pacotes Perdidos **LSR9** | - | - | - | - | - | - | - | 2 | - | - | - | 50 |
| Pacotes Perdidos LSR9 (%) | - | - | - | - | - | - | - | 0,008 | - | - | - | 0,011 |
| Pacotes Perdidos **LSR10** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos LSR10 (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no **Cliente** | - | - | - | - | - | - | - | - | - | - | - | - |
| Pacotes Perdidos no Cliente (%) | - | - | - | - | - | - | - | - | - | - | - | - |
| **Atraso** Fim-a-Fim (ms) | 5,043 | 5,308 | 5,924 | 5,343 | 5,012 | 5,298 | 5,886 | 5,310 | 5,177 | 5,457 | 6,061 | 5,473 |
| **Variação de Atraso** Fim-a-Fim (ms) | 7,340 | 7,261 | 7,607 | 7,282 | 0,828 | 0,816 | 0,813 | 0,790 | 0,085 | 0,085 | 0,085 | 0,085 |
| **Débito Effectivo** Fim-a-Fim (Mbps) | 7,814 | 8,318 | 8,864 | 8,349 | 10,000 | 10,622 | 11,859 | 10,451 | 592,372 | 625,180 | 696,137 | 627,127 |

Em suma, a solução mais viável para o aumento do número de clientes na rede é o aumento da largura de banda. Uma alternativa ao aumento da largura de banda para optimizar a eficiência da rede é a utilização de tecnologias que permitam um aumento do fluxo de tráfego na rede. Utilizou-se nesta dissertação a tecnologia *Ethernet* sobre MPLS. Através das simulações verificou-se que esta tecnologia tem grande influência no aumento do fluxo na rede em comparação com a rede *Ethernet* sobre IP. Isto deve-se ao facto de o processo de leitura do cabeçalho de cada pacote ser mais rápido e provocar menos congestionamento na rede. O MPLS permite a utilização da Engenharia de Tráfego e contribui para o aumento do fluxo na rede ao encaminhá-lo por outros caminhos que não sejam o caminho com menor saltos.

A Engenharia de Tráfego permite balancear o tráfego por toda a rede e contribuir para a eficiência da mesma. Verificou-se que o limite de clientes para *Ethernet* 10 Mbps sobre MPLS era de 2 clientes, para a rede *Ethernet* 100 Mbps sobre MPLS o limite de clientes era de 20 clientes enquanto que para a tecnologia *Ethernet* 1000 Mbps sobre MPLS o limite era de 26 clientes. Estes limites foram baseados no suposto que todos os serviços *Triple Play* estivessem a funcionar em simultâneo para os 26 clientes da rede *Ethernet* 1000 Mbps, como exemplo. Na realidade, todos os serviços do *Triple Play* raramente estão ligados todos em simultâneo para cada cliente, logo o número de clientes ainda pode aumentar. As simulações apresentadas nesta dissertação foram efectuadas de forma a verificar o comportamento da rede numa situação de pico. Estas situações de pico existem na rede mas é apenas durante um número de horas durante o dia ou em certas épocas

do ano. É de salientar que estes limites se aplicam às redes simuladas nesta dissertação conforme as configurações estipuladas em cada uma das redes. No caso de comparação de estes resultados com um caso real deve se ter em consideração o número de ligações e respectiva largura de banda, o número de nós, o meio de transmissão e as tecnologias de transporte. O número de ligações tem influência no volume de tráfego que circula na rede, uma vez que o aumento do número de ligações provoca o aumento da largura de banda na rede. Como fora observado durante as simulações, a largura de banda tem muita influência na determinação do número limite de clientes.

## 5.5 SOLUÇÃO DA ARQUITECTURA FINAL E CONCLUSÕES

Nesta secção é apresentada a solução da arquitectura que permite fornecer o encaminhamento óptimo ou quase óptimo do tráfego em redes *Triple Play* com base nas conclusões tiradas ao longo desta dissertação.

A arquitectura é constituída por duas redes, a rede de acesso e a rede núcleo. As conclusões obtidas para a rede de acesso foram baseadas na teoria do Capítulo 2. As conclusões obtidas para a rede núcleo foram baseadas na prática (simulações do simulador de rede NS-2.33) do Capítulo 5.

A rede de acesso é constituída por:

- Fibra óptica (de preferência) numa rede GPON e a tecnologia *Ethernet* ou
- No caso de aproveitar o cobre é necessário utilizar a tecnologia VDSL2

A infraestrutura da rede de acesso, conforme ilustrado na Figura 5.15, é constituída pelo meio de transmissão em fibra óptica numa distribuição FTTH (*Fiber to the Home*) e por vezes numa distribuição FTTC (*Fiber to the Curb*), por um sistema GPON e a tecnologia VDSL2. A utilização da fibra óptica permite disponibilizar ao utilizador final elevadas larguras de banda, baixos atrasos e baixas variações de atraso. O sistema GPON é constituído pelos equipamentos passivos OLT (*Óptical Line Terminal*), divisores ópticos e ONT (*Óptical Network Terminal*) na distribuição FTTH e constituído pela mistura de equipamentos passivos (OLT e divisores ópticos) e activos (ONU - *Óptical Network Unit*) na distribuição FTTC para reaproveitar o cobre que vai até à casa do subscritor. A taxa de transferência na rede GPON é de 1,2 Gbps [Allied Telesyn, 2004].

No caso da largura de banda ser dividida entre 24 utilizadores, é disponibilizado a cada cliente uma largura de banda de 50 Mbps. Esta taxa de transferência permite fornecer ao cliente pelo menos 4 canais IPTV (em simultâneo) de alta definição para além dos serviços VoIP e de dados. O transporte do tráfego *Triple Play* no meio de transmissão de cobre é efectuado através da tecnologia VDSL2. A distância entre o armário do ONU e a casa do utilizador final não deve ser superior a 1 km para manter a velocidade de *download* nos 50 Mbps de forma a suportar o serviço *Triple Play* com elevada qualidade de serviço.

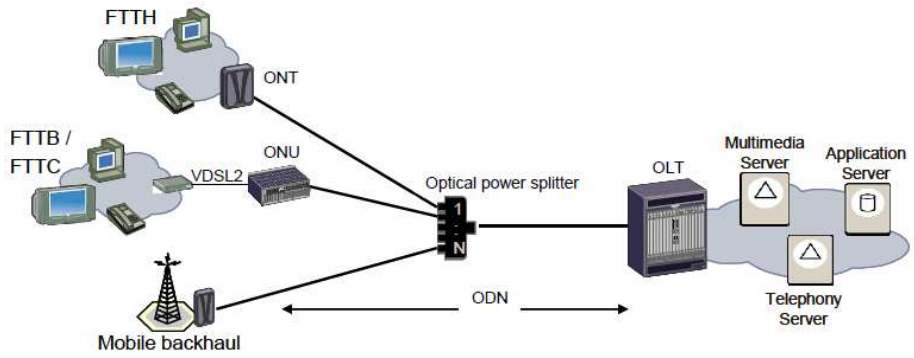



**Figura 5.15 – Solução da Arquitectura da rede de Acesso [ERICSSON, 2008]**

A solução da arquitectura da rede núcleo foi baseada nas conclusões tiradas ao longo deste trabalho (Capítulos 2, 3, 4 e 5) bem como nas simulações efectuadas no simulador de rede NS-2.33 (Capítulo 5). Baseado nas conclusões tiradas ao longo desta dissertação a solução da arquitectura da rede núcleo inclui a utilização:

- Da fibra óptica em toda rede núcleo;
- Da tecnologia de transporte *Ethernet*;
- Da implementação de uma rede MPLS;
- Da ferramenta de Engenharia de Tráfego, e;
- Do método de recuperação de falhas denominado Golbal *Haskin*;

A fibra óptica é o meio físico de transporte que permite reduzir a taxa de perda de pacotes (fundamental para o tráfego IPTV e o tráfego VoIP) e aumentar a taxa de transferência dos pacotes na rede. A tecnologia de transporte *Ethernet* apresenta a vantagem de fornecer às redes a capacidade de suportar elevados volumes de tráfego (1 Gbps), conforme visto no Capítulo 2.

No Cenário 1 foi concluído que a utilização da tecnologia MPLS na rede contribuía para uma maior eficiência da rede através do encaminhamento rápido dos pacotes pela rede. Foi também concluído neste cenário que a rede MPLS configurada com o protocolo de encaminhamento DS e o protocolo de distribuição de etiquetas *Control-Driven* apresentavam resultados que contribuía para a eficiência da rede. Desta forma a solução da arquitectura final utiliza a tecnologia MPLS juntamente com os protocolos acima referidos. A rede que utiliza a tecnologia *Ethernet* juntamente com a tecnologia MPLS é denominada uma rede EoMPLS (*Ethernet* sobre MPLS), como fora visto no Capítulo 2.

A tecnologia MPLS permite aplicar a ferramenta de Engenharia de Tráfego na rede. Esta ferramenta permite controlar o encaminhamento do tráfego de forma a balancear o tráfego pela rede e optimizar a sua eficiência. Esta ferramenta é muito útil para resolver o problema do congestionamento da rede, uma vez que permite encaminhar o tráfego por qualquer caminho da rede. Desta forma, é optimizada a utilização de todos os caminhos existentes na rede. Isto verifica-se nas simulações efectuadas no Cenário 2.

A resiliência da rede é um dos factores mais importantes numa rede que suporta o serviço *Triple Play*, uma vez que o mau funcionamento do serviço *Triple Play* é inaceitável pelo cliente final. As falhas na rede causam perdas de pacotes que contribuem para o mau funcionamento do serviço *Triple Play*. Desta forma, a rede deve ter implementado um método de recuperação de falhas para minimizar a percepção do mau funcionamento do serviço *Triple Play* pelo cliente final perante uma falha de rede. A tecnologia MPLS tem a capacidade de fornecer vários métodos de recuperação de falhas de rede. O Cenário 3 mostra como o método de recuperação de falhas denominado Global *Haskin* é o método que apresenta a menor taxa de perda de pacotes fundamental para o correcto funcionamento do serviço *Triple Play*.

O Cenário 4 representa a rede núcleo da solução da arquitectura proposta neste trabalho e mostra o funcionamento da mesma através de simulações. Este cenário foi criado de acordo com os resultados obtidos dos Cenários 1, 2 e 3. O Cenário 4 inclui quatro geradores de tráfego que aproximam a simulação do serviço *Triple Play* à realidade. Cada gerador de tráfego envia pacotes que incluem o cabeçalho *Ethernet* de forma a representar a utilização da tecnologia de transporte *Ethernet* na solução final da arquitectura.

A Figura 5.16 representa as várias camadas existentes na rede núcleo da arquitectura proposta neste trabalho. A camada física, a camada MPLS, a camada *Ethernet* e a camada de IP. A camada física é constituída por uma rede de fibra óptica que permite transmitir os pacotes fisicamente pela rede. A camada MPLS deve ser implementada e trata do encaminhamento dos pacotes pela rede. A camada *Ethernet* já existe nas redes núcleo e é reaproveitada para funcionar juntamente com a tecnologia MPLS e tornar a rede núcleo mais eficiente. A camada IP também é reaproveitada e trata de encaminhar os pacotes até ao destino quando estes não se encontrarem na rede núcleo.

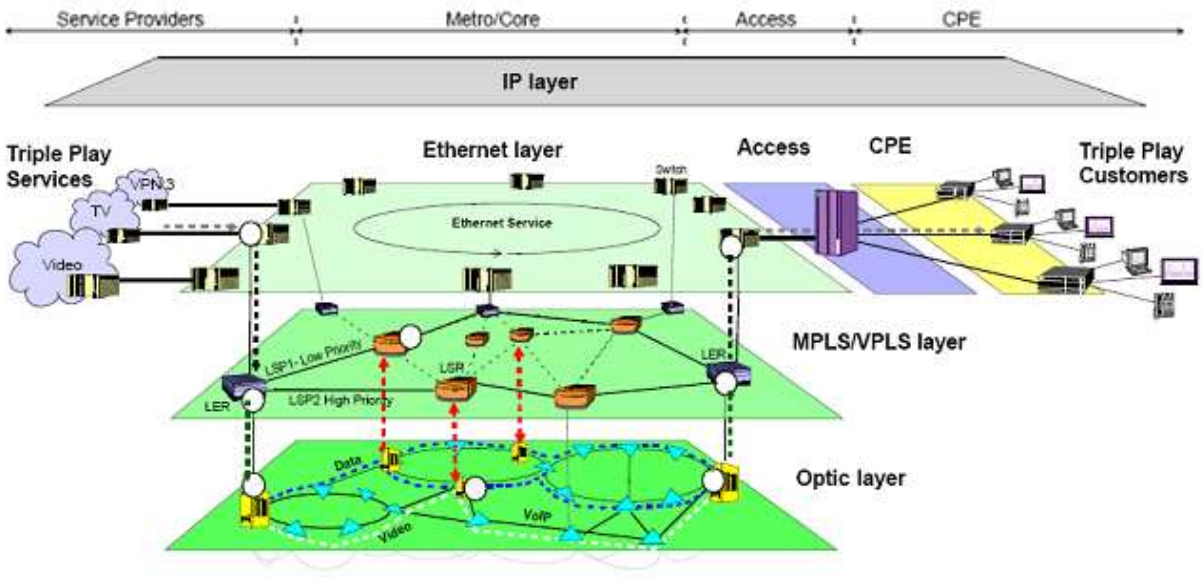



**Figura 5.16 – As várias camadas da rede núcleo em redes *Triple Play*.**

**Originalidade e relevância deste trabalho de dissertação**

Esta solução da arquitectura foi baseada nas conclusões obtidas ao longo desta dissertação tanto da parte teórica com da parte prática. Nesta dissertação e nesta arquitectura foram abordados todos os aspectos que fazem parte de uma rede que suporta o serviço *Triple Play,* desde a rede núcleo até à rede de acesso.

Foram realizadas, nesta dissertação, simulações para comparar as diferenças entre:

- Redes IP e Redes MPLS
- Todas as configurações aplicáveis na rede MPLS
- Redes MPLS sem e com a aplicação da ferramenta de Engenharia de Tráfego
- Os diferentes métodos de recuperação de falhas nas redes MPLS

As configurações das tecnologias que proporcionavam eficiência, resiliência e robustez à rede obtidas nas simulações acima referidas foram utilizadas no Cenário 4. Este cenário representa a solução da arquitectura proposta e serve para observar o comportamento do funcionamento da rede em situações extremas. É considerada uma situação extrema quando um cliente utiliza todos os serviços do serviço *Triple Play* em simultâneo. O Cenário 4 permitiu obter o valor limite de clientes numa da rede em situações extremas. Este cenário também permitiu obter resultados dos parâmetros de QoS de cada tipo de tráfego (Dados, VoIP e IPTV) existente numa rede *Triple Play.* Salienta-se que o tamanho do pacote de cada tipo de tráfego foi calculado em função do *codec* utilizado recentemente no mercado, ou seja, para o tráfego VoIP foi utilizado o *codec* G.711 e para o tráfego IPTV foi utilizado o *codec* MPEG-4.

Esta dissertação ajuda o administrador de rede a escolher os parâmetros de forma a adaptar a rede IP existente a uma rede que suporta o serviço *Triple Play* utilizando as componentes que tornam a IP existente numa rede mais eficiente, resiliente e robusta. As conclusões tiradas nesta dissertação permitem:

- Mostrar quais as componentes a ter em conta ao projectar uma rede que suporta o serviço *Triple Play* cujo fluxo de tráfego é significativamente mais elevado em comparação com redes que suportam outros tipos de serviços;
- Sugerir os elementos (baseados em simulações) a aplicar em redes existentes de forma a tornar as mesmas mais eficientes, resilientes e robustas;
- Mostrar quais as limitações das redes e estabelece soluções para ultrapassar estes limites numa dada rede;
- Visualizar o comportamento de cada tipo de tráfego numa dada rede;
- Analisar os resultados obtidos dos parâmetros de QoS de cada tipo de tráfego existente na rede *Triple Play* (Dados, VoIP e IPTV), e;
- Visualizar o comportamento de uma dada rede na presença de falhas.

# CAPÍTULO VI

# CONCLUSÕES E TRABALHOS FUTUROS

Cada vez mais, os consumidores de conteúdos multimédia são mais activos, participativos e exigentes, não só em relação à qualidade da imagem e som, mas também nos recursos e controlo sobre a programação. Estes novos clientes exigem dispositivos interactivos. Muito do que a televisão oferece acontece de uma forma analógica, sem qualidade, unidireccional, sem interactividade e com um número de canais limitados. Pelo contrário, o serviço IPTV é completamente digital, com um número ilimitado de canais e um elevadíssimo nível de interactividade. O IPTV não é apenas uma televisão moderna, mas sim uma tecnologia do futuro.

A realização deste trabalho foi motivada pelo aparecimento do serviço *Triple Play* que permite fornecer ao utilizador final o novo serviço IPTV bem como os serviços já conhecidos de dados e VoIP. O objectivo deste trabalho consistiu em encontrar a melhor solução para implementar uma rede *Triple Play* de forma a encontrar o encaminhamento óptimo, ou quase óptimo, para o tráfego. Sabe-se que as redes IP foram inicialmente concebidas apenas para a transferência de ficheiros entre computadores sem garantias da entrega de pacotes. Este conceito é inaceitável para os serviços VoIP e IPTV, uma vez que estes exigem a garantia dos requisitos de qualidade de serviço na rede para o seu correcto funcionamento. O desafio deste trabalho consiste em verificar como a rede IP suporte os requisitos de qualidade de serviço dos serviços de Dados, VoIP e IPTV. A selecção do encaminhamento óptimo, ou quase óptimo, implicou considerar a redução da taxa de perda de pacotes provocada por congestionamentos e falhas existentes na rede. A selecção do encaminhamento óptimo também implicou seleccionar a melhor solução que permitisse melhorar os requisitos da qualidade de serviço (atraso, variação de atraso, débito efectivo e perda de pacotes) da rede IP.

Na realização deste trabalho primeiro foi efectuado um levantamento dos requisitos de qualidade de serviço de cada serviço existente na rede *Triple Play* (Dados, VoIP e IPTV). Depois, fez-se um levantamento das tecnologias da rede de acesso e da rede núcleo disponíveis, para suportar as exigências da rede convergente *Triple Play.* Em terceiro, estudou-se os métodos de QoS existentes no mercado que permitem melhorar os parâmetros de qualidade de serviço das redes IP. Em quarto comparou-se os três tipos de simuladores de redes (J-SIM, OPNet e NS-2) mais populares de forma a escolher o mais adequado para a realização deste trabalho. Por fim, modelou-se quatro tipos de cenários e fez-se várias simulações para obter resultados e posteriormente analisá-los e tirar conclusões.

Após a análise aos vários tipos de rede de acesso concluiu-se que as redes de acesso em fibra óptica permitiam o suporte mais adequado ao serviço *Triple Play*, uma vez que a fibra óptica fornece elevadas larguras de banda e atrasos mínimos no transporte de dados. Esta solução implica um grande investimento monetário na infra-estrutura, tanto a nível do meio de transmissão como a nível dos equipamentos de rede, mas provê a demanda pelas elevadas larguras de banda por parte dos futuros clientes. Uma solução alternativa, mais económica, consiste em aproveitar o cobre de par entrançado existente na rede de acesso até à casa do utilizador final e aplicar a tecnologia VDSL2. Esta tecnologia permite suportar o serviço *Triple Play*, pois fornece a largura de banda necessária para suportar este serviço. Esta tecnologia apresenta a desvantagem da existência de ruído no meio de transmissão e também a redução da largura de banda que acontece quanto mais afastada estiver a casa do subscritor do equipamento de rede que permite aplicar a tecnologia VDSL2. Esta solução é mais económica do que a solução da rede de acesso em fibra óptica.

A tecnologia SDH (camada 1) foi a primeira tecnologia que permitiu fornecer elevadas larguras de banda através de um sistema síncrono e simples e foi utilizado durante muitos anos. Actualmente a tecnologia Ethernet (camada 2) é a tecnologia mais utilizada nas redes de telecomunicações devido ao seu custo reduzido e devido à sua natureza simples, robusta e ubíqua. A recuperação de falhas na rede SDH é efectuada através da atribuição de um caminho de protecção por cada caminho de trabalho. O caminho de protecção é apenas utilizado no caso de ocorrer uma falha. Este facto torna ineficiente a utilização da largura de banda na rede. O tempo de recuperação de falhas na rede SDH é de 50ms, mas a rede SDH não detecta falhas ocorridas nas camadas superiores da rede. O tempo reduzido de recuperação de falhas nas redes SDH é conseguido através de equipamentos de rede de elevado custo que detectam a falha e comutam automaticamente o tráfego para o caminho de protecção, sem a necessidade de avisar os restantes nós da rede. A tecnologia Ethernet apresenta tempos superiores de recuperação de falhas por pertencer à camada 2 da rede, uma vez que a falha é primeiro notificada a toda rede através de mensagens antes de comutar o tráfego.

A tecnologia denominada MPLS (*Multi-Protocol Label Switching*) está a ser seleccionada pelos provedores de serviços, pois esta tecnologia permite controlar o tráfego nas redes de telecomunicações. O MPLS utiliza CBR (*Constraint Based Routing*) para determinar qual o caminho preestabelecido a tomar para chegar até ao destino baseado nas restrições de QoS do tráfego e dos pacotes com etiquetas. Como os caminhos seleccionados pelo MPLS são estabelecidos de acordo com as restrições do tráfego, devem ser reservados recursos suficientes ao longo do caminho para garantir o transporte dos dados até ao destino. Isto faz com que os provedores de serviços tenham um maior controlo sobre as suas redes e assim poderem fornecer melhores parâmetros de QoS aos seus clientes.

A tecnologia MPLS permite aumentar o débito efectivo (*throughput*) existente na rede, uma vez que o processo de leitura do cabeçalho dos pacotes efectuado pelos encaminhadores é rápido. Foi verificado, através das simulações, que quando é utilizada a tecnologia Ethernet sobre a tecnologia MPLS (EoMPLS), os requisitos de qualidade de serviço são optimizados devido à natureza ubíqua e simples da tecnologia Ethernet combinada com a robustez, fiabilidade e utilização e eficiência proporcionada pela tecnologia MPLS.

O encaminhador MPLS apenas analisa a etiqueta alojada no cabeçalho do pacote para determinar o seu trajecto em vez de analisar o cabeçalho inteiro do pacote, como acontece na rede IP. A redução do tempo de análise do cabeçalho do pacote provoca um aumento no débito efectivo do tráfego na rede. Isto faz com que a rede MPLS seja mais eficiente do que a rede IP. Isto é verificado através das simulações que foram efectuadas neste trabalho com o simulador NS-2.33. A tecnologia MPLS permite aplicar a Engenharia de Tráfego. A Engenharia de Tráfego permite pré-estabelecer caminhos para chegar até ao destino. Esta informação é armazenada na etiqueta alojada no cabeçalho do pacote. Neste caso, o tempo de análise do cabeçalho é reduzido ainda mais, uma vez que o encaminhador sabe para onde deve encaminhar o pacote sem fazer cálculos sobre o seu trajecto para chegar até ao destino. Desta forma, o débito efectivo é superior ao valor apresentado pela solução da aplicação apenas da tecnologia MPLS na rede. Isto é demonstrado nas simulações realizadas com o simulador NS-2.33.

Os serviços de voz e de vídeo são intolerantes à perda de pacotes, pois esta provoca a incompreensão da mensagem de voz e o bloqueio da imagem de vídeo. A perda de pacotes pode ser provocada por ruído nas linhas de cobre de par entrançado ou por congestionamento do tráfego na rede. A rede MPLS permite reduzir a taxa de perda de pacotes em comparação com a rede IP, o que foi demonstrado com simulações efectuadas através do simulador NS-2. A Engenharia de Tráfego permite prevenir o congestionamento, balancear o tráfego pela rede e evitar a sobrecarga nos caminhos de menor distância até ao destino. A Engenharia de Tráfego permite reduzir ainda mais a taxa de perda de pacotes na rede. Existem vários métodos de recuperação de redes que podem ser aplicados nas redes MPLS, nomeadamente a recuperação global *Makam*, a recuperação global *Haskin*, a recuperação regional e a recuperação local. Verificou-se através das simulações que a recuperação Global *Haskin* apresentava a menor taxa de perda de pacotes, o maior número de reserva de recursos e o maior tempo de recuperação de falhas, devido ao seu modo recuperação de falhas. Verificou-se igualmente que o atraso provocado pelo elevado tempo de recuperação de falhas não excedia o limite dos requisitos de qualidade de serviço. O número elevado de recursos reservados deve-se à forma como é efectuada a recuperação de falhas pelo método *Haskin*. A perda de pacotes causa maior impacto no funcionamento do serviço do que o elevado atraso e o número

elevado de recursos reservados. Desta forma, decidiu-se que a recuperação Global *Haskin* é o método mais eficaz para ser utilizado numa rede *Triple Play*.

O encaminhamento óptimo, ou quase óptimo, está apresentado no Cenário 4 (secção 5.3.4), onde a rede consiste em quatro geradores de tráfego, um domínio MPLS e um nó cliente para receber o tráfego que representa um conjunto de clientes. Existe um gerador de Dados, um gerador VoIP, um gerador IPTV e um gerador Web. O tamanho dos pacotes utilizados nos geradores de Dados, VoIP e IPTV foi calculado de forma a representar o tamanho de pacotes Ethernet. Desta forma foi possível verificar, com precisão, a carga que uma rede EoMPLS pode suportar. O cenário 4 contém um domínio MPLS cujo encaminhamento do protocolo é calculado com base na menor distância até ao destino. A Engenharia de Tráfego é aplicada a meio da simulação e comuta o tráfego para outro caminho existente na rede para balancear o tráfego. O domínio MPLS funciona através da recuperação Global *Haskin* e, consequentemente, através da distribuição de etiquetas do plano de dados. Estes parâmetros de configuração atribuídos ao domínio MPLS delineiam o encaminhamento óptimo, ou quase óptimo, do tráfego na rede *Triple Play*. Posto isto, o objectivo do trabalho foi alcançado.

O cenário 4 permitiu também verificar qual o limite do número de clientes *Triple Play* possíveis existir numa rede *Triple Play*. Verificou-se que o limite do número de clientes *Triple Play* numa rede com largura de banda de 10 Mbps foi de 2, para uma rede de 100 Mbps foi de 20 clientes *Triple Play* e numa rede de 1 Gbps foi de 26 clientes *Triple Play*. Quando são excedidos os limites referidos para cada rede, a taxa de perda de pacotes, o atraso e a variação de atraso excedem o limite dos requisitos de qualidade de serviço do *Triple Play*. Salienta-se que estes limites foram verificados através das simulações efectuadas a uma determinada topologia de rede. Verificou-se que, ao adicionar mais ligações à topologia a largura de banda total da rede aumenta e aumenta consequentemente a sua capacidade de suportar um maior número de clientes *Triple Play*. Desta forma, a solução para introduzir mais clientes na rede é aumentar a largura de banda na rede.

Em conclusão, o encaminhamento óptimo, ou quase óptimo, do tráfego em redes *Triple Play* é conseguido através do meio de transmissão em fibra óptica e da tecnologia EoMPLS, onde é aplicada a Engenharia de Tráfego, é utilizado o protocolo de encaminhamento DV (*Distance Vector*), a distribuição de protocolos no modo *Data-Driven*, a recuperação Global *Haskin* e todas as vantagens que a tecnologia Ethernet proporciona.

**Trabalhos Futuros**

Como trabalhos futuros, algumas perspectivas de continuação deste trabalho de mestrado são:

- Modelar os cenários através do simulador NS-2.33 ou NS-3 com o encaminhamento do tráfego no modo multicast;
- Modelar cenários com redes mais complexas;
- Propor e implementar, um protótipo de um novo método de recuperação de falhas;
- Realizar simulações numa rede que suporta a tecnologia MPLS e o método de QoS denominado DiffServ;
- Realizar simulações atribuindo prioridades aos diferentes fluxos de tráfego, e;
- Realizar simulações do serviço *Triple Play* através do meio de transmissão sem fios (Wi-Fi e WiMAX).

# CAPÍTULO VII

# REFERÊNCIAS BIBLIOGRÁFICAS


**[Alaettinoglu et al, 2000]** Alaettinoglu, C., Jacobson, V., Yu, H. (2000). "Toward Millisecond IGP Convergence," draft-alaettinoglu-ISIS-convergence-00, November 2000, http://www. packetdesign.com/news/industry-publications/drafts/convergence.pdf, also talk at NANOG-20, October, 2000, http://nanog.org/mtg-0010/igp.html.

**[Alicart, 2005]** Alicart, X. O. (2005). "Design and Implementation of a Traffic Engineering Research Platform based on OPNET". M.Sc. Thesis - Lund University. Extraído de http://www.telecom.lth.se/ndg/research/publications/Theses/AlicartXO_MsThesis2005/AlicartXO_MsThesis2005.pdf.

**[Allied Telesyn, 2004]** Allied Telesyn (2004). "Active vs. PON". Technical Brief. Extraído de http://www.alliedtelesyn.com/media/pdf/active_vs_pon_a_wp.pdf.

**[Altgeld et al, 2005]** Altgeld, J. & Zeeman, J.D. (2005). "The IPTV/VoD Challenge: Upcoming Business Models". White Paper - International Engineering Consortium. Extraído de http://www-03.ibm.com/industries/media/doc/content/bin/VoDIPTVWhitepaperv2AltgeldZeeman_1.pdf

**[Amaro et al, 2000]** Amaro, J., & Lopes, R. (2000). "Rede Digital Comunitária: uma Rede sem Fios Metropolitana". Artigo – Instituto Politécnico de Bragança. Extraído de www.ipb.pt/~rlopes/confs/crc2000_ruf_rp.pdf

**[Andrade, 2003]** Andrade, A. (2003). "Modelagem e Análise de Desempenho de uma Rede Baseada em Tecnologia MPLS". Artigo - Universidade Federal de Santa Catarina. Extraído de www.inf.furb.br/seminco/2003/artigos/110-vf.pdf

**[ATI Technologies, 2005]** ATI Technologies (2005). "Introduction to H.264". White Paper. Extraído de http://ati.amd.com/products/pdf/h264_whitepaper.pdf

**[Barbosa, 2003]** Barbosa, F. R. (2003). "Presente e Futuro – Tecnologia, Sistemas e Redes". Apresentação em Fundação CPqD Campinas SP BRASIL. Extraído de http://www.lea.ufpa.br/redesopticas/comunicacoesopticaspresenteefuturo.ppt#317,14

**[Barbosa, 2006]** Barbosa, R. (2006). "Avaliação de Desempenho de Aplicações VoIP P2P". Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Pernambuco. Extraído de http://www.lbd.dcc.ufmg.br:8080/colecoes/sbrc/2006/st8_3.pdf.

**[Bakshi, 2006]** Bakshi, M. (2006). "VoIP/Multimedia over WiMAX". Student Survey Paper, April 2006. Extraído de http://www.cs.wustl.edu/~jain/cse574-06/ftp/wimax_voip/index.html

**[Borghers et al, 2008]** Borghers, E., & Wessa, P. (2008). "Statistical Distributions – Pareto Distribution - Example". Website - Office for Research, Development, and Education (ORDE) and Resa R&D. Extraído de http://www.xycoon.com/pareto.htm

**[Boucadair et al, 2004]** Boucadair, M., Morand, P., Asgari, H., Egan, R., Griem, J., Griffin, D., Spencer, J., Flegkas, P., Georgoulas, S., Hon Ho, K., Howarth, M., Pavlou, G., Trimintzios, P., Wang, N., Damilatis, T., & Georgatsos, P. (2004). "D2.1 - Implementation plan and high level engineering design of simulation models and testbed prototypes for inter-domain QoS delivery". Report - University College London, January 2004. Extraído de www.mescal.org/deliverables/MESCAL-D21-final.pdf

**[Boudani, 2002]** Boudani, A. (2002). "How MPLS is Implemented in NS". Report - A prepositional study - Irisa. Extraído de http://www.irisa.fr/armor/lesmembres/Boudani/research/mmt/stages/mplspimsm/1.%20Repport/PIMSM-MPLS-oNS.doc

**[Brodkin, 2007]** Brodkin, J (2007). "Understanding MPLS: MPLS in Layered Communications". Website – NotQuiteLeet.com, May 2007. Extraído de http://notquiteleet.com/2007/05/02/understanding-ip-communiations-mpls-in-layered-communciations/

**[Brun, 2004]** Bune, R. (2004). "Namespace TMath – Encapsulate Math Routines". Website - Fons Rademakers, 2004. Extraído de http://root.cern.ch/root/html/TMath.html

**[Caballero, 2007]** Caballero, M. J. (2007). "Triple Play Services and Protocols". WorkShop - Trend Communications. Extraído de http://www.trendcomms.com/trendweb/resource.nsf/vlFileURLLookup/Triple+Play+Formats/$FILE/triple.play.formats.protocols.pdf

**[Caballero 1, 2007]** Caballero, M. J. (2007). "IPTV – Pocket Guide". Pocket Guide - Trend Communications. Extraído de http://www.trendtest.com/trendweb/resource.nsf/vlFileURLLookup/IPTV.pocket.guide/$FILE/IPTV.Guide.pdf

**[Calle, 2004]** Calle, E. (2004). "Enhanced fault recovery methods for protected traffic services in GMPLS networks". M. Sc. Thesis - Universitat de Girona. ISBN 84-688-8630-0, Febuary 2004. Extraído de www.tesisenxarxa.net/TESIS_UdG/AVAILABLE/TDX-0920104-095653//teco.pdf

**[Calle et al, 2004]** Calle, E., Marzo, J., Urra, A. (2004). "Protection performance components in MPSL networks". Article - Universitat de Girona Computer Communications, ELSEVIER, July 2004. Extraído de http://eia.udg.es/~eusebi/papers/ecallecompcom2004.pdf.

**[Cisco, 2001]** Cisco Systems, Inc. (2001). "Quality of Service for Voice over IP". Solution Document.Extraído de http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.pdf

**[Cisco, 2003]** Cisco Cisco Systems, Inc. (2003). "CCNA Self-Study: CCNA Basics (CCNAB)". Article, March 2003. Extraído de http://www.ciscopress.com/articles/article.asp?p=31276&seqNum=1

**[Cisco, 2005]** Cisco Systems, Inc. (2005). "Voice over IP – Per call Bandwidth Consumption". Document ID: 7934. Extraído de http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

**[Cisco, 2006]** Cisco Systems, Inc. (2006). "Chapter 7: Ethernet Technologies". Internetworking Technology Handbook. Extraído de http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.pdf

**[Cisco, 2008]** Cisco Press. (2008). "Chapter 1: Introduction to First Mile Access Technologies". Article - Pearson Education. Extraído de http://www.ciscopress.com/content/images/chap01_158705129X/elementLinks/158705129Xcontent.pdf

**[Cisco 1, 2008]** Cisco Systems, Inc. (2008). "Optimizing video Transport in your IP Triple Play Network". White Paper, 2008. Extraído de http://www.cisco.com/en/US/prod/collateral/routers/ps368/prod_white_paper0900aecd80478c12.pdf

**[Cisco 2, 2008]** Cisco Systems, Inc. (2008). "Cisco ONS 15454 SDH Reference Manual". Product and Documentation Release 5.0, April 2008. Extraído de http://www.cisco.com/en/US/docs/optical/15000r5_0/15454/sdh/reference/guide/e45450r.pdf

**[Cheung, 2003**] Cheung, Y. (2003). "Multiprotocol Label Switching (MPLS) Using MPLS to Build an Application-Centric Network". White Paper, May 2003. Extraído de www.slb.com/media/services/consulting/infrastructure/mpls_whitepaper.pdf

**[ChipCenter-QuestLink 1, 2002**] ChipCenter-QuestLink. (2002). "Ethernet Technology – Part I". Website - ChipCenter-QuestLink. Extraído de http://archive.chipcenter.com/circuitcellar/march02/ancil-0302/c0302tsf1.htm
**[ChipCenter-QuestLink 2, 2002**] ChipCenter-QuestLink. (2002). "Ethernet Technology – Part II". Website - ChipCenter-QuestLink. Extraído de http://www.circellar.com/library/ccofeature/antonakos0402/index.asp

**[Chung et al, 1999**] Chung, J., & Claypool, M. (1999). "NS By Example". Website - Worcester Polytechnic Institute. Extraído de http://nile.wpi.edu/NS/overview.html

**[Clark et al, 1998]** Clark, D., & Fang, W. (1998). "Explicit Allocation of Best-Effort Packet Delivery Service". Article - IEEE/ACM Transactions on Networking, August 1998. Extraído de http://nms.lcs.mit.edu/6829-papers/p362-clark.pdf

**[Collins, 2001]** Collins, D. (2001). "Carrier Grade Voice Over IP". Book - McGraw-Hill. ISBN 0071406344, 9780071406345. Extraído de http://books.google.pt/books?id=PVIuN9Y5FGMC&printsec=frontcover&dq=Carrier+Grade+Voice+Over+IP&client=pub-5674445849125711

**[Fahmy, 2006]** Fahmy, S. (2006). "Fidelity/Scalability Tradeoffs in Protocol Evaluation". Paper - Perdue University, May 2006. Extraído de http://wwic2006.unibe.ch/talks/wwic06_fahmy.pdf

**[Fischer, 2007]** Fischer, A. J. (2007). "Tolerância a Falhas no MPLS". Trabalho de Mestrado - Pontifícia Universidade Católica do Paraná. Extraído de www.ppgia.pucpr.br/~jamhour/Download/pub/Mestrado%202007/Tolerancia_a_Falhas_em_MPLS_r4.pdf

**[Flask, 2007]** Flask, R. (2007). "Home Networking Success". Website - CedMagazine.com, April 2007. Extraído de http://www.cedmagazine.com/home-networking-success.aspx

**[FlexLight Networks, 2004]** FlexLight Networks (2004). "GPON – The Next Big Thing in Optical Access Networks". Article - FlexLight Networks, March 2004. Extraído de http://www.telmarkperu.com/Documentos/GPON.pdf

**[Foigel, 2007]** Foigel, J. (2007). "DSL e suas Evoluções". Website - TELECO Informações em Telecomunicações, Janeiro, 2007. Extraído de http://www.teleco.com.br/emdebate/joniofoigel01a.asp.

**[Francês et al, 2007]** Francês, C. R. L., & Seruffo, M. C. R. (2007). "Triple Play sobre ADSL2+ na Região Amazônica: Um Estudo de Caso envolvendo Experimentações e Simulações". Trabalho de Pós-Graduação em Ciências de Computação - Universidade Federal do Pará (UFPA). Extraído de http://www.ufpa.br/ppgcc/ppgcc/files/File/Seminario_Andamento/Redes%20de%20Computadore/Paper_seminario_de_andamento.pdf

**[Ganchev, 2003]** Ganchev, I. (2003). "Enhancement of NS2 Wireless BS with MPLS to provide a platform for future MuMAcWiN". Presentation University of Limerick: Presentation 1 for COST285 2nd MCM, Istanbul, 25–26 September 2003. Extraído de www.cost285.itu.edu.tr/tempodoc/TD_285_03_31_Ivan%20Ganchev.pdf

**[Gaeil, 2000]** Gaeil, A., & Woojik, C. (2000). "Design and Implementation of MPLS Network Simulator Supporting LDP and CR-LDP". M. Sc. Thesis - Eighth IEEE International Conference on Networks (ICON'00). Extraído de http://heim.ifi.uio.no/~johanmp/mpls/mpls.pdf

**[Gagnon, 2007]** Gagnon, N. (2007). "OON 2007 – Concórdia U". Workshop on Optimization of Optical Networks (OON) - EXFO, May 2007. Extraído de http://users.encs.concordia.ca/~bjaumard/Conferences_and_Seminars/OON_Workshops/OON_2007/Slides_OON_2007/OON_2007_EXFO_Gagnon.pdf

**[Goff, 2005]** Goff, D. (2005). "Optical Protection". Website – MrFiber.com. Extraído de http://www.mrfiber.com/Optical_Protection.htm

**[Goyal et al, 2003]** Goyal, M., Ramakrishnan, K., & Feng, W. (2003). "Achieving faster failure detection in ospf networks". Article - The Ohio State University, IEEE ICC. Extraído de http://web.cecs.pdx.edu/~wuchi/Papers/Goya.icc03.pdf

**[Heidemann et al, 2006]** Heidemann, J., Huang, P., Haldar, P., & Chen, X. (2006). "Extending Convergence Beyond IP Telephony". Article - Hewlett-Packard Development Company, L.P. Extraído de http://www.hp.com/rnd/itmgrnews/extending_convergence.htm.

**[Hogie et al, 2006]** Hogie, L., Bouvry, P., & Guinand, F. (2006). "An Overview of MANETs Simulation". Article - Universite du Luxembourg e Université du Havre. Extraído de http://pascal.bouvry.org/ftp/An%20Overview%20of%20MANETs%20Simulation.pdf

**[Huang, 2003]** Huang, C., & Messier, D. (2003). "Inter-Domain MPLS Restoration". Article - Carleton University, October 2003, Extraído de www.sce.carleton.ca/faculty/huang/drcn.pdf

**[Huston, 2003]** Huston, G. (2003). "Blurring the Lines". Website – Internet Society TM, November 2003. Extraído de http://ispcolumn.isoc.org/2003-11/blurring.html.

**[IEC a, 2007]** International Engineering Consortium. (2007). "Ethernet Passive Optical Networks". White Paper – Web ProForum Tutorials. The International Engineering Consortium. Extraído de http://www.iec.org/online/tutorials/acrobat/epon.pdf.

**[IEC b, 2007]** International Engineering Consortium. (2007). "Multiprotocol Label Switching (MPLS)". White Paper - Web ProForum Tutorials - The International Engineering Consortium. Extraído de http://www.iec.org/online/tutorials/acrobat/mpls.pdf.

**[IEEE 802.3, 2000]** IEEE. (2000). "Chapter 5: Internetworking Technology Overview. Ethernet/IEEE 802.3". Internetworking Technology Overview - IEEE. Extraído de http://www.members.tripod.com/~srohit/Ethernet.pdf

**[Infante, 2008]** Infante, I. (2008). "Rede IPTV MEO". Vídeo - Exame Informática. Extraído de http://www.youtube.com/watch?v=eV-9HWcQ6W8

**[Iselt, 2004]** Iselt, A., Kirstadter, A., Pardigon, A., & Schwabe, T. (2004). "Resilient Routing Using MPLS and ECMP". Article - Stuttgart University, Germany. Extraído de www.lkn.ei.tum.de/~akirstaedter/papers/2004_HPSR_POEM.pdf

**[ITU-T P.800, 1996]** ITU-T Recommendation P.800 (1996). "Methods for Subjective Determination of Transmission Quality". Geneve.

**[ITU-T P.830, 1996]** ITU-T Recommendation P.830 (1996). "Subjective Performance Assessment of TelephoneBand and Wideband Digital Codecs". Geneve.

**[ITU-T G.107, 1998]** ITU-T Recommendation G.107. (1998). "The E-Model, a computational model for use in transmission planning".

**[ITU-T P.862, 2001]** ITU-T Recommendation P.862 (2001). "An Objective Method for End-to-End Speech Quality Assessment of Narrow-Band Telephone Networks and Speech Codecs". Geneve.

**[IXIA, 2008]** ITU-T Recommendation P.862. (2008). "An Objective Method for End-to-End Speech Quality Assessment of Narrow-Band Telephone Networks and Speech Codecs". Geneve.

**[JSim 1, 2003]** JSim. (2003). "Evaluation of JSim". Website - DRCL JSim – Ohio State University. Extraído de http://www.j-sim.org/comparison.html#s1

**[JSim 2, 2003]** JSim. (2003). "A New MPLS model inside JSim". Website – Université catholique de Louvain. Extraído de http://www.info.ucl.ac.be/~bqu/jsim/mpls_desc.html

**[Juniper, 2007]** Juniper Networks, Inc. (2007). "Ethernet over MPLS". Presentation of Technology and Application Overview - Juniper Networks, September 2007. Extraído de http://sabb2006.tninternational.com/presentations/JuniperPanda.ppt

**[Kankkunen, 2004]** Kankkunen, A. (2004). "IP/MPLS as a basic architecture in future Telecom networks and new packet services". Website - Datacomm - Convergence Plus, Comnet Publishers Pvt. Ltd, September, 2004. Extraído de http://www.convergenceplus.com/sep04%20datacomm%2001.html

**[Kurose et al, 2005]** Kurose, J. F., & Ross K. W. (2005). "Capítulo 5: Redes de Computadores e a Internet". Apresentação da 3ª Edição, PEARSON Addison Wesley. Extraído de http://www.larces.uece.br/~celestino/Curso%20Redes_Kurose_2008/cap05.ppt#371,90

**[LEE, 2006]** Lee, K. (2006). "Modèle global pour la Qualité de Service dans les réseaux de FAI : intégration de DiffServ et de l'ingénierie de trafic basée sur MPLS". PhD Thesis - l'Université des Sciences et Technologies de Lille et l'Ecole Centrale de Lille. Extraído de http://hal.archives-ouvertes.fr/docs/00/11/20/88/PDF/these_Kyeongja.pdf

**[Leroux et al, 2006]** Leroux, A., Giguere, B. (2006). "SONET/SDH vs. ETHERNET: Migration and Testing issues". Application Note - EXFO Expertise Reaching out. Extraído http://documents.exfo.com/appnotes/anote152-ang.pdf

**[Lucio et al, 2003]** Lucio, G. F., Paredes-Farrera, M., Jammeh, E. Fleury, M., & Reed, M. J. (2003). "OPNET Modeler and Ns-2: Comparing the Accuracy of Network Simulators for Packet-Level Analysis using a Network Testbed". Article - University of Essex, United Kingdom. Extraído http://privatewww.essex.ac.uk/~fleum/weas.pdf

**[Macedo et al, 1999]** Macedo, C. G. F., Braga N. C. N., & Costa, Jr. N. (1999). "Tutorial: Redes ATM". Tutorial – I Workshop do Rio de Janeiro em Redes de Alta Velocidade. Extraído de http://www.rederio.br/downloads/pdf/atm.pdf.

**[Markopoulo et al, 2003]** Markopoulou, A., Tobagi, F., & Karam, M. (2003). "Assessing the quality of Voice Communications over Internet Backbones". Article - IEEE Transactions on Networking, Vol. 11 No. 5. Extraído de http://mmnetworks.stanford.edu/papers/markopoulou_ton03.pdf.

**[MC MCSE, 2008**] MC MSCE. (2008). "Basic Networking". Website - MC MSCE Certification Resources. Extraído de http://www.mcmcse.com/comptia/aplus/notes/network.shtml

**[Mauthe, 2008**] Mauthe, M. A. (2008). "A Unity-based QoS Model for Emergin Multimédia Applications". Presentation - LANCASTER University, United Kingdom. Extraído de http://www.comp.glam.ac.uk/NGMAST08/NGMAST2008_presentations/CA228_FMN/FMN_3/FMN_mu1.ppt#296,26,Simulation Traffic Generator

**[Miller et al, 2003]** Miller, J. A., Nair, R. S. Zhang, Z., & Zhao, H. (2003). "JSIM: A JAVA-BASED SIMULATION AND ANIMATION ENVIRONMENT". Article - University of Georgia. Extraído de http://reference.kfupm.edu.sa/content/j/s/jsim__a_java_based_simulation_and_animat_581817.pdf

**[Miras, 2002]** Miras, D. (2002). "A survey on network QoS needs of advanced Internet applications". Working Document - University College London - Internet 2 – QoS Working Group. Extraído de http://qos.internet2.edu/wg/apps/fellowship/Docs/Internet2AppsQoSNeeds.pdf

**[Morin, 2007]** Morin, V. (2007). "Preparing Networks for the Digital Entertainment Revolution". Ciena. Website – Total Telecom, December, 2007 Extraído de http://www.totaltele.com/View.aspx?ID=96987&t=4.

**[Moura, 2005]** Moura, N. T. (2005). "Voice over Internet Protocol – VoIP". Universidade Federal Fluminense – UFF Instituto de Computação. Article – Universidade Federal Fluminense. Extraído de http://voip.ic.uff.br/Voip_Survey.html.

**[Nokia, 2003]** Nokia For Business. (2004). "Advantages of SIP for VoIP". White Paper - Nokia Connecting People, October, 2003. Extraído de http://64.233.169.104/search?q=cache:_8v7cAP77IYJ:www.invictusnetworks.com/faq/Voice%2520over%2520IP%2520VoIP/Nokia%2520Whitepaper_SIP_for_VoIP.pdf+white+paper+h.323+vs+sip&hl=pt-PT&ct=clnk&cd=8&gl=pt&lr=lang_en

**[Nunes, 2006]** Nunes, M. S. (2006). "Redes de Acesso – Parte C – Tecnologias de acesso DSL". Texto de aulas - Instituto Superior Técnico – IST, Setembro 2006. Extraído de http://comp.ist.utl.pt/ec-ra/textos-aulas/ParteC-DSL.pdf

**[NS-2, 2000]** NS-2. (2000). "The Network Simulator – NS-2 – Change History". Website – University of Southern California. Extraído de http://www.isi.edu/nsnam/ns/

**[O´Driscoll, 2007]** O´Driscoll, G. (2007). "Next Gerneration IPTV Services and Technologies". Book - Wiley-Interscience. ISBN 0470163720, 9780470163726. Extraído de http://books.google.pt/books?id=enN3yukBAmEC&printsec=frontcover&client=pub-5674445849125711

**[Optical Network, 2006]** Optical Network. (2006). "1+1/1:1 Protection". Website – Optical Network.com, September 2006. Extraído de http://www.optical-network.com/terminology.php?letter=all&id=18

**[OST, 2006]** Omnitron Systems Technology, Inc. (2006). "802.3ah OAM for Carrier-Class Optical Ethernet in the First Mile". White Paper. Extraído de http://www.omnitron-systems.com/downloads/Omnitron_EFM_OAM.pdf?referrer=OAM

**[Owens et al, 2002]** Owens, K., Sharma, V., Oommen, M., & Hellstrand, F. (2002). "Network Survivability Considerations for Traffic Engineering IP Networks". Internet Draft - Traffic Engineering Working Group. Extraído de http://www.ietf.org/proceedings/02nov/I-D/draft-owens-te-network-survivability-03.txt

**[Pinnacle Systems, 2000]** Pinnacle Systems (2000). "MPEG-2 White Paper". White Paper, Febuary 2000. Extraído de http://www.pinnaclesys.com/files/MainPage/Professional/TopTabItems/products/dc1000/WhitePapers/DC1000-DVD1000MPEG2whitepaper.pdf

**[Poe, 2005]** Poe, R. (2005). "FTTX may boost optical transmissions outlays". America´s Network. Extraído de http://findarticles.com/p/articles/mi_m0DUJ/is_1_109/ai_n11836188/

**[Pepelnjak, 2007]** Pepelnjak, I. (2007). "10 MPLS Traffic Engineering Myths and half truths". Américas Network - Questex Media Group, Inc., January 2005. Extraído de http://searchtelecom.techtarget.com/tip/0,289483,sid103_gci1276977,00.html.

**[Perreira et al, 2004]** Perreira, V., Monteiro, E., & Barros, F. (2004). "Estudo do desempenho de VoIP na presence de tráfego best-effort". University de Coimbra - in Proc. of the Actas da 7ª Conferência sobre Redes de Computadores – CRC'2004 – Mobilidade, Segurança e Qualidade de Serviço na nova geração da Internet, pp. 49-60, CRC'2004 (7ª Conf. sobre Redes de Computadores), ESTG - Leiria - Portugal, October 2004. Extraído de http://www.cisuc.uc.pt/lct/dlfile.php?fn=818_pub_Simul_VoIP_CRC2004_CameraReady.pdf&get=1&idp=818&ext=

**[Petersson, 2005]** Petersson, J. M. O. (2005). "MPLS Based Recovery Mechanisms". M.Sc. Thesis - University of OSLO, May 2005. Extraído de http://folk.uio.no/johanmp/MPLS%20Based%20Recovery%20Mechanisms.pdf

**[Prakash, 2005]** Prakash, S. K. (2005). "Sonte Tutorial: Basic Frame Structure". Website Tutorial - ElectroSofts. Extraído de http://electrosofts.com/sonet/frame.html

**[RAD, 2008]** RAD Data Communication. (2008). "Chapter 1: Ethernet Access". RAD Data Communication Catalog. Extraído de www.pahldata.pt/rad/28208_chap01.pdf

**[RAD 1, 2008]** RAD Data Communication (2008). "What is SDH". Website - RAD Data Communication Catalog - Pulse, Inc. Extraído de http://www.pulsewan.com/data101/sdh_basics.htm

**[Redbooks, 2006]** Parziale, L., Britt, D., Davis, C., Forrester, J., Liu, W., Matthews, C., & Rosselet, N. (2006). "TCP/IP Tutorial and Technical Overview". IBM Book, Redbooks. ISBN: 0738494682

**[Rexford, 2006]** Rexford, J. (2006). "Route Optimization in IP Neworks. Chapter in Handbook of Optimization in Telecommunications", Article - Princeton University - Spring Science and Business Media. Extraído de www.cs.princeton.edu/~jrex/papers/opthand04.pdf

**[Rajagopal, 2008]** Rajagopal, A. (2008). "Achieving Superior Resiliency and Fast Convergence with Foundry´s MRP". Technical Document Version 2.0 - Foundry Networks, Inc. Extraído de http://www.foundrynet.com/pdf/wp-mrp.pdf

**[RFC 1131, 1989]** Moy, J. (1989). "OSPF – Open Shortest Path First". RFC Archive, October 1989. Extraído http://www.faqs.org/ftp/rfc/rfc1131.pdf

**[RFC 1633, 1994]** Braden, R., Clark, D., & Shenker, S. (1994). "IntServ – Integrated Services in the Internet Architecture". RFC Archive, June 1994. Extraído de http://www.ietf.org/rfc/rfc1633.txt

**[RFC 2205, 1997]** Braden, B., Zhang, L., Berson, S., Herzop, S., & Jamin, S. (1997). "RSVP – Resource Reservation Protocol". RFC Archive, September 1997. Extraído de http://www.isi.edu/in-notes/rfc2205.txt

**[RFC 2474, 1998]** Nichols, K., Blake, S., Baker, F., & Black, D. (1998). "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers". RFC Archive, December 1998. Extraído de http://www.ietf.org/rfc/rfc2474.txt

**[RFC 2475, 1998]** Carlson, M., Davis, E., Wang, Z., Weiss, W., Nichols, K., Blake, S., & Black, D. (1998). "An Architecture for Differentiated Services". RFC Archive, December 1998. Extraído de http://www.ietf.org/rfc/rfc2475.txt

**[RFC 3031, 2001]** Rosen, E., Viswanathin, A., & Callon, R. (2001). "Multiprotocol Label Switching Architecture". RFC Archive, January 2001. Extraído de http://www.ietf.org/rfc/rfc3031.txt

**[RFC 3272, 2002]** Awduche, D., Chiu, A., Elwaldin, A., Widjaja, I., & Xiao, X. (2002). "Overview and Principles of Internet Traffic Engineering". RFC Archive, May 2002. Extraído de http://www.ietf.org/rfc/rfc3272.txt

**[RFC 3469, 2003]** Mack-Crane, B., Makam, S., Owens, K., Huang, C., Cain, B., Jamoussi, B., Chiu, A., & Civanlar, S. (2003). "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery". RFC Archive, February 2003. Extraído de http://www.faqs.org/rfcs/rfc3469.html

**[RFC 4448, 2006]** Martini, L., El-Aawar, N., Heron, G., & Rosen, E. (2006). "Encapsulation of Ethernet over MPLS". RFC Archive, April 2006. Extraído de http://www.ietf.org/rfc/rfc4448.txt

**[Rozycki et al, 2008]** Rozycki, P., & Korniak, J. (2008). "Failure Detection and Notification in GMPLS Control Plane". Article - University of IT and Management Rzeszow, Poland. Extraído de www.kt.agh.edu.pl/files/publ_pdf/944

**[Sanchez, 2004]** Sanchez, W. P. (2007). "PON: Redes Ópticas de Acesso de Baixo Custo". Teleco. Website - TELECO Conhecimento em Telecomunicações, Junho 2004. Extraído de http://www.teleco.com.br/tutoriais/tutorialpon/Default.asp.

**[Salah et al, 2006]** Salah, K., Calyam, P., & Buhari, M. (2006). "Assessing readiness of IP networks to support desktop videoconferencing using OPNET". Article – ScienceDirect – ELSEVIER, January 2007. Extraído de www.osc.edu/research/networking/PDFs/vcopnet_jnca06.pdf

**[Santos, 2004]** Santos, A. P. S. (2004). "Qualidade de Serviço na Internet". Website - Rede Nacional de Ensino e Pesquisa. Extraído de http://www.rnp.br/newsgen/9911/qos.html.

**[Sardella, 2005]** Sardella, A. (2005). "Introduction to Automatic IP Multicast Without Explicit Tunnels". White Paper - Juniper Networks, Inc, March 2005. Extraído de http://www.juniper.net/solutions/literature/white_papers/200107.pdf

**[Schupke, 2005]** Schupke, D. (2005). "Comparison of p-cycle Configuration Methods For Dynamic Networks". IFIP Optical Networks & Technologies Conference (OpNeTec), Pisa, Italy, October 18-22, 2005. Siemens AG, Coporate Technology, Information and Communication. Extraído de http://www.dominic-schupke.de/papers/dynCycles_v3.pdf

**[SfR Fresh, 2007]** SfR Fresh. (2007). "Applications and transport agent API". The SfR Fresh Freeware/Shareware Archive. Extraído de http://www.sfr-fresh.com/unix/privat/ns-2.33.tar.gz:a/ns-2.33/doc/applications.tex

**[Spurgeon, 2000]** Spurgeon, C. E. (2000). "Ethernet: The Definitive Guide". O´Reilly Book - ISBN: 1-56592-660-9. Extraído de http://books.google.pt/books?id=Ur96H9bcbfgC&printsec=frontcover&client=pub-5674445849125711#PPP1,M1

**[Stephen, 2001]** Stephen A. T. (2001). "IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE". Wiley; 1st edition. ISBN: 978-0-471-03466-7

**[Stoica, 2004]** Stoica, I. (2004). "Stateless Core". Springer Book - ISBN 3540219609, 9783540219606. Extraído de http://books.google.pt/books?id=zyll7rvSMRAC&printsec=frontcover&source=gbs_summary_r&cad=0

**[Subramanian, 2002]** Subramanian, S. (2002). "Study of Traffic Engineering Algorithms and Framework". Independent Study Report - University of Nevada Las Vegas. Extraído de http://www.ee.unlv.edu/~venkim/opnet/IndependentStudy.pdf

**[Tanembaum, 2003]** Tanembaum, A. S. (2003). "Redes de Computadores". Prentice Hall Book – ISBN: 0-13-066102-3 – Fourth Edition. Extraído de http://books.google.pt/books?id=Pd-z64SJRBAC&printsec=frontcover&source=gbs_v2_summary_r&cad=0

**[Taylor & Francis Group, 2007]** Taylor & Francis Group, LLC. (2005). "Chapter 8: Internet Television". Article - Taylor & Francis Group, LLC. Extraído de http://www.ittoday.info/Articles/InternetTV.pdf

**[Tektronix, 2007]** Tektronix Inc. (2007). "A Guide to IPTV: The Technologies, the Challenges and How to Test IPTV". Technical Brief - Tektronix Inc. Extraído de http://www.tek.com/Measurement/App_Notes/25_20277/eng/25W_20277_0.pdf?wt=520&rgn=ww&from=303271X314253&link=/Measurement/App_Notes/25_20277/eng/25W_20277_0.pdf

**[Tellabs, 2007]** Tellabs. (2007). "Ethernet-over-SDH as an Ideal Access For IP/VPN Networks". Application Note. Extraído de http://www.tellabs.com/products/6000/tlab63xxipvpn.pdf

**[Tipton, 2007]** Tipton, F. H. (2007). "Information Security Management Handbook". Auerbach Publications – Taylor & Francis Group - CRC Press. ISBN: 0849374952, 9780849374951. Extraído de http://books.google.pt/books?id=B0Lwc6ZEQhcC&printsec=frontcover

**[Uzmi, 2006]** Uzmi, Z. (2006). "Quiz Number 9 - Solutions". Handouts - Lahore University of Management Sciences. Extraído de http://suraj.lums.edu.pk/~cs678s06/handouts/22_quiz9_solutions.pdf

**[Walker et al, 2002]** Walker, J. Q., Hicks, J. T. (2002). "The Essential Guide to VoIP Implementation and Management". Article - University of South Australia - NetIQ Corporation. Extraído de http://www.unisanet.unisa.edu.au/Resources/12258/MNT2005/Assignment%202%20Resources/VoIP%20and%20IP%20Telephony/NetIQ_VoIP_Chapter1.pdf

**[Weigle et al, 2004]** Weigle, M., Jeffay, K. (2004). "Web Traffic Generation in NS-2 with PackMime-HTTP". Website - Statistics Research, Bell Labs, Lucent Technologies and the University of North Carolina at Chapel Hill. Extraído de http://dirt.cs.unc.edu/packmime/

**[Wikipedia 2, 2008]** Wikipedia. (2008). "Triple Play (telecommunications)". Website – Wikipedia The Free Encyclopedia. Extraído de http://en.wikipedia.org/wiki/Triple_play_(telecommunications)

**[Wikipedia 4, 2008]** Wikipedia. (2008). "Digital subscriber line access multiplexer". Website – Wikipedia The Free Encyclopedia. Extraído de http://en.wikipedia.org/wiki/DSLAM

**[Wikipedia 5, 2008]** Wikipedia. (2008). "The Network Simulator – NS-2". Website – Wikipedia The Free Encyclopedia. Extraído de http://nsnam.isi.edu/nsnam/index.php/User_Information

**[Wimoesterer, 2006]** Wimoester, S. (2006). "Future-proof Telecom networks with VDSL2". Article - Infineon Technologies AG, January 2006. Extraído de www.eetasia.com/ARTICLES/2006JAN/PDF/EEOL_2006JAN02_RFD_NETD_TA.pdf?SOURCES=DOWNLOAD

**[Yip, 2002]** Yip, D. (2002). "Traffic Engineering Prioritized IP Packets Over Multi-Protocol Label Switching Networks". M. Sc. Thesis - Fraser University, April 2002. Extraído de www.cs.sfu.ca/~ljilja/cnl/pdf/danny_yip.pdf

**[Younis, 2007]** Younis, O. (2007). "Constraint Based Routing in the Internet: Basic Principles and recent Research". White Paper - Purdue University, June 2007. Extraído de www.cs.purdue.edu/homes/fahmy/papers/routing.pdf

**[Zultys, 2004]** Zultys Technologies. (2004). "Whitepaper. SIP vs. H.323: A Comparason". White Paper - University of South Australia - Zultys Technologies White Paper. Extraído de http://www.unisanet.unisa.edu.au/Resources/12258/MNT2005/Assignment%202%20Resources/VoIP%20and%20IP%20Telephony/SIP_vs_H323_white_paper__AU_.pdf

# Anexos

# Anexo A: Código e Parâmetros de simulação no NS-2

# Anexo B: Código e Parâmetros dos Cenários

# Anexo C: Código de Simulação – Ficheiros .tcl

# Anexo D: Código do Processamento de dados - Ficheiros .awk

UNIVERSIDADE da MADEIRA

DEPARTAMENTO DE MATEMÁTICA E ENGENHARIAS

# ANEXOS

## ENCAMINHAMENTO ÓPTIMO DO TRÁFEGO EM REDES *TRIPLE PLAY*


**Sandy Carmo Relva Rodrigues**

Licenciada em Engenharia de Electrónica e Telecomunicações

Universidade da Madeira

**Orientador**

Professor Doutor Paulo Nazareno Maia Sampaio

Dissertação apresentada para a obtenção do grau de

Mestre em Engenharia de Telecomunicações e Redes

Madeira

2009

# Anexo A: Código e Parâmetros de simulação no NS-2

## A Simulação MPLS no NS-2

Nesta secção descrevem-se os comandos utilizados para simular a topologia MPLS. Os comandos referentes ao funcionamento básico da simulação NS-2 e ao processamento de dados não são mencionados nesta secção. Para mais informações deve ser consultado o manual do NS-2 [VINT, 2000] e os ficheiros de código nos Anexos C e D.

Começa-se por descrever os comandos que criam a topologia. De seguida são apresentados os comandos dos protocolos de encaminhamento, os protocolos de distribuição de etiquetas e os LSP. Posteriormente, descreve-se os comandos que permitem aplicar a Engenharia de Tráfego e os comandos utilizados na recuperação de falhas na rede.

### Comandos para Criar a Topologia MPLS

Entre o comando – MPLS ON e o – MPLS OFF declaram-se todos os nós MPLS que existem no domínio MPLS. No caso de se querer simular uma rede IP, basta configurar o comando – MPLS ON para – MPLS OFF. Os comandos utilizados para criar os nós MPLS são:

```
$ns node-config –MPLS ON
set LSR1 [$ns mpls-node]
….
$ns node-config –MPLS OFF.
```

As ligações entre os nós são configuradas para funcionar no modo *duplex* (informação trocada nos dois sentidos), para ter uma largura de banda desejada (10/100/1000 Mbps), um atraso de 1ms que simula a fibra óptica e a fila funciona no modo *Droptail* ou FIFO (*First In First Out*). Os comandos utilizados para criar as ligações entre os nós MPLS são:

```
$ns duplex-link $n0 $LSR1  10Mb  1ms DropTail
```

### Comandos para Configurar o Modo de Encaminhamento do Protocolo

O NS-2 permite configurar o encaminhamento dos protocolos. Os modos mais utilizados são o modo de encaminhamento de protocolo DV (*Distance Vector*) e o modo de encaminhamento de protocolo LS (*Link State*). Apenas pode ser seleccionado um único modo para a rede MPLS. Estes encaminhamentos não são utilizados na rede IP, são utilizados apenas na rede MPLS. A rede IP é simulada ao comentar o modo de encaminhamento do protocolo. Os comandos utilizados para criar as ligações entre os nós MPLS são:

```
$ns rtproto DV
$ns rtproto LS.
```

### Comandos para Configurar o Modo de Distribuição de Etiquetas através do Protocolo LDP

Os agentes LDP são configurados em todos os nós MPLS através do código abaixo citado. Os comandos “$m enable-reroute “new” ” e “$m enable-reroute “drop” ” são utilizados de acordo com o modo de distribuição de etiquetas pretendido. Estes dois comandos não podem ser utilizados ao mesmo tempo.

```
for {set i 0} {$i < n} {incr i} {
        set a LSR$i
        for {set j [expr $i+1]} {$j < 5} {incr j} {
```

```
            set b LSR$j
            eval $ns LDP-peer $$a $$b
        }
        set m [eval $$a get-module "MPLS"]
        $m enable-reroute "new"
        #$m enable-reroute "drop"
}
```

Após configurar o LDP em todos os nós MPLS, configura-se, através dos comandos seguintes, os diferentes pacotes LDP com cores diferentes.

```
$ns ldp-request-color $color
$ns ldp-mapping-color $color
$ns ldp-withdraw-color $color
$ns ldp-release-color $color
$ns ldp-notification-color $color
```

Como fora referido anteriormente, existem dois modos de distribuição de etiquetas: o modo *Control-Driven* e o modo *Data-Driven.* O comando “MPLSnode” refere-se, por exemplo, ao nó “$LSR1”. Desta forma, configuram-se todos os nós MPLS para funcionar no modo desejado. Os comandos utilizados para escolher o modo de distribuição de etiquetas são:

```
[$MPLSnode get-module "MPLS"] enable-control-driven
[$MPLSnode get-module "MPLS"] enable-data-driven
```

Os comandos a seguir descritos podem ser aplicados ao modo *Data-Driven* para melhorar o seu desempenho. O comando “enable-on-demand” possibilita a distribuição de etiquetas no momento em que é necessário. O comando “enable-ordered-control” permite controlar a distribuição de forma ordenada.

```
[$MPLSnode get-module "MPLS"] enable-on-demand
[$MPLSnode get-module "MPLS"] enable-ordered-control
```

O LSP é pré-estabelecido através do comando seguinte, onde o FEC é o nó de destino, o “er” é o encaminhamento explícito do LSP, o “LSPid” é a identificação dada ao caminho e o “rc” é o apontador do LSP (que é sempre -1).

```
[$MPLSnode get-module "MPLS"] make-explicit-route fec er LSPid rc
```

**Comandos para Aplicar a Engenharia de Tráfego através da utilização do modo ER-LSP**

Segundo [Yip, 2002], é possível aplicar a Engenharia de Tráfego no NS-2 através do comando abaixo citado. O “phb” é sempre configurado a -1.

```
[$MPLSnode get-module "MPLS"] flow-erlsp-install fec phb LSPid
```

# Anexo B: Código e Parâmetros dos Cenários

## Cenário 1 – Diferenças Entre a Rede IP e a Rede MPLS

Os parâmetros da simulação IP estão apresentados na Tabela 5.2. Os parâmetros da simulação MPLS estão apresentados na Tabela 5.3.

**Tabela 1 – Parâmetros da simulação IP do Cenário 1**

| | |
|---|---|
| Simulação IP | $ns node-config -MPLS OFF |
| | Data-Driven |
| | [$LSR1 get-module "MPLS"] enable-data-driven |
| | [$LSR2 get-module "MPLS"] enable-data-driven |
| | [$LSR3 get-module "MPLS"] enable-data-driven |
| | [$LSR4 get-module "MPLS"] enable-data-driven |
| | [$LSR5 get-module "MPLS"] enable-data-driven |
| | [$LSR6 get-module "MPLS"] enable-data-driven |
| | [$LSR7 get-module "MPLS"] enable-data-driven |
| | Data-Driven – on demand |
| | Classifier/Addr/MPLS enable-on-demand |
| | Data-Driven – order control |
| | Classifier/Addr/MPLS enable-ordered-control |
| | Control-Driven |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |

**Tabela 2 – Parâmetros da simulação MPLS do Cenário 1**

| | |
|---|---|
| Simulação MPLS | $ns node-config -MPLS ON |
| | Data-Driven ou Data-Driven – on demand ou Data-Driven – order control ou Data-Driven – on demand – order control. |
| | $ns rtproto DV ou $ns rtproto LS |
| | $ns at 0.10 "[$LSR7 get-module MPLS] ldp-trigger-by-withdraw 8 -1" |
| | $ns at 0.20 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1000 -1" |
| | $ns at 0.20 "[$LSR1 get-module MPLS] make-explicit-route 7 1_2_3_4_7 1001 -1" |

# Cenário 2 – Funcionamento da Engenharia de Tráfego

**Tabela 3 – Parâmetros da simulação IP do Cenário 2**

| | |
|---|---|
| Simulação IP | $ns node-config -MPLS OFF |
| | Control-Driven |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |

**Tabela 4 – Parâmetros da simulação MPLS do Cenário 2**

| | |
|---|---|
| Simulação MPLS | Parâmetros da Simulação IP |
| | $ns node-config -MPLS ON |
| | $ns rtproto DV |
| | $ns at 0.10 "[$LSR7 get-module MPLS] ldp-trigger-by-withdraw 8 -1" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_2_3_4_7 1000 -1" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1001 -1" |

**Tabela 5 – Parâmetros da simulação MPLS-TE do Cenário 2**

| | |
|---|---|
| Simulação MPLS-TE | Parâmetros da Simulação MPLS |
| | 1000 Bytes |
| | $ns at 0.50 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1000" |
| | 2000 Bytes |
| | $ns at 0.48 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1000" |
| | $ns at 0.87 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1001" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_2_3_4_7 1002 -1" |
| | $ns at 1.26 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1002" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1001 -1" |
| | $ns at 1.60 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1001" |
| | 3000 Bytes |
| | $ns at 0.29 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1000" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1001 -1" |
| | $ns at 0.48 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1001" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_2_3_4_7 1002 -1" |
| | $ns at 0.58 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1002" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1001 -1" |
| | $ns at 1.63 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1001" |

## Cenário 3 – Métodos de recuperação de falhas

De forma a ser possível comparar os valores simulados na rede sem falhas com os valores simulados na rede com falhas é necessária a configuração da rede IP e MPLS sem falhas. Estas configurações estão representadas na Tabela 5.8, na Tabela 5.9 e Tabela 5.10.

**Tabela 6 – Parâmetros da simulação IP e MPLS sem falhas do Cenário 3**

| | |
|---|---|
| Simulação sem falhas na rede IP e na rede MPLS | $ns node-config –MPLS OFF |
| | Recuperação na rede IP |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |

**Tabela 7 – Parâmetros da simulação da Recuperação na rede IP do Cenário 3**

| | |
|---|---|
| Simulação da Recuperação na rede IP | $ns node-config -MPLS ON |
| | $ns at 0.10 "[$LSR7 get-module MPLS] ldp-trigger-by-withdraw 8 -1" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1000 -1" |
| | Recuperação Regional - Local Dinâmico sem o protocolo de encaminhamento DV |
| | $m enable-reroute "drop" |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |

**Tabela 8 – Parâmetros da simulação da recuperação na rede MPLS do Cenário 3**

| | |
|---|---|
| Simulação da Recuperação na rede MPLS | $ns node-config -MPLS ON |
| | $ns rtproto DV |
| | $ns at 0.10 "[$LSR7 get-module MPLS] ldp-trigger-by-withdraw 8 -1" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1000 -1" |
| | Recuperação Regional - Local Dinâmico |
| | $m enable-reroute "drop" |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |

As recuperações Global *Makam*, Regional e Local são configuradas no NS-2 através da Engenharia de Tráfego. A recuperação Global *Haskin* tem a particularidade de utilizar o modo “Data-Driven” em conjunto com o comando “$m enable-reroute "new" ” e com o comando “reroute-binding” de forma a ser simulado no NS-2. Quando não é utilizado o comando “$m enable-reroute "new" ” a eficiência da rede diminui, ou seja, são enviados menos pacotes até ao destino. Os tempos dos encaminhamentos explícitos e das junções, através do comando “reroute-binding”, devem ser respeitadas, caso contrário a simulação não funciona no modo de recuperação Global Haskin. Estas configurações encontram-se representadas na Tabela 5.11. A simulação da recuperação nas redes IP ou de “melhor esforço” é efectuada no NS-2 através do comando da Engenharia de tráfego “flow-erlsp-install” e sem o modo de encaminhamento de protocolos DV. A simulação dos vários métodos das recuperações de falhas é efectuada através do comando da Engenharia de tráfego “flow-erlsp-install”.

**Tabela 9 – Parâmetros da simulação da recuperação na rede MPLS-TE do Cenário 3**

| | |
|---|---|
| Simulação da Recuperação na rede MPLS-TE | $ns node-config -MPLS ON |
| | $ns rtproto DV |
| | $ns at 0.10 "[$LSR7 get-module MPLS] ldp-trigger-by-withdraw 8 -1" |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_5_6_7 1000 -1" |
| | Recuperação Global Makam |
| | $m enable-reroute "drop" |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 1_2_3_4_7 1001 -1" |
| | $ns at 0.51 "[$LSR1 get-module MPLS] flow-erlsp-install 8 -1 1001" |
| | Recuperação Global Haskin |
| | $m enable-reroute "new" |
| | Classifier/Addr/MPLS enable-on-demand |
| | Classifier/Addr/MPLS enable-ordered-control |
| | [$LSR1 get-module "MPLS"] enable-data-driven |
| | [$LSR2 get-module "MPLS"] enable-data-driven |
| | [$LSR3 get-module "MPLS"] enable-data-driven |
| | [$LSR4 get-module "MPLS"] enable-data-driven |
| | [$LSR5 get-module "MPLS"] enable-data-driven |
| | [$LSR6 get-module "MPLS"] enable-data-driven |
| | [$LSR7 get-module "MPLS"] enable-data-driven |
| | $ns at 0.10 "[$LSR1 get-module MPLS] make-explicit-route 7 2_3_4_7 1001 -1" |
| | $ns at 0.20 "[$LSR7 get-module MPLS] make-explicit-route 7_6_5_1_1001 1004 -1" |
| | $ns at 0.30 "[$LSR1 get-module MPLS] reroute-binding 8 -1 1004" |
| | $ns at 0.30 "[$LSR5 get-module MPLS] reroute-binding 8 -1 1004" |
| | $ns at 0.30 "[$LSR6 get-module MPLS] reroute-binding 8 -1 1004" |
| | Recuperação Regional - Local Dinâmico |
| | $m enable-reroute "drop" |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |
| | $ns at 0.10 "[$LSR5 get-module MPLS] make-explicit-route 7 5_3_4_7 1002 -1" |
| | $ns at 0.50 "[$LSR5 get-module MPLS] flow-erlsp-install 8 -1 1002" |
| | Recuperação Local - Fast reroute |
| | $m enable-reroute "drop" |
| | [$LSR1 get-module "MPLS"] enable-control-driven |
| | [$LSR2 get-module "MPLS"] enable-control-driven |
| | [$LSR3 get-module "MPLS"] enable-control-driven |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |
| | $ns at 0.10 "[$LSR5 get-module MPLS] make-explicit-route 7 5_3_4_6_7 1003 -1" |
| | $ns at 0.50 "[$LSR5 get-module MPLS] flow-erlsp-install 8 -1 1003" |

## Cenário 4 – Limites da Rede *Triple Play*

Na Tabela 5.12 estão representadas as configurações das simulações MPLS sem falhas. Nas Tabelas 5.13 e 5.14 podem ser observadas as configurações das simulações MPLS-TE sem falhas e MPLS com falhas “Deterministic”. O comando de falhas “Deterministic” permite a criação na rede de falhas aleatórias com o tempo não definido.

**Tabela 10 – Parâmetros da simulação MPLS sem falhas do Cenário 4**

| | |
|---|---|
| MPLS sem falhas | $ns node-config -MPLS ON |
| | $ns rtproto DV |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_5_6_7_10 1005 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_8_9_10 1006 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_8_6_7_10 1007 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_8_6_7_9_10 1008 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_8_9_7_10 1009 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_5_6_8_9_10 1010 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_5_6_8_9_7_10 1011 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_5_6_7_9_10 1012 -1" |

**Tabela 11 – Parâmetros da simulação MPLS-TE sem falhas do Cenário 4**

| | |
|---|---|
| Simulação MPLS-TE sem falhas | $m enable-reroute "drop" |
| | [$LSR4 get-module "MPLS"] enable-control-driven |
| | [$LSR5 get-module "MPLS"] enable-control-driven |
| | [$LSR6 get-module "MPLS"] enable-control-driven |
| | [$LSR7 get-module "MPLS"] enable-control-driven |
| | [$LSR8 get-module "MPLS"] enable-control-driven |
| | [$LSR9 get-module "MPLS"] enable-control-driven |
| | [$LSR10 get-module "MPLS"] enable-control-driven |
| | $ns at 0.10 "[$LSR10 get-module MPLS] ldp-trigger-by-withdraw 11 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_8_9_10 1000 -1" |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 4_5_6_7_10 1001 -1" |
| | Engeneharia de Tráfego sem perdas significativas |
| | $ns at 2.1 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1005" |
| | Engeneharia de Tráfego com perdas significativas |
| | $ns at 0.141 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1005" |
| | $ns at 0.16 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1006" |
| | $ns at 0.173 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1007" |
| | $ns at 0.183 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1010" |
| | $ns at 0.196 "[$LSR4 get-module MPLS] flow-erlsp-install 11 -1 1009" |

**Tabela 12 – Parâmetros da simulação MPLS com falhas do Cenário 4**

| | |
|---|---|
| Simulação MPLS com falhas | $m enable-reroute "new" |
| | ********** Recuperação Global Haskin |
| | Classifier/Addr/MPLS enable-on-demand |
| | Classifier/Addr/MPLS enable-ordered-control |
| | [$LSR4 get-module "MPLS"] enable-data-driven |
| | [$LSR5 get-module "MPLS"] enable-data-driven |
| | [$LSR6 get-module "MPLS"] enable-data-driven |
| | [$LSR7 get-module "MPLS"] enable-data-driven |
| | [$LSR8 get-module "MPLS"] enable-data-driven |
| | [$LSR9 get-module "MPLS"] enable-data-driven |
| | [$LSR10 get-module "MPLS"] enable-data-driven |
| | |
| | $ns at 0.10 "[$LSR4 get-module MPLS] make-explicit-route 10 5_6_7_10 1001 -1" |
| | $ns at 0.2 "[$LSR10 get-module MPLS] make-explicit-route 10 9_8_4_1001 1003 -1" |
| | $ns at 0.3 "[$LSR4 get-module MPLS] reroute-binding 11 -1 1003" |
| | $ns at 0.3 "[$LSR8 get-module MPLS] reroute-binding 11 -1 1003" |
| | $ns at 0.3 "[$LSR9 get-module MPLS] reroute-binding 11 -1 1003" |
| | |
| | $ns rtmodel Deterministic {0.3 0.9 0.4} $LSR4 $LSR8 |
| | $ns rtmodel Deterministic {0.3 0.9 0.4} $LSR8 $LSR9 |
| | $ns rtmodel Deterministic {0.3 0.9 0.4} $LSR9 $LSR10 |