UNIVERSIDADE FEDERAL FLUMINENSE
CENTRO TECNOLÓGICO
MESTRADO EM ENGENHARIA DE TELECOMUNICAÇÕES

ALEXSANDRO BARBOSA PAES

UMA ABORDAGEM PRAGMÁTICA PARA ANÁLISE E PROJETO DE REDES WAN

NITERÓI
2008

ALEXSANDRO BARBOSA PAES

UMA ABORDAGEM PRAGMÁTICA PARA ANÁLISE E PROJETO DE REDES WAN

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Comunicação de Dados Multimídia

Orientador: Prof^{o} Carlos Alberto Malcher Bastos, D.sc

Niterói

2008

ALEXSANDRO BARBOSA PAES

UMA ABORDAGEM PRAGMÁTICA PARA ANÁLISE E PROJETO DE REDES WAN

Dissertação apresentada ao Curso de Mestrado em Engenharia de Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre. Área de Concentração: Comunicação de Dados de Multimídia

Aprovada em _____de_____ de 2008

BANCA EXAMINADORA

_____

Prof^{o} Carlos Alberto Malcher Bastos, D.sc – Orientador
Universidade Federal Fluminense

_____

Prof^{o} Luiz Cláudio Schara Magalhães, Phd
Universidade Federal Fluminense

_____

Prof^{a} Débora Christina Muchaluat Saade, D.Sc.
Universidade Federal Fluminense

_____

Prof^{o} Anilton Salles Garcia, D.Sc.
Universidade Federal do Espírito Santo

Niterói

2008

Dedico este trabalho à minha família, meus pais e minha noiva.

AGRADECIMENTOS

Ao prof. Dr. Carlos Alberto Malcher Bastos pela sua ajuda e sua grande capacidade de orientar. Sem seu direcionamento seria impossível realizar este trabalho. Seus ensinamentos não serviram apenas para esse trabalho, mas para meu encaminhamento na vida profissional e pessoal. Espero que voltemos a trabalhar num futuro próximo.

Ao Prof.Dr. Anilton Salles Garcia, que mesmo a distância foi sempre presente e contribui de maneira essencial neste trabalho.

Ambos os professores são referência profissionais para muitos colegas e profissionais. Fazem da docência não apenas um ofício, mas uma vocação.

Aos professores Débora, Schara e Luis Pinto que contribuíram para minha formação de pós-graduação.

A coordenação do Mestrado e os professores, que fazer da UFF uma grande instituição, tão importante para o Estado do Rio de Janeiro e o Brasil.

A minha família que sempre compreendeu minha ausência em vários momentos.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRAFÍCOS

LISTA DE FLUXOGRAMAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

AF	**Assured Forward**
AS	**Autonomous System**
ATM	**Asynchronous Transfer Mode**
BA	**Behavior Aggregate**
BGP	**Border Gateway Protocol**
CBR	**Constraint-Based Routing**
CE	**Customer Router Edge**
CIR	**Committed information rate**
COS	**Class Of Service**
CR-LDP	**Constraint-Based LSP Setup using LDP**
CSPF	**Constrained Shortest Path Forwarding**
DHCP	**Dynamic Host Configuration**
DNS	**Domain Name Service**
DSCP	**DiffServ CodePoints**
DWDM	**Dense Wavelength Division Multiplexing**
ECMP	**Equal-Cost Multi-Path**
EGP	**Exterior Gateway Protocol**
EoS	**Ethernet over Sonet**
EXP	**Experimental Field**
FEC	**Forwarding Equivalence Classes**
FIFO	**First-In-First-Out**
FTP	**File Transfer Protocol**
GE	**Gigabit Ethernet**
GFP	**Generic Framing Procedure**
HDLC	**High-level Data Link Control**
IETF	**Internet Engineering Task Force**
IGP	**Interior Gateway Protocol**
IP	**Internet Protocol**
ISDN	**Integrated Services Digital Network**
IS-IS	**Intermediate-System - to - Intermediate-System**
ISO	**International Organization for Standardization**
ISP	**Internet Service Provider**
L2TP	**Layer Two Tunneling Protocol**
LAN	**Local Area Network**
LCAS	**Link Capacity Adjustment Scheme**
LDP	**Label Distribution Protocol**
LER	**Label Switch Edge Router**
LIB	**Label Information Base**
LSP	**Label Switched Path**
LSR	**Label Switch Router**
MBGP	**Multiprotocol BGP**
MIB	**Management Information Base**
MPLS	**MultiProtocol Label Switching**

MPLS-TE	**Multiprocol Label Switching Traffic Engineering**
MSTP	**Multiple Spanning Tree Protocol**
MTU	**Maximum Transfer Unit**
NAT	**Network Address Translation**
NS	**Network Simulator**
OSI	**Open Systems Interconnection**
OSPF	**Open Shortest Path First**
P	**Provider Router**
PE	**Provider Router Edge**
PHB	**Per-Hop-Behavior**
PIM	**Protocol Independent Multicast**
PIR	**Peak Information Rate**
PoS	**Packet over Sonet**
PPP	**Point to Point Protocol**
PPTP	**Point-to-Point Tunneling Protocol**
PQ	**Priority Queuing**
PREA	**Packet Ring Edge Aggregator**
QoS	**Quality of Service**
RD	**Route Distinguish**
RED	**Random Early Detection**
RFC	**Request for Comments**
RIP	**Routing Information Protocol**
RMON	**Remote Monitoring**
RPR	**Resilient Packet Ring**
RPT	**Resilient Packet Transport**
RSTP	**Rapid Spanning Tree Protocol**
RSVP	**Resource Reservation Protocol**
RSVP-TE	**Resource Reservation Protocol Traffic Engineering**
SDH	**Synchrouns Digital Hierarchy**
SLA	**Service Level Agreement**
SLS	**Service Level Specifications**
SONET	**Synchrouns Optical Network**
SNMP	**Simple Network Management Protocol**
STP	**Spanning Tree Protocol**
TCP	**Transport Control Protocol**
TDM	**Time-Division Multiplexing**
TE	**Traffic Engineering**
TOS	**Type Of Service**
TTL	**Time to Live**
UDP	**User Datagram Protocol**
VCAT	**Virtual Concatenation**
VLAN	**Virtual Local Area Network (802.1Q)**
VPLS	**Virtual Private LAN Service**
VPN	**Virtual Private Network**

VRF	**Virtual Private Network Routing and Forwarding Tables**
WAN	**Wide Area Network**
WDM	**Wavelength-Division Multiplexing**
WFQ	**Weighted Fair Queuing**
WRED	**Weighted Random Early Detection**
WRR	**Weighted Round Robin**

RESUMO

O objetivo desta dissertação é apresentar algumas características das soluções de transporte para *WAN*, assim como a apresentação das facilidades que o uso do *Multiprotocol Label Switching Architecture (MPLS)* pode trazer para interligar e aumentar o desempenho das redes.

Na dissertação é realizado um estudo de caso de uma infra-estrutura pertencente a uma empreasa do setor elétrico. O estudo abrange questões como topologia de rede, gerência, escalabilidade e qualidade de serviço, que são analisados e testados na plataforma de simulação OPNET®. O principal objetivo do trabalho é propor melhorias para o caso estudado e servir como referências para projetos de redes WAN para empresas de grande porte ou operadores.

Palavras chaves: Redes, OPNET®, MPLS, simulação e engenharia de tráfego.

ABSTRACT

The focus of this work is to present some characteristics of the transport solutions to WAN, as well as, the presentation of Multiprotocol Label Switching Architecture (MPLS) utilities that could be established to connect network and improve network performance. This is a case study about Energy Company. That will cover the network topology, scalability, quality of service and management. These issues will be tested, analyzed in OPNET® simulation platform.

The main goal is to make improvements for this network and serve as reference to enterprise and ISP WAN network.

Keywords: Network, OPNET®, MPLS, Simulator and Traffic Engineering.

1. Introdução

Na década de 90, com o surgimento das redes corporativas baseadas em microcomputadores e a padronização tecnológica provida pelo protocolo *IP*, tornou-se possível a interconexão de redes distintas. Neste contexto, as grandes corporações perceberam os benefícios do fornecimento de múltiplos serviços baseados em uma infra-estrutura única. As redes convergentes podem proporcionar para as empresas maior facilidade de gerenciamento e diminuição de custo, com reflexo direto na diminuição do custo operacional.

Os benéficos oferecidos pelas redes convergentes motivaram as empresas a migrarem suas redes tradicionais para infra-estruturas convergentes. Nos últimos anos esta tendência tem se acelerado, principalmente em virtude da abundância de oferta de equipamentos e banda larga. Com isso, as redes tradicionais estão migrando, de forma rápida, para soluções convergentes. Entretanto, questões como: integrar diferentes tecnologias de *WAN* (*Wide Area Network*), suporte a serviços de tempo real e gerenciamento centralizado, ainda não foram resolvidas.

Atualmente, a convergência é o grande desafio das redes de telecomunicações. Quanto mais perto as redes chegarem da total convergência, mais eficientes serão as soluções de serviços e atendimento a demandas especificas. Interoperabilidade entre os serviços das diferentes redes é um ponto chave. A interoperabilidade é um ponto importante porque as soluções de rede apresentadas pelos fornecedores de equipamentos não são homogêneas e requerem diferentes artifícios técnicos para se interconectarem.

Nas grandes corporações já existe uma infra-estrutura legada que não pode ser substituída integralmente. A arquitetura convergente permite a realização de novos investimentos em infra-estrutura, preservando parte do parque de equipamentos já instalado, possibilitando assim, o atendimento à crescente demanda por novos serviços de telecomunicações.

Dentro deste contexto, as empresas demandam "*Know-how*" no desenvolvimento do projeto de migração de suas redes para este novo paradigma. Os novos projetos de rede precisam estar aderentes a esta nova estrutura e precisam manter os serviços existentes.

O objetivo da dissertação é apresentar uma proposta de abordagem para análise de projetos de redes convergentes objetivando a proposição de melhorias técnicas e operacionais. Questões como integração entre diferentes protocolos, desempenho da rede, suporte a qualidade de serviço, topologia de rede escalar, gerência amigável, dentre outras, precisam ser analisadas com foco no estudo de caso.

Mais especificamente, a dissertação pretende analisar os benefícios do uso do *Multiprotocol Label Switching Architecture (MPLS)* na engenharia de tráfego, na integração com outros protocolos *WAN*, no tempo de recuperação da rede em caso de falha e especificações técnicas-funcionais dos equipamentos. A análise dos benefícios da qualidade de serviço (*QoS*) também é objetivo da dissertação. O uso de simulação computacional e testes de campo fazem parte da proposta apresentada nesta dissertação e permitem a comprovação das premissas assumidas no desenvolvimento da mesma.

Ao fim do trabalho, o principal resultado esperado é a construção de uma abordagem pragmática e eficaz de avaliação e proposição de melhorias para projeto de redes convergentes. Espera-se que as propostas ofertadas pela dissertação tragam maior desempenho, qualidade e adaptabilidade da rede as necessidades do estudo de caso.

As principais contribuições deste trabalho são: apresentar uma metodologia customizada para análise de projetos de redes convergentes para analistas e administradores de rede, identificar os benefícios do *MPLS* numa rede real e trazer melhorias operacionais e funcionais para uma rede operativa.

A dissertação está estruturada como segue:

O capítulo 2 apresenta uma síntese dos principais trabalhos realcionados com o tema central da dissertação e que serviram de referência teórica para este trabalho.

O capítulo 3 discute as tecnologias *WAN*, o conceito *Metro Ethernet* e os benefícios do *MPLS*. Este capítulo tem como objetivo, apresentar algumas características de soluções existentes para *WAN*, assim como a apresentação das facilidades que o uso do *Multiprotocol Label Switching Architecture (MPLS)* pode trazer para interligar e aumentar o desempenho das redes.

O capítulo 4 apresenta uma proposta de abordagem pragmática de análise de projeto de rede WAN. A abordagem tem o objetivo de organizar o trabalho através de uma metodologia que especifique as atividades que devem ser realizadas, como são feitas e ordem de cada atividade. A organização e eficácia são os enfoques da metodologia.

O capítulo 5 apresenta o estudo de caso sobre a Rede *WAN* de uma empresa do setor elétrico. Este capítulo tem com objetivo compreender a rede em questão e propor, seguindo a abordagem pragmática proposta, melhoramentos, tomando como base os conhecimentos adquiridos nos estudos preliminares deste trabalho. Também são apresentadas algumas simulações com o objetivo de comprovar as premissas apresentadas no estudo teórico.

O capítulo 6 deste trabalho apresenta as conclusões extraídas dos estudos e sugere temas para novas pesquisas.

2. Trabalhos relacionados

Este capítulo tem por objetivo apresentar uma síntese das principais referências bibliográficas estudadas durante o desenvolvimento da dissertação e que estão diretamente relacionadas com os objetivos centrais da dissertação. Tais referências abordam aspectos de Engenharia de Tráfego, Qualidade de Serviço, Tecnologias *WAN* e Metodologias de projeto de Redes.

2.1. Engenharia de Tráfego

A Engenharia de Tráfego trata de aspectos relacionados a medições, caracterização, modelagem e controle de tráfego. Um dos objetivos da Engenharia de Tráfego é melhorar o desempenho da rede em termos de uso racional de recursos evitando congestionamento. No caso de congestionamento, adaptabilidade do tráfego para amenizar suas conseqüências.

A Engenharia de Tráfego associada ao *MPLS* surge como uma solução para problemas de congestionamento provocados por escolha de rota mais curtas, típico funcionamento em redes IP. O uso de *LSPs (Label Switch Path) MPLS* com banda garantida evita esse tipo de problema e possibilita o melhor uso da infra-estrutura.

A principal referência foi o artigo "***Performance measurements of MPLS traffic engineering and QoS***" [5]. Este artigo evidencia a eficiência do *MPLS* no suporte a engenharia de tráfego. Prover qualidade de serviço e engenharia de tráfego na Internet é muito importante, especialmente para suportar os requisitos de tempo real e aplicações de missão

críticas. Para este propósito, a *Internet* atual precisa aceitar a introdução de novas tecnologias que permitam a capacidade de controlar melhor o comportamento da rede. O *MPLS* (*Multiprotocol Label Switching*) é tecnologia emergente, que os operadores de rede consideram como uma solução para prover qualidade de serviços e engenharia de tráfego em redes *IP*.

Os serviços diferenciados para diferentes fluxos de tráfego e otimização do desempenho são importantes para o alcance das metas desejadas. Nas redes IP, os protocolos de roteamento *IGPs* (*Interior Gateway Protocol*), tais como *OSPF* (*Open Shortest Path First*) e *IS-IS* (*Intermediate System-Intermediate System*), usam algoritmo de roteamento baseado no destino, sem considerar outros parâmetros da rede, tais como disponibilidade de banda. Com isso, todo tráfego pode seguir para o mesmo caminho e deixar outros caminhos ociosos. Como resultado, degradação do *throughput*, aumento do atraso e perda de pacote podem ocorrer. A chave deste problema é a engenharia de tráfego que tem habilidade de alocar o tráfego dentro da rede de forma flexível, a fim de minimizar congestionamentos e melhorar o desempenho.

O artigo apresenta os protocolos de distribuição de rótulo (*CR-LDP (Constraint Routing – Label distribution protocol) e RSVP-TE (Resource reSerVation Protocol)*) que determinam o caminho *MPLS (LSP)* através da rede. O estabelecimento do *LSP* respeita restrições de requisitos, tais como banda e atraso. Depois, as informações de associação de rótulo (*Label Binding*) são distribuídas ao longo de uma rota pré-definida.

A "***RFC2702 - Requirements for Traffic Engineering over MPLS***" [4] é outro documento importante e referência nesta dissertação. A RFC apresenta os requisitos de

configuração para engenharia de tráfego sobre *MPLS*. Nela são identificadas as necessidades funcionais requeridas numa rede para implementar políticas que facilitem a eficiência e confiabilidade em domínios *MPLS*. A RFC-IETF (*Request for Comment - Internet Engineering Task Force*) aponta o uso da engenharia de tráfego para otimização dos recursos da rede e alcançar maior desempenho. A engenharia de tráfego também tem se tornado uma indispensável funcionalidade em muitas redes devido ao alto custo das redes e competição natural da Internet. Uma abordagem para resolver problemas de tráfego dentro de *IGPs* é o uso de redes sobrepostas, tais como *IP* sobre *ATM* ou *IP* sobre *Frame Relay*. O modelo de rede sobreposta é o desenho da topologia da rede pela criação de uma topologia virtual sobreposta a rede física. A topologia virtual é construída através de circuitos virtuais que aparecem como links físicos para os protocolos *IGPs*. O modelo de redes sobrepostas provém serviços adicionais para suportar tráfego e controle de recursos, incluindo: (1) roteamento baseado em restrições; (2) suporte a configuração de caminho explícito; (3) controle de admissão e (4) divisão de tráfego. Todas essas características permitem o funcionamento de uma variedade de configurações de engenharia de tráfego. O *MPLS* permite também o suporte às facilidades citadas.

2.2. Qualidade de Serviço

A qualidade de serviço na *Internet* está ligada ao aumento do grau de satisfação do usuário final e a possibilidade de funcionamento de novas mídias em redes tipicamente de dados. Com o tratamento diferenciando ou integrado pode-se prover mecanismos que garantam um SLA (Service Level Agreement) combinada. Os artigos "***Converged Services over MPLS***" [20], "***A Monitoring and Measurement Architecture for Traffic Engineered IP***

Network" [1] e ***"Experiences with Class of Service (CoS) translations in IP/MPLS Networks"*** [28] foram instrumentos importantes na confecção desta dissertação.

O primeiro artigo coloca o *MPLS* e *QoS* como pontos chaves para o aumento do grau de satisfação do usuário final e a possibilidade de funcionamento de novas mídias. Com o tratamento diferenciando de classes de serviços torna possível implantar mecanismos que garantam um *SLA* (*Service Level Agreement*) pré-configurada. As características do *QoS MPLS* representam a capacidade de prover níveis diferenciados de serviços e garantia de recursos da rede. Esta capacidade tipicamente inclui uma seleção de técnicas necessárias para gerenciar banda, atraso, variação de atraso e perdas de pacotes da rede. Por exemplo, a habilidade de marcar pacotes com certa prioridade combinado com gerencia de *buffer* e esquemas de filas asseguram a qualidade do tráfego de voz na rede que tem fortes restrições de atraso e variação de atraso na sua transmissão. O *MPLS* possui um campo chamado de *CoS* (*EXP*) e seu valor será usado para determinar o tipo de tratamento (*queuing* e *scheduling*) do pacote na rede [20].

O segundo artigo especifica a sistemática de funcionamento do modelo diferenciado de qualidade de serviço no *MPLS*. O encaminhamento de tráfego em redes com *QoS* pode encontrar uma diferenciação dentro algumas classes de serviços. Como as redes tentam oferecer diferentes tipos de serviço pelo uso de mecanismo de engenharia de tráfego, serviços de monitoração começam aumentar de importância para provimento de *QoS* fim a fim e serviços garantidos. O artigo mostra também a importância das informações de medições que necessitam ser coletadas em finas granularidades e por classe de serviço *QoS. O* artigo apresenta uma arquitetura de medição e monitoração de rede com foco na qualidade de serviço [1].

No terceiro artigo são apresentadas experiências com classes de serviços traduzidas de *IP* para *MPLS*. É mostrado neste artigo o resultado obtido pelo uso de *MPLS CoS* com alocação de banda relativa. O efeito do uso de *WFQ (Weighted Fair Queuing)* por classe para tráfego de altas taxas e rajada. Mostra a eficácia do *MPLS* para alocação de banda relativa e a prevenção de perdas para classes inferiores de prioridade. Neste artigo também é discutido o efeito de inadequados mapeamentos de *MPLS CoS* em redes interconexão de redes [28].

2.3. Tecnologias *WAN*

O artigo "***Performance Comparison of Resilient Packet Ring, Packet over Sonet (Synchronous Optical Network) and Gigabit Ethernet for Network design***" [40] e o livro "***Metro Ethernet***" [15] abordam as tecnologias *WAN* com detalhamento e sobre uma ótica comparativa. Questões como eficiência, compatibilidade, recuperação a falhas e gerenciamento são tratados por estes trabalhos.

O primeiro artigo, "*Performance Comparison of Resilient Packet Ring, Packet over Sonet (Synchronous Optical Network) and Gigabit Ethernet for Network design*" [40], realiza um comparativo entre os padrões *RPR, PoS e GE*. Questões como recuperação a falhas, desempenho da transmissão de dados e, QoS são testadas e avaliadas. O artigo defende o uso do *RPR* como principal solução para redes metropolitanas e com alta demanda de tráfego. Entretanto especifica a necessidade da rede ter uma topologia anel para perfeito funcionamento do *RPR*.

O livro *Metro Ethernet* [15] possui um temática abrangente e apresenta diversas informações sobre protocolos de *WAN* (*RPR,Etherner over Sonet e Gigabit Ethernet*), protocolo *Ethernet*, *MPLS* e *Virtual Privete Network*. O livro descreve o *RPR* como um protocolo importante no desenvolvimento de serviços de dados em *Metro Ethernet*. O *RPR* é apresentado como um novo protocolo de controle de acesso ao meio (*MAC*) que é desenhado para aperfeiçoar gerência de banda e facilitar o desenvolvimento dos serviços de dados sobre redes em anéis. Sendo este uma nova tecnologia de transmissão de pacotes em anéis que usa fibra não-utilizadas, *Wavelegth Division Multiplexing* (*WDM*) e *Sonet/SDH*. Além do *RPR*, o *EOS* (*Ethernet over Sonet*) é apresentado como uma opção de protocolo para redes *Metro Ethernet*. O *EOS* resolve problemas do emprego de serviços *Metro Ethernet* em infra-estruturas *SDH/SONET* legadas. O livro descreve o *MPLS* como solução de integração de protocolos, engenharia de tráfego e qualidade de serviço em âmbito *Metro Ethernet*.

2.4. Projetos de Redes WAN

A dissertação "**Proposta de Metodologia para Projetos de Redes *WAN* Multimídia com Suporte a Requisitos de Qualidade de Serviço**" [9] apresenta uma metodologia capaz de organizar e estabelecer os caminhos necessários para se projetar redes *WAN* com requisitos de qualidade de serviço. A metodologia desenvolvida é aplicada ao um ambiente real e é testada com sucesso. A simulação computacional é utilizada neste trabalho para verificar o impacto das demandas futuras e garantir que novas demandas não degradem outros serviços disponíveis na infra-estrutura existente. Outro objetivo da metodologia é maximizar a utilização da rede para uma melhor relação custo benefício.

Os livros “Projeto de Redes *Top-Down*” [25] e “Projeto de Interconexão de Redes – *Cisco Internetworking Design (CID)”* [41] são também referências sobre projeto de redes. Ambos apresentam aspectos práticos de projetos de rede e servem como uma guia para a prática. Os livros abordam o avanço tecnológico como um fator crítico no desenvolvimento de projetos de rede. O projeto de interconexão dessas novas redes exige um planejamento cuidadoso e coordenado que envolve a utilização de hardware e software de fabricantes diferentes em um único ambiente, o hardware sendo composto por uma combinação de dispositivos e acessórios com diferentes graus de complexidade e o software caracterizado por sistemas de uso geral (aplicativos de usuários) e também de uso específico (sistemas operacionais de rede). Para lidar com essa complexidade crescente e assegurar sua sobrevivência no mercado, as empresas têm investido na interligação de suas redes segundo estruturas que seguem metodologias e padrões. Estas bibliografias têm como objetivo abordar alguns aspectos importantes na caracterização da metodologia e a modelagem utilizada para elaborar e desenvolver de um projeto de redes.

No capítulo a seguir é apresentado um estudo teórico sobre as principais tecnologias de *WAN*.

3. Tecnologias *WAN*

As redes *WANs* apresentam diferentes soluções no que tange a camada dois do modelo de referência OSI (*Open Systems Interconnection)*, doravante denominado modelo *OSI*, como: *Resilient Packet Ring (RPR), Gigabit Ethernet (GE) e Packet over Sonet (PoS) e Ethernet over Sonet (EoS)* [15]. Essas tecnologias são atualmente utilizadas por diferentes operadoras de serviços de telecomunicações.

As soluções *WAN* que utilizam o enquadramento *Ethernet* são comumente chamadas de *Metro Ethernet*. O *Metro Ethernet* é um tipo de arquitetura *WAN* em franca expansão e é importante sua apresentação nesta dissertação.

O *MPLS* também é apresentado neste capítulo. Os benefícios de sua utilização são verificados na maioria arquitetura de *WAN* existente. A implementação da engenharia de tráfego, qualidade de serviço e integração com outras tecnologias de rede são pontos fortes desta tecnologia.

3.1. *Metro Ethernet*

O termo *Metro Ethernet* é utilizado para descrever uma rede Metropolitana (*MAN*) que disponibiliza serviços de conectividade utilizando o protocolo *Ethernet*. O *Metro Ethernet* pode ser considerado como um conceito “guarda-chuva”, porque envolve diversos padrões e soluções existentes. Sua arquitetura basicamente é: composta de diferentes *LANs* espalhadas geograficamente e ligadas através de uma rede *WAN* [21].

As redes *Metro Ethernet* funcionam sobre vários tipos de tecnologias, como as que funcionam como infra-estrutura de camada física, tais como: *RPR (Resilient Packet Ring)*; *Sonet (Synchronous Optical Network)/SDH (Synchronous Digital Hierarchy); Gigabit Ethernet e DWDM (Dense Wavelength Division multiplexing)*; e como as de infra-estrutura de transporte: *Internet Protocol (IP), ATM, Frame Relay e MPLS*. A seguir a Figura 1 – Arranjo *Metro*. [21] ilustra arranjos possíveis *Metro Ethernet*.

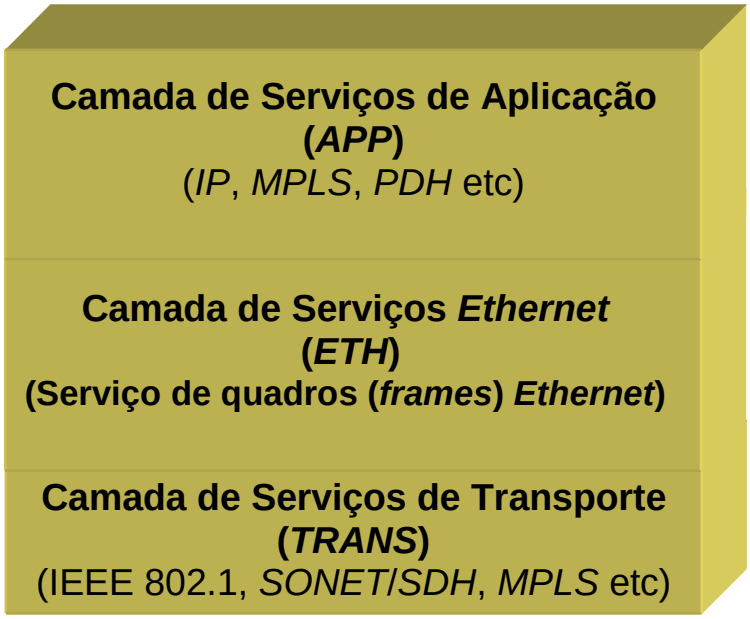


Figura 1 – Arranjo *Metro*. [21]

Basicamente os desenhos das topologias *Metro Ethernet* possuem três camadas (TRANS, ETH, e APP). As camadas transporte (TRANS) e aplicação (APP) podem funcionar com diferentes protocolos. O administrador ou projetista deve utilizar as opções que melhor se aplicam às suas necessidades. O uso dos protocolos *IP* e *MPLS* são as opções mais comuns na camada de aplicação. Ambos trazem confiabilidade (mais fáceis de convergir em caso de problema), flexibilidade (possibilidade de conviver com diferentes protocolos) e maior facilidade de operação [15].

O *Metro Ethernet* disponibiliza basicamente dois tipos de serviço: *Ethernet Line Services* (E-Line/serviço ponto a ponto) e *Ethernet LAN Services* (E-LAN/ serviço multiponto-multiponto) [21].

O *Ethernet* oferece diversas facilidades sendo a principal a grande aceitação do mercado, possível através de preço mais baixo do que outras interfaces existentes.

3.1.1. *MAC (Medium Access Control) Learning*

O *MAC Learning* permite que *switches Ethernet* aprendam endereços *MAC* das estações da rede. Os *switches* através deste conhecimento evitam o *broadcasting* comum do protocolo *Ethernet* [15]. O *MAC Learning* utiliza o *Flooding* quando um switch recebe um pacote com endereço *MAC* de destino desconhecido. Basicamente ele consiste no envio do pacote por todas as interfaces do nó, exceto a interface que recebeu o quadro [15].

3.1.2. *VLAN Tagging*

O *VLAN Tagging* é o campo responsável pela identificação do quadro para uma determinada *VLAN* e pela identificação de qual prioridade este quadro teria diante de outros na fila de encaminhamento. A Figura 2 – Campos do 802.1Q. [10] mostra o formato *IEEE 802.1Q* [16].

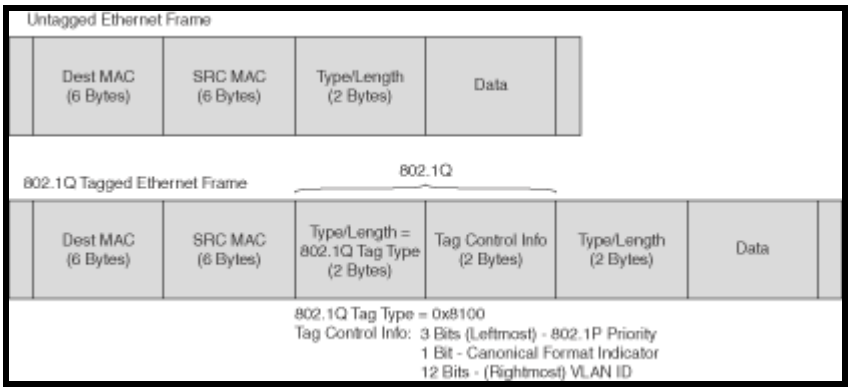


Figura 2 – Campos do 802.1Q. [10]

O *IEEE 802.3q* faz a adição de quatro octetos ao quadro *Ethernet*. Esses quatro octetos são os bits responsáveis tanto pela identificação da *VLAN* (*Virtual Local Area Network*) quanto pela marcação da prioridade do quadro, referente à norma IEEE 802.1p[15]. O valor do campo 802.1p é responsável por carregar a informação de "user_priority" através da *LAN*. O campo possui três bits que são capazes de representar oito diferentes níveis de prioridades (de 0 a 7)[16].

Para permitir que diversas *VLAN* transitem por uma mesma porta *Ethernet*, deve-se utilizar o conceito de porta agregada. Esta porta comumente é utilizada para interligar switches com diversas *VLAN* configuradas entre eles [15].

O *Ethernet* oferece algumas restrições de escalabilidade. Em relação a escalabilidade, o padrão 802.1q define 12 bits para criação de *VLAN*. Assim, pode-se ter no máximo 4096 *VLANs* configuradas numa mesma rede *Ethernet* [15].

3.1.3. *Spanning Tree Protocol* (*STP*)

Este protocolo é responsável por montar a árvore de encaminhamento de uma rede Ethernet. Toda a matriz de encaminhamento *Ethernet* é construída a partir do *Spanning-Tree*

Protocol, este é necessário principalmente para evitar loop. Questões como otimização de banda e retardo não são consideradas. Em suma, o *Ethernet* não oferece engenharia de tráfego visto as limitações do protocolo *RPR* responsável garantia de convergência da rede em caso de falha em enlace ou nó da rede [40].

O *RSTP (Rapid Spanning Tree Protocol)* é uma evolução de *STP* que permite uma convergência num tempo menor do que o *STP* convencional. O tempo de detenção de falha é reduzido para menos de 1 segundo [15].

O *MSTP* (*Multiple Spanning Tree Protocol)* foi originalmente definido pelo *IEEE802.1s*. Este padrão permite a configuração de *Spanning Tree Protocol* por *VLAN*. O *MSTP* cria a matriz de encaminhamento *Ethernet* por *VLAN*, considerando apenas os nós pertencentes a uma determinada *VLAN* [15].

3.1.4. Suporte às aplicações

A seguir são listadas algumas aplicações suportadas pelas redes *Metro Ethernet*, segundo o *Metro Ethernet Forum* [21]:

- LAN de vídeo/ treinamento;
- Pré-impressão jornalística;
- CAD (*Computer Aided Desing*)/CAM (*Computer Aided Manufacturing*);
- Backup corporativo/servidores e recuperação de dados;
- Transferência de dados médicos;
- Modelagem científica;
- Aplicações de armazenamento.

3.2. *Gigabit Ethernet*

O *Gigabit Ethernet (GE)* é padronizado pelo *IEEE 802.3z*. A vasta utilização do *Ethernet* em redes locais (LAN) e o seu baixo custo facilitaram a aceitação do *Gigabit Ethernet* pelo mercado. O *Ethernet* e o *Gigabit Ethernet* foram desenhados especificamente para tráfegos baseados em quadros e oferecem vantagens para redes estatísticas. O padrão *IEEE* 802.3z realizou sensíveis alterações no padrão *Ethernet*. Assim como o *Fast Ethernet*, o padrão permite o modo de operação *half / full-duplex* e possui alterações na camada física, uma delas foi a codificação 8B/10B [15].

O padrão *GE* utiliza o mesmo formato de quadro *Ethernet* e apenas foi inserida uma extensão para adaptar o GE no modo half-duplex (neste modo o tamanho mínimo do pacote foi aumentado) [15]. O cabeçalho *IEEE* 802.3 e o cabeçalho *IEEE* 802.3z são ilustrados pelas Figura 3 - Quadro *IEEE 802.3.* [10] e Figura 4 - Quadro *IEEE 802.3z.* [10].

Várias extensões do *IEEE* (*Institute of Electrical and Electronics Engineers*) servem de suporte para ao funcionamento do GE. Dentre estas se têm: *VLAN Tagging*, *Spanning Tree Protocol, Rapid Spanning Tree Protocol e Multiple Spanning Tree Protocol* [15].

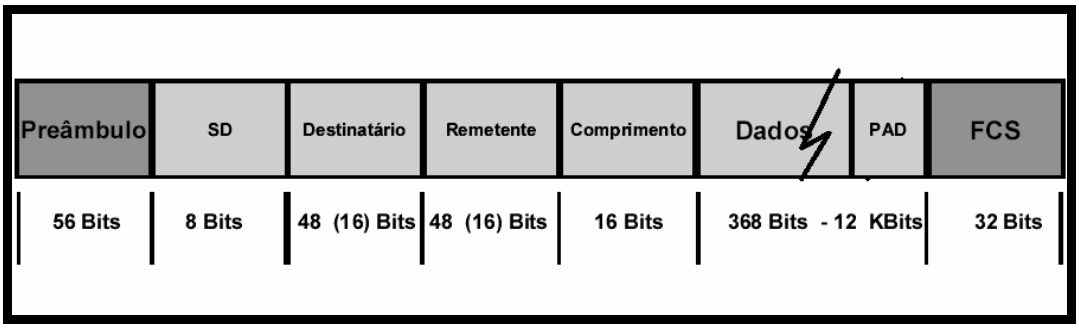


Figura 3 - Quadro *IEEE 802.3.* [10]

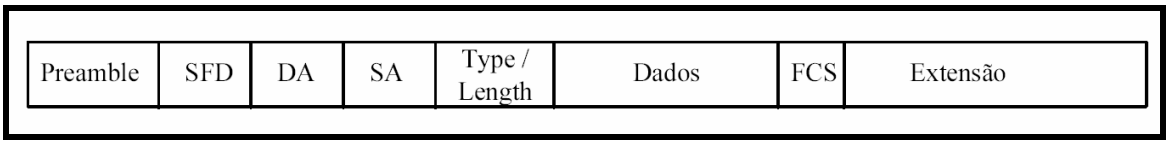


Figura 4 - Quadro *IEEE 802.3z.* [10]

3.3. *Resilient Packet Ring* (*RPR*)

O *Resilient Packet Ring (RPR)* é uma tecnologia de camada dois do modelo *OSI* para *WAN*, definida pelo padrão *IEEE 802.17 Working Group* em 2003. No desenvolvimento desse padrão buscou-se desenhar um protocolo de comunicação de *WAN* para funcionar em redes com topologia em anel. Procurou-se também inserir funcionalidades que permitissem fácil gerenciamento de rede, eficaz sistema de proteção a falhas, independência da camada física e alta velocidade de comutação.

3.3.1. Funcionamento do *RPR*

A tecnologia *RPR* basicamente utiliza dois anéis de fibra. Ao invés de um anel transmitir e o outro ser backup (configuração típica de outras redes em anel), esta tecnologia utiliza os dois anéis simultaneamente no seu funcionamento. Uma configuração padrão é a utilização de um anel transmitindo tráfego de dados e o outro anel para transmissão de informações de controle, mas é possível manter os dois anéis transmitindo informações de dados simultaneamente [17]. Alguns exemplos de informações de controle são: atualização de topologia, controle de banda e proteção [17].

As mensagens de controle de banda permitem a negociação de banda entre os nós do anel. O *RPR* também tem a habilidade de diferenciar prioridades entre diferentes quadros que

trafegam no anel, permitindo assim a implementação de qualidade de serviço (*QoS*) na camada dois [15].

O *RPR* permite uma independência de funcionamento da camada física. Em outras palavras, pode-se dizer que o RPR pode conviver com diferentes padrões de camada física sem prejuízo para o seu funcionamento e essa característica possibilita uma fácil aceitação do *RPR* pelos provedores de serviços [40].

Seguem exemplos de protocolos de camada física aceitos pelo RPR: fibra óptica (*Gigabit Packet PHY*); *Wavelegth Division Multiplexing* (*Gigabit Packet PHY*) e Sonet/SDH (GFP/HDLC) [39].

Para transporte dos quadros *RPR* sobre o *SDH* é necessário utilizar os formatos de enquadramento *Generic Framing Procedure (G.7041)* ou *HDLC-framing* [15].

O *GFP* permite a interoperabilidade entre diferentes equipamentos e permite diferentes tipos de protocolos como cliente [18]. Uma característica importante do *GFP* é permitir adaptar os containeres virtuais de acordo com as necessidades das tecnologias clientes. A Figura 5 – Exemplo de enquadramento *GFP*. *[23]* exemplifica o formato de enquadramento *GFP*.

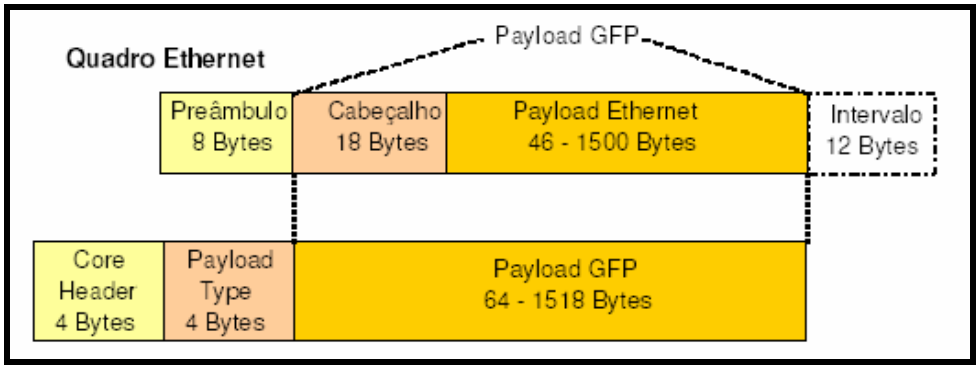


Figura 5 – Exemplo de enquadramento *GFP. [23]*

3.3.2. Cabeçalho *RPR*

O cabeçalho *RPR* possui sete campos, descritos a seguir [17]:

O *Destination Address* é o endereço do nó de destino do anel. Possui o comprimento de seis bytes;

O *Source Address* é o endereço do nó de origem do anel. Possui o comprimento de seis bytes;

O *Payload Type* identifica o tipo de protocolo que está sendo transmitido pelo *RPR*. Possui o comprimento de dois bytes;

O *Class of Service (CoS)* é o classificador utilizado para implementar *QoS* no anel. Possui o comprimento de três bits;

O *Extension Bit* (E) identifica extensão do cabeçalho *RPR.* Possui o comprimento de um bit;

O *Time to Live (TTL)* é análogo ao *TTL* do *MPLS* e *IP;*

O *Flow ID* é o campo que permite a inserção de rótulos, análogos aos do *MPLS*, e através da extensão do protocolo *RPR/RPT* é possível criar circuitos virtuais. Os circuitos

virtuais permitem uma baixa latência e banda garantida para um determinado fluxo. Este campo possui o comprimento de 20 bits de extensão, análogo ao rótulo *MPLS* [17].

Para se criar uma rede mista *MPLS/RPR*, pode-se utilizar dois procedimentos. O "*Label Stack*" que corresponde o empilhamento do rótulo *RPR* com o *MPLS* e o "*Label Swapping*" que é troca do rótulo *RPR* pelo rótulo *MPLS* nas mudanças para cada domínio *RPR* [34].

3.3.3. Processo de encaminhamento *RPR*

No padrão 802.17 os quadros que não pertencem ao nó são processados de forma diferenciada. Processamentos dos tipos: *Switching* e *Buffering*, não são realizados neste caso [15]. A simplicidade do processo decisório traz menor carga de processamento para os switches *RPR* e maior velocidade de comutação dos quadros. Essa característica traz vantagens para o desempenho da rede. A Figura 6 - Processo de encaminhamento *RPR*. [17] apresenta o encaminhamento *RPR*.

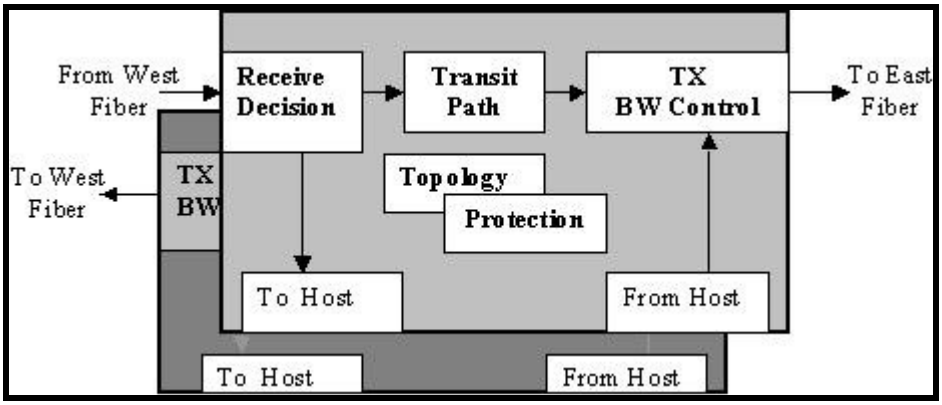


Figura 6 - Processo de encaminhamento *RPR*. [17]

As etapas de encaminhamento do *RPR* são [15]:

O *Receive Decision* é responsável pela análise do endereço *MAC* no *RPR*. Os quadros *Multicast* são copiados para o *host* e continuam a atravessar a rede através do *Transit Path*. Já os quadros *Unicast* fazem apenas uma das opções entre o direcionamento para *host* (parte interna da rede) ou reencaminhamento do quadro dentro do anel (*Transit Path*);

O *Transit Path* permite que os quadros continuem circulando no anel. No encaminhamento dos quadros, o *RPR* tem uma carga de processamento menor do que a do *Gigabit Ethernet*, porque o protocolo apenas inspeciona os itens: endereço, *TTL* e *CRC*, não realizando tarefas de "*switching*" e "*buffering*" como o *Ethernet*;

O *Transmit and Bandwidth Control* é o dispositivo responsável pelo controle de banda que permite a priorização de quadros e controle de banda baseados em mecanismos de escalonamento.

A própria topologia em anel, típica do protocolo *RPR*, favorece as transmissões *Multicast* e *Broadcast*. Já o protocolo *Ethernet*, tipicamente configurado com topologia em malha, requer diferentes formas replicações de quadros para alcançar diferentes destinos [15].

3.3.4. Aprovisionamento de Nós *RPR*

Em relação a simplicidade no aprovisionamento, pode-se fazer uma comparação com as redes *SDH*/*SONET*. Nas redes *SONET* os circuitos entre dois nós da rede devem ser configurados pelo operador nó a nó (configurar caminho manualmente). Já no *RPR*, o operador simplesmente necessita determinar a banda e requisitos de *QoS*, o controle *RPR*

reconhece o novo nó automaticamente através de um algoritmo de descobrimento de topologia ativado por evento e periodicamente [39].

O aprovisionamento automático do *RPR* é permitido através de uma facilidade do protocolo (algoritmo de descobrimento de topologia) que permite a inserção e remoção de um nó no anel sem a intervenção manual na gerência de rede. Após a inserção de um nó no anel, o novo nó emite uma mensagem de descobrimento que circula no anel requisitando o endereço *MAC* das estações associadas ao anel. A mensagem é repassada nó a nó pelo anel, e cada novo emissor insere seu endereço *MAC* de origem. Quando a mensagem retorna para o emissor, é possível conhecer toda a topologia da rede e os respectivos endereços *MAC* de cada nó da rede [39].

3.3.5. Classificação de quadros e Qualidade de Serviço

O protocolo *RPR* contém em seu cabeçalho um campo chamado *CoS (Class of Service)*, com três bits (análogo ao campo *EXP* do *MPLS*), que serve como classificador de prioridade. Através deste campo, é possível priorizar determinados quadros que trafegam pela rede, para que metas de qualidade sejam alcançadas. Alguns serviços disponibilizados pelas redes demandam critérios rígidos de qualidade, como, por exemplo, voz sobre *IP* e vídeo sobre *IP*, que necessitam de baixa latência, baixa variação do retardo e banda [34].

O *RPR* possui também um mecanismo para controle de banda para fazer o ajuste de determinados fluxos, como, por exemplo, os fluxos *TDM*. Um mecanismo comum encontrado nos equipamentos para este controle é o *WRED (Weighted Random Early Detection)* [40].

3.3.6. Recuperação de falhas

A recuperação de falhas no *RPR* ocorre em torno de 50ms (tempo igual ao SONET/SDH). Em relação ao tipo de recuperação, tem-se o *Wrapping* e *Steering* [40].

O *Wrapping* envolve só a estação que tem seu enlace comprometido, o tempo de convergência independe do tamanho do anel e é menor do que o *Steering*. Na Figura 7 – Exemplo de *Wrapping* e *Steering [43]*. é possível observar que o maior esforço de comutação fica a cargo do S3, que comuta o tráfego para o sentido inverso de transmissão utilizando outra fibra.

O *Steering* requer que todas as estações do anel recebam a informação de falha, para assim, desenhar um novo mapa de rede. O tempo de convergência do *Steering* é superior ao *Wrapping* e é proporcional ao tamanho do anel. O *Steering*, através da camada de controle *RPR*, redireciona o sentido do tráfego utilizando a mesma fibra.

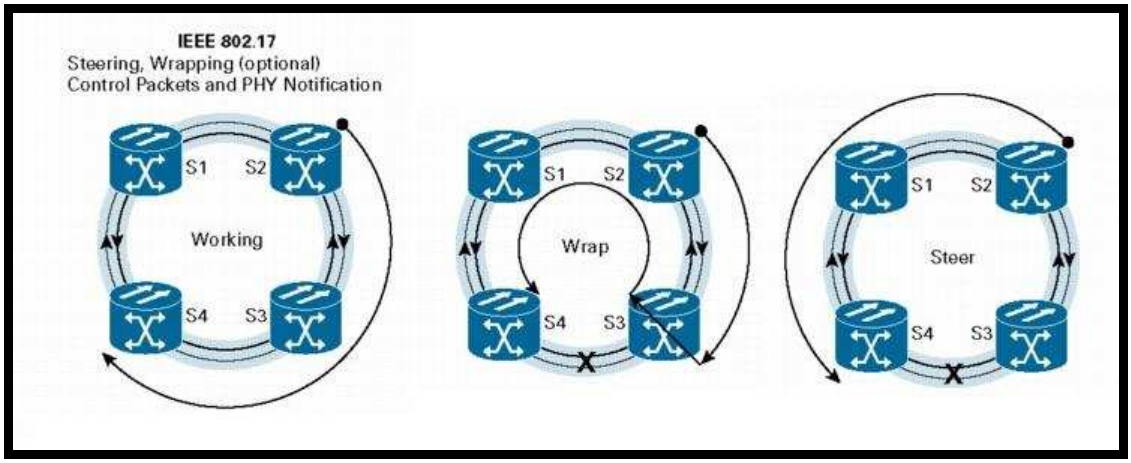


Figura 7 – Exemplo de *Wrapping* e *Steering [43]*.

3.3.7. Emulação de circuitos *TDM*

O *IEEE 802.17 Working Group* desenvolveu uma extensão do padrão IEEE 802.17, chamado de *Resilient Packet Transport (RPT),* que possibilita a emulação de circuitos *TDM* nas redes *RPR*. O *RPT* faz parte do padrão *IEEE 802.17 RPR Protocol* e é essencialmente uma adaptação do *RPR* para trabalhar com necessidades típicas dos provedores de serviços de telecomunicações. O *RPT* reserva recursos de banda nos switches *RPR* para alcançar as métricas restritas dos circuitos típicos *TDM* e os switches recebem referência de relógio externa para sincronização de tempo [17].

3.4. *Packet over Sonet* (*PoS*)

O *Packet over Sonet (PoS)* foi desenvolvido para permitir o transporte de pacotes *IP* em redes *SONET/SDH*. Esta tecnologia teve uma boa aceitação em provedores de serviços de telecomunicações, por permitir novos serviços de transmissão de dados e permanecer com a infra-estrutura já instalada para transmissão de serviços *TDM* (principalmente para transmissão de tronco de voz). Os padrões que suportam esta solução são: *RFC-1661 The Point-to-Point Protocol (PPP), RFC-1662 PPP in HDLC framing e RFC-2615 PPP over SONET/SDH* [39].

Este padrão tenta obter a confiabilidade do *SDH* e a flexibilidade do *IP*. Esses dois grandes pilares representam as principais vantagens deste padrão.

As principais vantagens do *SONET/SDH* são: tempo de resposta e largura de banda garantida; rápido esquema de restauração a falha; suporte a transmissões a longa distância para conexões *TDM* transmitidas de forma independente. As redes *SONET/SDH* provêem banda garantida em forma de circuitos com banda fixa. Como apresenta tempo de recuperação

a falha de 50ms [40], permite o funcionamento de aplicações com restrições rígidas de atraso e banda, como por exemplo, redes que suportam serviços telefônicos [39].

3.4.1. Restauração de falhas *SONET/SDH*

A topologia mais comum em redes *SONET/SDH* é a topologia em anel. A topologia em anel permite recuperação a falha em 50ms (milisegundos) e é necessário duplicidade de infra-estrutura (fibra e placa) para suportar a contingência [7]. A capacidade de tráfego no anel é configurada de forma que 50% da banda disponível é utilizada para transmissão e os outros 50% são reservados para proteção (linha de proteção). Este tipo de proteção não pode ser configurado em anéis compostos por segmentos de diferentes capacidades (VC-3, VC-4 e STS-12) [7], situação que pode ocorrer quando um arco do anel de capacidade menor é acoplado em um anel com capacidade maior.

As falhas não reparáveis pelo *SONET/SDH*, só são reparadas através da camada três. Os protocolos de roteamento permitem aos roteadores aprenderem sobre as mudanças topológicas sofridas pela rede. Estes propagam novas informações de rotas para os outros roteadores da rede, a fim de restabelecer uma nova topologia. Os protocolos de roteamento *Open Shortest Path First* (*OSPF*), *Integrated IS-IS*, e *Border Gateway Protocol* (*BGP*) são alguns exemplos de protocolos de roteamento existentes e que são responsáveis pelo restabelecimento da rede em caso de problema [40].

A seguir, na Figura 8 – Uso do protocolo de roteamento. [6], é ilustrado um exemplo de falha onde é necessário o uso do protocolo de roteamento para convergência da rede.

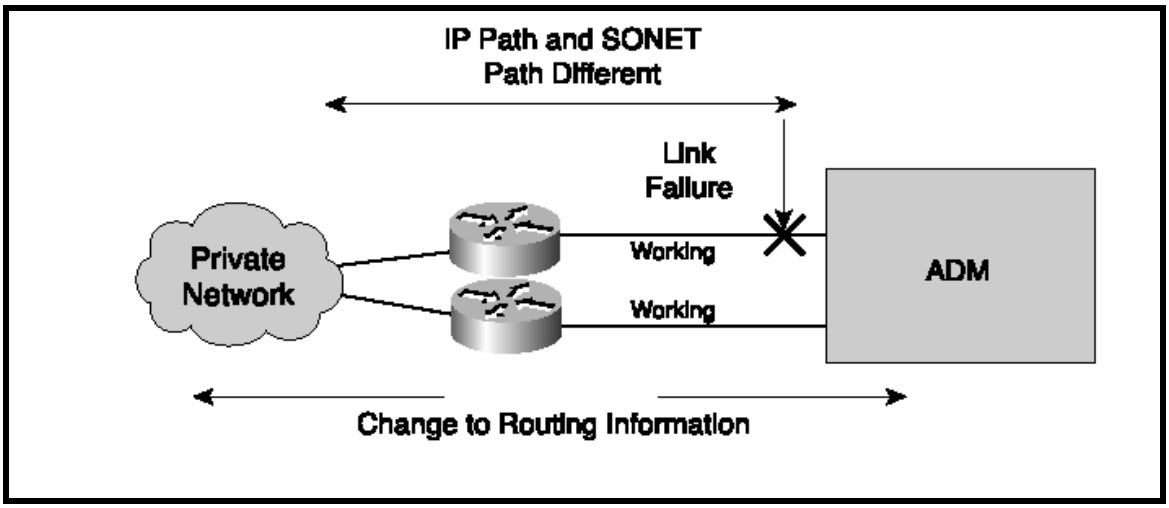


Figura 8 – Uso do protocolo de roteamento. [6]

3.4.2. Qualidade de serviço

O *Packet over Sonet (ou Ethernet over Sonet)* não implementa suporte ao *QoS* na camada dois do modelo *OSI*. Toda a atividade de *QoS* é realizada pelas camadas superiores. As redes típicas *PoS*, implementam *QoS* através do protocolo *IP*.

3.4.3. Encapsulamento do *PoS*

O padrão de encapsulamento do *PoS* determina que o datagrama *IP* deve ser encapsulado num quadro PPP (*Point-to-Point Protocol*) e posteriormente num quadro *HDLC-framing* (*High-level Data Link Control*). Na Figura 9 – Exemplo de encapsulamento *HDLC-Framing.* [6] é apresentado o formato do cabeçalho *PPP/HDLC-framing* padrão do *PoS*.

O *PPP/HDLC-framing* é um padrão de enquadramento usado pelo *PoS* e pode transportar diferentes tipos de protocolos. O protocolo *PPP* possui um campo que informa qual protocolo está sendo transportado [35].

A combinação *PPP/HDLC* permite a utilização de um protocolo orientado a caracteres (*PPP)* e um protocolo orientado a bit (*HDLC*). O *PPP* permite a definição do protocolo transportado através do campo protocolo e no *HDLC* o campo de verificação é utilizado (mais robusto do que o *PPP*). O *HDLC* inclui endereço, controle, e campo de protocolo, no seu processo de enquadramento [34] [35].

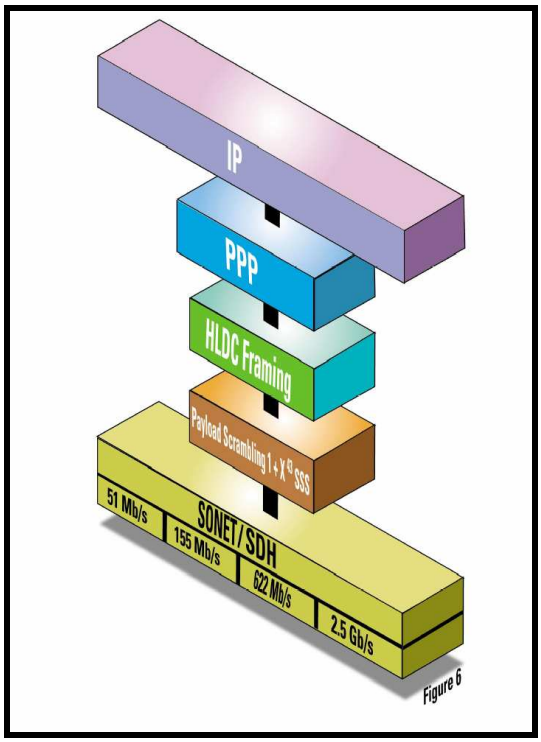


Figura 9 – Exemplo de encapsulamento *HDLC-Framing.* [6]

3.5. *Ethernet over Sonet*

O *Ethernet over Sonet* é uma tecnologia que aproveita a infra-estrutura *SDH* existente para o transporte de quadros *Ethernet*. A *Ethernet* beneficia-se das vantagens do *SDH* no transporte de seus quadros. As principais vantagens são: resiliência e restauração a falhas em 50ms em caso de queda do enlace e baixa latência (circuito dedicado) [10].

O *EoS* oferece as mesmas facilidades do *PoS*, só que o quadro transportado é o *Ethernet*, e não *IP*. São utilizados neste caso os padrões *GFP – Generic Framing Procedure (G.7041), VCAT– Virtual Concatenation (G.707), LCAS – Link Capacity Adjustment Scheme (G.7042) e VLAN – Virtual Local Area Network (802.1Q).* Uma das principais diferenças entre os padrões é o enquadramento (*PoS* utiliza o *PPP/HDLC* e *EoS* utiliza o *GFP*) [10].

O *GFP* apresenta vantagens sobre o enquadramento *PPP/HDLC*. Primeiramente é a quantidade de tipos de protocolos que podem ser suportados por este tipo de enquadramento. O campo tipo de protocolo possui quatro bytes, enquanto que o *PPP/HDLC* tem apenas dois *bytes*.

Outra vantagem é que o *GFP* permite dois tipos de enquadramento: transparente e baseado em quadro. O transparente coloca todo quadro de outro protocolo no *payload* de transporte (ideal para quadro de protocolos proprietários ou protocolos de uso diferenciado). O modo baseado em quadro permite otimização do protocolo (um exemplo é o enquadramento *Ethernet*: o *GFP* extrai os bits de preâmbulo). O *PPP/HDLC* funciona numa configuração similar ao modo transparente apenas, não oferece assim um grau de flexibilidade igual ao *GFP* [18].

O *VCAT* permite a criação de enlaces agregados que possibilita uma alocação de banda mais eficiente, pois evita o desperdício de banda. Um exemplo é uma ligação de 10Mbps numa infra-estrutura *SONET/SDH*. Sem o *VCAT* é necessário utilizar um VC3 (48Mbps), enquanto que com o uso do enlace virtual é possível obter uma concatenação 5xVC12 (VC-12 é uma ligação de 2Mbps). A utilização do *VCAT* traz benefícios para o desempenho das conexões *SDHs* [10].

O *LCAS* permite o gerenciamento dinâmico da utilização de banda nos enlaces agregados. Com este protocolo é possível aumentar ou diminuir largura de banda sem afetar o tráfego. O protocolo permite também proteção do tráfego, transmitindo os quadros por diferentes conexões. Sua utilização é facilmente compreendida através da seguinte ilustração: na hipótese de haver a queda de um dos VC-12 num container virtual 5xVC-12, quem gerenciará o roteamento dos quadros que eram encaminhados pelo enlace defeituoso? A resposta é o protocolo *LCAS* [10].

3.6. Comparação entre os protocolos

3.6.1. *Gigabit Ethernet*

As interfaces do *Gigabit Ethernet* oferecem um custo inferior ao *RPR* sendo esta a principal vantagem do *Gigabit Ethernet* sobre o *RPR*. O *GE* permite ainda diferentes arranjos de topologia física enquanto o *RPR* permite apenas topologias em anel [15].

Em relação ao *Packet over Sonet*, o *Gigabit Ethernet* oferece custo inferior de instalação, maior facilidade de operação e permite interconexões com outros protocolos [40].

São desvantagens do GE: não garante serviços baseados em circuitos virtuais TDM (como PABX de voz) e não possui engenharia de tráfego para prover um maior balanceamento de cargas nos enlaces utilizados [40].

3.6.2. *Resilient Packet Ring*

As vantagens do *RPR* sobre o *PoS* são: simplicidade no aprovisionamento de circuitos e qualidade de serviço, maior facilidade na operação da rede e permissão do funcionamento em diferentes tipos de infra-estruturas de rede física [40].

Em relação ao *Gigabit Ethernet*, o *RPR* oferece: restauração a falha mais rapidamente (o *GE* depende do *Spanning Tree Protocol*), menor carga de processamento no encaminhamento de quadros, funcionamento em diferentes tipos de padrões de tecnologias da camada física e maior facilidade em transmissões *Multicast e Broadcast* [34].

3.6.3. *Packet over Sonet e Ethernet over Sonet*

O *PoS* em relação ao *GE* e *RPR*, permite manutenção de serviços típicos *TDM* com maior confiabilidade. O *RPR* depende da extensão *RPT* para manutenção destes serviços e o *Gigabit Ethernet* não oferece suporte.

Mesmo não sendo recomendado, o *PoS* permite a criação de redes físicas com topologia anel e malha. O *RPR* funciona apenas em topologia anel.

O *PoS* oferece uma velocidade de restauração, em caso de falha no enlace, em torno de 50ms. O *GE* depende do protocolo *Spanning Tree Protocol* para restaurar a falha e o tempo de convergência é em torno de 30 segundos [40].

Os protocolos *Packet over Sonet* e o *Ethernet over Sonet* apresentam características de funcionamento similares. A principal diferença entre o *Packet over Sonet* e o *Ethernet over Sonet* é a flexibilidade no transporte de protocolos de camadas superiores. Neste aspecto o

protocolo *EoS* oferece vantagens sobre o *PoS*. Como o protocolo *Ethernet* é um protocolo de camada dois do modelo *OSI*, pode transportar diferentes tipos de protocolos de camada três (*IP, IPX, Appletalk e MPLS*), enquanto que o *PoS* permite apenas o transporte de pacotes *IP*.

3.6.4. Comparativo entre os protocolos

Os padrões *RPR, PoS e GE* são soluções de camada dois utilizadas *em WAN*. Todos estes apresentam vantagens e desvantagens. Para efeitos comparativos, foi criada uma tabela com seis itens analisados. Os itens são: recuperação a falhas, desempenho da transmissão de dados, QoS, custo, serviços TDM e Interconexões.

A recuperação a falha corresponde a habilidade da rede em voltar a transmitir informações após a ocorrência de uma falha. A pontuação máxima (melhor opção) é o número 3 e a pontuação mínima é 1. A capacidade de recuperar as falhas num intervalo de tempo pequeno é uma característica importante para as redes. O suporte a sistemas em tempo real nas redes atuais traz consigo requisitos restritos de disponibilidade de serviço.

O desempenho de transmissão é a capacidade de transportar volume de dados (*throughput*). Quanto maior a capacidade de transporte, maior será a pontuação. Pontuação máxima é 3 e mínima 1.

O item *QoS* é o suporte a esta facilidade e sua eficiência. A pontuação maior será aplicada para o protocolo que melhor funcione com o *QoS*. Pontuação máxima é 3 e mínima 1.

O custo corresponde ao preço médio para aquisição desta tecnologia. Neste caso quanto menor o preço, maior será a pontuação. O menor preço receberá pontuação 3 e o maior preço receberá pontuação 1.

O serviço *TDM* é a capacidade de oferecer serviços tipicamente providos por redes *SDH* (*Synchronous Digital Hierarchy*) e redes *PDH* (*Plesyochronous Digital Hierarchy*). Um exemplo destes serviços é a transmissão de canais de voz, vídeo e sinais de automação com requisitos máximos de latência e variação a retardo. Nesta avaliação a pontuação máxima é obtida em virtude da capacidade de prover estes serviços.

A opção interconexão representa o grau de interoperabilidade e compatibilidade entre diversas tecnologias de rede. A facilidade de interconexão do protocolo recebe a pontuação máxima. A Tabela 1- Quadro Comparativo de tecnologias de *WAN*. apresenta uma síntese da comparação entre os protocolos.

Quesitos	*RPR*	*PoS/EoS*	*GE*
Recuperação a falhas	**3**	**2**	**2**
Desempenho na transmissão de dados	**2**	**1**	**3**
QoS	**3**	**1**	**2**
Custo	**1**	**2**	**3**
Serviços *TDM*	**2**	**3**	**1**
Interconexões	**3**	**1**	**3**
Total	**14**	**10**	**14**

Tabela 1- Quadro Comparativo de tecnologias de *WAN*.

O protocolo *RPR* apresenta a maior pontuação no item recuperação a falha. Além de apresentar um tempo de recuperação baixo (em torno de 50ms), este protocolo apresenta uma maior robustez à falha se comparado com *PoS*. O *RPR* apresenta uma inovação, chamada de

Steering Mode, que permite uma sincronização entre as estações para negociação e ajuste de banda após uma ocorrência de falha. Esta facilidade permite uma falha dupla e uma falha única num anel, sem comprometimento da transmissão de dados [40].

O *GE* apresenta uma melhor pontuação no item desempenho de transmissão. Basicamente devido ao menor *overhead* e suporte a redes em malhas.

A *QoS* é melhor suportada pelo *RPR* do que os demais. O *RPR* permite o mecanismo *priority queuing* (utilizado no GE) e permite o controle de banda através do módulo chamado *Transmit and Bandwidth Control*. Este módulo possui ferramentas de controle de escalonamento e descartes (um exemplo de ferramenta utilizado por equipamentos *RPR* é o *WRED*) [40].

Em relação ao custo, a melhor opção foi o *GE*. Seu custo menor é oriundo da economia de escala. A família de tecnologia *Ethernet* possui uma aceitação universal em redes locais e é praticamente um padrão sem concorrente no contexto *LAN*.

A tecnologia *PoS* recebeu a maior pontuação no item serviço *TDM*. Para obter circuitos dedicados basta configurar canais dentro da estrutura *SDH* para determinados tráfegos. Para canais de baixa velocidade, os equipamentos *SDH* oferecem interfaces de acoplamento para estes canais nos Multiplexadores *SDH*. O *SDH* permite a criação de circuitos dedicados que obedecem criteriosamente restrições de banda, atraso e variação de atraso.

Na opção interconexão a menor pontuação foi do *PoS/ EoS*. Essas tecnologias como próprio nome já indica (pacote e Ethernet), especifica a tecnologia que é transportada. No caso do *PoS* trata-se do transporte de pacotes *IP* (pacote é nome típico da estrutura de transmissão do *Internet Protocol*) e o *EoS* é o quadro *Ethernet*. As tecnologias *RPR* e *Gigabit Ethernet* permitem o transporte de outros protocolos na sua camada superior. Ambas as tecnologias possui um item que indica no cabeçalho o protocolo transportado na camada superior.

O *RPR* é uma solução adequada para redes típicas em anéis, um exemplo são as redes de TV a cabo. O *RPR* diminui a complexidade na operação das redes, na implementação de *QoS*, na recuperação de falha e balanceamento de tráfego. Em contrapartida apresenta um custo alto de adoção, sendo superior aos demais, e permite apenas a topologia em anel [40].

O *PoS* é ideal para redes de serviços legados *TDM*. Pode manter os antigos serviços *TDM* e ativar novos serviços de transmissão de dados com mais facilidade. Suas desvantagens são: dificuldade na implementação de *QoS*, na operação da rede e principalmente na recuperação de falhas não resolvidas pela camada física *SDH* [40].

O *GE* apresenta um menor preço de adoção, facilidade na operação e utilização de banda superior ao demais. Sua principal desvantagem é falta de suporte a emulação de circuitos virtuais, para aprovisionamento de serviços típicos *TDM*. Sendo uma rede ideal para transmissão de dados [40].

A conclusão final aponta os protocolos *RPR* e o *Gigabit Ethernet* como as melhores opções. Entretanto, é importante ressaltar a larga adoção do GE. Esta característica permite melhores condições de preço, continuidade tecnologia, facilidade de instalação e operação.

3.7. *MPLS*

O *MPLS* é um mecanismo avançado de encaminhamento de pacotes que suporta qualidade de serviço. Um roteador que suporta *MPLS* também é chamado de "*Label Switching Router*" (*LSR*). Um caminho *MPLS* é chamado de "*Label Switching Path*" (*LSP*) [29]. No *MPLS* são inseridos rótulos nos pacotes por roteadores (*LSR*) no seu ingresso em um domínio *MPLS*. Esses rótulos são usados para encaminhamento de pacotes nos *LSPs MPLS* da rede. Todo pacote pode ser dividido dentro de subgrupos também chamados de *FEC* ("*Forward Equivalence Class"*). A idéia é de que os pacotes que pertençam aos mesmos subgrupos respeitem os mesmos critérios de encaminhamento. A classificação de pacotes em *FECs* é feita usando filtrador de pacotes que examina os campos do cabeçalho que contém endereço de origem, endereço de destino e número de porta [31].

No *MPLS* os *LSPs* explícitos podem ser usados para configurar diferentes redes lógicas sobre uma mesma rede física. Estes *LSPs* podem ser considerados conexões virtuais que carregam fluxos agregados pela *FECs* em *LSR MPLS* da rede [44].

O rótulo utilizado no *MPLS* é de tamanho fixo e é utilizado como índice na tabela de encaminhamento [27]. Ele é agregado ao pacote *IP* na entrada de uma topologia *MPLS* e é retirado na saída. A Figura 10 - Rótulo *MPLS. [30]* ilustra o formato do cabeçalho *MPLS.*

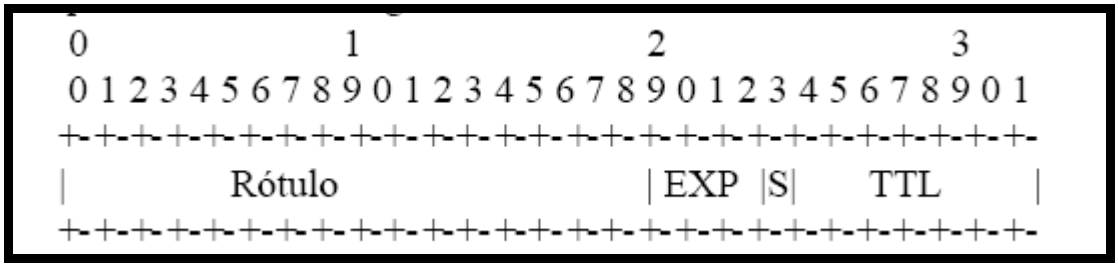


Figura 10 - Rótulo *MPLS. [30]*

O campo *CoS* (*Class of Service*) é experimental e tem sido utilizado para classificar os pacotes em classes de qualidade de serviços. O campo *stack* indica se existe ou não empilhamento. O campo *TTL* (*Time to Live*) tem a mesma função que no pacote *IP* convencional e existe para manter a compatibilidade com ferramentas de diagnóstico de rede e para detectar loops [9].

O *LSR* (*Label Switching Router*) é um dispositivo que faz o encaminhamento dos pacotes dentro do domínio *MPLS* baseado no rótulo agregado. Em cada *LSR* a tabela de encaminhamento é consultada e o rótulo é alterado para um novo valor. O protocolo *LDP* (*Label Distribution Protocol*) é responsável pela troca de informações de rótulos e manter atualizadas as tabelas de encaminhamento dos *LSRs* em toda rede [31].

O *LER* (*Label Edge Routers*) é um *LSR* que se encontra na borda da rede, ou seja, na entrada ou na saída da mesma. Na entrada da rede, este dispositivo, além das funções normais de um LSR, é responsável por agregar um rótulo ao pacote e atribuir este pacote a uma *FEC*. Quando na saída, deve retirar o rótulo que foi agregado ao pacote para que o mesmo possa ser encaminhado pela rede *IP* convencional [31].

3.7.1. Engenharia de Tráfego

A engenharia de tráfego está relacionada com a otimização do desempenho operacional das redes. O maior objetivo da engenharia de tráfego é a facilidade operacional e reconfiguração da rede, enquanto simultaneamente, são otimizados recursos e desempenho. Esta facilidade tem se tornado uma indispensável funcionalidade devido ao alto custo das redes e competição natural da Internet [4].

A chave do desempenho associado com a engenharia de tráfego pode ser modelada em visão orientada a tráfego e visão orientada a recurso.

Os objetivos do modelo orientado a tráfego incluem aspectos que permitem o uso de qualidade de serviço em tráfego menos “prestigiado”. Questões como: diminuir perda de pacote, diminuição do atraso, aumento do *throughput* e obediência a níveis de serviços, são metas deste modelo.

Os objetivos do modelo orientado a recursos incluem aspectos pertencentes a otimização dos recursos utilizados pela rede. A eficiente gestão dos recursos da rede é um meio de se obter os objetivos de desempenho almejados. Em particular, deseja-se que os recursos sejam manipulados de maneira a evitar congestionamento (over) ou subutilizados (under) [4]. Diminuir o congestionamento da rede é o objetivo primordial tanto do modelo orientado a tráfego como orientado a recursos.

O interesse principal de qualquer um dos dois modelos é evitar os congestionamentos prolongados, mais importantes de serem tratados do que os congestionamentos transientes oriundos de rajadas. Os congestionamentos tipicamente se manifestam sobre dois cenários: quando os recursos da rede são insuficientes ou inadequados para acomodar a carga de tráfego

e quando os fluxos de tráfego são ineficientes mapeados entre os recursos disponíveis, causando assim em alguns casos “over-utilized” enquanto que em outros “under-utilized” [4].

O primeiro tipo de problema de congestionamento pode ser resolvido por expansão de capacidade da rede ou técnicas de controle de congestionamento. O controle de congestionamento clássico está voltado para adequar a demanda de tráfego dentro das disponibilidades de recursos. Técnicas clássicas de controle de congestionamento incluem: limitação de taxa, janela de controle de fluxo, gerência de filas dos roteadores e outros [4].

O segundo tipo de problema de congestionamento, oriundo de alocação ineficiente de recursos, pode ser usualmente resolvido através da engenharia de tráfego. Em geral, congestionamentos resultantes de alocação ineficiente de recursos podem ser resolvidos pela adoção de políticas de balanceamento de carga. O objetivo desta estratégia é diminuir ao máximo o congestionamento ou diminuir ao máximo a utilização dos recursos, dentro de uma alocação de recursos eficientes. Quando os congestionamentos são minimizados por uma alocação de recursos eficientes; pacotes perdidos diminuem, atrasos diminuem e “throughput” aumenta. Em suma, a percepção da qualidade de serviço é amplificada para o usuário [4].

É clara a importância do balanceamento de carga nas otimizações de desempenho das redes. Entretanto, as características funcionais da engenharia de tráfego devem ser flexíveis o suficiente para que os administradores de rede possam implementar outras políticas, como tarifação e aprovisionamento.

As ferramentas de controle oferecidas pelos protocolos *IGPs* (*Interior Gateway Protocol*) não são adequadas para engenharia de tráfego [14]. Isso torna difícil promover

políticas efetivas para melhoramento do desempenho baseadas em roteamento de rede, inclusive *IGPs* baseados em "*Shortest Path Algorithms*", que contribuem significativamente para congestionar numa rede. O algoritmo do tipo *SPF* geralmente é baseado em simples métricas aditivas. Deste modo, parâmetros como disponibilidade de banda e característica de tráfego não são fatores considerados nas decisões de roteamento. Conseqüentemente, congestionamentos ocorrem com freqüência quando: múltiplos fluxos convergem para determinados enlaces ou fluxos roteados para um enlace que não tem banda suficiente para acomodá-lo [27].

O *MPLS* oferece possibilidade de automatizar aspectos funcionais da engenharia de tráfego. Os atrativos do *MPLS* para engenharia de tráfego podem ser atribuídos aos seguintes fatores: [4]

- Os caminhos explícitos *MPLS* podem ser facilmente implementados por ação manual ou ação automática (através de protocolo);
- Os caminhos podem ser potencialmente eficientes em restauração a falhas na rede;
- Características de tráfego podem ser associadas à LSPs;
- Associação de recursos a determinados LSPs e fluxos de tráfego;
- O *MPLS* permite agregação de fluxos;
- Utilização de roteamento com restrição de recursos.

A engenharia de tráfego apresenta três itens que são críticos no seu funcionamento e apresentam um alto grau de complexidade na sua implementação. Estes itens são: (1) como mapear pacotes dentro de uma *FEC*, (2) como mapear *FEC* dentro de fluxos de tráfego e (3) como mapear fluxo de tráfego dentro de topologias de redes físicas através de *LSPs*. O *Framework Constraint-Routed* (*CR*) é utilizado para selecionar caminhos para os fluxos de

tráfego adequados, obedecendo as restrições impostas pelas configurações de comportamento de tráfego [4]. O *CR* não faz parte do *MPLS*, mas ambos precisam ser usados em conjunto para se alcançar o desempenho esperado na engenharia de tráfego.

Os protocolos *CR-LDP* (*constraint-routed LDP*) e *RSVP-TE* (Resource *ReSerVation Protocol with Traffic Engineering*) determinam os caminhos através da rede, ambos verificam restrições e utilizam protocolos de roteamento [3]. O protocolo de roteamento (IGP) é importante para determinar a topologia da rede e alcançabilidade de cada nó. As configurações de restrições permitem que os *LSPs* sejam estabelecidos com os requisitos pré-estabelecidos, tais como largura de banda e atraso [19].

Depois, os roteadores (*LSRs*) trocam informações de rótulo através do protocolo *LDP*. A troca de informações pode ser: conservadora ou liberal. A troca conservadora é aquela que ocorre ao longo de uma rota pré-definida, ou *LSP*. Já a troca liberal permite que roteadores, mesmo não envolvidos na rota, recebam informações de rótulo [31]. A troca conservadora permite a construção de tabelas de encaminhamento menores, conseqüentemente menor processamento no encaminhamento de pacotes. A troca liberal permite uma convergência mais dinâmica, em virtude de outros roteadores possuírem um conhecimento da rede [4]. O *RSVP* informa o rótulo também, mas apenas para os *LSRs* envolvidos no caminho. No quesito troca de informações de label, o *RSVP* possui menos recursos do que o *LDP*. Algumas implementações mesmo usando o *RSVP-TE* para reserva de recurso em *LSPs*, utilizam o *LDP* para a troca de informações de rótulo [27].

No ingresso da rede, o *LSR* associa um rótulo para os pacotes quando os mesmos entram na rede [2]. A associação de rótulo baseia-se no grupo *FEC*. O *MPLS* permite a

associação de vários fluxos a uma mesma *FEC.* A *FEC* contém as informações de requisitos por *LSP* [4].

A Figura 11 – Exemplo de funcionamento da Engenharia de Tráfego. [5] apresenta um exemplo de engenharia de tráfego do *MPLS*. O *LSP* 1 foi criado num caminho de menor custo *OSPF*, já o segundo utiliza o outro percurso. Nas restrições configuradas para o *LSP* 2, foi inviável o mesmo utilizar o percurso do *LSP* 1 [5].

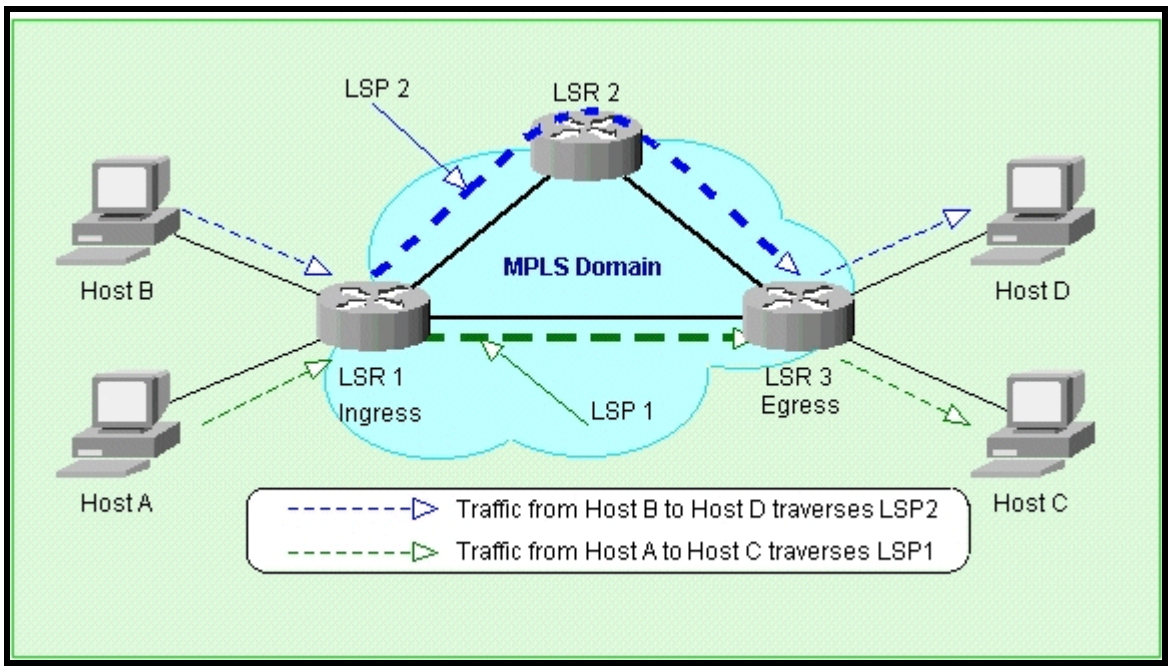


Figura 11 – Exemplo de funcionamento da Engenharia de Tráfego. [5]

3.7.2. *Resource Reservation Protocol - Traffic Engineering (RSVP-TE)*

O *RSVP-TE* oferece a possibilidade de mover os fluxos para diferentes caminhos, além dos "caminhos mais curtos" escolhidos pelos protocolos de roteamento IGP. Esta manobra permite uma melhor distribuição do tráfego e um uso mais eficiente dos recursos da rede [4].

As falhas na rede, de uma maneira geral, podem ser restauradas por *Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Open Shortest Path First (OSPF)* e *Intermediate System-to-Intermediate System (IS-IS)* [15]. No entanto, esses protocolos não garantem que os novos caminhos escolhidos (pós-falha), mantenham o mesmo *SLA* do caminho anterior. Já o *RSVP-TE* pode solucionar este problema [32].

Resumidamente, podem-se sintetizar algumas facilidades do *RSVP-TE*: [15]

● Habilidade de manter o *SLA* em novos caminhos em caso de falha na rede;

● Permite a obtenção de uma maior eficiência do uso dos recursos da rede, a fim de alcançar e manter o *SLA* contratado;

● Capacidade de restaurar a comunicação da rede, após a ocorrência de uma falha, dentro de um tempo aceito pelo *SLA* contratado.

Originalmente, o *RSVP* foi desenhado para ser um protocolo de sinalização para reserva de recurso (definido pela *RFC 2205 – Resource ReServation Protocol/Version I*)[45]. Posteriormente, o RSVP foi estendido para dar suporte a engenharia de tráfego, assim se chamando de *RSVP-TE*. O *RSVP-TE* apresenta as seguintes facilidades: [15]

● Estabelecimento de caminho de envio – O *RSVP* pode ser usado para estabelecer um *LSP* através da troca de informações de rótulo. Função análoga ao do *Label Distribution Protocol (LDP)*;

● Estabelecimento de caminho explícito – O *RSVP-TE* é usado para estabelecer um *LSP* ao longo de uma rota explícita criada respeitando restrições especificadas. Este *LSP* pode ser criado novamente usando outros *LSRs* em caso de falha;

● Reserva de recurso – O *RSVP-TE* reserva recursos da rede para um determinado fluxo de transporte.

Para estabelecer um túnel *LSP*, o *LSR* de ingresso envia uma mensagem de caminho (“*Path Message*”) até o *LSR* de egresso, que responderá posteriormente com mensagem de reserva (“*Reservation Message-RESV*”). Após completar este “acordo”, o *LSP* está criado. A mensagem de caminho (*path*) indica o caminho através do qual o *LSP* deve passar e a mensagem de reserva (*RESV*) estabelece caminho e reserva a banda para o *LSP* [32].

3.7.3. *Fast Reroute Protocol*

Um dos requisitos para engenharia de tráfego é a capacidade de “re-rotear” *LSPs* estabelecidos. O *Fast Reroute* inclui [33]: seleção de critérios administrativos que permitam o “re-roteamento” de LSP, quando, por exemplo, os requisitos de *QoS* não forem atendidos; o “re-roteamento” em caso de falha de algum dos recursos do *LSP* e permite retornar para o *LSP* original após o reparo da falha.

No caso de falha na rede, o túnel backup, já deve estar pré-definido. A operação da rede não pode, ou não deve, ser interrompida enquanto o “re-roteamento” estiver em curso. Esta concepção é chamada de “*make-before-break*” [33].

O *RSVP-TE* é um protocolo que permite o funcionamento do “*make-before-break*”. O *RSVP* utiliza sua capacidade de reserva para prevenir que recursos do caminho backup sejam preservados, mesmo sem utilização [27].

O intervalo de tempo do “re-roteamento” a falhas de *LSPs* é crucial para manutenção da *SLA* contratado, principalmente para aplicações em tempo real. O *MPLS* usando o *Fast Reroute* permite a convergência em apenas 50 milisegundos [15].

O *RSVP-TE (Fast Reroute)* permite dois métodos de estabelecer caminhos de contingência, são eles: reparo fim a fim e reparo local [15].

O reparo fim a fim de *LSPs* consiste num método em que todo o caminho é substituído. No caso de falha em um caminho, um novo caminho fim a fim é estabelecido [15].

O reparo local de *LSPs* permite o reparo de apenas uma parte do caminho, não sendo necessário estabelecer um novo caminho fim a fim. Essa solução traz um menor tempo de convergência, ideal para aplicações em tempo real.

Uma outra solução é "*Facility Backup*". Ao invés da falha acionar uma nova configuração *LSP*, esta solução cria um único *LSP backup* que servirá para todos (ou uma parte) os *LSP* operacionais. Antes da falha, o *LSP* já está criado e pronto para trabalhar. Esta solução tende a ter um tempo de convergência menor [27].

3.7.4. Qualidade de Serviços no *MPLS*

As características de *QoS* do *MPLS* representam a capacidade de prover níveis diferenciados de serviços e garantia de recursos da rede. Esta capacidade tipicamente inclui uma seleção de técnicas necessárias para gerenciar banda, atraso, variação de atraso e perdas de pacotes da rede **[28]**. Por exemplo, a habilidade de marcar pacotes com certa prioridade, combinada com gerência de *buffer* e esquema de filas, garantem a qualidade de serviço necessária para os diferentes perfis de tráfego da rede. A voz, por exemplo, tem fortes restrições de atraso e variação de atraso na sua transmissão **[5].**

Em redes *MPLS*, quando o pacote chega ao *LSR*, o rótulo *MPLS* é usado para determinar a interface de saída e o pacote recebe um novo rótulo. Entretanto, o cabeçalho *MPLS* possui um campo chamado de *EXP* (*experimented bit*), também chamado de *CoS* (*Class of Service*), e seu valor é usado para determinar o tipo de tratamento (*queueing e scheduling*) do pacote na rede[20]. Este campo não é alterado em cada salto. Na Figura 12 – Campo EXP no cabeçalho *MPLS.* [11] é mostrado o campo *EXP* e este possui apenas três *bits*, permitindo assim um máximo de oito classes [5].

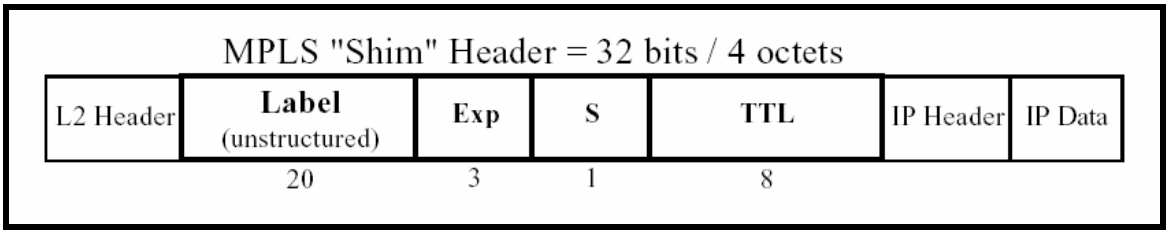


Figura 12 – Campo EXP no cabeçalho *MPLS*. [11]

Através deste campo pode-se promover o modelo de qualidade de serviço *Diffserv* dentro da nuvem *MPLS*. A vantagem do *Diffserv* é ser um modelo "escalavél" [5].

No *QoS MPLS* existem duas diferentes maneiras de marcar o tráfego para controle do *QoS*. Isto significa que quando um tráfego *IP* entra num *LSP*, os *bits CoS* no cabeçalho *MPLS* podem ser tratados de duas maneiras [5]:

Na primeira maneira, chamada de "*Experimental Bit Inferred Label Switched Path (E-LSP)*", informações de fila são codificadas dentro do campo experimental (EXP) do cabeçalho *MPLS* [5]. Uma vez que o campo *EXP* permite oito diferentes marcações *CoS*, esta informação é usada como valor de classe de serviço. Assim, diferentes pacotes podem ser recebidos com diferentes marcações dependendo dos seus requisitos, podendo, desta maneira, receber diferentes tratamentos ao longo do caminho [20].

Na segunda, também chamada de "*Label Inferred Label Switched Path (L-LSP*)", a associação do rótulo com pacotes *MPLS* especifica como um pacote deve ser tratado dentro da nuvem *MPLS*. A classe de serviço é mapeada através da *FEC*. Em outras palavras, este método respeita a *FEC* e o campo EXP não é utilizado [5]**.**

3.8. Benefícios do *MPLS* nas redes *RPR, PoS, EoS e GE*

3.8.1. Benefícios do *MPLS* para o *RPR*

O *MPLS* traz benefícios e agrega valor aos protocolos de nível dois do modelo *OSI* (*RPR, Packet over Sonet, Ethernet over Sonet e Gigabit Ethernet*). Em relação ao RPR podem-se destacar os seguintes benefícios [40]:

● Permite a conexão de diferentes áreas *RPR* através de uma rede única *MPLS*;

● Conexão de redes *RPR* com diferentes tipos de rede de camada dois modelo *OSI;*

● Total separação do plano de controle do plano de dados (favorecendo assim o desenvolvimento de melhorias para a rede);

● Criação de *VPNs MPLS*;

● Aumenta a escalabilidade dos endereços de rede e criação de uma hierarquia na rede.

Na Figura 13 - Facilidades adicionais *MPLS e RPR*. [42] é apresentado um resumo ilustrativo das facilidades *MPLS* e *RPR*.

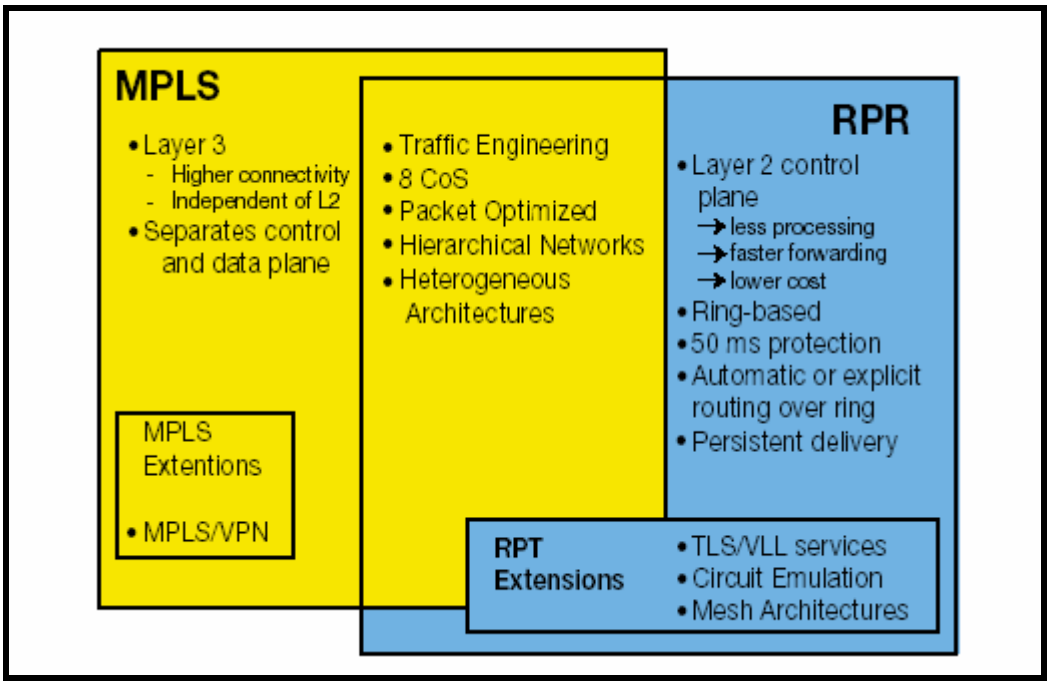


Figura 13 - Facilidades adicionais *MPLS e RPR*. [42]

O *RPR* permite dois tipos de implementações do MPLS: *label stack* ou *label swapping* [40].

O *Label Stack* é o modelo que utiliza o empilhamento de rótulos. A vantagem do empilhamento (*stack*) é que a operação das redes *MPLS* e *RPR* fica transparente e mantém bem claro a delimitação de funcionamento de cada uma, trazendo uma menor complexidade na operação das redes. A desvantagem é o aumento de overhead que, conseqüentemente, diminui a banda útil de transmissão.

O *Label Swapping* é o modelo que realiza troca de rótulo. A vantagem é a diminuição do *overhead* e o melhor aproveitamento da banda. A desvantagem é o aumento de processamento e memória na troca de cabeçalho e uma maior complexidade de operação.

3.8.2. Benefícios do *MPLS* para o *POS e EoS*

O *MPLS* pode ser utilizado pelo *PoS e EoS*. Essa implementação permite às redes disponibilizarem várias facilidades do *MPLS*, tais como [15]:

- Permite a conexão com redes que utilizam diferentes tecnologias de camada dois;
- Suporte a engenharia de tráfego;
- Qualidade de serviço;
- Viabilizar a total separação do plano de controle do plano de dados. Favorecendo assim o desenvolvimento de melhorias para o protocolo;
- Recuperação de falha usando mecanismos do próprio *MPLS;*

● Criação de uma hierarquia na rede.

Um exemplo de funcionamento do *MPLS over Sonet* está na Figura 14 – Empacotamento *MPLS* em redes *EoS. [7]*. O rótulo *MPLS* será empacotado dentro do *payload* do *PPP /HDLC* e no destino é desempacotado. Através da análise do rótulo *MPLS* é possível obter informações de *LSP* e *QoS*.

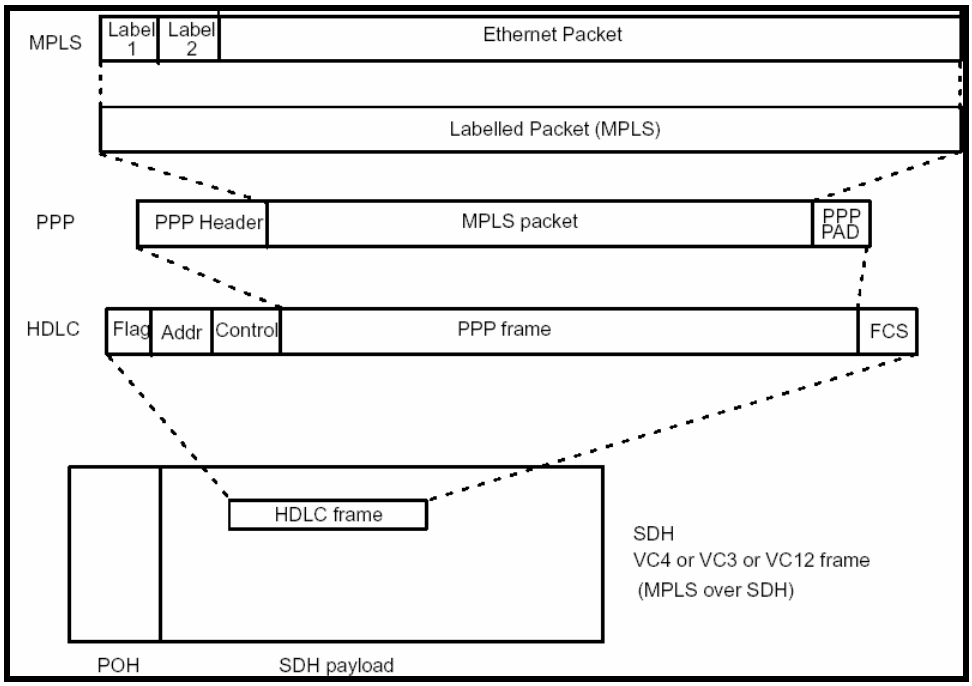


Figura 14 – Empacotamento *MPLS* em redes *EoS. [7]*

3.8.3. Benefícios do *MPLS* para o *GE*

Como no *PoS* e *RPR*, o *MPLS* pode ser uma importante ferramenta para convergência e aumento das facilidades da rede *GE*. O *MPLS* pode implementar engenharia de tráfego, permitindo assim uma melhor utilização dos enlaces da rede. Os provedores de serviços de telecomunicações podem implementar redes *MPLS* para configurar rotas explícitas nos seus *backbones* para atender determinados requisitos de caminho e banda [39].

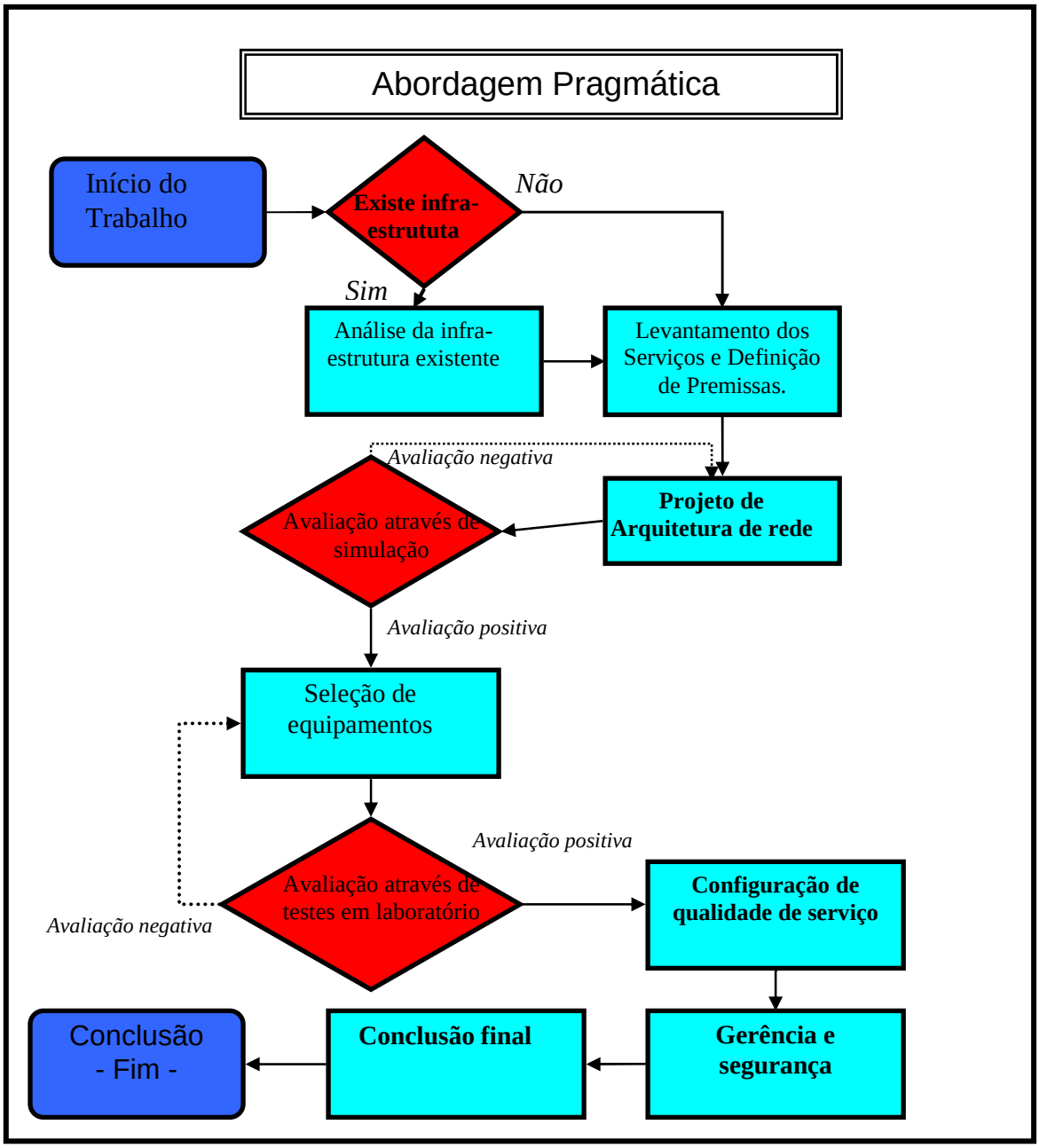
O plano de controle *MPLS* pode ser utilizado para recuperação de falhas, ao invés do *STP*. Novas soluções *MPLS* vêm sendo desenvolvidas para este caso, tais como: *Fast Reroute, RAPID, Bidirecional Forwarding* [15]. O uso do *MPLS* pode aumentar a escalabilidade dos endereços da rede, visto que o padrão 802.1q permite apenas 4096 *Virtual Local Area Network* (*VLAN*) e criação de uma hierarquia de endereços na rede. O *MPLS* facilita também a conexão de redes *GE* com outras redes de camada dois do modelo *OSI* [40].

Este capítulo apresentou um resumo das principais tecnologias *WAN* investigadas nesta dissertação. O capítulo a seguir expõe uma proposta de aborgadem pragmática para análise e projeto de rede WAN que é utilizada no estudo de caso.

4. Abordagem Pragmática em Projetos e Análise de rede

O desenvolvimento de um projeto de rede requer uma metodologia para melhor organização e eficiência do trabalho. A qualidade e eficiência de uma infra-estrutura de rede estão intimamente ligadas ao sucesso do projeto. A seleção adequada da tecnologia utilizada, a confiabilidade da rede e a operacionabilidade da rede devem estar alinhados com as necessidades dos usuários. Para ser considerado eficiente, um projeto precisa satisfazer diversos requisitos, desde funcionalidades operacionais até o desempenho dos sistemas e equipamentos destinados à topologia. A função do projeto é elaborar uma estrutura eficiente, baseada em uma metodologia de trabalho e utilizando técnicas e ferramentas adequadas.

Aplicando-se os conceitos de uma metodologia criada previamente é possível determinar as reais necessidades dos usuários, estabelecer as técnicas de pesquisa e levantamento de dados e proceder também a identificação dos meios materiais e estruturais do projeto. Uma outra vantagem em se utilizar uma metodologia refere-se à natureza dos projetos das modernas redes de comunicação. Como os projetos são geralmente grandes e complexos, exigindo a participação de um grupo de profissionais para sua realização, o trabalho pode ser dividido e organizado através de uma metodologia que especifique também as atividades que devem ser realizadas, como são realizadas e em que momento deve acontecer cada atividade. No Fluxograma 1 – Síntese das etapas da abordagem pragmáticapode ser observado as etapas existentes no processo de abordagem pragmática de análise e projeto de rede apresentado nesta dissertação.



Fluxograma 1 – Síntese das etapas da abordagem pragmática.

4.1. Análise da infra-estrutura existente

O primeiro ponto é a análise da infra-estrutura de rede existente, para casos em que o ambiente já possua rede instalada. Nesta etapa é necessário o levantamento de topologia, ocupação dos enlaces, pontos críticos da rede, possibilidades de interconexão e grau de

escalabilidade da rede. Em muitos projetos a infra-estrutura já possui uma topologia e esta é ampliada ou integrada ao um novo trecho de rede. A análise da infra-estrutura permite identificar se é possível à integração da topologia legada com o projeto de rede.

A caracterização da topologia existente demanda a criação de um mapa de rede, incluindo todos os segmentos e sua respectiva posição geográfica. Além do mapa, o levantamento dos equipamentos existentes e as principais restrições da arquitetura, necessitam ser estudados e documentados.

4.2. Levantamento dos Serviços e Definição de Premissas

O levantamento dos serviços e definição de premissas está ligada a avaliação dos serviços que trafegam pela rede [41] e definição de critérios para composição do projeto.
O levantamento dos serviços avalia latência máxima exigida, banda passante, variação do retardo e número de acesso, por tipo de aplicação. Já a definição de premissas são metas macro que a topologia deve respeitar e possuir, como por exemplo, suporte a *Virtual Private Network* (*VPN*).

O levantamento dos serviços consiste na avaliação dos serviços providos pela rede. É necessário o estudo teórico de demanda de tráfego e requisitos funcionais por aplicação. Uma análise em laboratório, ou em campo, do comportamento da aplicação através de um *sniffer* é importante porque validade a análise teórica. Além da caracterização do perfil de tráfego da aplicação, é importante compreender geograficamente como as aplicações trocam

informações. A localização dos principais servidores é o principal item desta atividade. A conclusão deste trabalho permite caracterizar o tráfego de total da rede.

A definição de premissas varia conforme a organização e usuários. Entretanto, alguns requisitos básicos têm presença garantida em um bom projeto de redes [41]. Dentre eles pode-se destacar: escalabilidade, funcionalidade, adaptabilidade, gerenciamento e custo. As premissas particulares podem ser adquiridas através de entrevistas com usuários (ou futuros usuários da rede) e através de peculiaridades já existente na rede. A avaliação do custo é presente nesta etapa e todo projeto depende dos recursos financeiros disponíveis para sua realização. As premissas básicas apontam para os tipos de tecnologias que devem ser utilizadas e equipamentos.

Tanto o levantamento de serviços quanto a definição de premissas são vitais para boa execução do projeto e uma falha nesta etapa pode trazer conseqüências na conclusão e aceitação do projeto.

4.3. Projeto da arquitetura da rede

A implantação de uma topologia de rede para dar suporte a um dado conjunto de aplicações não é uma tarefa muito simples. Cada arquitetura possui características que afetam sua adequação as aplicações utilizadas. As soluções não podem ser definitivas e devem permite adequações futuras. Muitos requisitos devem ser observados individualmente e

cuidadosamente, o que torna qualquer análise bastante difícil e complexa. Em muitos casos deve-se dar preferência por soluções segmentadas.

A segmentação da rede permite a criação de uma rede hierárquica que é composta por camadas com funções especificas e equipamentos. O projeto é segmentado em camadas, e estas são: camada núcleo, camada distribuição e camada acesso. Esta divisão é recomendada pelas principais recomendações de *NGN (Next Generation Network)* existentes [41]. Cada camada apresenta as seguintes características: o núcleo é formado por equipamentos de alta capacidade e alto desempenho; a distribuição é formada por equipamentos de média capacidade e desempenho, e permitem o aprovisionamento de diversos serviços e suporta diferentes facilidades; o acesso é responsável por prover a conectividade dos usuários aos elementos da rede de distribuição e deve possuir um custo menor.

A confecção da topologia precisa ser feita respeitando os conceitos de segmentação e os enlaces precisam estar dimensionados para o tráfego estimado. A avaliação da redundância da topologia é um item importante na composição da topologia e o grau de disponibilidade da rede deve estar alinhado com os requisitos funcionais das aplicações e o custo alocado para implantação da rede.

Caso a topologia possua ferramentas de engenharia de tráfego e qualidade de serviço, a criação da topologia deve usufruir dessas facilidades e prever na montagem da topologia o funcionamento das mesmas. A utilização de simulação computacional nesta atividade permite testar diferentes arranjos e verificar a topologia mais adequada para ser utilizada pela empresa. A simulação precisa refletir a topologia estudada com maior realismo possível e os

resultados observados na simulação não têm caráter definitivo, pelo contrário, servem como realimentação para o trabalho, permitindo a realização de ajustes de configuração.

Para execução da simulação é necessário definir os cenários e os dados que são extraídos de cada ensaio. A confecção do cenário depende dos tipos de tecnologias utilizadas pela rede e ferramentas existentes na rede. Os principais cenários simulados são: teste de topologia e testes de ferramentas.

O teste da topologia é basicamente uma simulação de desempenho de diferentes arranjos de rede buscando o melhor desenho topológico para o estudo de caso. O principal objetivo desta simulação é comprovar o melhor desempenho das topologias propostas frente a outras topologias possíveis.

O teste de facilidade consiste em analisar os benefícios de uma determinada ferramenta na topologia. Como por exemplo, o uso do *MPLS*. O uso do *MPLS* traz realmente benefícios para a topologia? Quais? Existe ganho no desempenho da rede? Quanto? Todos estes questionamentos podem ser resolvidos com o auxílio da simulação.

4.4. Seleção de equipamentos

A seleção de hardware é executada após a confecção da topologia. Os equipamentos devem estar aptos a se interligarem na topologia planejada e precisam respeitar a capacidade demandada pelas as aplicações [25]. Todas as facilidades demandadas pela topologia e pelos serviços necessitam estar mapeadas na escolha dos equipamentos. O equipamento deve

suportar as facilidades exigidas e demandas futuras. Esta etapa envolve a documentação fornecida pelos fabricantes para selecionar os componentes de hardware mais adequados para a infra-estrutura da *WAN*. Os dispositivos de *WAN* incluem roteadores, switches e equipamentos de transmissão (modem e multiplexadores). Este processo de seleção envolve considerações a respeito das funções e recursos disponibilizados em cada dispositivo em particular, inclusive suas capacidades de expansão e gerenciamento. Obviamente que o custo de aquisição do equipamento também deve fazer parte do processo de decisão.

Nesta etapa a avaliação técnica dos equipamentos através de testes práticos em laboratório ou em campo, serve como uma comprovação eficaz dos itens analisados teoricamente.

4.5. Configuração da qualidade de serviço

A inclusão de *QoS* na rede significa promover níveis diferenciados de serviços e garantia de recursos da rede. No *portfolio QoS* existem ferramentas de gerenciamento de banda e gerenciamento de atraso. O *QoS* em redes multiserviços é indispensável.

A qualidade de serviço está diretamenta ligada à arquitetura da rede, a demanda de tráfego e as características dos equipamentos da topologia. Estrategicamente, as configurações de qualidade de serviço necessitam ser projetadas após as etapas levantamentos dos serviços, arquitetura da rede e seleção de equipamentos.

As atividades que compõem a configuração de qualidade de serviço são:

● Definição do número de classes de serviço;

- Correlação de classe com serviços da rede;
- Definição do perfil de tráfego por classe;
- Escolha do tipo de marcação;
- Definição do ponto de marcação;
- Opção pelo tipo de política de escalonamento;
- Definição de banda máxima por classe.

Tal como o projeto de arquitetura de rede, a simulação computacional pode auxiliar no processo de configuração de *QoS*.

4.6. Gerência e segurança

Essa etapa está ligada a operacionabilidade e administração da rede [25]. As configurações selecionadas impactam na complexidade e custo operacional durante todo tempo de vida da rede. Um ponto muito importante em qualquer rede é a facilidade de uso e manutenção dos recursos disponibilizados, tanto para os usuários quanto para seus administradores. A rede deve possuir um conjunto básico de componentes e ferramentas capazes de oferecer um ambiente operacional de fácil manuseio. Há uma variedade de ferramentas de *SNMP* e *RMON* disponíveis que permitem um gerenciamento de rede próativo. Além disso, o ambiente de gerência deve possuir uma única interface operacional e uma base de dados também única. A principal atividade nessa etapa é avaliar as condições de gerenciamento da infra-estrutura estudada, verificando sua aderência com as práticas atuais de gerenciamento e necessidades dos administradores da rede.

A segurança está ligada ao acesso à informação. A topologia necessita ter requisitos de segurança que impeçam o acesso a sua infra-estrutura. O nível de segurança está vinculado a aspecto particulares do negócio. Na etapa de definição de premissas é importante a definição do nível de segurança. A principal atividade nessa etapa é avaliar as condições de segurança da infra-estrutura frente aos padrões vigentes e necessidades do negócio.

4.7. Estudo comparativo e avaliação final

Para a conclusão da abordagem é necessária a realização de um estudo comparativo entre as topologias estudadas e as facilidades. Os resultados apresentados no comparativo são usados na avaliação final. A avaliação final é a conclusão da aplicação da abordagem pragmática proposta na rede em análise. Além das conclusões, na avaliação podem existir recomendações técnicas como, por exemplo, uso de outros equipamentos ou outras tecnologias. A avaliação final deve conter os pontos chaves do estudo e também deve ter uma conclusão objetiva da avaliação.

Este capítulo apresentou uma proposta de abordagem pragmática para análise de projetos de rede que é utilizada, para fins de validação, no estudo de caso apresentado adiante. O capítulo a seguir expõe uma análise de um projeto de rede real de uma empresa do setor elétrico brasileiro.

5. Estudo de Caso

A empresa estudada atua no sistema elétrico brasileiro na geração e distribuição de eletricidade, presente no Distrito Federal e nos estados de São Paulo, Minas Gerais, Rio de Janeiro, Espírito Santo, Goiás, Tocantins, Mato Grosso, Paraná e Rondônia, onde funciona o Escritório de Construção de Porto Velho. A Empresa conta com um complexo de dez usinas hidrelétricas, além de Peixe Angical (TO), em construção, e duas termelétricas, totalizando uma potência de 9.467 MW. Conta, ainda, com 19.277,5 km de linhas de transmissão e 44 subestações, garantindo o fornecimento de energia elétrica em uma região onde estão situados 51% dos domicílios brasileiros e que responde por 65% do PIB brasileiro [46].

Para suporte as atividades operacionais e administrativas, a empresa possui uma extensa rede de telecomunicações. Esta rede possui enlaces próprios e alugados e sua abrangência corresponde aos estados de Goiás, Minas Gerais, Rio de Janeiro, Paraná, Espírito Santo e São Paulo.

O estudo de caso baseia-se numa avaliação de projeto de rede de dados, desenvolvido pelo fornecedor, para este empresa. Atualmente a empresa possui uma rede IP com enlaces alugados, capacidade da rede inferior à demanda atual e pouco uso da infra-estrutura *SDH* instalada. Os principais objetivos desse projeto são: utilizar a infra-estrutura existente *SDH* para promover a conexão entre os sites e aumentar a capacidade de transmissão de dados. A utilização da infra-estrutura *SDH* permite também o cancelamento dos enlaces alugados trazendo para rede diminuição do custo operacional.

5.1. Análise da infra-estrutura existente

A análise de infra-estrutura objetiva avaliar o estado atual da rede existente para efetuar uma comparação com a nova proposta de topologia para a rede. O escopo da rede existente aponta para questões como: interesse de tráfego, largura de banda dos enlaces, tipos de equipamentos e esquema de contingência existente.

Na topologia existente, os sites considerados como nós de núcleo são Adrianópolis, Furnas, Samambaia e Tijuco Petro. Os sites localizados no nível de distribuição são Campinas e Botafogo. Existe o nível de acesso que é composto por pontos de borda de rede.

O principal ponto observado na infra-estrutura existente é o formato não estruturado na rede. Os principais enlaces do núcleo apresentam capacidades de transmissão distintas. As bandas de transmissões dos enlaces de núcleo são majoritariamente múltiplos de VC-12 (Nx2Mbps). Os enlaces que ligam os sites localizados no nível de acesso são na sua maioria VC-12 (2Mbps). A topologia atual apresenta vários enlaces com origem num mesmo nó, possui assimetria nos enlaces redundantes e não utiliza ferramentas de engenharia de tráfego. A topologia não possui mecanismo de qualidade de serviço configurado.

Em relação a equipamentos, a rede utiliza roteadores Cisco 2500 e Cisco 3600 do fornecedor Cisco, *switches LAN Ethernet* variados (Cisco, 3COM e outros) e Mux PDH *NewBrigde.*

A análise aponta para existência de fragilidade na recuperação a falha e contingência da topologia em questão. A assimetria de banda dos enlaces é o principal responsável. O site

Botafogo, por exemplo, possui um enlace principal de 48Mbps (2xE3) e enlaces de contingência de 10Mbps (5xVC-12) e 2Mbps (VC-12). Na ocorrência de falha o enlace de contingência de 10Mbps suporta apenas 20% da banda total e o de 2Mbps somente 4%. Na Figura 15 – Topologia da Rede Legada (infra-estrutura existente)é apresentada a infra-estrutura existente e em funcionamento.

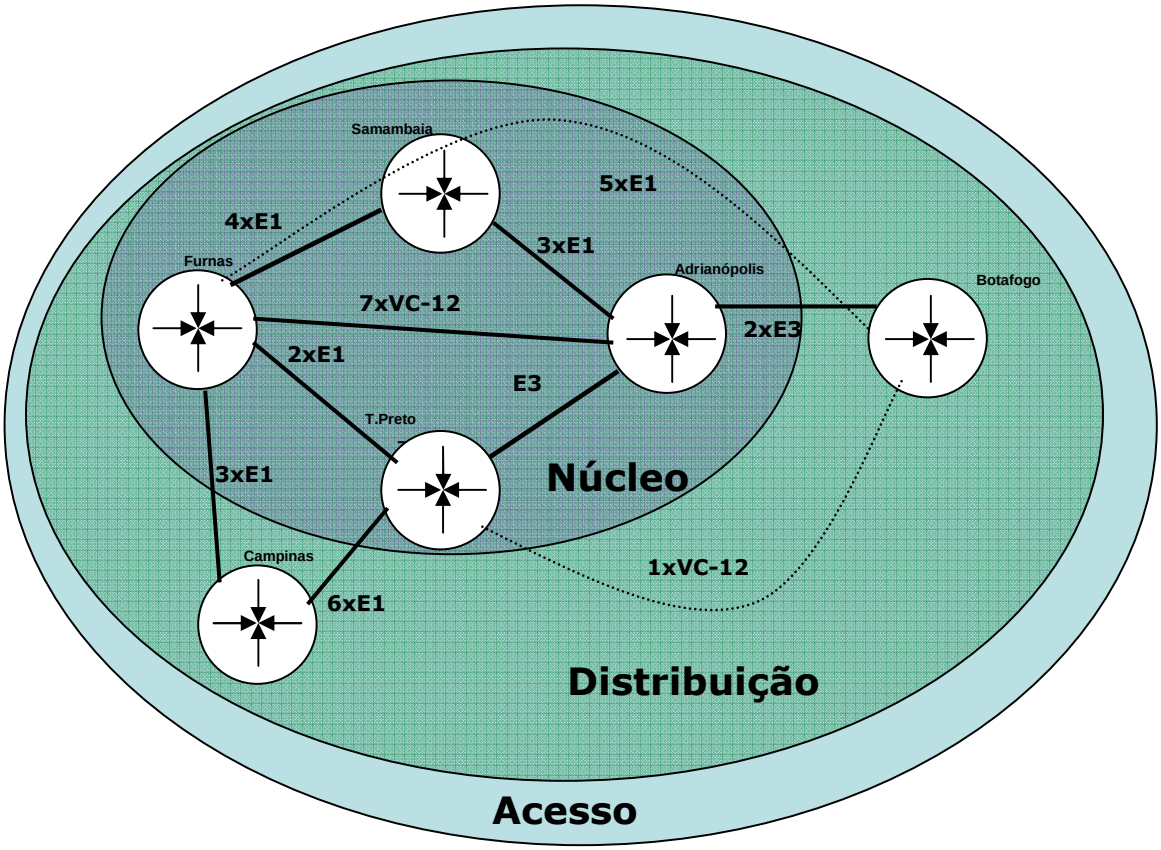


Figura 15 – Topologia da Rede Legada (infra-estrutura existente).

Os roteadores Cisco 2500 só possuem interfaces *PDH E1* (2Mbps) e *T1*(1,5Mbs) [10]. A interface E1 corresponde a padronização européia e a interface T1 representa a padronização nipo-americana. Os sites Adrianópolis, Botafogo e Tijuco Preto são exceções porque possuem enlaces *E3* (34Mbps) e têm o equipamento Cisco 3600. O Cisco 3600 não suporta interfaces *SDH*, mas possui interfaces E3 (34Mbs) [10]. Para adequação dessa

topologia a uma infra-estrutura física totalmente *SDH* é necessário a troca de todos os roteadores Cisco2500 e Cisco 3600.

5.2. Levantamento dos serviços e definição de premissas

A avaliação dos serviços que trafegam pela rede é um item que permite explicitar previamente questões como latência máxima exigida, banda passante, variação do retardo e número de acesso. As principais aplicações que trafegam por esta rede multi-serviço são: *SAP*, VoIP, circuito fechado de TV (CFTV), aplicativos ligados a automação do sistema elétrico e correio eletrônico.

O *SAP* é um sistema de automação de gestão corporativa e pode ser tipificado como um *ERP* (*Enterprise Resource Planning*). Esse sistema possui diferentes módulos que são utilizados em diferentes áreas nas empresa, como, por exemplo, os módulos financeiros e compras. Este sistema possui larga escala de utilização na empresa do estudo de caso. Seu fornecedor é a empresa *SAP Systems*. No que tange a caracterização do tráfego, o *SAP* com interface *Citrix* utiliza uma banda máxima de aproximadamente 5000 bytes por segundo (ou 40Kbps) [13]. O *Citrix* é uma ferramenta de metaframe para acesso de aplicações e servidores remoto. O *SAP* dispõe esta opção de interface na sua utilização.

Os aplicativos de automação estão ligados diretamente ao negócio da empresa e são considerados os serviços mais críticos da empresa. Os principais aplicativos são: acionamento de controle (até 64Kbps), esquema de emergência (19Kbps) e proteção de segurança (64Kbps). Todos estes aplicativos permitem a gerência de operação remota do complexo sistema de automação elétrico. Como exemplo pode ser citado o acionamento de controle

remoto, ferramenta esta que possibilita a realização de comandos remotos de turbinas e comutadores elétricos, evitando assim a intervenção humana “in-loco”. Esses aplicativos demandam alta disponibilidade e retardo máximo até 100ms (milisegundos).

Os serviços de VoIP e CFTV dependem do tipo de codificação utilizada para verificação da banda. A característica mais importante na rede para suporte a estes serviços é a variação do retardo.

O acesso à internet e o correio eletrônico possuem grau de criticidade menor para o interesse do negócio, mas são largamente utilizados pelos usuários da rede. Sua característica de transmissão se baseia em rajadas.

A etapa de definição de premissas é avaliação dos requisitos e facilidades que os equipamentos e a topologia devem apresentar. Este levantamento facilita principalmente no estudo dos equipamentos. As principais premissas são:

● A engenharia de tráfego é um item importante porque possibilitará diminuição de custo e melhor aproveitamento dos enlaces. O custo é um aspecto relevante neste projeto;

● A qualidade de serviço é necessária nesta topologia devido a variedade de aplicações e serviços providos pela rede. Um exemplo são as aplicações de automação que requerem pequenos retardo e baixa perda;

● O suporte a *Virtual Private Network (VPN)* permite segregação de grupos de usuários usando a mesma infra-estrutura de rede. O provimento de serviço de transmissão para outras empresas do grupo e sigilo de informação são aspectos providos por *VPN*. A *VPN* é aspecto importante nesta rede devido a complexidade do negócio e abrangência da empresa;

● A segmentação da rede nos níveis núcleo, distribuição e acesso, traz para rede maior capacidade de expansão, facilita o aprovisionamento de novos sites e diminui a complexidade operacional da rede. Quesito importante numa rede que está em expansão.

5.3. Arquitetura de rede

A topologia da rede possui um core *MPLS* composto pelos equipamentos: placa *ISA PREA*, *Omniswitch 7700* e *Multiplex SDH Alcatel*. O transporte dos quadros *Ethernet* no núcleo da rede utiliza o encapsulamento *MPLS* em *VC SDH*. O *MPLS* é utilizado para gerenciar fluxos de dados de pacotes transportados sobre uma infra-estrutura *SDH*. Os quadros são identificados e classificados na entrada da nuvem *MPLS* e seguem dentro do núcleo da rede utilizando a pilha de protocolos de sinalização *MPLS*. Os pacotes são agregados em *FECs* (*Forwarding Equivalence Class*) para configuração de perfis de comportamento [7]. A Figura 16 – Encapsulamento MPLS em VC SDH.[7] ilustra o processo de encapsulamento dessa arquitetura.

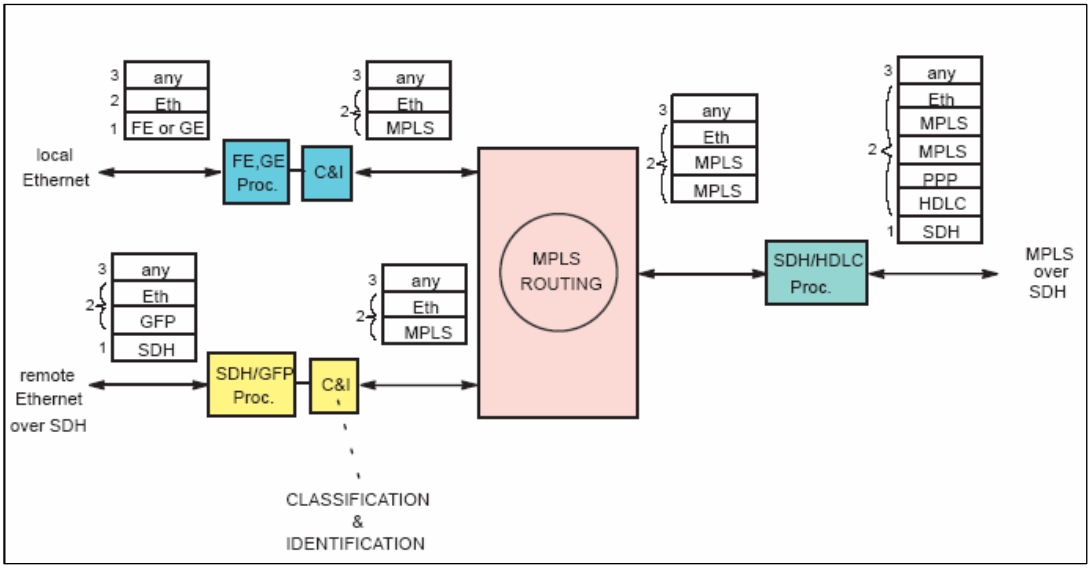


Figura 16 – Encapsulamento MPLS em VC SDH.[7]

O *MPLS* opera no nível dois e utiliza o *SDH* como sua camada física para transportar e agregar os vários fluxos de pacotes de dados. A técnica MPLS consiste em anexar um ou mais rótulos (label) aos pacotes de dados [29] permitindo o envio entre os nós da rede sem inspeção do cabeçalho do nível três e dois, somente observando o rótulo *MPLS* anexado. A placa *PREA* (*Packet Ring Edge Aggregator*) é um modelo de equipamento do fornecedor e é indicada para operar em uma rede anel *SDH* [7].

Na topologia em questão, os caminhos são criados estaticamente (através da intervenção humana). O *MPLS* permite também a criação de caminhos dinamicamente (sem intervenção humana), mas os equipamentos envolvidos não permitem esta alternativa. Um importante aspecto dos caminhos *MPLS* (*LSP*) é a capacidade de prover transporte para uma simples *VPN*, ou múltiplas *VPNs*. O *LSP* pode oferecer vários tipos de topologias lógicas sobrepostas em uma mesma rede física [4].

Nessa arquitetura o *MPLS* permite o empilhamento de rótulos [29] e existem dois níveis de empilhamento. O primeiro nível de empilhamento é *Inner Tunnel* (caminho interno) e o segundo é o *Outer Tunnel* (caminho externo). O *Outer Tunnel* facilita o mapeamento de *VC SDH* através da agregação de *Inner Tunnels* e possibilita a criação de *Transit Point* (ponto de trânsito) [7]. O ponto de trânsito é um ponto onde o rótulo *Inner Tunnel* é analisado para verificação do encaminhamento. Após a criação do *Outer Tunnel*, é inserido em vários *Inner Tunnel* (VLAN ou grupo de VLANs). Em relação ao aprovisionamento de *QoS*, é possível privilegiar os fluxos com maior demanda de banda dentro de um *Outer Tunnel*[7].

No que se refere ao roteamento, a placa *ISA PREA* não oferece suporte a protocolos de roteamento típicos *IP* (*OSPF, RIP e IS-IS*). O *Omniswitch* 7700, através do *OSPF* (*Open Shortest Path First*), é responsável pela definição das rotas de toda a rede. Todos os pacotes que passam por este equipamento recebem uma etiqueta de *VLAN* (*Virtual Local Area Network*). As *VLANs* podem ser locais (host conectados na mesma rede) ou remotas (conexão entre roteadores). A placa *ISA PREA* utiliza as *VLANs* remotas no seu processo de encaminhamento. Para escolha das *VLANs*, o Omniswitch utiliza os endereços IP dos pacotes. Os *Omniswitch* 7700 estão diretamente conectados aos equipamentos de transporte *SDH* através da placa *ISA* no nível distribuição ou ligado no *SDH* através da placa *ISA PREA* no nível núcleo e distribuição.

No estudo de caso, o conjunto placa *ISA PREA* e *Omniswitch* 7700 realizam as atividades de núcleo e distribuição. A segmentação da rede em níveis, modelagem proposta para redes NGN, não é respeitada nesta proposta. Essa descaracterização pode trazer problemas de escalabilidade, dificuldade de aprovisionamento, desempenho e redundância.

As redes que possuem um formato não estruturado (ou segmentado) apresentam problemas pelo excessivo número de nós adjacentes sem diferenciação de capacidade. Cada nível apresenta sua especificação funcional.

A camada de núcleo é formada por roteadores e/ou switches de alta capacidade e desempenho. Esses equipamentos devem possuir elevada disponibilidade.

A camada de distribuição é formada por equipamentos de média capacidade e desempenho, e permitem o aprovisionamento de diversos serviços.

O acesso é responsável por prover a conectividade dos usuários aos elementos da rede de distribuição. Na **Figura 17** – Topologia de rede proposta pelo fornecedor.é ilustrada a Topologia da rede apresentada pelo forneceedor.

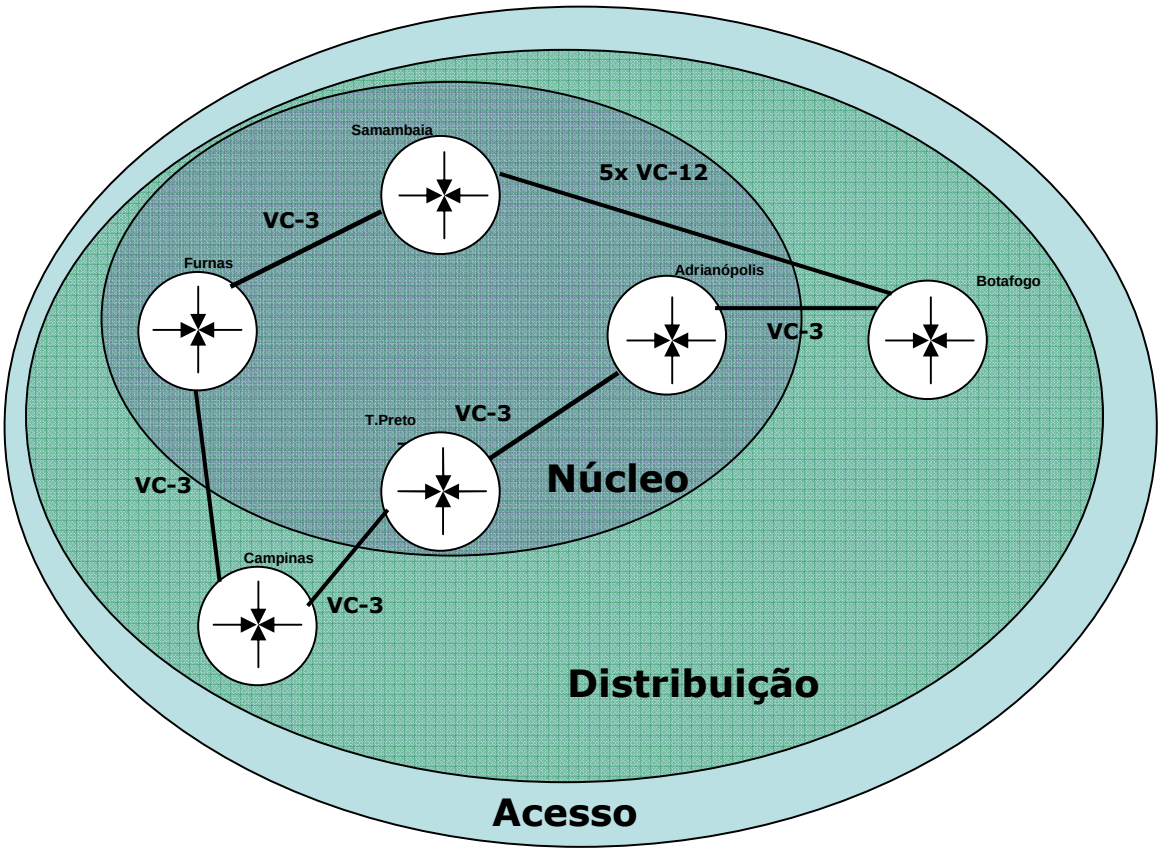


Figura 17 – Topologia de rede proposta pelo fornecedor.

A segmentação total de atividades entre os equipamentos de *WAN* (roteadores) e equipamento de *LAN* (*Switch-Router ou Switches*) é apontada como importante nesta dissertação. Como a troca não é possível, um novo arranjo topológico traz maior grau de segmentação da rede, escalabilidade e maior desempenho. Outro ponto é o desenho do núcleo da rede em anel. O anel inclui ainda equipamentos do nível de distribuição e possui arcos com enlaces de menor largura de banda, prejudicando a eficiência de facilidades como engenharia de tráfego e redundância. A criação de enlaces não respeitando estritamente o desenho em

anel, possibilita uma maior flexibilidade na criação de enlaces, conseqüentemente, traz ganhos para a engenharia de tráfego e opções de redundância.

Em relação a engenharia de tráfego, a topologia em anel simples dificulta o balanceamento de carga em pontos com maior carga. Para balanceamento de tráfego do site Furnas, por exemplo, é necessária a passagem do tráfego por Samambaia e Campinas. Como Campinas é um site caracterizado como ponto de distribuição e Samambaia possui uma banda menor do que 34Mbps na ligação com Botafogo, não é recomendado que seja adotada esta configuração. Os sites Campinas e Botafogo apresentam diversas ligações com sites de acesso que sobrecarregam sua capacidade de comutação.

No que tange ao aspecto redundância, como exemplo, pode ser citado a ligação Adrianópolis <-> Botafogo. O site Botafogo, através da ligação com Adrianópolis de VC-3 (34Mbps), injeta um alto tráfego de dados na rede. Nesta localidade existem diversos servidores, saída internet e etc. Em caso de problema no site Adrianópolis, a única saída para esta massa de dados é o site Samambaia, que possui apenas uma ligação de 5x VC-12 (10 Mbps).

Na borda da rede o transporte de quadros é feito através da *Ethernet over SDH*. O placa *ISA Ethernet* realiza o encapsulamento de quadros *Ethernet em VCs SDH*. Cada porta *Ethernet* da placa *ISA* pode ser mapeada em VC-12, VC-3, VC-4 ou concatenação de VC-12. A placa *ISA* permite concatenação de VCs (até 5x VC-12) na rede *SDH*. Para garantir o esquema de proteção através dos módulos *ISA Ethernet*, pode ser utilizado uma alternativa de agrupamento de dois (dois) grupos de concatenação, um grupo com 6Mbps (3x VC-12) e outro de 4Mb/s (2x VC-12), que funcionam como um enlace virtual único. Este controle é

feito pelo *OmniSwitch* 7700, através da função *Link Aggregation*, segundo o protocolo IEEE 802.3ad. Para obter esta facilidade, é necessário selecionar a opção "*qos classifyl3*" no *Omniswitch* [7].

A contingência nos pontos de acesso é realizada através de links de 512kbps ou 8xDS0, ligando os *Omniswitch* diretamente e utilizando enlaces contratados. A dissertação recomenda o aumento de banda dos enlaces de contingência. A diferença de banda entre o enlace principal e o de contingência é um ponto crítico e o uso de qualidade de serviço neste contexto é primordial.

5.3.1. Confecção da topologia

Na dissertação são propostas duas novas topologias. Uma topologia composta por enlaces VC-3 (34Mbps) e outra VC-4 (139Mbps). Ambas as topologias objetivam aumentar o grau de segurança operacional para o problema de queda de enlace e falhas de equipamentos, maior eficiência através da engenharia de tráfego e ganhos de escalabilidade para rede. As novas topologias devem respeitar as premissas iniciais que são: engenharia de tráfego, qualidade de serviço e uma arquitetura segmentada.

A primeira topologia proposta por este trabalho foi a com enlaces VC-3. A Tabela 2 - Mudanças requeridas para implementação da nova tecnologia.sintetiza as principais mudanças necessárias e a Figura 18 – Topologia proposta na dissertação com enlaces VC-3.ilustra a topologia proposta pela dissertação.

Enlaces	Topologia proposta pelo Fornecedor	Topologia proposta pelo trabalho - Interfaces	Motivo
Samambaia <-> Botafogo	5 x VC12 - projeto fornecedor	VC-3	Para permitir maior escoamento do tráfego de Botafogo em caso de falha no site Adrianópolis.
Samambaia <-> Adrianópolis	Não existe ligação no projeto fornecedor	VC-3	Permitir uma opção de escoamento de tráfegos Adrianópolis <-> Samambaia, sem passar por Botafogo.
Furnas <-> Tijuco Preto	Não existe ligação no projeto fornecedor	VC-3	Garantir uma melhor estruturação do núcleo e viabilizar a construção de opções de caminhos no processo de engenharia de tráfego.
Samambaia <-> Furnas	VC3 - Projeto fornecedor	VC-3	Permitir a construção de caminhos redundantes para a engenharia de tráfego e aumentar a capacidade de transporte entre estes sites.
Tijuco Preto <-> Adrianópolis	VC3 - Projeto fornecedor	VC-3	Permitir a construção de caminhos redundantes para a engenharia de tráfego e aumentar a capacidade de transporte entre estes sites.

Tabela 2 - Mudanças requeridas para implementação da nova tecnologia.

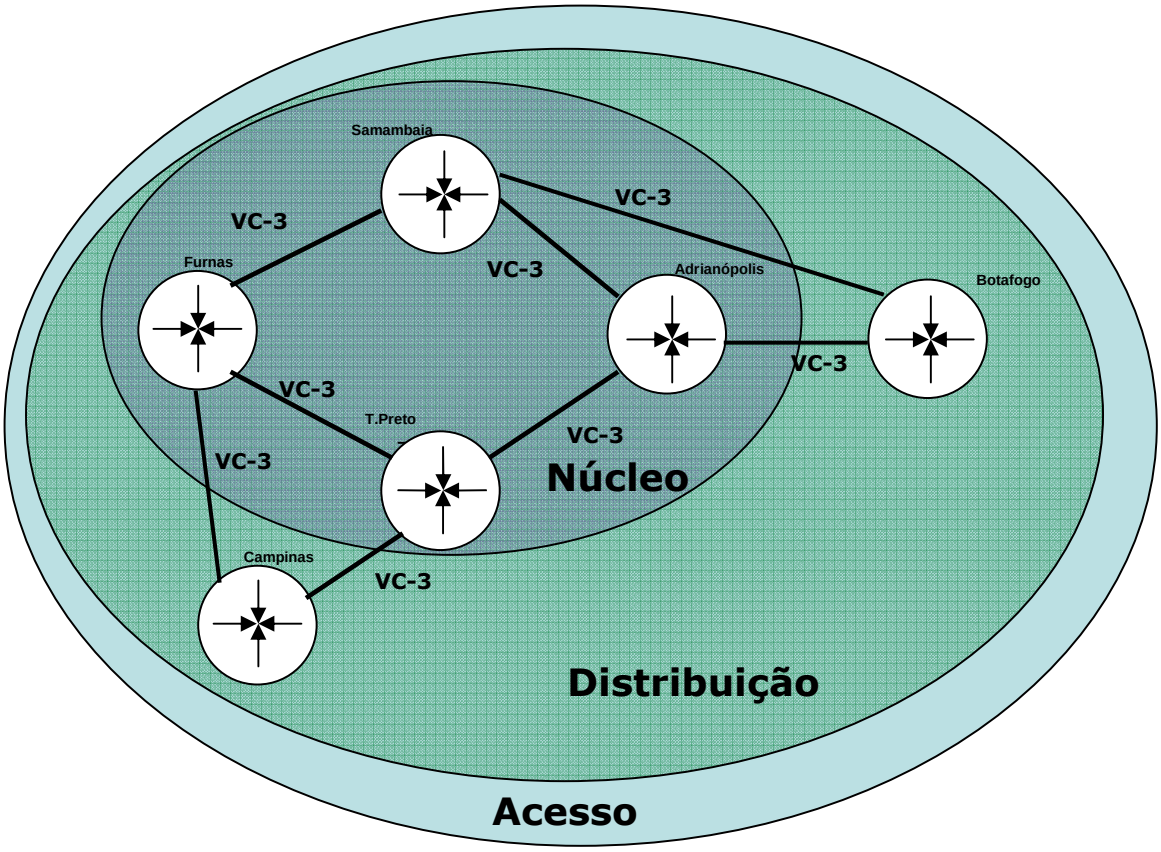


Figura 18 – Topologia proposta na dissertação com enlaces VC-3.

A topologia proposta insere dois novos enlaces (Furnas <-> Tijuco Preto e Samambaia <-> Adrianópolis) e substitui um enlace de 5xVC-12 por um enlace VC-3 (Samambaia <-> Botafogo). Não é necessário aquisição de novos equipamentos para suportar esta nova topologia. A segunda topologia é idêntica à primeira, exceto os enlaces que são VC-4. A Figura 19 - Topologia proposta na dissertação com enlaces VC-4.apresenta a topologia proposta pela dissertação com enlaces VC-4.

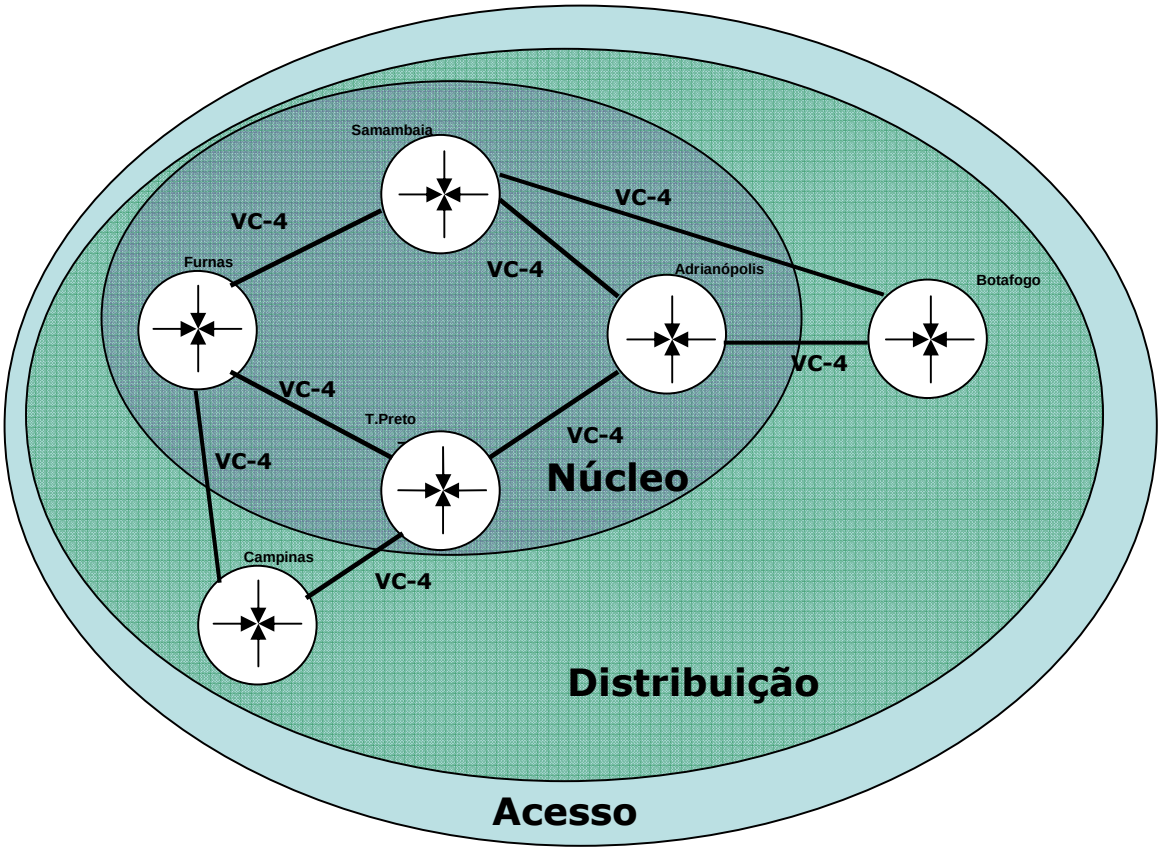


Figura 19 - Topologia proposta na dissertação com enlaces VC-4.

O núcleo (Adrianópolis, Furnas, Samambaia e Tijuco Preto) tem os enlaces ampliados e formam um anel de 139Mbps. A segunda topologia pretende oferecer maior capacidade de transmissão e permitir a rede suportar aumento de demanda não projetada.

As placas *ISA PREA* não permitem concatenação de VC-4 e suportam apenas dois canais VC-4 para cada direção. Para contornar este problema uma opção é utilizar mais de uma placa em cada localidade. O equipamento 1660SM permite o funcionamento de até quatro placas *ISA PREA* em cada chassi. Os pontos centrais da rede (Furnas, Adrianópolis, Tijuco Preto, Samambaia, Botafogo e Campinas) podem receber uma configuração de duas (ou mais) placas *ISA PREA*. Na Tabela 3 – Resumo com alterações da topologia.são apresentadas as adições e remoções de enlaces e a composição de placa necessária no

equipamento 1660SM. Para implantação da topologia com enlaces VC-4 faz-se necessário a aquisição de quatro placas *ISA PREA*.

Sites	Adição de placa	Números de placas existentes	Total de placas	Adição de Enlaces	Enlaces já existentes	Total de Enlaces	Enlaces subtraídos
Furnas	1	1	2	3 xVC-4 1XEthernet	2xVC-3 1xEthernet	3xVC-4 2xEthernet	2xVC-3
Samambaia	1	1	2	3xVC-4	2xVC-3 5xVC-12 1XEthernet	3xVC-4 1xEthernet	2xVC-3 5xVC-12
Adrianópolis	1	1	2	3xVC-4	2xVC-3	3xVC-4	2xVC-3
Botafogo	1	1	2	1xVC-4 1XEthernet	5xVC-12 1xVC-4 1xVC-3 1XEthernet	2xVC-4 2xEthernet	5xVC-12 1xVC-3

Tabela 3 – Resumo com alterações da topologia.

O uso da simulação permite a validação das topologias sugeridas através da análise dos diferentes arranjos de rede. A simulação busca o melhor desenho topológico para o estudo de caso e está aderente com as etapas definidas na abordagem programática. As topologias testadas são:

- Topologia do projeto original (core da rede basicamente anel);
- Topologia proposta pela dissertação com enlaces VC-3 (34Mbps);
- Topologia proposta pela dissertação com enlaces VC-4 (139Mbps).

A simulação consiste em seis ensaios, cada ensaio analisa uma das topologias com ou sem engenharia de tráfego. Através da avaliação de utilização de cada enlace é possível verificar a distribuição dos tráfegos na rede. Primeiramente é testada a topologia sem

engenharia de tráfego para identificação dos seus benefícios e sua real necessidade. Depois da recuperação dos resultados, a topologia é configurada novamente com a inserção dos *LSPs* estáticos com balanceamento de carga, disponíveis através de ferramentas de engenharia de tráfego, suportada pelos equipamentos adquiridos.

Foram criados diferentes fluxos de tráfego, oriundos de diversas origens para diferentes pontos. Cada fluxo de tráfego recebeu diferentes configurações de perfis (tamanho de pacote, taxa de bits e etc.). Além dos fluxos de tráfego aleatórios, foram configuradas trocas de dados entre as aplicações em diversas localidades (criadas no ambiente simulado) como carga de tráfego para rede. O cenário possui as aplicações correio eletrônico, *FTP*, videoconferência e voz. A Figura 20 – Fluxos criados na simulação.ilusta graficamente os fluxos de tráfegos criados na topologia simulada.

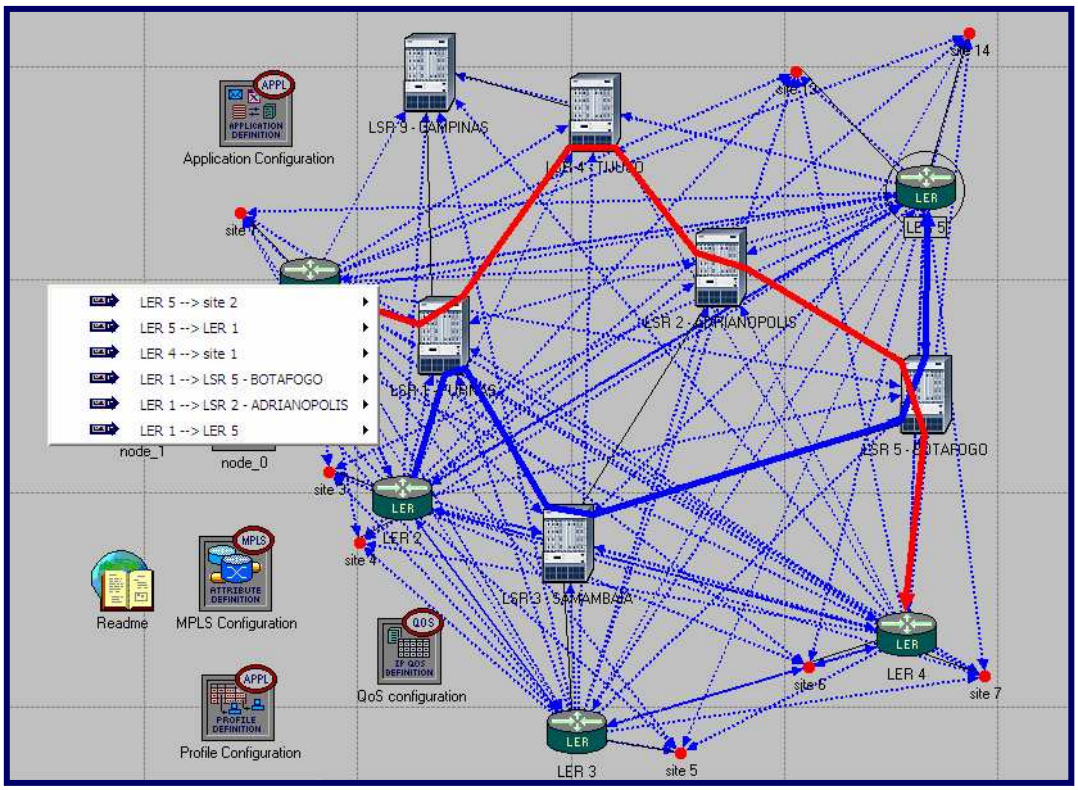
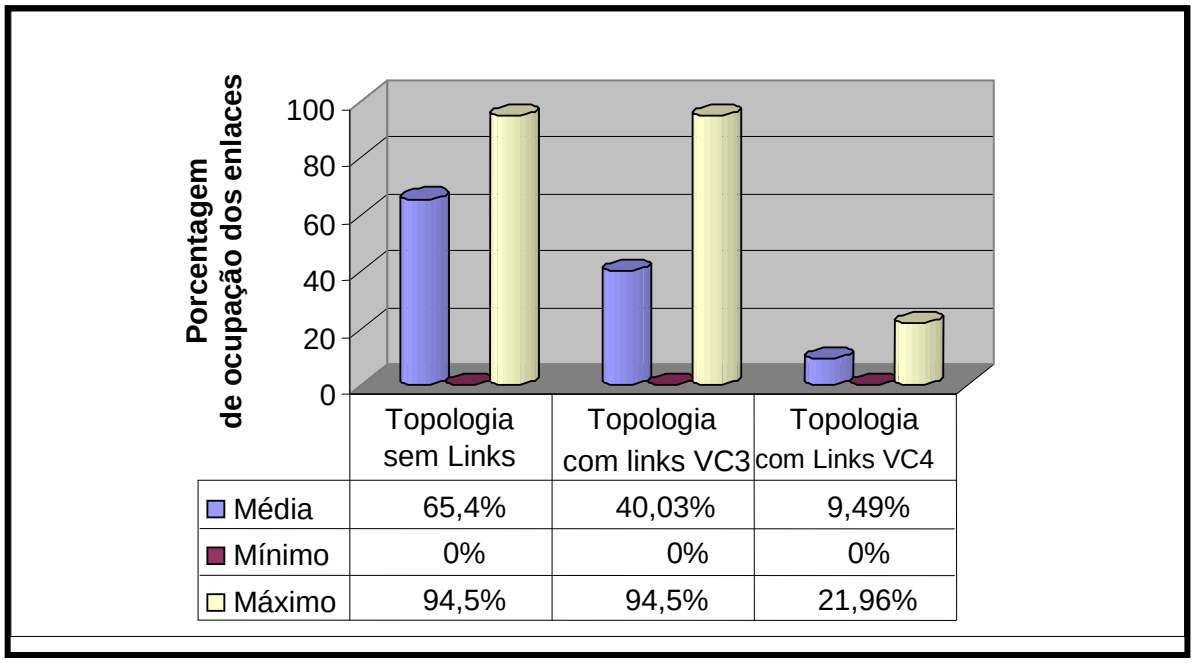


Figura 20 – Fluxos criados na simulação.

O resultado com a ocupação dos enlaces sem engenharia de tráfego é apresentado resumidamente no Gráfico 1 – Ocupação dos Enlaces (sem engenharia de tráfego).. Sem a engenharia de tráfego, a topologia proposta por este trabalho traz poucos benefícios em relação a topologia original. A média de utilização dos enlaces apresentou um valor menor, mas os enlaces com ocupação crítica permaneceram com valor equivalente. A média foi menor na topologia proposta basicamente devido aos novos enlaces inseridos.



	Topologia sem Links	Topologia com links VC3	Topologia com Links VC4
Média	65,4%	40,03%	9,49%
Mínimo	0%	0%	0%
Máximo	94,5%	94,5%	21,96%

Gráfico 1 – Ocupação dos Enlaces (sem engenharia de tráfego).

A topologia proposta nesta dissertação trouxe maiores benefícios para rede com a utilização de engenharia de tráfego. As topologias propostas pela dissertação apresentaram uma menor ocupação dos enlaces, comparada com a topologia proposta pelo fornecedor, e uma melhor distribuição do tráfego pelo enlaces da rede. Esta avaliação é facilmente observada quando os valores máximos, disponíveis no Gráfico 2 – Ocupação dos Enlaces (com engenharia de tráfego).são comparados. Os enlaces críticos têm sua ocupação diminuída e distribuída para enlaces com um maior índice de ociosidade. Esta característica resulta em

uma menor propensão a ocorrência de problemas de congestionamento e descarte, bem como um maior grau de escalabilidade para rede. Resumidamente, a rede suportará um maior grau de expansão para suporte a novos serviços.

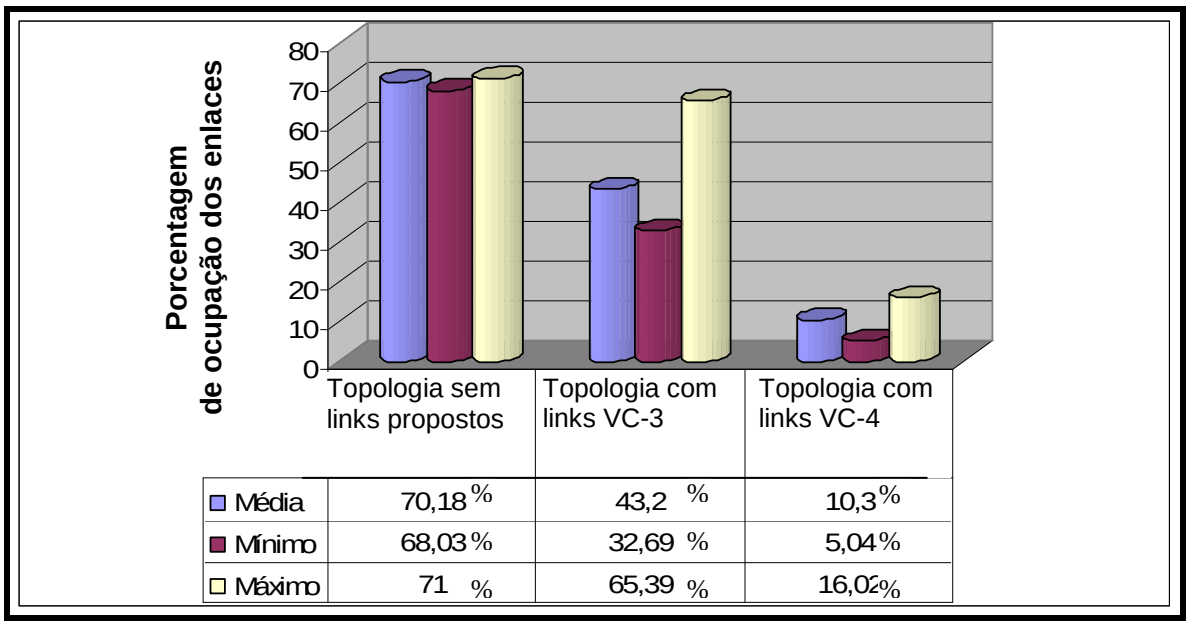


Gráfico 2 – Ocupação dos Enlaces (com engenharia de tráfego).

Por meio dos resultados encontrados, foi verificado que a topologia proposta nessa dissertação com enlaces *VC-3* e *VC-4* apresenta uma maior grau de segurança operacional para problemas de queda de enlace. O uso da engenharia de tráfego traz benefícios para as topologias proposta, permitindo homogeneidade nas ocupações dos enlaces.

5.3.2. Uso do *MPLS*

O uso do *MPLS* oferece o suporte a engenharia de tráfego. A engenharia de tráfego está relacionada com a otimização do desempenho operacional das redes. Sua utilização permite uma diminuição de custo da infra-estrutura, tornando-a uma ferramenta indispensável

nas redes de comunicação de dados. A utilização de uma boa estratégia de alocação de recursos é muito importante para maximização do desempenho da rede.

Na topologia analisada, os *LSPs MPLS* são criados estaticamente. Isso acontece porque a placa *ISA PREA* não oferece suporte a protocolos de roteamento típicos *IP* (*OSPF*, *RIP* e *IS-IS*). O roteador *Omniswitch* localizado nas bordas, através do *OSPF versão 2*, é quem determina a alcançabilidade da rede para os nós.

Para verificação dos benefícios do uso do *MPLS* nesta solução, foram testados dois cenários possíveis de funcionamento da rede.

● Primeiramente é utilizado o protocolo *IP* para definição dos caminhos da rede. Toda a inteligência da rede se concentra no *Omniswitch*, que utiliza o *OSPF* para definição dos caminhos. O protocolo *MPLS* não existe neste ambiente, conseqüentemente, não é utilizada a placa *ISA PREA*;

● O segundo ambiente é testado o uso do *MPLS*. Através da placa *ISA PREA* é possível criar caminhos estáticos (*LSPs MPLS*) e *OSPF* permite obter alcançabilidade da rede.

Foram criados tráfegos do site Furnas para Botafogo. Através da ocupação dos enlaces por este tráfego é possível analisar o caminho prioritário da rede.

5.3.2.1. Simulação – Rede baseada em *IP*

Na configuração deste ambiente foi habilitado o protocolo de roteamento (*IGP*) nos equipamentos da rede e também foram criados tráfegos *FTP* dos *sites* (1, 2, 3 e 4) para o *LERs* (5 e 6).

Na Figura 21 - Rede baseada em *IP (simulação uso do MPLS).*tem-se a topologia testada e os caminhos dos fluxos de tráfego. A seta representa o caminho dos fluxos de dados do site Furnas para o site Botafogo. Pode-se verificar através da figura que todos os fluxos seguem um mesmo caminho, escolhido pelo protocolo de roteamento *IGP*, não permitindo assim uma utilização homogênea dos recursos da rede.

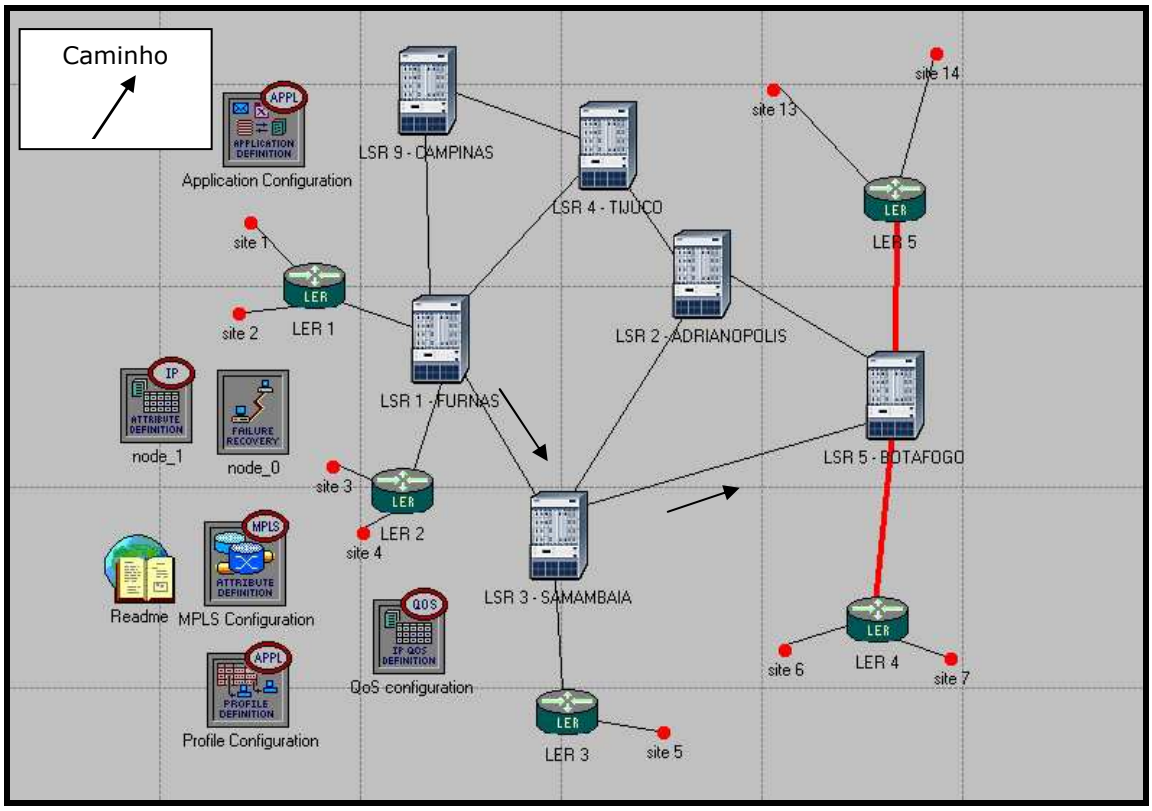


Figura 21 - Rede baseada em *IP (simulação uso do MPLS).*

Foram explicitados em cinza os enlaces que foram inutilizados pela configuração *IGP*. Na Tabela 4 - Ocupações dos enlaces da rede baseada em *IP*.pode-se verificar a distribuição de tráfego nos enlaces do *backbone*.

Enlaces	*Throughput* (Kbps)	Grau de Utilização
site 1 <-> LER 1	**230,343**	**1**
site 2 <-> LER 1	**230,343**	**1**
LER 1 <-> LSR 1 - Furnas	**460,731**	**2**
site 3 <-> LER 2	**220,141**	**1**
site 4 <-> LER 2	**220,141**	**1**
LER 2 <-> LSR 1 - Furnas	**440,298**	**2**
site 5 <-> LER 3	**220,141**	**1**
LSR 1 - Furnas <-> LSR 3 - Samambaia	**910,029**	**3**
LSR 1 - Furnas <-> LSR 4 - Tijuco	**0**	**0**
LSR 4 – Tijuco <-> LSR 2 - Adrianópolis	**0**	**0**
LSR 2 - Adrianópolis <-> LSR 5 - Botafogo	**0**	**0**
LSR 3 - Samambaia <-> LSR 2 - Adrianópolis	**0**	**0**
LSR 3 - Samambaia <-> LSR 5 - Botafogo	**1130,17**	**4**
Grau de utilização (de 0 a 4)		
0	Utilização muito baixa	De 0% a 20%
1	Utilização baixa	De 20% a 40%
2	Utilização média	De 40% a 60%
3	Utilização alta	De 60% a 80%
4	Utilização muito alta	De 80% a 100%

Tabela 4 - Ocupações dos enlaces da rede baseada em *IP*.

A análise desta simulação indica que a infra-estrutura baseada apenas em *IP* não permite uma utilização homogênea dos recursos da rede. Na simulação em questão, foi verificado que os enlaces Furnas <-> Tijuco, Tijuco <-> Adrianópolis, Adrianópolis <-> Botafogo e Samambaia <-> Adrianópolis, estão com uma utilização caracterizada como

muito baixa. Entretanto, os enlaces Samambaia <-> Botafogo e Furnas <-> Samambaia, estão com uma utilização **muito alta**.

A utilização inadequada de determinados enlaces pode prejudicar o desempenho global da rede. O uso da engenharia de tráfego permite a diminuição da ociosidade de determinados enlaces e divide os fluxos de tráfego, permitindo assim uma melhor utilização dos recursos.

5.3.2.2. Simulação – Rede baseada em *MPLS* e *IP*

A solução proposta para o estudo de caso utiliza configuração de caminhos estáticos *MPLS* no núcleo da rede. Através da placa *ISA PREA*, são criados os caminhos (*LSP MPLS*) no núcleo da rede. O *LSP MPLS* é criado de forma estática e necessita ser criteriosamente planejado. A placa *ISA PREA*, utilizada na solução, não oferece suporte a protocolos de roteamento típicos *IP*, tais como *OSPF, RIP* e *IS-IS*. Os *Omniswitchs* localizados nas bordas, através do uso do *OSPFv2*, determinam a alcançabilidade da rede para os nós.

O objetivo desta simulação é verificar a eficiência desta configuração no contexto estudado.

As configurações dos *LSPs* criados são apresentadas na Figura 22 – Rede baseada em *MPLS IP (simulação uso do MPLS).*. Resumidamente tem-se o *LSP 1* (seta losango) que suporta o tráfego dos sites 3,4 e 5 para os sites 13 e 14 e o *LSP* 2 (seta aberta) que suporta o tráfego dos sites 1 e 2 para o site 6 e 7. Obs.: Uma das principais dificuldades neste trabalho foi configurar os *Push*, *Swap* e *Pop* do *LSR*, que são feitas *hop-by-hop*.

Verifica-se que os fluxos seguem caminhos distintos respeitando a configuração *MPLS*. A Tabela 5 – Ocupações dos enlaces da rede baseada em *MPLS IP*. contém a utilização dos enlaces representando em cinza o enlace que obteve utilização muita pequena. Não foi observada utilização muita alta no *backbone*.

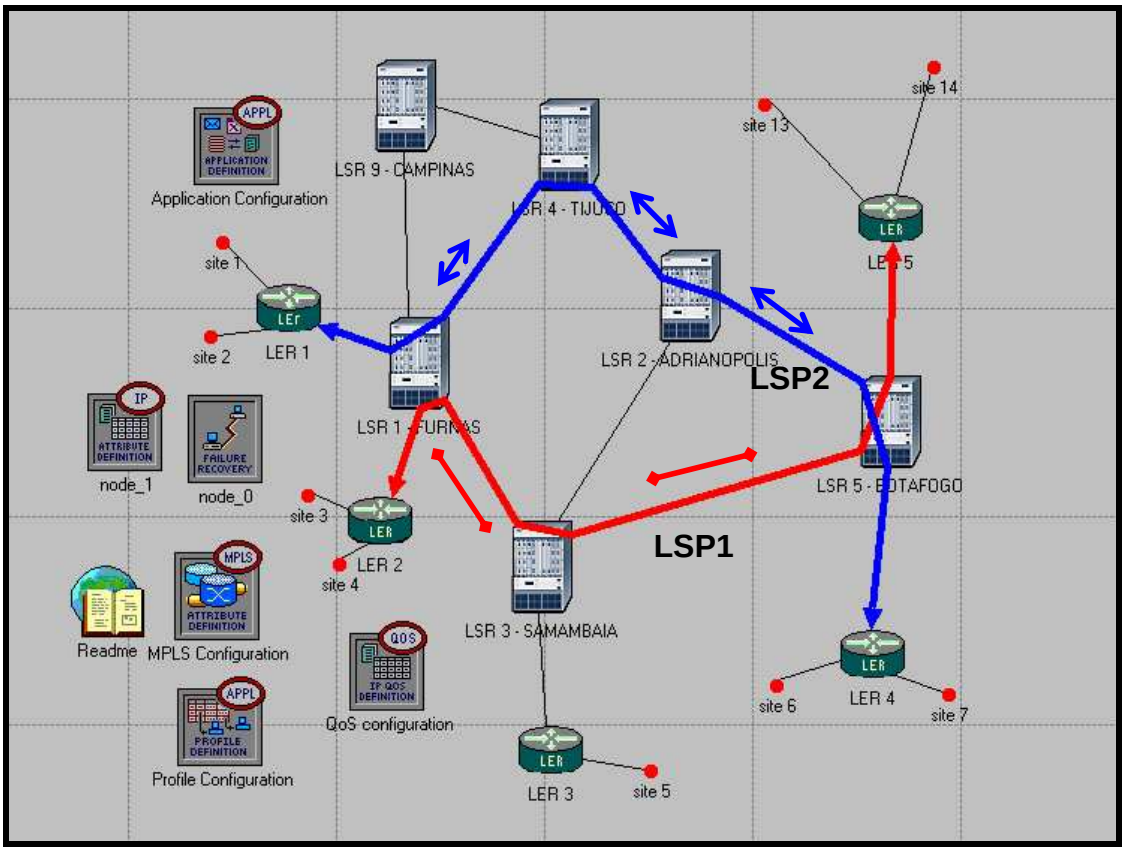


Figura 22 – Rede baseada em *MPLS IP (simulação uso do MPLS).*

Enlaces	*Throughput* (Kbps)	Grau de Utilização
site 1 <-> LER 1	**230,343**	**1**
site 2 <-> LER 1	**230,343**	**1**
LER 1 <-> LSR 1 - Furnas	**460,731**	**2**
site 3 <-> LER 2	**220,141**	**1**
site 4 <-> LER 2	**220,141**	**1**
LER 2 <-> LSR 1 - Furnas	**440,298**	**2**
site 5 <-> LER 3	**220,141**	**1**

LSR 1 - Furnas <-> LSR 3 - Samambaia	**440,298**	**2**
LSR 1 - Furnas <-> LSR 4 - Tijuco	**460,731**	**2**
LSR 4 - Tijuco <-> LSR 2 - Adrianópolis	**46,731**	**2**
LSR 2 - Adrianópolis <-> LSR 5 - Botafogo	**460,731**	**2**
LSR 3 - Samambaia <->LSR 2 - Adrianópolis	**0**	**0**
LSR 3 - Samambaia <-> LSR 5 – Botafogo	**660,439**	**2**
Grau de utilização (de 0 a 4)		
0	Utilização muito baixa	De 0% a 20%
1	Utilização baixa	De 20% a 40%
2	Utilização média	De 40% a 60%
3	Utilização alta	De 60% a 80%
4	Utilização muito alta	De 80% a 100%

Tabela 5 – Ocupações dos enlaces da rede baseada em *MPLS IP*.

O comportamento desta topologia difere da anterior (Rede *IP*), basicamente porque é possível balancear o tráfego da rede, permitindo a criação de uma rede onde os enlaces apresentam utilização mais homogênea. Com os mesmos tráfegos da simulação anterior, não foi observado nenhum enlace com uma utilização nível quatro ou nível zero (métrica de utilização máxima e mínima), exceção feita apenas para a ligação Samambaia <-> Adrianópolis, que não possui *LSP* criado para este enlace. Operacionalmente, pode ser criado um *LSP* que utilize este enlace.

A análise desta simulação indica que a infra-estrutura existente permite a construção de engenharia de tráfego, mas a dinâmica das configurações ocorre de modo estático.

Foi verificado que a engenharia de tráfego (modo estático) traz benefícios para a rede em questão. A possibilidade de criar caminhos ao longo da rede permite uma melhor

utilização de *enlaces* e de equipamentos. Esta topologia permite a diminuição da ociosidade de determinados enlaces e divide os fluxos de tráfego, permitindo assim uma utilização mais homogênea dos recursos disponíveis da rede.

No intuito de enriquecer este trabalho, é simulada a criação de dois túneis para um mesmo par origem/ destino. A solução consiste na utilização de uma ou mais placas *ISA PREA*, criando caminhos distintos para um mesmo destino que possui alta demanda de tráfego. Para simular esta solução são criados dois *LSPs* para o mesmo destino, passando por diferentes enlaces em cada nó. Nesta simulação foram habilitados os tráfegos do site 3 e site 4 (conectados ao site Furnas) para o *LER 5* (conectado em Botafogo). Os dados do site três foram configurados para utilizarem o *LSP 1* (linha contínua) e do site 4 para utilizarem o LSP 2 (linha pontilhada). A Figura 23 - Rede baseada em *MPLS IP* (dois caminhos com mesmo destino).demonstra graficamente a criação de dois caminhos com o mesmo destino na topologia analisada.

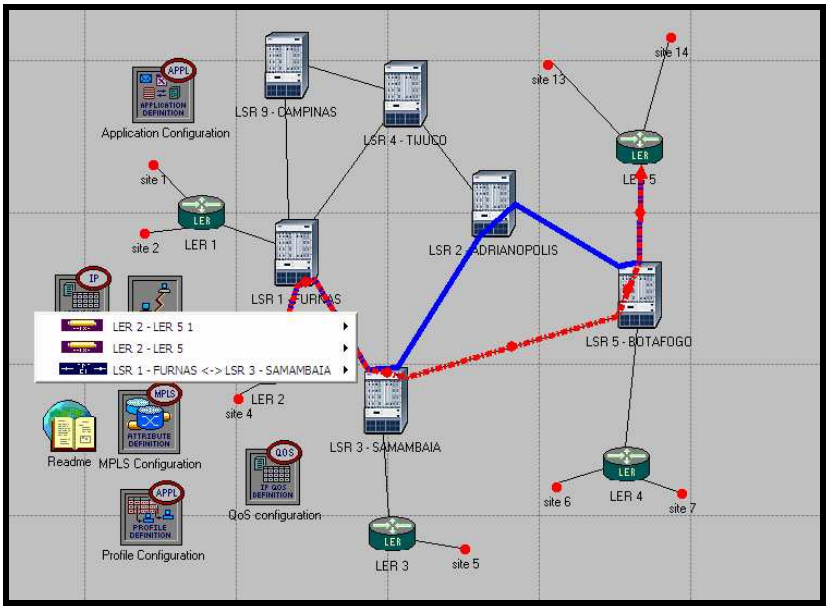


Figura 23 - Rede baseada em *MPLS IP* (dois caminhos com mesmo destino).

Foi verificado nesta simulação que tráfegos com mesmo par origem-destino podem ser configurados para trafegarem em caminhos (*LSPs*) distintos, utilizando *enlaces* e placas *ISA PREA* distintas. Essa configuração é possível através da configuração de *LSPs MPLS* no modo estático. Na Tabela 6 – Distribuição de tráfego usando os dois *LSPs.*é possível verificar a distribuição dos tráfegos através das configurações de *LSPs* estáticas da placa *ISA PREA*, utilizando dois caminhos para um mesmo destino.

A utilização da configuração de mais de uma placa *ISA PREA* em cada localidade e a utilização de engenharia de tráfego provida pelas configurações *MPLS* disponíveis, permite uma capacidade de *throughput* maior, já que permite um maior escoamento do tráfego através do balanceamento de carga entre diferentes enlaces e placas.

Enlaces	*Throughput* (Kbps)	Grau de Utilização
site 3 <-> LER 2	220,141	1
site 4 <-> LER 2	220,141	1
LER 2 <-> LSR 1 – Furnas	440,298	2
LSR 1 - Furnas <-> LSR 3 – Samambaia	440,298	2
LSR 3 - Samambaia <-> LSR 5 - Botafogo	220,141	1
LSR 3 - Samambaia <-> LSR 2 - Adrianópolis	220,141	1
LSR 2 - Adrianópolis <-> LSR 5 - Botafogo	220,141	1
Grau de utilização (de 0 a 4)		
0	Utilização muito baixa	De 0% a 20%
1	Utilização baixa	De 20% a 40%
2	Utilização média	De 40% a 60%
3	Utilização alta	De 60% a 80%
4	Utilização muito alta	De 80% a 100%

Tabela 6 – Distribuição de tráfego usando os dois *LSPs*.

5.3.3. Recuperação a falhas

A capacidade de realizar uma recuperação a falhas em um pequeno intervalo de tempo é uma característica importante para as redes atuais. A demanda crescente de um alto grau de *SLA* e suporte a sistema em tempo real, fazem com que as redes atuais respondam rapidamente e pró – ativamente a este problema.

Para verificação deste requisito é testado o cenário IP e o MPLS IP. Nas simulações a seguir, o ponto de falha foi o mesmo em todos os ensaios. Para a falha ser gerada é necessário a utilização da ferramenta *"Fail Rec Config"* do *OPNET*®. Nesta ferramenta podem ser configuradas falhas de *enlace* e falha de equipamento. A convergência da rede é realizada através do protocolo *OSPF* operante no *Omniswitch*. O tempo de convergência teórico do *OSPF* é de 15 a 45 segundos [47], a variação é proveniente do tamanho da rede e das tabelas de roteamento.

Para efeito de simulação, todos os cenários foram configurados para utilizar o enlace Samambaia <-> Adrianópolis como enlace prioritário de roteamento. Para exemplificação, foi criada uma falha entre o *LSR2* e o *LSR3*, após aproximadamente 35 segundos de simulação. O intuito destas simulações foi verificar o tempo de convergência de cada um ambiente e comparar o comportamento da solução frente as demais.

5.3.3.1. Simulação baseada em rede *IP*

Nesta simulação é utilizada a topologia com enlaces *VC-3* proposta na dissertação. São testados os dois cenários de configuração possíveis nesta topologia. São eles: topologia *IP* e

topologia *MPLS IP*. O cenário desta seção é a topologia *IP*. Nas seções a seguir é testado o outro cenário.

O *Omniswitch,* através do *OSPFv2,* é quem determina a alcançabilidade da rede para os nós. A solução permite a convivência com uma convergência via *SDH*. Apenas os sites que possuírem redundância de fibra, podem conviver com esta facilidade. Os sites que possuem redundância de fibra são:

- Furnas;
- Samambaia;
- Adrianópolis;
- Tijuco Preto;
- Botafogo.

Os demais sites apenas convivem com a redundância via protocolo de roteamento. Os equipamentos necessariamente devem estar com o protocolo de roteamento habilitado. O intuito desta simulação foi verificar o tempo de convergência da solução numa arquitetura puramente IP.

Na Figura 24 – Ponto de falha / Simulação baseada em rede *IP*.tem-se a topologia com o respectivo ponto de falha na rede. A falha ocorre no enlace que liga o *LSR2* e o *LSR3,* após aproximadamente 35 segundos de simulação.

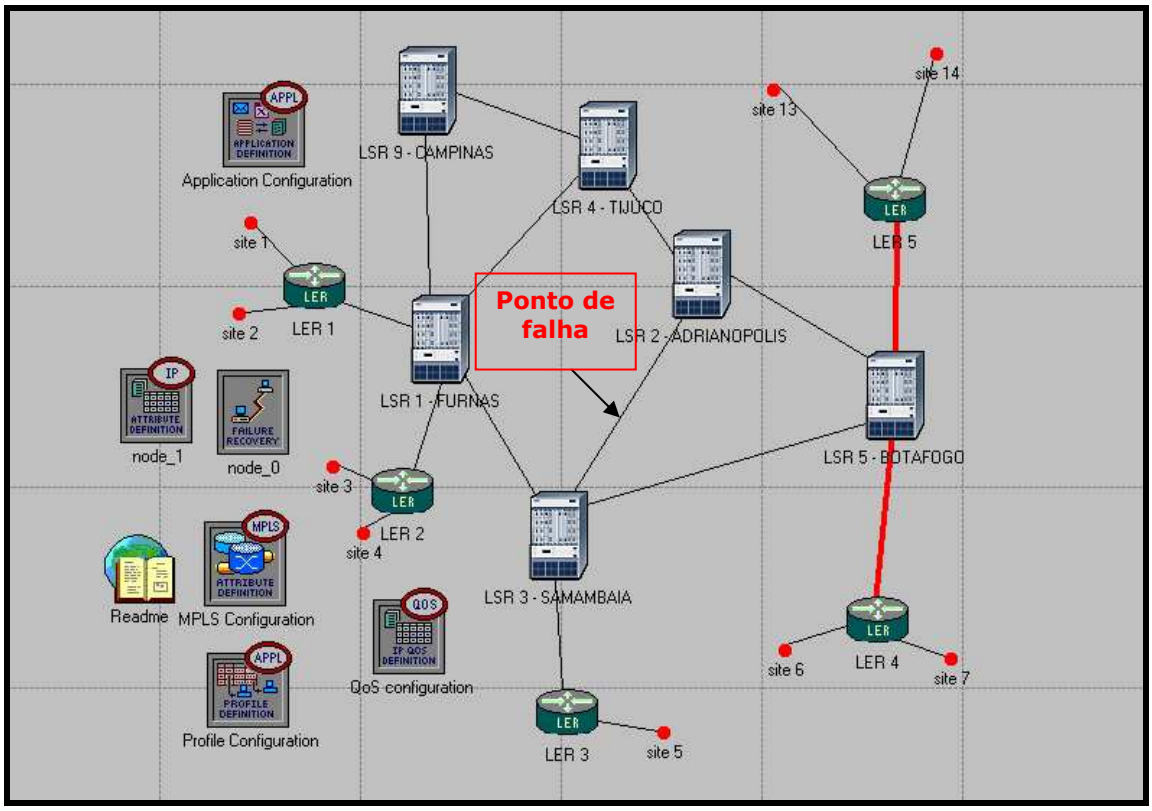


Figura 24 – Ponto de falha / Simulação baseada em rede *IP*.

Após a falha no enlace *LSR 3* <-> *LSR2*, o roteador verifica o problema e utiliza informações do protocolo *OSPF* para determinar uma saída alternativa para os fluxos de dados. No caso especifico a saída especificada foi a *LSR 3* <-> *LSR 5*.

Através dos gráficos de disponibilidade do *OPNET®* pode ser verificada a ocupação de cada enlace. Este gráfico permite a identificação do problema e da utilização do enlace alternativo. Na Figura 25 - Gráfico de tempo de convergência *(*rede *IP).* é apresentada a utilização do enlace *LSR 3* <-> *LSR 2* e *LSR 3* <-> *LSR5*. A figura reflete o tempo de convergência da rede, em outras palavras o tempo de recuperação pós-falha em um enlace. O gráfico superior da figura representa o enlace que apresenta problema e o gráfico inferior o enlace que supre a falha.

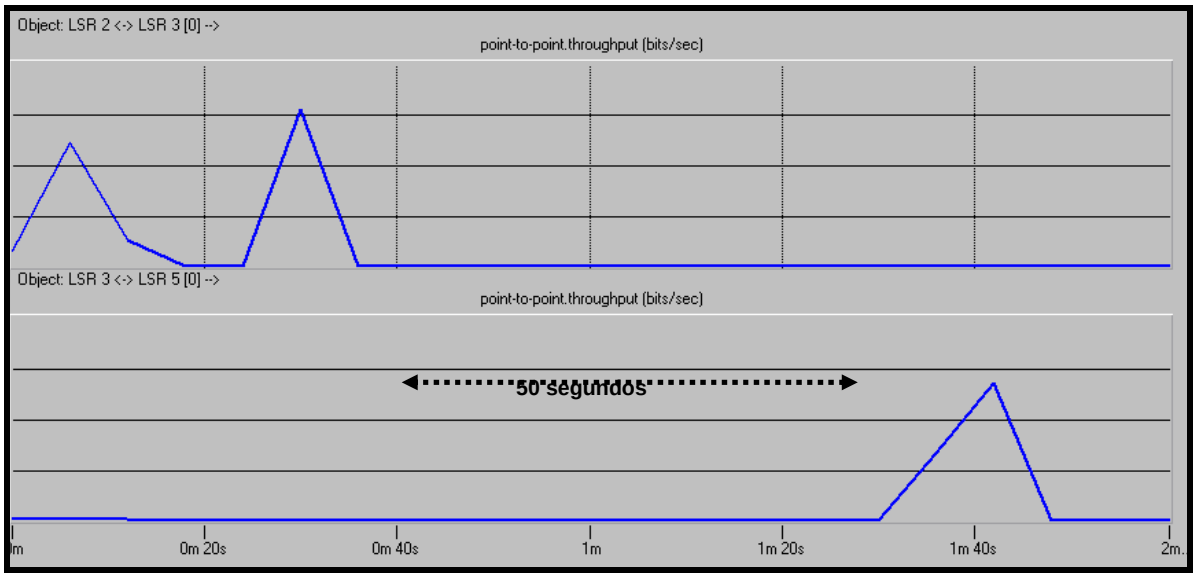


Figura 25 - Gráfico de tempo de convergência *(rede IP).*

O intervalo de convergência é de 50 segundos neste ambiente. Este tempo é necessário para o outro enlace assumir o tráfego que estava sendo transportado pelo enlace principal.

5.3.3.2. Simulação baseada em rede *MPLS* e *IP*

Nesta simulação é verificado o tempo de convergência da topologia *MPLS IP*. A simulação, tal como solução real, utiliza configuração de caminhos estáticos *MPLS* no núcleo da rede e utiliza também os *switches-Routers* (análogos ao *Omniswitch)* para permitir a convergência da rede, em caso de falha em nós ou enlaces.

Como já citado anteriormente, a solução utiliza os *Omniswitches* para processar o *OSPF* porque as placas *ISA PREA* não oferecem suporte a protocolos de roteamento típicos *IP*. Para permitir a redundância de caminho, são criados dois caminhos *MPLS/SDH* para um mesmo destino. O caminho de contingência deve ter um custo maior *OSPF*. Só é utilizado este tipo de contingência, quando a falha não for tratada pela contingência da camada física

(*SDH*). Os sites que possuem redundância de fibra podem conviver com esta facilidade. Os sites Furnas, Samambaia, Adrianópolis e Tijuco Preto, possuem redundância física (fibra).

A simulação tem com objetivo verificar o tempo de convergência em caso de problema numa arquitetura *MPLS e IP*. Utilizou-se na simulação a mesma topologia e o mesmo tráfego das simulações anteriores, exceção feita à criação de um novo *LSP*, entre Samambaia e Botafogo, para permitir a opção de convergência do *LSP* original. A Figura 26 – Ponto de falha / Simulação baseada em rede *MPLS IP*.ilustra a topologia com o respectivo ponto de falha na rede. A falha ocorre no enlace que liga o *LSR2* e o *LSR3* e ocorre após aproximadamente 35 segundos após o início da simulação.

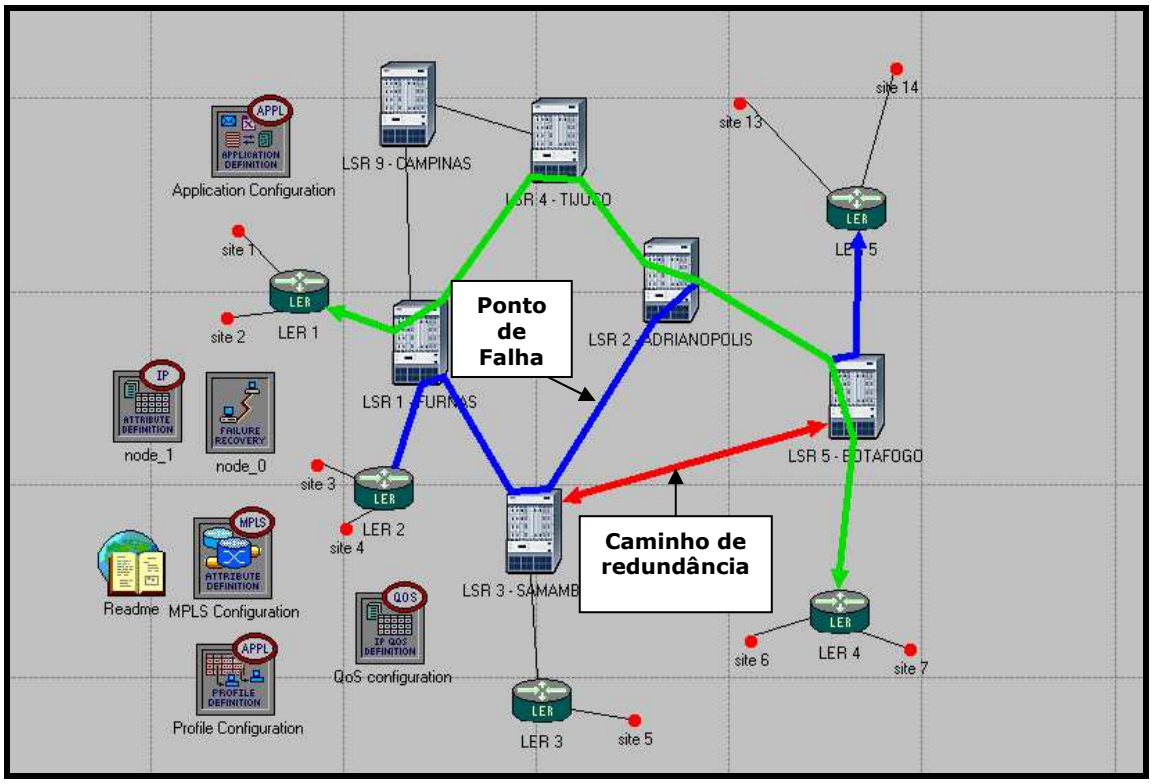


Figura 26 – Ponto de falha / Simulação baseada em rede *MPLS IP.*

O resultado do *OPNET*® com a ocupação dos enlaces LSR 3 <-> LSR 2 e LSR 3 <-> LSR5 é apresentado na Figura 27 - Gráfico de tempo de convergência *(*rede *MPLS IP).* A

figura permite visualizar o tempo de recuperação a falhas da topologia com os protocolos *MPLS IP* configurados. O gráfico superior da figura representa o enlace que apresentará problema após 35 segundos de simulação e o gráfico inferior representa a curva de utilização do enlace redundante.

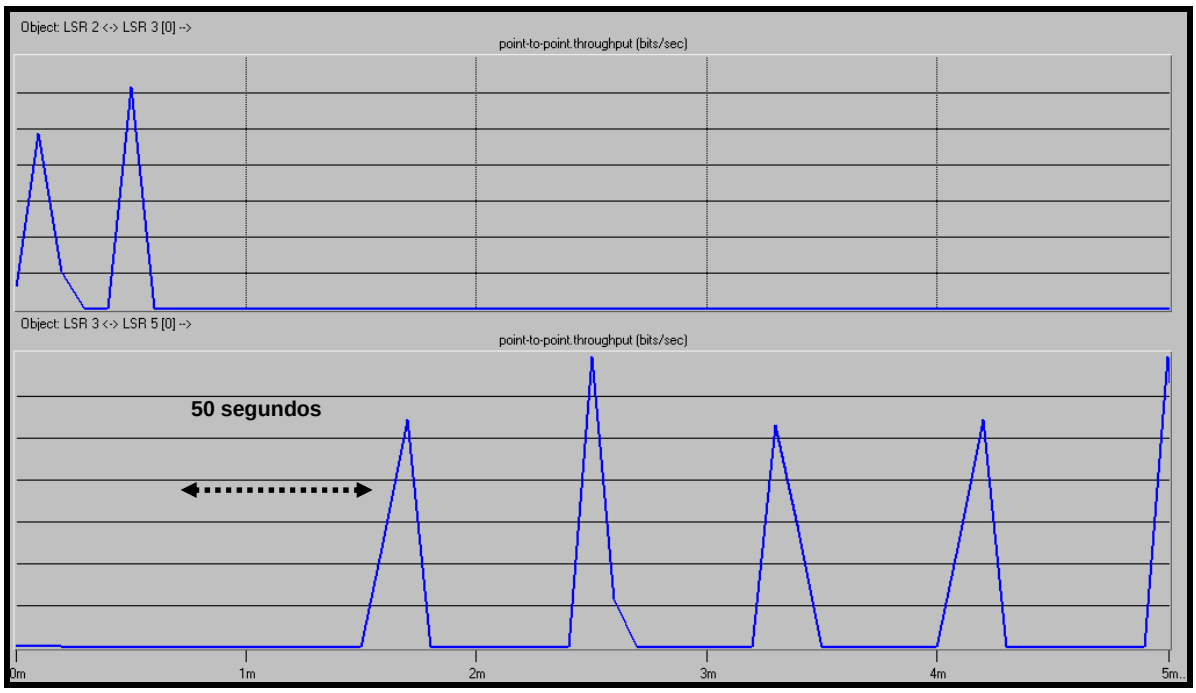


Figura 27 - Gráfico de tempo de convergência *(*rede *MPLS IP).*

O intervalo de convergência é de 50 segundos neste ambiente, igual ao encontrado na topologia de *rede IP*. Como a redundância está totalmente ligada ao *OSPF*, já era esperado que os tempos fossem equivalentes. O *Fast Reroute* neste contexto traz benefícios para a rede analisada. Todas as referências utilizadas neste trabalho indicam um intervalo de convergência do Fast Reroute abaixo dos verificados neste teste, em torno de 1 segundo. No entanto, os equipamentos utilizados na topologia não suportam esta facilidade.

O *Fast Reroute* neste contexto traria benefícios para a rede analisada. Todas as referências utilizadas neste trabalho indicam um intervalo de convergência do *Fast Reroute*

abaixo nos verificados neste teste, em torno de 1 segundo. Mas os equipamentos utilizados na solução não suportam esta facilidade.

Para fins de simulação são configurados nos equipamentos a facilidade *Fast Reroute*, sobre a mesma topologia, e são verificados os tempos de recuperação a falha. A Figura 28 - Gráfico de *throughput* / Rede baseada em *Fast Reroute*.apresenta o tempo de recuperação da rede utilizando o *Fast Reroute*. O intervalo de recuperação a falha é de aproximadamente 2 segundos. Este tempo ficou acima do esperado, visto que as referências sobre o protocolo indicam tempos inferiores a 1 segundo. Entretanto, o tempo de convergência em 2 segundos é inferior ao do *IP*. Entretanto é importante ressaltar que os equipamentos utilizados na solução não suportam esta facilidade.

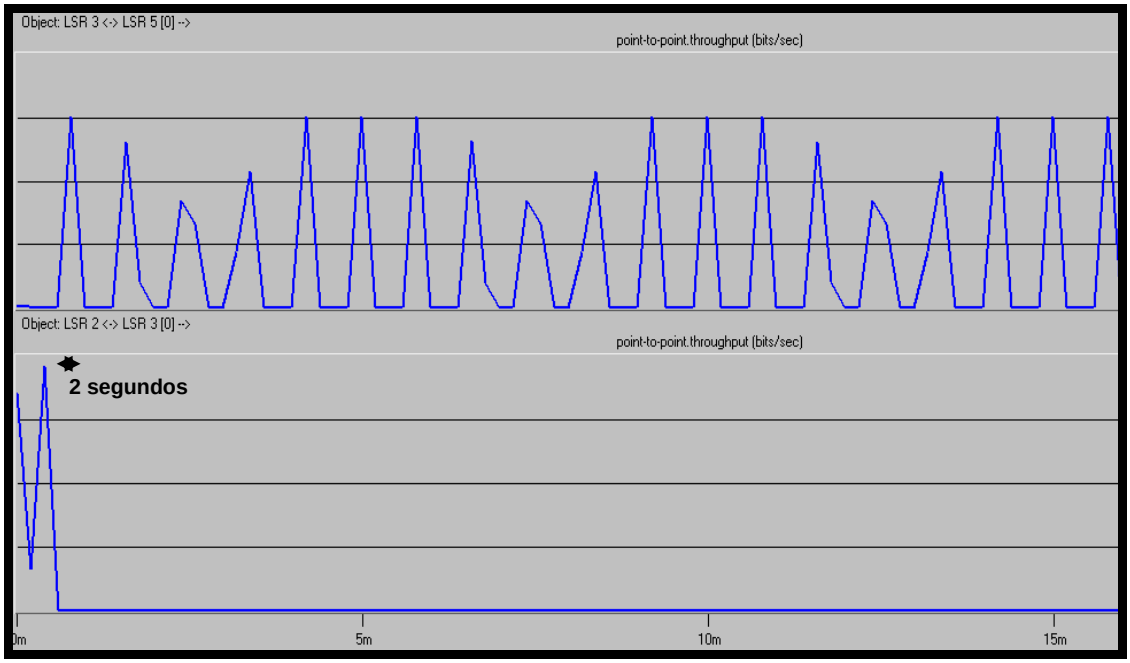


Figura 28 - Gráfico de *throughput* / Rede baseada em *Fast Reroute*.

5.4. Estudo dos Equipamentos

Este estudo permite analisar se os equipamentos selecionados estão aptos a integrarem a topologia planejada, se possuem a capacidade demandada e disponibilizam as facilidades requeridas pela topologia. Este estudo deve ser realizado após a análise de premissas e estudo da topologia da rede.

No Anexo I é realizada uma análise dos principais equipamentos oferecidos pelo mercado e é sugerida aquisição do equipamento Alcatel 7750. No comparativo este equipamento recebeu a maior pontuação. O equipamento foi também bem avaliado no *MPLS Forum* (Paris, 2005) [24] num teste de funcionalidade e interoperabilidade entre diversos equipamentos, descrito como "*Provider*" (P) pelos fabricantes.

Como a troca não é factível, a dissertação enfoca os equipamentos existentes na topologia proposta pelo fornecedor (estudo de caso).

5.4.1. *Omniswitch*

O *OmniSwitch* 7700 é utilizado na função de roteador *IP* e *switch Ethernet* com capacidade de concentrar as portas *Ethernet*, *Fast Ethernet* e *Gigabit Ethernet*. Sua configuração possui módulo de gerência e fontes de alimentação redundantes, além de módulos *Ethernet* e *Gigabit Ethernet*. O equipamento está tanto no núcleo da rede como na borda e permite a rede conhecer informações de alcançabilidade, através do protocolo *OSPF* (*Open Shortest Path First*). Na Tabela 7 – Resumo de funcionalidades do *Omniswitch.* [8] é possível verificar as principais funcionalidades desse equipamento.

Funcionalidade	Situação	Observação
Suporte a QoS	Possui	Baseado em políticas

		estruturadas em função de parâmetros e ações
Definição de prioridades	Possui	IEEE 802.1p e TOS/DSCP
Suporte a Sinalização RSVP	Não Possui	
QoS nas portas de saída	Possui	Não descreve como é feito o escalonamento
Uso na borda da rede	Possui	Opera em camada 2 e camada 3
Definição de políticas para fluxos individuais	Possui	Importante para aplicações críticas
Suporte a IEEE 802.1Q	Possui	
Roteamento OSPF	Possui	
Roteamento RIP	Possui	
Roteamento BGP	Possui	
Roteamento IS-IS	Não Possui	
Suporte a DVMRP	Possui	
Suporte a IP Multicast	Possui	
Policiamento de tráfego	Não Possui	Não implementa balde furado
Definição de banda mínima	Possui	Para políticas de QoS
Definição de banda máxima	Possui	Para políticas de QoS
Definição de máximo buffer alocado	Possui	Para políticas de QoS
Suporte a NAT	Possui	
Suporte a ACL	Possui	
Políticas de Server Load Balancing	Possui	

Tabela 7 – Resumo de funcionalidades do *Omniswitch.* [8]

5.4.2. Placa *ISA PREA (Integrated Service Adapter - Packet Ring Edge Aggregator)*

A placa *ISA PREA* é utilizada para a criação da nuvem *MPLS* no *backbone* do subsistema *SDH*. A placa *ISA PREA* permite conexões *Ethernet/SDH* e *SDH/Ethernet* através do *MPLS*. O sistema de gerência permite a configuração de conexões entre fluxo local com fluxo remoto. O *Omniswitch* não possui interfaces *SDH*, tornando assim obrigatório a utilização deste equipamento. Estes fluxos podem estar mapeados em uma ou mais *VPN* (*Virtual Private network*). Na Figura 29 – Empilhamento de protocolo. [7] é mostrado o

formato do empilhamento dos protocolos e na Tabela 8 – Resumo de funcionalidades da placa *ISA PREA*. [7] tem-se as facilidades suportadas pelo equipamento.

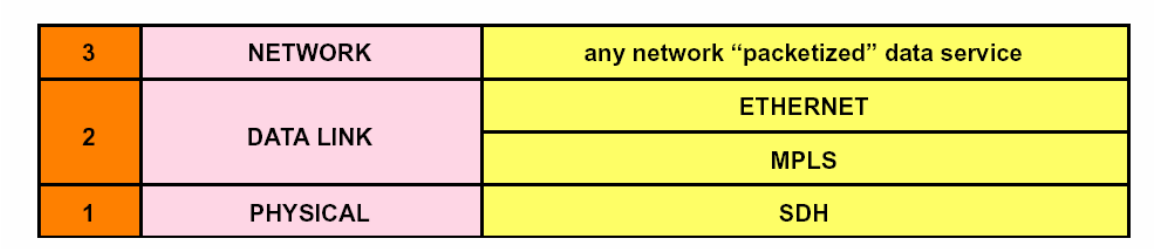


Figura 29 – Empilhamento de protocolo. [7]

Funcionalidade	Situação	Observação
Compartilhamento de Largura de Banda do SDH	Possui	Entre portas/serviços Metro Ethernet
Agregação de Tráfego	Possui	
Gerenciamento de Tráfego	Possui	Baseado em 3 classes de CoS e SLA
Suporte a conexões ponto a ponte	Possui	
Suporte a conexões ponto a multiponto	Possui	
Suporte a conexões multiponto	Possui	
Classificação de pacotes	Possui	Baseado em prioridade e endereço de destino, por porta, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3, Label MPLS, IP TOS/Diffserv
Escalonamento de pacotes	Possui	De acordo com SLA Ethernet, baseado em HOL e WFQ.
Mapeamento de interfaces físicas	Possui	IEEE 802.3, IEEE 802.3u, IEEE 802.1z, IEEE 802.3x, Ethernet over SDH
Policiamento de tráfego	Possui	Baseado em duplo balde furado usando CIR, CBS, PIR e PBS
Níveis de SLA	Possui	Serviços garantidos, serviços regulados e BE

Congestion Avoidance	Possui	Baseado em Tail Drop e WRED e IEEE802.3x
Ethernet/GFP/Ethernet/SDH	Não Possui	
Ethernet/MPLS	Possui	
Ethernet/MPLS/MPLS	Possui	
Ethernet/MPLS/MPLS/PPP/HDLC/SDH	Possui	
LP Ethernet	Possui	Possibilitado através de roteamento de rótulos MPLS.
LP virtual Ethernet	Possui	Possibilitado através de roteamento de rótulos MPLS.
Multiplexagem de Ethernet em LP virtual	Possui	
LAN virtual Ethernet	Possui	IEEE 802.1Q/MPLS
Acesso em Banda Larga	Possui	
Roteamento MPLS	Possui	
OSPF	Não possui	
RIP	Não possui	
IS-IS	Não possui	
BGP	Não possui	
Suporte a RSVP-TE	Possui	Estabelecimento do LSP
Sinalização LPD	Possui	Para troca de informações de rótulos MPLS
Sinalização CR-LDP	Não possui	

Tabela 8 – Resumo de funcionalidades da placa *ISA PREA*. [7]

Em relação a placa *ISA PREA* pode-se concluir que:

- Implementa uma pilha *Metro Ethernet* (*Ethernet/MPLS/SDH*);
- Possibilita o compartilhamento estatístico de largura de banda;
- Suporta engenharia de tráfego do *MPLS*;
- Trabalha com mecanismos de policiamento de tráfego;
- Implementa o *Congestion Avoidance*;
- Possibilita a implementação de *QoS* no núcleo da rede;
- Não suporta protocolos de roteamento *IP*.

5.4.3. Placa *ISA Ethernet*

A placa *ISA Ethernet* permite agregar e transportar tráfego *Metro Ethernet* sobre uma rede *SDH*. Na arquitetura de rede proposta esta placa está no nível de distribuição da rede. Suas características se assemelham a *ISA PREA*, exceto no quesito *MPLS, QoS* e suporte a conexão multiponto. Esta placa não oferece suporte ao *MPLS e QoS.* Na Tabela 9 – Resumo de funcionalidades da placa *ISA Ethernet*. [7] tem-se as facilidades suportadas pelo equipamento.

Funcionalidade	Situação	Observação
Compartilhamento de Largura de Banda do SDH	Possui	Entre portas/serviços Metro Ethernet
Agregação de Tráfego	Possui	
Gerenciamento de Tráfego	Não Possui	
Suporte a conexões ponto a ponte	Possui	
Suporte a conexões ponto a multiponto	Não Possui	
Suporte a conexões multiponto	Não Possui	
Classificação de pacotes	Não Possui	
Escalonamento de pacotes	Não Possui	
Mapeamento de interfaces físicas	Possui	IEEE 802.3, IEEE 802.3u, IEEE 802.3x, Ethernet over SDH
Policiamento de tráfego	Não Possui	
Níveis de SLA	Não Possui	
Congestion Avoidance	Possui	Baseado em IEEE802.3x
Ethernet/GFP/Ethernet/SDH	Possui	
Ethernet/MPLS	Não Possui	
Ethernet/MPLS/MPLS	Não Possui	
Ethernet/MPLS/MPLS/PPP/HDLC/SDH	Não Possui	
LP Ethernet	Possui	
LP virtual Ethernet	Possui	Apenas ligações ponto a ponto
Multiplexagem de Ethernet em LP virtual	Possui	Apenas ligações ponto a ponto
LAN virtual Ethernet	Não Possui	
Acesso em Banda Larga	Possui	
Roteamento MPLS	Não Possui	

OSPF	Não possui	
RIP	Não possui	
IS-IS	Não possui	
BGP	Não possui	
Suporte a RSVP-TE	Não Possui	
Sinalização LPD	Não Possui	Para troca de informações de rótulos MPLS
Sinalização CR-LDP	Não possui	

Tabela 9 – Resumo de funcionalidades da placa *ISA Ethernet*. [7]

Em relação a placa *ISA Ethernet* pode-se concluir que:

● Implementa uma pilha *Metro Ethernet* (*Ethernet/GFP/SDH*);

● Possibilita o compartilhamento estatístico de largura de banda;

● Permite apenas ligações *Lan-to-LAN*;

● Realiza controle de fluxo através do protocolo IEEE802.3x. A placa envia informações de contenção para o emissor;

● Não suporta protocolos de roteamento *IP* e *QoS*.

5.4.4. Sistema *SDH 1660SM*

O equipamento 1660SM é um multiplexador *SDH* e é responsável pela infra-estrutura SDH desta rede. A topologia da rede possui core *MPLS/SDH* composto pelos equipamentos: placa *ISA PREA*, *Omniswitch* 7700 e Multiplexador 1660SM. O transporte dos quadros no núcleo da rede utiliza a infra-estrutura física *SDH*. As placas *ISA PREA* e *ISA Ethernet* são subsistemas do 1660SM e estas são acopladas em bastidores de placas auxiliares deste equipamento. O 1660SM possui capacidade de transmissão de até 10Gbps (STM64), mas o estudo de caso está configurado com capacidade máxima STM-4 (622Mbps) [7].

5.4.5. Laboratório com testes das funcionalidades

Esta parte tem por objetivo testar em laboratório e utilizando-se os equipamentos reais, questões consideradas relevantes no estudo teórico feito anteriormente nesta dissertação. O intuito deste laboratório é validar algumas características técnicas dos equipamentos utilizados na topologia.

O laboratório do teste contém três *Omniswitch* 7700, três placas *ISA Ethernet*, três placas *ISA PREA, MUX SDH 1660SM, seis switches Cisco e gerador de tráfego InterWatch*. Os testes consistem em análise do *QoS* do *OmniSwitch*, *QoS* da placa *ISA PREA* e convergência *OSPF*.

Para fim ilustrativo, tem-se a Figura 30 **– Topologia do laboratório de teste.**com a topologia de rede em que os testes foram realizados.

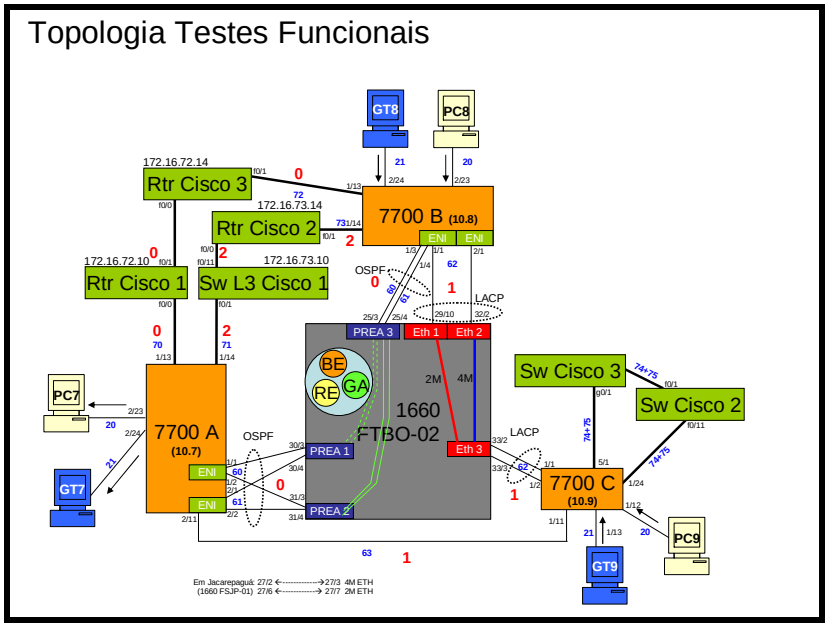


Figura 30 – Topologia do laboratório de teste.

No que tange ao O *Omniswitch,* foi verificado que o equipamento permite quatro níveis de prioridades, configuração de banda máxima e o algoritmo em funcionamento por padrão é o *Strict Priority*. Segundo a referência estudada, o *Omniswitch* suporta estes três algoritmos: *Priority Weighted Round Robin*, *Weighted Round Robin* e *Strict Priority*. A principal vantagem de utilizar o *Weighted Round Robin* é assegurar uma banda mínima para cada grupo de fluxo. Esta banda mínima permite o funcionamento de aplicações menos privilegiadas pelo *QoS.* As configurações de Qualidade de Serviço (*QoS*) do *Omniswitch* devem estar alinhadas com as configurações da placa *ISA*, que são baseadas em *WFQ*, para permitir maior eficiência no escalonamento do tráfego. O *Omniswitch* apresenta alto grau de justiça para tráfegos com configurações similares de *QoS*, e possui software de gerência (*Omnivista*) simples de operar e eficiente. No entanto, este software apenas é utilizado nas configurações dos *Omniswitches* da Series 7000 e 8000. A placa *ISA PREA* não suporta configurações através deste software, conforme já citado no trabalho conceitual, e faz-se necessário a utilização de ferramentas distintas para realizar uma configuração de *QoS* ponta a ponta.

Em relação a placa *ISA PREA*, os resultados apontam que as configurações de *QoS* da placa são estáticas e o algoritmo utilizado é o *Weighted Fair Queuing.* As sobras das bandas não utilizadas, em cada fila, não são reaproveitadas por outras classes de serviço que demandam banda para transmissão.

O tempo de convergência do *OSPF* foi de apenas 18 segundos. Este tempo menor já era esperado devido ao ambiente de teste ser menor e mais simplificado, se comparado com um ambiente de rede de uma empresa de grande porte. Este equipamento funcionando num ambiente típico de produção, a tendência é que o tempo se aproxime de valores entre 30

segundos até 60 segundos. Um intervalo de interrupção como este pode impactar aplicações de *real-time* e aplicações críticas como automação.

Na Tabela 10 – Resumo dos resultados dos testes realizados no Laboratório.é possível verificar um sumário dos resultados observados no teste realizado no laboratório da empresa analisada.

OMNISWITCH (QoS)		Placa ISA PREA(QoS)	
Políticas de QoS	IP/MAC/802.1Q	Políticas de QoS	Necessita receber pacotes já marcados
Marcação de QoS	TOS/DSCP/802.1p	Marcação de QoS	Marcação no EXP MPLS
Números de fila (máx)	4	Números de fila (máx)	3
Configuração de banda máxima	Configuração suportada	Configuração de banda máxima	Configuração de banda estática por fila (1)
Configuração de banda mínima	Configuração não suportada	Configuração de banda mínima	Configuração de banda estática por fila (1)
Filas por porcentagem	Configuração não suportada	Filas por porcentagem	Configuração não suportada
Tamanho de buffer p/ fila	Configuração não suportada	Tamanho de buffer p/ fila	Configuração suportada
(1) A placa *ISA PREA* possui a configuração de 3 perfis de QoS. São eles: banda garantida, banda regulada e banda "best effort".			
Recuperação a falhas			
Recuperação OSPF apenas		18 segundos	
Recuperação LACP (porta física/ sem necessidade de recomposição do grupo LACP)		menos de 1 segundo	

Tabela 10 – Resumo dos resultados dos testes realizados no Laboratório.

5.5. Qualidade de Serviço

O transporte dos quadros *Ethernet* no núcleo da rede é realizado através das placas *ISA PREA*, utilizando o encapsulamento *MPLS* em *VCs SDH*. O *MPLS* é utilizado para gerenciar fluxos de dados de pacotes transportados através de uma infra-estrutura *SDH*. Os quadros são identificados e classificados na borda da rede pelo *Omniswitch* e posteriormente são marcados novamente pela placa *ISA PREA* com rótulos *MPLS* e encaminhados para o *backbone*.

A solução baseada nas placas *ISA* (*Integrated Service Adapter*) *Ethernet* e *ISA PREA* (*Integrated Service Adapter - Packet Ring Edge Aggregator*) permite agregar e transportar tráfego *Metro Ethernet* sobre uma rede *SDH*. Nesta topologia os quadros são multiplexados estatisticamente e priorizados com base na *CoS* (*Class of Service*). O *CoS* é inserido pelos *Omniswitch* de borda, através de critérios pré-estabelecidos, funcionando assim como marcador de *QoS*. Toda rede posteriormente utiliza esta marcação para priorizar pacotes e respeitar critérios de desempenho essenciais para determinados serviços. Como exemplo, pode-se citar serviços de voz sobre IP, vídeo e sinais de automação.

A placa *ISA PREA* permite três perfis de *QoS*: BE (*Best Effort*), Min-BW (banda regulada) e BW (banda garantida). O *HOL* (*Head of Line*) é usado para tráfego garantido e WFQ (*Weighed Fair Queuing*) é usado para o tráfego regular e Best Effort. Por analogia ao ATM, podem-se definir os perfis de tráfego como: Regulado (VBR), Garantido (CBR) e *Best Effort* (UBR). A Figura 31 - Perfis de QoS suportados pela placa *ISA PREA*. [7] ilustra os perfis de *QoS* existentes na solução.

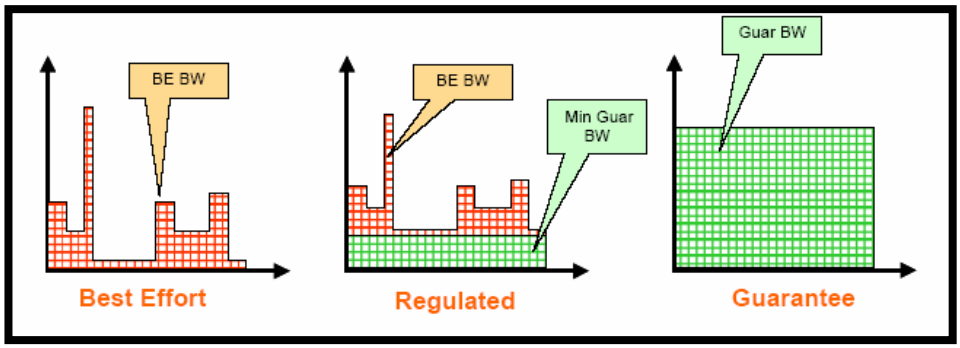


Figura 31 - Perfis de QoS suportados pela placa *ISA PREA*. [7]

O *HOL* é um algoritmo similar ao *PQ* (*Priority Queuing*). Suas principais vantagens são a baixa carga computacional e previsibilidade (atraso é determinado pelo tamanho da fila). A principal desvantagem é o desequilíbrio entre fluxos de prioridades diferentes [7].

O *WFQ* é um algoritmo que assegura porcentagem da banda para cada fila. Sua principal vantagem é assegurar uma banda mínima para cada grupo de fluxo. Esta banda mínima possibilita o funcionamento de aplicações com restrições, como, por exemplo, aplicações com requisitos específicos de banda [38]. A principal desvantagem é a complexidade do algoritmo.

Como já foi citado anteriormente, a placa *ISA PREA* funciona com dois tipos de caminhos: *Outer Tunnel* e *Inner Tunnel*. O *Outer Tunnel* tem a característica de ser um agregador de *Inner Tunnels* e ser diretamente mapeado em *VCs SDH*. O *Outer Tunnel* é responsável pelo *QoS* em toda rede *MPLS*. A cada salto de um pacote *MPLS* na rede, a configuração de QoS do *Outer* é observada. No tocante as classes de serviço, a placa *ISA PREA* oferece suporte apenas ao padrão 802.1p. Para funcionamento do *QoS* no núcleo da rede é necessário que o *Omniswitch* realize a marcação de *QoS* (802.1p) dos pacotes. A placa utiliza o algoritmo de descarte de pacote *WRED (Weighed – Random Early Discarding*) [7].

Na Figura 32 – Exemplo de configuração de *QoS* na placa *ISA PREA*[7]. verifica-se os perfis de *QoS* suportado pela placa *ISA PREA*.

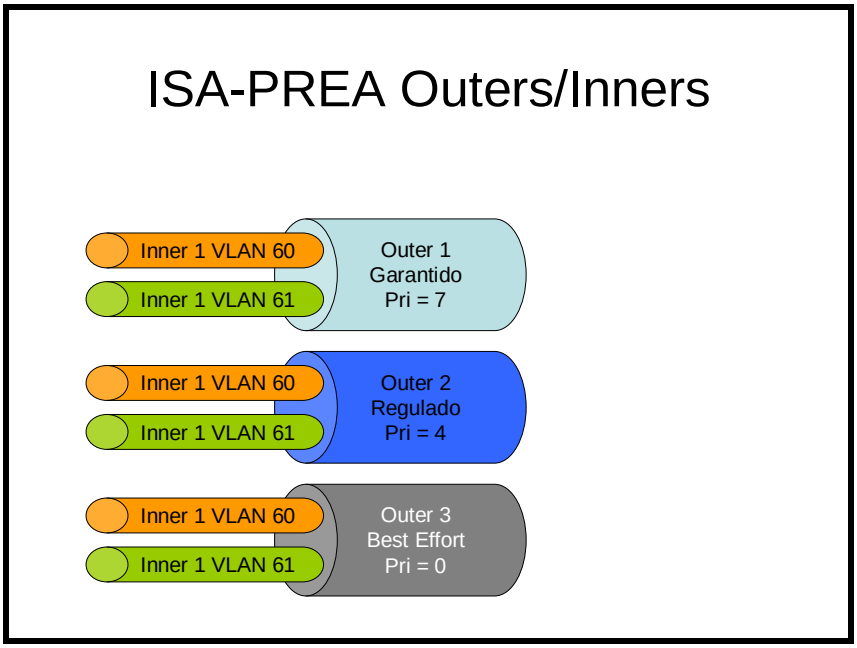


Figura 32 – Exemplo de configuração de *QoS* na placa *ISA PREA*[7].

O *Omniswitch* permite a configuração de políticas de *QoS* para tráfegos de saída e permite também a classificação de tráfego. Os fluxos que atendem a uma dada política são colocados em uma fila correspondente, enquanto os demais são colocados nas filas default "*Best Effort*" [8].

A acomodação de diversas aplicações em apenas três perfis de tráfego, número de filas máximas suportadas pelos equipamentos existentes na solução, não é o recomendado neste contexto. O ajuste fino, tão importante para as aplicações críticas a latência ou vazão, não é factível; assim sendo, é recomendada a utilização de um número maior de filas que permitirá uma configuração apurada para cada tipo de serviço. Outro ponto crítico é incompatibilidade entre os sistemas de gerência da *ISA PREA* e do *Omniswitch*. Para aprovisionamento e medição do *QoS* é importante que se tenha uma leitura fim a fim da rede.

Para solucionar esta questão outras arquiteturas foram analisadas. Como por exemplo, a eliminação das placas *ISA PREA*. O Omniswitch não possui interfaces seriais, não podendo assim se ligar diretamente ao *MUX SDH*. O uso da família de placa *ISA* é necessário principalmente para adaptação de interface.

A substituição da placa *ISA PREA* pela placa *ISA Ethernet* no *backbone* apresenta-se como uma alternativa. Entretanto esta substituição traria as seguintes conseqüências:

● A falta de suporte a ligação multiponto traz um grau menor de flexibilidade para rede, já que toda ligação será diretamente mapeada em um VC de origem e destino determinado. A placa *ISA Ethernet* suporta apenas ligações *LAN-to-LAN*. Em virtude dessa característica, o administrador de rede deve criar diversas configurações de conexão *SDH* para ligar sites distantes. As ligações entre sites que atravessam mais de um *MUX SDH* necessitam de configurações especificas site a site. Essas configurações exigem esforço mão-de-obra e maior grau de risco operacional (visto a maior intervenção humana nesta operação). Resumidamente, esta placa não permite a utilização de múltiplas ligações entre sites num mesmo *VC SDH*.

● Menor capacidade de encaminhamento. A placa *ISA PREA* possui uma capacidade de comutação de 1,2Gbps enquanto que a placa *ISA Ethernet* possui uma capacidade de 622Mbps.

● As operações como marcação, *shaping* e priorização não são realizadas por este hardware. A placa não possui suporte a *QoS*.

A melhor opção para este caso é a utilização da placa *ISA ES*. A placa faz parte do conjunto de soluções do fornecedor para *Metro Ethernet*. A placa é suportada pelo conjunto

SDH (*MUX SDH 1660 SM*) e permite comutação de quadros *Ethernet* baseada em endereço MAC e IEEE 802.1q. Esta placa permite redes virtuais *Ethernet* (ligações Multipontos entre sites *Ethernet*), suporta funcionalidades de *QoS* e permite agregação de diferentes fluxos *Ethernet*.

As capacidades de comutação da placa *ISA ES* é similar a *ISA PREA*, igual a 1,2Gbps, não havendo assim queda de desempenho. Esta placa é mais adequada para substituir a placa *ISA PREA* do que a *ISA Ethernet*. Entretanto sua adoção traz como conseqüência a perda do suporte à engenharia de tráfego para a infra-estrutura planejada. Esta facilidade é provida através do nível de controle *MPLS*, não existente nesta placa. O uso da placa *ISA Ethernet* também implica na perda da engenharia de tráfego.

Na placa *ISA ES* todo controle de tráfego do *backbone* é provido através do protocolo *Spanning Tree Protocol* (*Ethernet*). O protocolo *STP* não utiliza métricas como banda e salto, tal como os protocolos *IGP*, basicamente cada *switch* processa o *STP* com base em informações recebidas de switches vizinhos [39]. O protocolo *STP* não oferece engenharia de tráfego e não observa métricas de desempenho na escolha dos nós da árvore. Este protocolo não evita problemas de congestionamento e não permite uma distribuição igualitária dos tráfegos entre os recursos existentes da rede. A placa *ISA ES* oferece também apenas três classes de *QoS*.

A substituição da placa *ISA PREA* pela *ISA ES* é desaconselhável nesse contexto, principalmente devido à engenharia de tráfego, que não é suportada pela placa *ISA ES*.

Utilizando o conjunto *Omniswitch/ placa ISA PREA/ Mux SDH*, arquitetura proposta pelo fornecedor, podem ser realizados ensaios para verificação do suporte ao dobro de filas existe (de três para seis filas) utilizando a infra-estrutura atual. São verificadas duas opções possíveis.

● A primeira opção utiliza o mecanismo de engenharia de tráfego proposto nesta dissertação que preconiza a duplicidade de caminho via engenharia de tráfego para prover seis classes. A Figura 33 – Primeira opção de solução proposta para o QoS. ilustra esta opção. A topologia adotada nessa seção é a composta por VC-4.

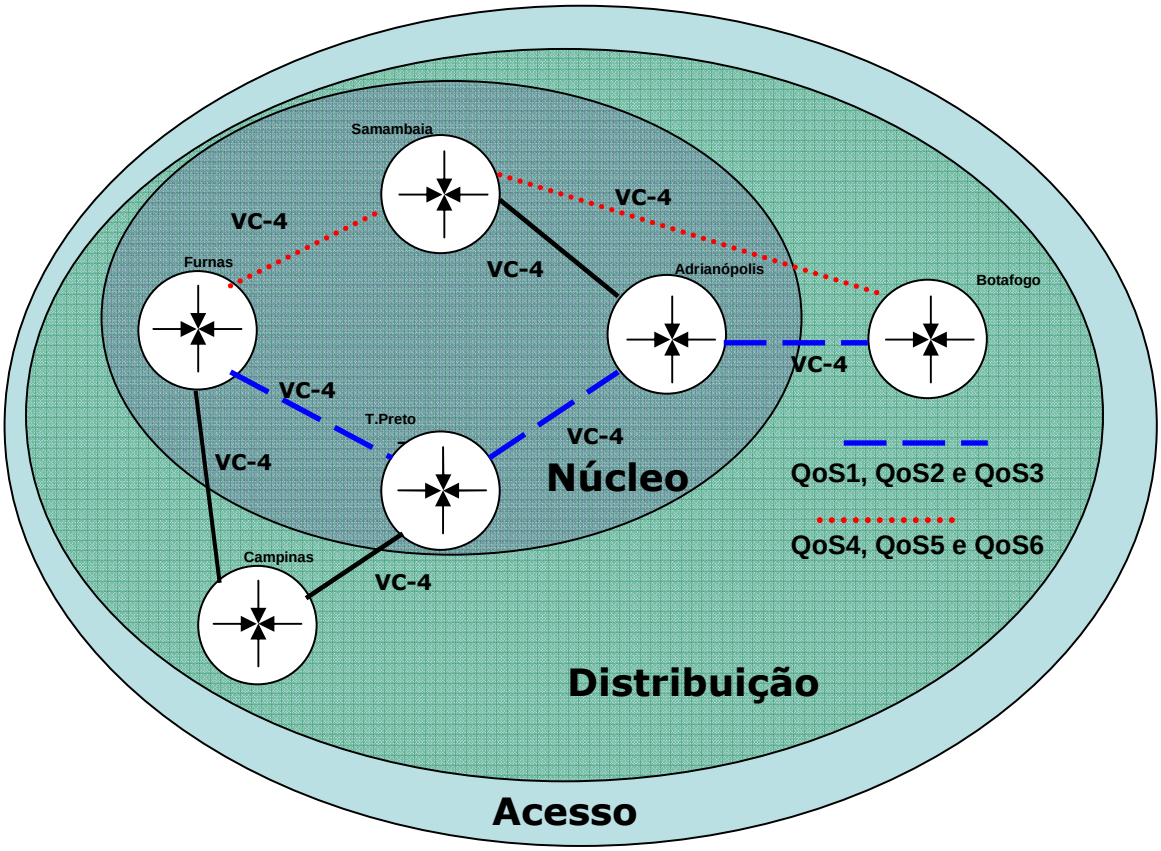


Figura 33 – Primeira opção de solução proposta para o QoS.

O caminho tracejado longo passa pelos site Furnas, Tijuco Preto, Adrianópolis e Botafogo. Este caminho disponibiliza três classes de QoS (banda garantida, banda regulada e

melhor esforço). Já o caminho pontilhado curto compreende os nós Furnas, Samambaia, Adrianópolis e Botafogo. Este caminho disponibiliza também três classes de QoS análogo ao caminho tracejado. Somando os dois caminhos têm-se seis classes.

Entretanto questões operacionais trazem alto grau de complexidade para implantação da primeira opção. Uma questão crítica é a ocorrência de falha em um dos caminhos. Os seis serviços utilizam um mesmo caminho configurado para suportar apenas três classes. Esta ocorrência aumenta a possibilidade de descartes de quadros, e principalmente, descaracterizando as condições iniciais de qualidade de serviços planejadas.

Outro ponto crítico é a segmentação do tráfego respeitando as configurações de *QoS*. As configurações de caminhos são estáticas e utilizam o endereço *IP* para determinação de caminho. Para permitir esta configuração os endereços *IPs* dos *endpoints* devem ser distintos. Por exemplo, os endereços dos *endpoints* da classe de serviço 2 (serviço *SAP*) devem ser diferentes da classe dos *endpoints* da classe de serviço 5 (correio eletrônico). Nas redes atuais esta configuração é muito complexa porque um mesmo terminal utiliza diversos tipos de serviços. A dissertação recomenda a utilização de balanceamento de tráfego através do *OSPF*, com isso, fica impossível utilizar está segmentação porque a escolha de caminho é aleatória.

● A segunda opção é prover a duplicação dos caminhos no núcleo da rede através da aquisição de novos enlaces físicos. A configuração do *backbone* sugerida estabelece quatros caminhos (dois por direção), e com isso, é possível a criação de seis classes de serviços. A Figura 34 **– Segunda opção de solução proposta para o QoS.** apresenta a topologia dessa opção.

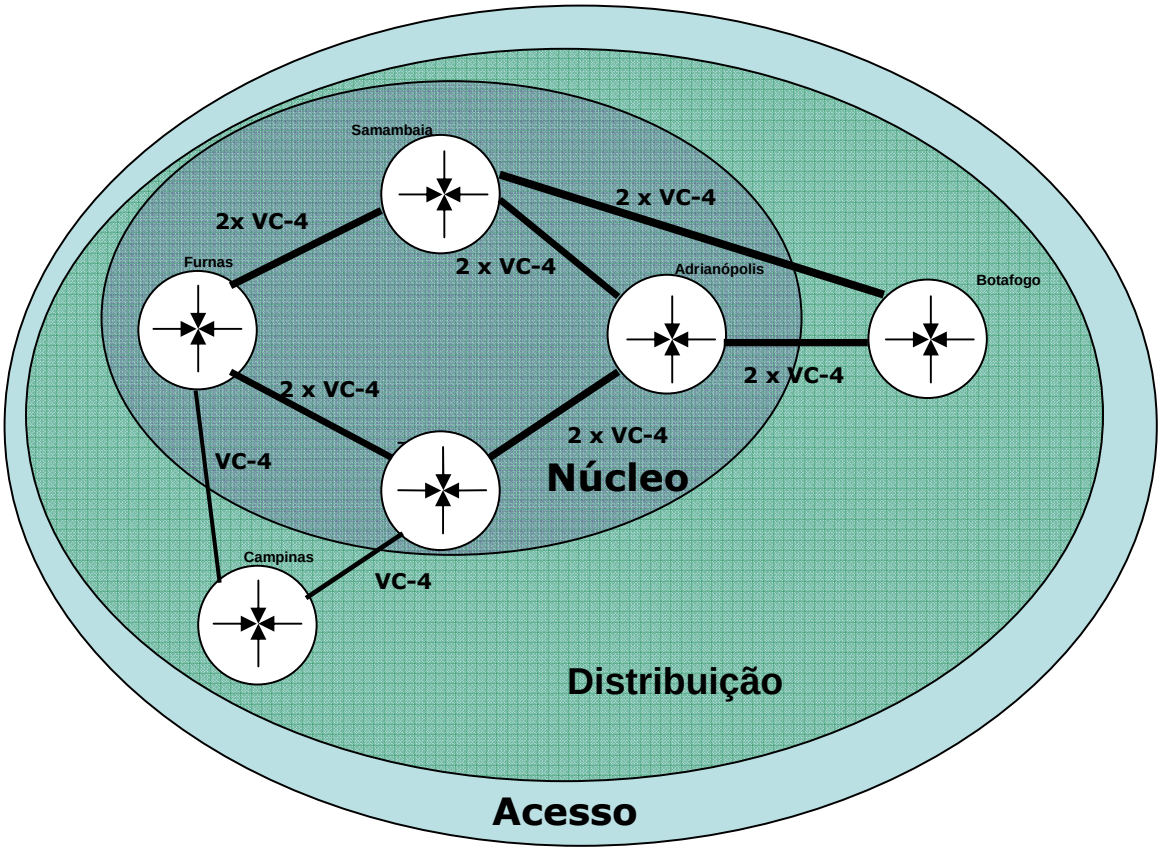


Figura 34 – Segunda opção de solução proposta para o QoS.

A segunda opção demanda a aquisição de novas placas *ISA PREA* e contratação de novos enlaces. Para implantação desta opção faz-se necessária a aquisição de novas cinco placas nas seguintes localidades (Furnas, Samambaia, Botafogo, Adrianópolis e Tijuco Preto) e a contratação de seis enlaces VC-4 (139,2Mbps). As aquisições de placas são necessárias para instalação dos novos enlaces. Nesta topologia cada caminho possui dois VC-4 e três classes são configuradas para cada VC. Assim, cada direção do anel possibilita a existência de seis classes de serviços, visto que cada caminho possui dois VCs. Nessa configuração a ocorrência de falha em um dos caminhos não traz problema porque a classe 1 (por exemplo) existente no primeiro caminho também existe no segundo caminho. Todavia, a questão de segmentação também é crítica nesta solução.

Para escolha entre os dois VCs o mecanismo de controle continua sendo o endereçamento *IP*. A segmentação só é possível se os serviços forem utilizados por terminais diferentes (endereços *IP* diferentes). A opção de caminho é resolvida pelo protocolo *OSPF* que utiliza o endereçamento *IP* como referência. Para a segmentação funcionar o mecanismo de controle deve, por exemplo, ser porta *TCP* ou *UDP*. Mas a solução atual não permite esta facilidade.

Ambas as soluções só são viáveis se dentro da topologia os terminais acessarem diferentes serviços. Dessa forma é possível segmentar endereços IPs em diferentes caminhos e direções. Comumente, essa configuração é possível pelo lado dos servidores, visto que cada serviço utiliza um servidor dedicado para seu funcionamento. Entretanto, pelo prisma do cliente esta configuração não é difícil de ser implementada. Os clientes acessam diferentes aplicações e serviços, como por exemplo, o *SAP* e correio eletrônico, de um mesmo terminal simultaneamente.

Em virtude da complexidade apresentada pelas opções testadas, que prospectam a adoção de mais de três filas de QoS na rede estudada, é sugerida a utilização da topologia proposta nesta dissertação com os três níveis de *QoS* padrões. Baseado neste aspecto, a disposição de serviço por classe é:

- BW (banda garantida) – Aplicações de tempo real (Voz sobre IP, vídeo conferência e Web TV);
- Min-BW (banda regulada) – Aplicações ligadas ao negócio (*SAP*, Correio Eletrônico, software de gestão administrativa e negócio);
- BE (Best Effort) – Aplicações não cooperativas (Internet, *Intranet*, *backup* de servidores, acesso a outros programas e FTP).

Para evitar problemas de dimensionamento inadequado, as configurações das filas devem ser em caráter de "*super-aprovisionado*". Esta prática aumenta o custo operacional, todavia atenua a limitação de três filas imposta pela solução. Para verificar a condição atual desta rede, é descrita a seguir a banda nominal disponível por classes na rede, considerando a relação de 30% para banda garantida, 40% para banda regulada e 30% para melhor esforço.

A banda disponível no backbone da rede para a classe garantida é 41,7Mbps. Esta banda permite 108 sessões de videoconferências simultâneas funcionando a 386Kbps ou 1390 sessões simultâneas de *Voip* utilizando o protocolo G729.

A banda disponível para classe regulada é 56Mbps. Esta banda permite 1400 sessões simultâneas do aplicativo *SAP*. Uma sessão simples do aplicativo *SAP* com interface *Citrix* utiliza uma banda máxima de aproximadamente cinco KiloBytes por segundo (ou 40Kbps) [13].

A banda disponível no backbone para classe de melhor esforço é 41,7Mbps.

Na Tabela 11 **- Disposição de Banda por Fila em cada localidade.** é apresentada a disposição de banda por localidade sugerida nesta dissertação:

Localidade	Garantido	Regulado	Melhor Esforço
Zona Samambaia			
Brasília	**1Mbps**	**2Mbps**	**1Mbps**
Corumbá	**1Mbps**	**2Mbps**	**1Mbps**
Gurupi	**1Mbps**	**2Mbps**	**1Mbps**
Itumbiara	**1Mbps**	**2Mbps**	**1Mbps**
Samambaia	**3Mbps**	**4Mbps**	**3Mbps**
Zona Furnas			
Furnas	**3Mbps**	**4Mbps**	**3Mbps**

Itutinga	**1Mbps**	**2Mbps**	**1Mbps**
Marimbondo	**1Mbps**	**2Mbps**	**1Mbps**
P. Colômbia	**1Mbps**	**2Mbps**	**1Mbps**
Poços	**1Mbps**	**2Mbps**	**1Mbps**
Zona Tijuco Preto			
Foz de Iguaçu	**1Mbps**	**2Mbps**	**1Mbps**
Guarulhos	**1Mbps**	**2Mbps**	**1Mbps**
Mogi	**1Mbps**	**2Mbps**	**1Mbps**
Tijuco Preto	**4Mbps**	**5Mbps**	**4Mbps**
Zona Adrianópolis			
Adrianópolis	**3Mbps**	**4Mbps**	**3Mbps**
C. Paulista	**1Mbps**	**2Mbps**	**1Mbps**
Grajaú	**1,5Mbps**	**2Mbps**	**1,5Mbps**
Imbariê	**1Mbps**	**2Mbps**	**1Mbps**
Jacarepaguá	**1,5Mbps**	**2Mbps**	**1,5Mbps**
Santa Cruz	**1Mbps**	**2Mbps**	**1Mbps**
Zona Botafogo			
Botafogo	**6Mbps**	**8Mbps**	**6Mbps**

Tabela 11 - Disposição de Banda por Fila em cada localidade.

Todas as localidades receberam bandas acima de 4Mbps e classes de qualidade de serviço superiores a 1Mbps. Para exemplificação das condições funcionais mínimas do estudo de caso, o site Santa Cruz possui 1Mbps de banda para as classes garantido/melhor esforço e 2Mbps para regulado. Nesta localidade é possível ocorrer simultaneamente duas sessões de videoconferência a 384Kbps, sete canais de voz sobre IP, cinqüenta sessões *SAPs* e treze usuários internet (*download* à 10KBps). As classes: Regulado e Melhor Esforço, utilizam recursos excedentes da rede, apenas a classe Garantido obedece às restrições impostas pela configuração. A topologia proposta nesta dissertação permite a criação de classes com abundância de bandas disponíveis mediante as condições de tráfego atuais da rede legada (análise da infra-estrutura existente). Na rede atual os enlaces de borda possuem banda de 2Mbps (na maioria das localidades) e o backbone é composto por enlaces E3 (34Mbps).

A dissertação propõe o uso da engenharia de trafego que permite dobrar as bandas estipuladas acima em condições normais da rede (sem ocorrência de falha em enlaces e equipamentos). A banda disponível para os tráfegos garantidos sobe para 93Mbps no núcleo da rede.

Para o perfeito funcionamento desta topologia é importante o controle de tráfego entrante. As ferramentas de policiamento de tráfego existentes no *Omniswitches* precisam ser utilizadas (facilidade testada com êxito no AnexoII). Os *Omniswitches* marcam os quadros de entrada através de critérios configurados e são responsáveis pelo escalonamento de quadros nas bordas da rede. Os fluxos que atendem a uma dada política são colocados em uma fila correspondente, enquanto os demais são colocados nas filas default "*Best Effort*". O escalonamento realizado nas extremidades é mais crítico porque a banda dos enlaces é inferior a do backbone, principalmente quando os enlaces de contingência são utilizados.

Uma outra possibilidade é o tráfego automação. Este tráfego é de suma importância para o negócio da empresa e demanda disponibilidade e qualidade diferenciada. Existem duas opções para adequação desse tráfego: a primeira opção é acomodar esse tráfego numa quarta fila (configurada apenas no Omniswitch) e no núcleo seria configurado na fila de banda garantida no núcleo da rede. Para tal é necessário "super-aprovisionar" a classe garantida e utilizar uma acurada configuração de banda máxima na borda para os demais tráfegos existentes na fila. A segunda opção é mapear o tráfego direto nos *VC SDH* sem passar pela infra-estrutura *MPLS/SDH*.

Outro ponto importante é o sistema de aprovisionamento de *QoS*. Os sistemas de gerência da *ISA PREA* e do *Omniswitch* são diferentes e não interagem entre si [7] [8]. Para

aprovisionamento e medição do *QoS* é importante que se tenha uma visão integrada da rede. A troca dos equipamentos do núcleo de rede traz uma maior facilidade neste quesito. Ao invés de aprovisionar *QoS* em dois equipamentos distintos (*ISA PREA* e *Omniswitch*), só é necessária a configuração em apenas um equipamento. Consta no Anexo I um estudo sobre os equipamentos de mercado e é sugerido o Alcatel 7750 para utilização nesta infra-estrutura. Entretanto a troca de equipamento não é uma opção viável.

5.6. Gerência e segurança

5.6.1. Gerência

A placa *ISA PREA* oferece suporte ao protocolo *SNMP*, mas para ativação desta facilidade, faz-se necessário configurar túneis dentro do equipamento *SDH*. O sistema *SDH* está baseado na arquitetura *TMN* (*Telecommunications Management Network*) OSI, e esta arquitetura não suporta os protocolos de gerência IP (SNMP, Telnet e ICMP). A configuração do túnel permite o funcionamento do *SNMP* e outras facilidades.

Os equipamentos *OmniSwitch* 7700 possibilitam o monitoramento e gerência através dos protocolos *SNMP* e *RMON*. Através desses protocolos, outros sistemas de gerência podem ser utilizados para monitoramento (o *HP OpenView*, por exemplo). Para outros sistemas de gerência monitorar o *Omniswitch*, é necessário carregar a *MIB* do equipamento na gerência.

A topologia não disponibiliza um sistema único para gerencia de falha, desempenho e configuração. Ambos os equipamentos possuem softwares de gerência proprietários do

mesmo fornecedor, mas não são compatíveis. O sistema de gerência do *Omniswitch* é o *OmniVista* e da placa *ISA PREA* é o *Alcatel 1354 Brodband Manager*. A dissertação propõe um sistema integrado de falha que opere com *Traps SNMPs* (tecnologia compatível com as duas plataformas).

5.6.2. Segurança

A placa *ISA PREA* não implementa lista de controle de acesso (*ACLs*) nas camadas 3 e 4 do modelo OSI. O *Omniswitch* suporta listas de controle de acesso baseadas em endereço *IP* e portas *TCP* e *UDP*. Toda vez que se desejar filtrar acesso tomando com base itens referentes a camada 3 ou 4, faz-se necessário colocar um *Omniswitch* antes da placa *ISA PREA*. Resumidamente, se forem criadas políticas de segurança baseadas em critérios da camada 3 e 4 do modelo OSI, não é possível injetar tráfegos de usuários direto na placa *ISA PREA*. Para atenuar esta questão faz-se necessário colocar todas as políticas de restrições nos *Omniswitch* de borda.

Em relação a autenticação, o *Omniswitch* permite autenticação através dos padrões *RADIUS* e *LDAP*, entretanto, a placa *ISA PREA* utiliza um padrão proprietário de autenticação. Consequentemente, os administradores da rede precisam administrar dois sistemas distintos de autenticação. A administração de dois bancos de autenticação acarreta maior esforço de mão-de-obra e mais complexidade de operação.

Em relação a configuração de autenticação do *OSPF*, propõe-se a habilitação do *MD5* nas interfaces *OSPF* para aumentar a segurança do protocolo de roteamento, evitando assim ataques ao protocolo de roteamento [22].

5.6.3. *Virtual Private Network*

Os equipamentos existentes permitem apenas *VPN L2 MPLS* (modelo *Martini Draft*). O túnel da solução, como do Martini, pode ser estabelecido usando *LDP* entre dois pontos diretamente conectados [15]. A solução insere o conceito de *MPLS over SONET*, não registrada no padrão original Martini, mas comuns em implementações de fornecedores como Cisco e Alcatel [10] [7].

O equipamento *Omniswitch* não suporta *VPN*, ficando a cargo da placa *ISA PREA* este trabalho. A placa *ISA PREA* implementa apenas *VPN* na camada 2 [7] [8].

A solução estudada não suporta a arquitetura padrão *VPLS* (*Virtual Private LAN Service*). A arquitetura de equipamentos de Borda (PE) e equipamentos de Núcleo (P), típica da configuração não é suportada pela solução.

5.7. Estudo comparativo e avaliação final

Nesta dissertação é sugerida uma nova topologia e a configuração da camada *MPLS* na rede. O intuito desta nova configuração é aumentar o grau de segmentação da rede, escalabilidade e maior desempenho.

Para trazer uma maior flexibilidade e desempenho para os sites de núcleo, foi redesenhada a topologia com adição de novos enlaces e aumento de banda dos enlaces já existentes. A proposta desta topologia é criar um núcleo que recebe a grande massa de dados.

Algumas localidades possuem enlaces ampliados e novos enlaces são adicionados. As topologias foram testadas e as configurações propostas pela dissertação apresentam melhores resultados do que a proposta pelo fornecedor. Os resultados apontam que as topologias propostas nessa dissertação (tanto a topologia com VC-3 quanto à com VC-4) apresentam ganhos de escalabilidade e disponibilidade. Na Tabela 12 - Resumo dos resultados das simulações.é apresentado um breve sumário dos resultados observados.

Itens	**Topologias**		
Itens analisados	**Topologia original do fornecedor**	**Topologia com links propostos (VC-3)**	**Topologia com links propostos (VC-4)**
Teste de topologia	Baixo grau de escalabilidade e menor segurança em caso de falha	Grau de escalabilidade médio e maior segurança em caso de falha	Alto escalabilidade e maior segurança em caso de falha
Engenharia de tráfego	Baixa eficiência da engenharia de tráfego e dificuldade na configuração	Alta eficiência da engenharia de tráfego e facilidade na configuração	Alta eficiência da engenharia de tráfego e facilidade na configuração
Recuperação a falhas	Tempo de convergência depende do *OSPF* e menores opções de caminho	Tempo de convergência depende do *OSPF e* mais opções de caminho (principalmente caminho críticos)	Tempo de convergência depende do *OSPF* e mais opções de caminho (principalmente caminho críticos)

Tabela 12 - Resumo dos resultados das simulações.

É importante observar que o uso da engenharia de tráfego com a inserção dos *LSPs* estáticos, disponíveis através de ferramentas do *MPLS*, traz benefícios para a rede. As configurações de caminhos (*LSP MPLS*) ao longo da rede permitem uma melhor utilização de *enlaces* e de equipamentos. O uso da engenharia de tráfego permite diminuição da ociosidade de determinados enlaces e uma maior homogeneidade na utilização dos recursos da rede.

No que tange ao tempo de recuperação a falhas da rede, as topologias apresentam um quadro similar. O intervalo de convergência da rede, em caso de falha, nas redes baseadas em *IP* e baseadas em *MPLS IP* foram de 50 segundos. A explicação para esta similaridade é que o protocolo responsável pela convergência em ambos os casos é o *OSPF*. Outra observação importante é que as topologias propostas na dissertação apresentam mais opções de caminho em caso de falha.

Um outro ponto importante é a importância do *QoS* para rede em questão. A porta remota da placa *ISA PREA* possui um *backplane* menor do que a porta local, havendo assim a possibilidade de descartes no processo de encaminhamento de quadro. Para suporte a serviços diferenciados faz-se necessário a utilização de ferramentas de *QoS* para priorização e tratamento diferenciados para tráfego de tempo real e tráfegos de maior interesse da empresa.

No próximo capítulo é apresentada a conclusão da dissertação.

6. Conclusão

Os principais ingredientes para confecção de um projeto de rede incluem conhecimento técnico, objetivos claros sobre o que se deseja alcançar, planejamento para execução de todas as etapas envolvidas e foco nas necessidades do cliente. A construção de uma abordagem pragmática facilitou a reunião destas características. A metodologia proposta neste trabalho demonstrou-se eficiente no estudo de caso e facilitou o processo de proposição de melhorias para a infra-estrutura.

A aplicação da abordagem pragmática, apresentada na dissertação na rede em estudo, gerou como resultado a proposição de uma nova topologia, com o intuito de trazer uma maior flexibilidade e desempenho para os sites de núcleo. A topologia atual não possui uma segmentação perfeita entre os níveis da rede e os equipamentos de núcleo possuem vazão menor do que a recomendada. Isso dificulta a realização de projetos de expansão da rede, assim como novos aprovisionamentos de serviços. A análise dos resultados das simulações apontou a topologia recomendada nesta dissertação como a melhor opção para a rede utilizada no estudo de caso, se comparada com a topologia sugerida pelo fornecedor. A nova topologia demonstrou ser mais eficiente para o funcionamento da engenharia de tráfego e redundância a falhas.

O uso da engenharia de tráfego na topologia proposta permite a configuração dos caminhos dos tráfegos ao longo da rede. Esta facilidade permite a diminuição da ociosidade de determinados enlaces e divide os fluxos de tráfego, permitindo assim uma utilização mais

homogênea dos recursos disponíveis da rede. Além de configurar os caminhos utilizados na topologia, é possível reservar recursos de equipamento e enlaces.

No aspecto convergência de rede, as simulações utilizando as tecnologias adotadas na topologia atual da rede apontam para um intervalo de convergência da rede, nas redes baseadas em *IP* e baseadas em *MPLS/IP*, em torno de 50 segundos. O protocolo responsável pela convergência em ambos os casos foi o *OSPF* e este tempo está diretamente ligado a convergência deste protocolo. Se utilizada a topologia proposta após a aplicação da abordagem pragmática apresentada, esta convergência se dá em 2 segundos tomando-se por base a utilização do protocolo Fast Reroute *MPLS*.

As conclusões apresentadas atestam a viabilidade da abordagem pragmática proposta, assim como os resultados do estudo de caso demonstram que, com tal abordagem torna-se possível avaliar diferentes cenários tcnológicos e gerar comparações objetivas entre os mesmos.

6.1. Principais contribuições

A dissertação apresentou um modelo analítico para projetos de rede eficiente. O modelo foi testado com sucesso no estudo de caso e poderá ser utilizados por administradores, projetistas e engenheiros de rede em atividades típicas de análise de rede.

As principais contribuições deste trabalho foram: apresentar uma metodologia customizada para análise de projetos de redes convergentes para analistas e administradores

de rede, identificar os benefícios do *MPLS* numa rede real e trazer melhorias operacionais e funcionais para uma rede operativa.

6.2. Trabalhos futuros

No tocante ao estabelecimento de caminhos comutados por rótulos (*LSP MPLS*), apesar de existirem propostas de solução para o problema, não existe uma padronização que aprofunde e detalhe o funcionamento desses mecanismos, sendo que algumas dessas alternativas não são compatíveis com todos os protocolos de roteamento existentes. Devido a esse fato, sugere-se como possibilidade de trabalho futuro a criação de caminhos dinâmicos otimizados tomando como base o contexto situacional da rede.

No estudo de caso, as configurações de caminhos *MPLS* (*LSP*) são feitas estaticamente. Esta circunstância traz dificuldade de implementação, perda de desempenho e recuperação a falhas. Buscando solucionar tais limitações, a sugestão é propor um algoritmo para estabelecimento de *LSPs* baseado nas informações de gerência do sistema *MPLS*, detalhando um conjunto de passos para se construir caminhos comutados por rótulo de forma dinâmica e controlada.

7. Bibliografia

[1] A. H. Asgari, S. Van den Berghe, C. Jacquenet, P. Trimintzios, R. Egan,D. Goderis, L. Georgiadis, E. Mykoniati, P. Georgatsos, D. Griffin, "**A Monitoring and Measurement Architecture for Traffic Engineered IP Networks**", (www.ist-tequila.org), IST2001, Set, 2001.

[2] J. Ash, M. Girish, E. Gray, B. Jamoussi, G. Wright, "**RFC 3213 - Applicability Statement for CR-LDP**", site: www.ietf.org, Jan, 2002.

[3] P. Aukia, M. Kodialam, P.V. Koppol, T.V. Lakshman, H.Sarin, B. Suter, "**Rates: A Server for MPLS Traffic Enginering**", IEEE Network Magazine, pages 34–41, Mar, 2000.

[4] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, "**RFC 2702 - Requirements for Traffic Engineering Over MPLS**", site: www.ietf.org, Set, 1999.

[5] T. Bayle, R. Aibara, K. Nishimura, "**Performance measurements of MPLS traffic engineering and QoS**", Proceedings of the 11th Annual Internet Society Conference, INET2001, Stockholm, Sweden, Jun, 2001.

[6] **Site home.agilent.com**, http://www.home.agilent.com/agilent/facet.jspx?kt=1&cc=US&lc=eng&k=packet+over+sonet, acessado em Set,2006.

[7] **Site alcatel.com**, http://www1.alcatel-lucent.com/products/productsummary.jsp?category=Optics&productNumber=a1660sm&subCategory=Multiservice+SDH, acessado em Set, 2006.

[8] **Site alcatel.com**, http://www1.alcatel-lucent.com/products/productsummary.jsp?category=Carrier+Ethernet+IP/MPLS+%26+ATM+

Networks&productNumber=os7000&subCategory=Carrier+Ethernet+Switch/Routers, acessado em Set, 2006.

[9] M. Bortoloso, “**Proposta de Metodologia para Projeto de Redes WAN Multimídia com Suporte a Requisitos de Qualidade de Serviço**”, dissertação de Mestrado, Universidade Federal do Espírito Santo, VITÓRIA, Ago, 2006.

[10] **Site cisco.com**,

http://www.cisco.com/en/US/products/hw/optical/ps2001/products_white_paper0900aecd802ccffe.shtml , acessado em Mar, 2007.

[11] **Site cisco.com**, http://www.cisco.com/en/US/tech/tk389/tk214/tech_brief09186a0080091a8a.html, acessado em Nov, 2006.

[[12] **Site cisco.com**, http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b08.html, acessado em Jan, 2007.

[13] **Site sap.com**, http://www36.sap.com, acessado em Dez, 2007.

[14] B. Fortz, M. Thorup, "**Internet traffic engineering by optimizing OSPF weights**", IEEE INFOCOM, vol. 2, pp. 519-528, Mar, 2000.

[15] S. Halabi, “**Metro Ethernet**”, Ciscopress.com, 1ª Edition, ISBN: 158705096X, Out, 2003.

[16] **Site IEEE**, WWW.IEEE.org, acessado em Out,2006.

[17] **Site IEEE 802.17 working group**, WWW.IEEE802.org/17/, acessado em Out, 2006.

[18] ITU-T Series G : Transmission Systems and Media, Digital Systems end Networks, Digital terminal equipments – General, Series Y: Global Information Infrastructure and Internet Protocol Aspects, Internet protocol aspects – Transport Generic framing procedure (GFP).

[19] B. Jamoussi, L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, M. Girish, E. Gray, J. Heinanen, T. Kilty, A. Malis, "**RFC 3212 - Constraint-Based LSP Setup using LDP**", site: www.ietf.org, Jan, 2002.

[20] Andrew G. Malis, "**Converged Services over MPLS**", IEEE Communications Magazine, Set, 2006.

[21] **Site Metro Ethernet Forum**, http://www.metroethernetforum.org/Presentations.htm, acessado em Mar, 2007.

[22] J. Moy, "**RFC 2328 - OSPF Version 2**", site: www.ietf.org, Abr, 1998.

[23] B.O. Monteiro, R. Fernandes, A.M. Alberti, "**Análise Experimental da Eficiência do Mapeamento Ethernet sobre GFP em Redes SDH**", II Workshop de Ciência e Tecnologia em Comunicações Ópticas da Unicamp, Campinas, Fev,2005.

[24] MPLS WORD Congress Large-Scale Multi-Vendor Layer 2 VPN with MPLS, http://www.ipmplsforum.org/tech/MPLSWorldCongress2005-WhitePaper.pdf, Public Interoperability Event, Paris, Mar 2005.

[25] P. Oppenheimer, "**Projeto de redes Top-Down**", Editora Campus, 1ª edição,1999.

[26] **Site OPNET® Simulator**, http://www.Opnet.com, acessado em mar, 2007.

[27] E. Osborne, A. Simha, "**Traffic Engineering with MPLS**", ciscopress.com, 1ª Edition, ISBN 85-352-1076-8, 2003.

[28] R. Prabagaran, J. B. Evans, "**Experiences with Class of Service (CoS) translations in IP/MPLS Networks**", 26th Annual IEEE International Conference on Local Computer Networks (LCN'01), vol. 00, p. 243, 2001.

[29] E. Rosen, Y. Rekhter, "**RFC 2547 - BGP/MPLS VPNs**", site: www.ietf.org, Mar, 1999.

[30] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta, "**RFC 3032 - MPLS Label Stack Encoding**", site: www.ietf.org, Jan, 2001.

[31] E. Rosen, A. Viswanathan e R. Callon, "**RFC 3031- Multiprotocol Label Switching Architecture**", site:www.ietf.org, Jan, 2001.

[32] C. Semeria, "**RSVP Signaling Extensions for MPLS Traffic Engineering**", Juniper Networks Inc., www.juniper.net/techcenter/techpapers/rsvp_signalling.htm, 2000.

[33] V. Sharma, F. Heelstrand, "**RFC 3469 - Framework for MPLS-based Recovery**", site: www.ietf.org, Fev,2003.

[34] S. Shepard, "**Metro Area Networking**", Mcgraw-Hill Professional, 1ª Edition, ISBN: 0071399143, 2002.

[35] W. Simpons , "**RFC 1661 - The Point-to-Point Protocol**", site: www.ietf.org, Jul,1994.

[36] W. Simpons ,"**RFC 1662 - PPP in HDLC-like Framing**", site: www.ietf.org, Jul,1994

[37] A. Sodder, "**Providing Scalability in L2 Virtual Private Networks by using a MAC-n-MAC Frame Encapsulation and a Larger Service-tag**",IEEE 802.1 Interim Meeting, Jan, 2003.

[38] A. Tanenbaum, "Redes de Computadores", Ed.Campus, 4ª edição, Brasil, 2003.

[39] D. Warren, D. Hartmann, "**Building Cisco Metro Optical Networks (METRO)**", Ciscopress, 1ª Edition , ISBN: 1587050706, Ago, 2003.

[40] F. Wong, C. Wong, L. Ngoh , W. Wong , "**Performance Comparison of Resilient Packet Ring, Packet over Sonet and Gigabit Ethernet for network design**", International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), pag 680-687, Jul,2003.

[41] M. H. Birkner, "**Projeto de Interconexão de Redes – Cisco Internetworking Design – CID**", Pearson Education do Brasil, 1ª Edição, 2003.

[42] Site scientificatlanta.com, http://www.scientificatlanta.com/newscenter/whitepapers.htm, acessado em Jan,2008.

[43] site cisco.com, http://www.cisco.com/en/US/prod/collateral/optical/ps5724/ps2006/prod_white_paper0900aecd802cd018_ns579_Networking_Solutions_White_Paper.html , acessado Dez,2007.

[44] J. Moon Chung, "**Analysis of MPLS Traffic Engineering**", Proceedings of the 43rd IEEE Midwest Symposium, Circuits and Systems, Jul, 2000.

[45] L. Zhang, S. Berson, S. Herzog, S. Jamin, "**RFC2205 - Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification**", site: www.ietf.org, set,1997.

[46] Site furnas.com. br, http://www.furnas.com.br, acessado em Dez,2007.

[47] X. Wang, C. Schulzrinne, H. Stirpe, P.Wu, "***IP Multicast Fault Recovery in PIM over OSPF***", Network Protocols2000, Proceedings 2000 International Conference, Japan, 2000.

ANEXO I - Estudo Comparativo de Equipamentos

Introdução

O objetivo deste anexo é apresentar um estudo comparativo dos equipamentos em termos de suas funcionalidades. São considerados os equipamentos que exercem diferentes atividades numa rede. O primeiro grupo de equipamentos tem características de *"Border" (*ou borda). Estes equipamentos se localizam nos limites da rede, introduzindo e retirando os fluxos na rede. São eles: placa *ISA PR_EA* (Alcatel), *Omniswitch* 7700 (Alcatel) e *Black Diamond* 6808 (*Extreme Networks*). O segundo grupo são os equipamentos de "*Core*", que se localizam no centro da rede e comutam os fluxos para seus respectivos destinos. Quanto maior o tamanho de rede, maior deverá ser sua capacidade de comutação. Os equipamentos são *Black Diamond* 10808 (*Extreme Networks*), CISCO 6500 (CISCO) e Alcatel 7750 (Alcatel), todos considerados "*CarrierClass*". Para confecção desta comparação são usadas informações de *datasheet* de produtos e páginas *web* oficial dos respectivos fornecedores.

Na rede o conjunto "*placa ISA PREA e Omniswitch 7700*" realiza as atividades de *Core* e *Border*.

Em relação à escolha dos equipamentos, foram levados em consideração os principais fornecedores do mercado e seus equipamentos com maior aceitação.

Protocolo de Gerência

	BORDER	CORE

ITENS	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Protocolos Gerência						
SNMPv1	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
SNMPv2	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
SNMPv3	**Não**	**SIM**	**Não**	**SIM**	**Não**	**Não**
RMON 1	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
RMON 2	**Não**	**Não**	**SIM**	**SIM**	**Não**	**SIM**
Telnet	**SIM**	**SIM**	**SIM**	**SIM**	**Não**	**SIM**

Tabela – Protocolo de Gerência.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de **6** funcionalidades = Nota 10 (Máxima)
Total de 5 funcionalidades = Nota 8,3
Total de 4 funcionalidades = Nota 6,6
Total de 3 funcionalidades = Nota 5
Total de 2 funcionalidades = Nota 3,3
Total de 1 funcionalidade = Nota 1,6
Total de 0 funcionalidade = Nota 0

Tabela– Pontuação do item: Protocolo de Gerência.

Conclusão:

A placa ISA PREA não suporta o SNMP versão 2, apenas a versão1. O SNMPv2 traz novas funcionalidades como, por exemplo, otimização do processo "GET" que não estão acessíveis na placa ISA PREA. Todos os equipamentos oferecem algum tipo de protocolo de gerência, mas o Black Diamond 10808 permite todas as opções pesquisadas. O conjunto (ISA PREA e Omniswitch) também não oferece suporte a RMONv2, funcionalidade esta que possibilita a monitoração de protocolos acima da camada três (ou camada de rede).

Marcação e Classificação

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Marcação e Classificação de Quadros e Pacotes						
TOS (Type of Service)	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
DIFFSERV	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IEEE 802.1P (Traffic Class)	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IEEE 802.1Q (VLAN)	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
MPLS	**SIM**	**Não**	**SIM**	**SIM**	**SIM**	**SIM**

Tabela – Marcação e Classificação.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 5 funcionalidades = Nota 10 (Máxima)
Total de 4 funcionalidades = Nota 8
Total de 3 funcionalidades = Nota 6
Total de 2 funcionalidades = Nota 4
Total de 1 funcionalidade = Nota 2
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Marcação e Classificação.

Conclusão:

Todas as opções enumeradas são suportadas pelos equipamentos, exceto o Omniswitch que não suporta o MPLS.

Internet Protocol

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Internet Protocol						
IPv4	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IPV6	**Não**	**Não**	**Não**	**SIM**	**SIM**	**SIM**
DHCP	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
NAT	**Não**	**SIM**	**SIM**	**SIM**	**Não**	**SIM**

Tabela – Internet Protocol.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 4 funcionalidades = Nota 10 (Máxima)
Total de 3 funcionalidades = Nota 7,5
Total de 2 funcionalidades = Nota 5
Total de 1 funcionalidade = Nota 2,5
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Internet Protocol.

Conclusão:

A solução apresentada pelo fornecedor não suporta IPv6 e a placa ISA PREA não implementa DHCP ou NAT (essa função será realizada apenas pelo Omniswitch). O fato do conjunto (ISA PREA e Omniswitch) não suportar o IPv6 demandará a necessidade de troca parcial ou total dos equipamentos da rede em caso de "upgrade" para o IPv6.

Protocolo de Roteamento

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Protocolo de Roteamento IP						
RIPv1	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
RIPv2	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
OSPFv1	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
OSPFv2	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IS-IS	**Não**	**Não**	**Não**	**SIM**	**SIM**	**SIM**
BGP-4	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**

Tabela – Protocolo de Roteamento.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 7 funcionalidades = Nota 10 (Máxima)
Total de 6 funcionalidades = Nota 8.5
Total de 5 funcionalidades = Nota 7.0
Total de 4 funcionalidades = Nota 5,7
Total de 3 funcionalidades = Nota 4.2
Total de 2 funcionalidades = Nota 2,8
Total de 1 funcionalidade = Nota 1,4
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Protocolo de Roteamento.

Conclusão:

A placa ISA PREA não suporta nenhum protocolo de roteamento. Deste modo, apenas o equipamento Omniswitch tem informações de alcançabilidade na solução. Como o Omniswitch suporta o OSPFv2, é possível disponibilizar algumas facilidades como balanceamento de carga e segurança, que foram incorporadas na versão 2 do protocolo OSPF.

Padrões *Ethernet*

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Padrões Ethernet						
IEEE 802.1W	**SIM**	**SIM**	**Não**	**SIM**	**SIM**	**SIM**
IEEE 802.3x	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IEEE 802.3s	**SIM**	**Não**	**Não**	**Não**	**SIM**	**SIM**
IEEE 802.3u (Fast Ethernet)	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IEEE 802.3z (Gigabit Ethernet)	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IEEE 802.3ad	**SIM**	**Não**	**SIM**	**SIM**	**SIM**	**SIM**

Tabela – Padrão Ethernet.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 6 funcionalidades = Nota 10 (Máxima)
Total de 5 funcionalidades = Nota 8,3
Total de 4 funcionalidades = Nota 6,6
Total de 3 funcionalidades = Nota 5
Total de 2 funcionalidades = Nota 3,3
Total de 1 funcionalidade = Nota 1,6
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Padrão *Ethernet*.

Conclusão:

Os equipamentos suportam a maioria dos padrões. É importante registrar que o Omniswitch não suporta o padrão IEEE 802.3ad e a placa ISA PREA tem apenas uma saída local Gigabit Ethernet e quatro saídas Ethernet/ Fast Ethernet.

Protocolo *Multicast*

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Multicast						
DVRMP	**Não**	**SIM**	**SIM**	**Não**	**Não**	**SIM**
MBGP	**Não**	**Não**	**Não**	**SIM**	**SIM**	**SIM**
PIM-SM	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
PIM-DM	**Não**	**Não**	**SIM**	**Não**	**SIM**	**SIM**
IGMP *snooping*	**Não**	**Não**	**SIM**	**Não**	**SIM**	**SIM**
IGMPv1	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
IGMPv2 (RFC 2236)	**Não**	**Não**	**SIM**	**SIM**	**SIM**	**SIM**
IGMPv3	**Não**	**Não**	**Não**	**SIM**	**SIM**	**SIM**

Tabela – Protocolo Multicast.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 8 funcionalidades = Nota 10 (Máxima)
Total de 7 funcionalidades = Nota 8,7
Total de 6 funcionalidades = Nota 7,5
Total de 5 funcionalidades = Nota 6.2
Total de 4 funcionalidades = Nota 5
Total de 3 funcionalidades = Nota 3,7
Total de 2 funcionalidades = Nota 2,5
Total de 1 funcionalidade = Nota 1,2
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Protocolo Multicast.

Conclusão:

O equipamento ISA PREA não oferece suporte aos protocolos Multicast. No Omniswitch essa funcionalidade também é muito restrita, inclusive não suporta o IGMPv2. O IGMPv2 traz

várias melhorias com pedido de logout (comando Leave) do grupo e está mais apto às necessidades atuais para comunicações Multicast.

Interfaces Ethernet

ITENS	BORDER			CORE		
	Placa ISA – PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Interfaces Ethernet						
10/100 Base TX *auto-negotiating*	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
1000BaseT	**Não**	**SIM**	**SIM**	**SIM**	**Não**	**SIM**
1000 Base-SX	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
1000Base-LX	**SIM**	**SIM**	**Não**	**SIM**	**SIM**	**SIM**
1000 Base LH	**Não**	**SIM**	**Não**	**Não**	**Não**	**Não**
10 Gbase LX4 – CWDM	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**
10 Gbase LR/ LW	**Não**	**Não**	**Não**	**SIM**	**Não**	**Não**
10 Gbase ER/ EW	**Não**	**Não**	**Não**	**SIM**	**Não**	**Não**

Tabela – Interfaces Ethernet.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 8 funcionalidades = Nota 10 (Máxima)
Total de 7 funcionalidades = Nota 8,7
Total de 6 funcionalidades = Nota 7,5
Total de 5 funcionalidades = Nota 6.2
Total de 4 funcionalidades = Nota 5
Total de 3 funcionalidades = Nota 3,7
Total de 2 funcionalidades = Nota 2,5
Total de 1 funcionalidade = Nota 1,2
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Interface Ethernet.

Conclusão:

O equipamento ISA PREA possui apenas uma porta Giga Ethernet e não suporta 10Giga Ethernet e o Omniswitch não suporta interfaces 10Giga Ethernet.

Interfaces Synchronous Digital Hierarchy (SDH)

ITENS	BORDER			CORE		
	Placa ISA – PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Interfaces						
SDH STM-1	SIM (configurado)	Não	16	Não	16	16
SDH STM-4	SIM (configurado)	Não	8	Não	16	4
SDH STM-16	SIM (configurado)	Não	Não consta	Não	4	2
ATM STM-4	Não	Não	8	Não	4	2
ATM STM-1	Não	Não	16	Não	16	2

Tabela – Interfaces SDH.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 5 funcionalidades = Nota 10 (Máxima)
Total de 4 funcionalidades = Nota 8
Total de 3 funcionalidades = Nota 6
Total de 2 funcionalidades = Nota 4
Total de 1 funcionalidade = Nota 2
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Interface SDH.

Conclusão:

A placa ISA PR_EA utiliza o sistema de transmissão do equipamento Alcatel 1660SM para ter interfaces SDH. O equipamento 1660SM oferece facilidades de configuração e expansão, conforme as necessidades operacionais apresentadas. O equipamento Omniswitch não oferece interfaces SDH, ficando dependente da placa ISA PREA ou saídas Ethernet do equipamento 1660SM para integrar o sistema.

Conexões

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Conexões						
Suporte a conexões ponto a ponto	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
Suporte a conexões ponto a multiponto	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
Suporte a conexões multiponto	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**

Tabela – Conexões.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 3 funcionalidades = Nota 10 (Máxima)
Total de 2 funcionalidades = Nota 6,66
Total de 1 funcionalidade = Nota 3,33
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Conexões.

Conclusão:

Todos os tipos de conexão são suportados pelos equipamentos. Deve-se considerar que as conexões mencionadas são camada (OSI) dois.

Software de Gerência

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Software de Gerência						
Gerência de falhas	SIM	SIM	SIM	SIM	SIM	SIM
Gerência de desempenho	SIM	SIM	SIM	SIM	SIM	SIM
Gerência de configuração de devices	SIM	SIM	SIM	SIM	SIM	SIM

Tabela – Software de Gerência.

Software de Gerência de Rede	
Placa ISA PR_EA	Gerência NR 7.1 ISA PR_EA 1.1 NE4.2B
Omniswitch	OmniVista
Black Diamond 6808	EPICenter Network Management
Black Diamond 10808	EPICenter Network Management
Alcatel 7750	Alcatel 5620 Service Aware Manager (SAM)
CISCO 6500	CISCO Works

Tabela – Equipamento/Software de Gerência.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 3 funcionalidades = Nota 10 (Máxima)
Total de 2 funcionalidades = Nota 6,66
Total de 1 funcionalidade = Nota 3,33
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Software de Gerência.

Conclusão:

Na solução proposta os softwares de gerência do ISA PREA e Omniswitch são diferentes e não "conversam" entre si. Com isso, a operação terá que operar os dois sistemas paralelamente.

Lista de Acesso (ACLs)

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Segurança						
ACL na camada 2	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
ACL na camada 3	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
ACL na camada 4	**Não**	**SIM**	**SIM**	**SIM**	**Não**	**SIM**

Tabela – Lista de Acesso.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 3 funcionalidades = Nota 10 (Máxima)
Total de 2 funcionalidades = Nota 6,66
Total de 1 funcionalidade = Nota 3,33
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Lista de Acesso.

Conclusão:

A placa ISA PREA não implementa lista de controle de acesso (ACLs) nas camadas 3 e 4. Apenas o Omniswitch implementa essas ACL. Resumidamente, restrições baseadas em endereço IP, portas TCP e UDP, são realizadas apenas pelo Omniswitch na topologia existente.

Protocolo de Autenticação

ITENS	BORDER			CORE		
	Placa ISA – PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Autenticação						
Radius	**Não**	**SIM**	**SIM**	**SIM**	**SIM**	**SIM**
LDAP	**Não**	**SIM**	**Não**	**Não**	**Não**	**Não**
Telnet	**Não**	**Não**	**SIM**	**SIM**	**Não**	**SIM**
TACACS	**Não**	**Não**	**SIM**	**SIM**	**SIM**	**SIM**

Tabela – Protocolo de Autenticação.

Nota: A placa *ISA PREA* utiliza um software de gerência proprietário do fornecedor.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 3 funcionalidades = Nota 10 (Máxima)
Total de 2 funcionalidades = Nota 6,66
Total de 1 funcionalidade = Nota 3,33
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Protocolo de Autenticação.

Conclusão:

O protocolo de autenticação da ISA PREA é um protocolo proprietário e faz parte do software de gerência do equipamento. Existem vantagens em trabalhar com um protocolo de autenticação padrão, um deles é um maior conhecimento prévio do seu funcionamento e interoperabilidade em outras plataformas.

Qualidade de Serviço

ITENS	BORDER			CORE		
	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Paradigma de QoS						
Serviços Diferenciados	Não	SIM	SIM	SIM	SIM	SIM
Serviços Integrados	SIM	Não	SIM	Não	SIM	Não

Tabela – Qualidade de Serviço.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 2 funcionalidades = Nota 10 (Máxima)
Total de 1 funcionalidade = Nota 5
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: QoS.

Conclusão:

A placa ISA PREA implementa três classes de serviços, que são: Classe Garantida, Classe Regulada e Classe Melhor Esforço. O Omniswitch suporta qualidade de serviço através de quatro classes de serviços (padrão). A união destas duas facilidades é importante para alcançar metas de qualidade para as diferentes demandas de tráfego. O maior problema na solução é não existir um sistema de aprovisionamento de QoS que integre os dois principais equipamentos (placa ISA e Omniswitch).

Engenharia de Tráfego

	BORDER	CORE

ITENS	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
Engenharia de Tráfego						
OSPF-TE	**Não**	**Não**	**Não**	**Não**	**SIM**	**Não**
MPLS-TE	**SIM**	**Não**	**SIM**	**Não**	**SIM**	**SIM**
CR-LDP	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**
RSVP-TE	**SIM**	**Não**	**SIM**	**Não**	**SIM**	**Não**

Tabela – Engenharia de Tráfego.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 4 funcionalidades = Nota 10 (Máxima)
Total de 3 funcionalidades = Nota 7,5
Total de 2 funcionalidades = Nota 5
Total de 1 funcionalidade = Nota 2,5
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Engenharia de Tráfego.

Conclusão:

A placa ISA PREA implementa o RSVP-TE com o MPLS para criação de caminho com reserva de recurso. Os caminhos são criados com os recursos necessários para um determinado fluxo. É importante ressaltar que a solução não permite a criação dinâmica de caminhos LSP, apenas estática. Essa característica poderá trazer dificuldades em situações que necessitem resiliência do sistema (como, por exemplo, falha em enlaces ou devices).

Tipos de VPNs (Virtual Private Networks)

	BORDER	CORE

ITENS	Placa ISA - PREA	OMNISWITCH	BlackDiamond 6808	BlackDiamond 10808	Alcatel 7750	Cisco 6500
VPN						
MPLS-VPN L3 (BGP)	**Não**	**Não**	**Não**	**Não**	**SIM**	**Não**
MPLS-VPN L3 (LDP)	**Não**	**Não**	**Não**	**Não**	**Não**	**Não**
MPLS-VPN L2 (Martini Draft)	**Sim**	**Não**	**SIM**	**SIM**	**SIM**	**Não**
MPLS-VPN L2 (VPLS)	**Sim**	**Não**	**SIM**	**SIM**	**SIM**	**Não**

Tabela – Tipos de VPN.

A tabela a seguir apresenta os critérios utilizados na avaliação.

Total de 4 funcionalidades = Nota 10 (Máxima)
Total de 3 funcionalidades = Nota 7,5
Total de 2 funcionalidades = Nota 5
Total de 1 funcionalidade = Nota 2,5
Total de 0 funcionalidade = Nota 0

Tabela - Pontuação do item: Tipos de VPN.

Conclusão:

A placa ISA PREA implementa apenas VPN na camada dois. Apenas o modelo Martini Draft pode ser utilizado. O VPLS não é suportado pela solução. O equipamento Omniswitch não implementa VPN, ficando a cargo da placa ISA PREA este trabalho. Essa limitação é importante porque a placa ISA PREA só implementa VPN na camada 2, e estas apresentam baixa escalabilidade.

Resultado do Comparativo das Facilidades

Tabela - Comparativo de facilidades.

ITENS	ISA PR_EA	OMNI	BD6808	BD10808	A7750	C6500
Protocolo de gerência	**3,3**	**8,3**	**8,3**	**10**	**5**	**8,3**
Marcação e Classificação	**10**	**8**	**10**	**10**	**10**	**10**
Internet Protocol	**2,5**	**7,5**	**7,5**	**10**	**7,5**	**10**
Protocolo de Roteamento	**0**	**7**	**7**	**8,5**	**8,5**	**8,5**
Padrão Ethernet	**10**	**6,6**	**6,6**	**8,3**	**10**	**10**
Protocolo Multicast	**0**	**3,7**	**7,5**	**6,2**	**8,7**	**10**
Interfaces Ethernet	**3,7**	**6,2**	**3,7**	**7,5**	**3,7**	**5**
interfaces SDH	**6**	**0**	**7,5**	**0**	**10**	**10**
Conexões	**10**	**10**	**10**	**10**	**10**	**10**
Software de Gerência	**10**	**10**	**10**	**10**	**10**	**10**
Segurança (ACL)	**3**	**10**	**10**	**10**	**7**	**10**
Protocolo de Autenticação	**0**	**6,6**	**6,6**	**6,6**	**6,6**	**6,6**
Qualidade de Serviço	**5**	**5**	**10**	**5**	**10**	**5**
Engenharia de Tráfego	**5**	**0**	**5**	**0**	**7,5**	**2,5**
Tipos de VPN	**5**	**0**	**5**	**5**	**7,5**	**0**
TOTAL	**73,5**	**88,9**	**114,7**	**107,1**	**122**	**115,9**

ITENS	ISA PR_EA	OMNI	BD6808	BD10808	A7750	C6500
Portas Ethernet	**4**	**192**	**768**	**480**	**60**	**241**
Portas Gigabit Ethernet	**1**	**16**	**128**	**480**	**20**	**82**
Portas 10 Gigabit Ethetnet	**Não**	**Não**	**10**	**48**	**2**	**20**
Disponibilidade	baixa	baixa	**alta**	**alta**	média	média

Tabela - Disponibilidade de Interface.

Observação: Existem dois modelos de placa *ISA PREA*: uma placa com quatro portas 10/100Mbps e uma placa com um porta 1000Mbps.

Capacidade de Comutação

ITENS	ISA PR_EA	OMNI	BD6808	BD10808	A7750	C6500
Fabric Capacity	**1,8 Gbps**	**64 Gbps**	**256 Gbps**	**1.6 Tbps**	**400 Gbps**	**720 Gbps**
Capacidade	**Baixa**	**baixa**	média	**alta**	alta	alta

Tabela - Capacidade de Comutação.

Conclusão do Comparativo

Fazendo uma comparação entre os equipamentos, pode-se considerar o conjunto *(ISA PREA e Omnswitch*) equivalente ao equipamento *Black Diamond 6808,* caracterizado comercialmente como equipamento de Borda (*Border*). O *Black Diamond* 6808 possui ainda interface *SDH,* que o conjunto não possui e para tal necessita de um terceiro equipamento (Alcatel 1660SM).

Os equipamentos de *Core* apresentam uma maior pontuação no quesito capacidade de comutação. Neste quesito é importante explicitar a deficiência da *ISA PREA*. Foram pesquisados outros equipamentos com característica de borda e verificou-se que estes também apresentavam um maior valor de *Fabric Capacity*:

► DES 6300 (fabricante *DLINK*) com valor igual a 31,00 Gbps;

► DES 1200 (fabricante *DLINK*) com valor igual a 9,6 Gbps.

É importante ressaltar que a capacidade de comutação é uma das principais características para o bom desempenho da rede.

Em relação a facilidades do equipamento, o uso do conjunto (placa *ISA PREA* com *Omniswitch*) traz uma pontuação próxima a outro equipamento de borda pesquisado, *Black Diamond* BD6808. Já na tabela de portas *Ethernet* deve-se observar o número pequeno de portas Gigabit e falta da porta de 10 *Gigabit* no conjunto (*ISA PREA + Omniswitch*). Isso representa um limitante se for necessário um aumenta do número de pontos de acesso de alta velocidade.

Após analisar as principais funcionalidades dos equipamentos da rede estudada, podem-se destacar as seguintes **conclusões gerais**:

► É possível se obter informações sobre gerência de falhas, gerência de desempenho e gerência de configuração. No entanto, com a topologia estruturada com a placa *ISA PREA* e no *Omniswitch*, faz-se necessário à ativação dos sistemas de gerência dos dois equipamentos, uma vez que não há interoperabilidade entre eles. Isso leva à necessidade de uma terceira ferramenta de gerência para que se possa ter uma visão integrada da rede através do sistema de gerência;

► Podem ser implementados os mecanismos de classificação de pacotes do tipo *TOS, Diffserv, IEEE 802.1P*, *IEEE 802.1Q* no *Omnswitch* e apenas o *IEEE 802.1p* na placa ISA;

► O mecanismo de classificação *MPLS* somente é implementado na placa *ISA PR-EA;*

► A solução proposta está baseada no protocolo *IPv4*. Funções de *DHCP* e *NAT* podem ser implementadas no *Omniswitch*;

► Através do Omniswitch podem ser implementados os protocolos de roteamento *RIPv1*, *RIPv2*, *OSPFv1*, *OSPFv2* e *BGP-4*. Com o uso do *OSPFv2* é possível a configuração de balanceamento de carga na rede;

► O suporte à comunicação multicast é muito restrito;

► A placa *ISA PREA* possui dois modelos de placa *ISA PREA*: uma placa com 4 portas 10/100Mbps e uma placa com 1 porta 1000Mbps;

► A placa *ISA PREA* suporta mapeamento *SDH* do tipo STM-1, STM-4, STM-16, através do equipamento Alcatel 1660SM;

► A placa *ISA PREA* não suporta interfaces *ATM*;

► A solução proposta permite o funcionamento *Ethernet, Gigabit, e SDH*. Deve-se observar o número pequeno de portas *Gigabit* e a falta de portas 10Gigabit dificulta possíveis expansões de velocidades em pontos de acesso;

► Foi analisado também o *Switch Fabric* da placa *ISA PREA* e o valor máximo *throughput* de dados é 1,8 Gb/s. Este valor é muito menor que o dos outros equipamentos estudados inclusive o *Omniswitch* (64Gbps) e consequentemente pode trazer problemas de capacidade operacional para a rede;

► A solução proposta possibilita o suporte a conexões Ponto a Ponto e Ponto-Multiponto;

► O mecanismo de autenticação é implementado no *Omniswitch* e é baseado nos padrões *RADIUS e LDAP*;

► A solução proposta admite a utilização do mecanismo *Intserv/RSVP-TE* através da placa *ISA PREA* e *Diffserv* no Omniswitch;

► Os mecanismos de *QoS* somente estão explicitamente descritos na documentação da placa *ISA PREA* (*WFQ, WRED, Leaky Bucket*), enquanto no *Omniswitch* é feita apenas uma citação genérica de quatro classes de QoS (default) por porta;

► A solução proposta suporta a implementação de *VPN L2*, através da placa *ISA PREA*. É possível a utilização de MPLS-VPN L2 (Martini Draft).

Em suma, observando as funcionalidades dos equipamentos pode-se concluir que, quando utilizados em conjunto, a placa *ISA PREA* e o *Omniswitch*, não apresentam um grau de eficiência compatível com demais equipamento de *CORE* analisados, principalmente o item backplane. É importante ressaltar os resultados apresentados pelo equipamento Alcatel 7750, além de suportar a maioria das facilidades estudadas, possui um excelente *backplane* e permite interligações com interfaces *SDH WAN e PDH WAN*. Este equipamento é fortemente recomendado para substituir o conjunto *ISA PREA/Omniswitch.*

ANEXO II - Teste das facilidades dos equipamentos

1 - Testes de QoS no Omniswitch

QoS Shaping

O nível de acesso da rede utiliza a placa *ISA Ethernet*. As portas Ethernet da placa *ISA* podem ser mapeadas em VC-12, VC-3, VC-4 ou concatenação de VC-12 ou VC-3. O *Omniswitch 7700* é o responsável em perceber, através do protocolo de roteamento IGP (*OSPF*), que a saída principal (ligação SDH) está defeituosa e opta pela rota de contingência. Esta solução agrega os fluxos prioritários e envia através de enlaces de 512kbps ou 8xDS0 para outro *Omniswitch*.

O *Omniswitch 7700* possui grande importância nas localidades não atendidas pelo *Backbone* (*placa ISA PREA*). Primeiramente, porque este equipamento é o responsável pelo roteamento do *site* na ocorrência de falha do enlace. O *Omniswitch* 7700 utiliza o protocolo OSPF para detectar e rotear para o enlace redundante. Outro ponto importante é que essas localidades são atendidas por enlaces de pequena capacidade. Os enlaces têm bandas de 512Kbps, majoritariamente. O ponto mais crítico desta solução é a diferença de banda entre os enlaces principais e os de contingência. Os enlaces principais são de 10 Mbps e o redundante apenas 512Kbps. Para diminuir possíveis problemas de transmissões para serviços e aplicações críticos ao negócio faz-se necessária a utilização de ferramentas de QoS. A escolha dos serviços com maior prioridade é crucial para a rede.

Conforme observado no trabalho conceitual, os softwares de gerência do *ISA PREA* e *Omniswitch* são diferentes e não interagem entre si. Para realizar as configurações de QoS utilizou-se o *OmniVista* e configurou-se também via script na interface CLI do equipamento.

No primeiro cenário foram testados dois fluxos do *Omniswitch 7700C* para o 7700B da Figura . Neste cenário foram testadas prioridade, banda mínima e máxima e marcação na camada 3 (IP).

O fluxo 1 recebeu prioridade máxima e a banda mínima limitada a 512Kbpbs. A política de marcação levou em consideração o endereço de origem 10.9.20.11/24.

O fluxo 2 recebeu prioridade baixa e banda máxima limitada a 256Kbps. A política de marcação levou em consideração o endereço de origem 10.9.21.11/24.

O *Interwatch* foi configurado para gerar 2 fluxos de 1 Mbps para cada uma dessas políticas descritas.

O *Omniswitch* permite apenas configuração de 4 níveis de prioridade. Este conceito pode ser observado na interface de configuração da **Figura A** e também nas documentações mais recentes do equipamento.

A **Figura A** representa a interface gráfica de configuração de *QoS* do *Omniswitch* (*OmniVista*). É possível verificar na caixa combo "*Priority*" que existem apenas 4 níveis de prioridades. Na parte mais abaixo aparecem configurações de *shaping* e marcação.

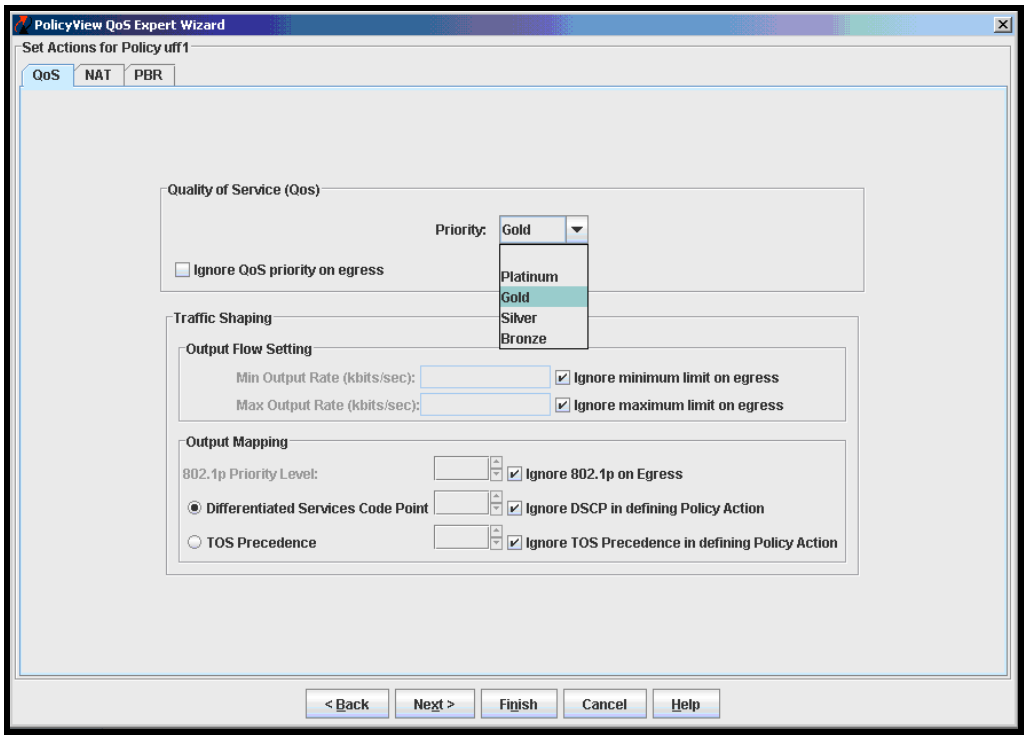


Figura A – Interface de configuração de QoS do OmniVista.

A configuração de banda mínima apresentou problema na interface de configuração do *OmniVista* e na interface *CLI*. Foi tentado carregar esta configuração nos outros *Omniswitch* e todos apresentaram o mesmo status.

A configuração de QoS carregada no 7700 C foi:

qos trust ports fragment timeout 60 reflexive timeout 60 nat timeout 300
Linha responsável pela habilitação do QoS em todas as portas (cometário).

policy condition uff1Condition from ldap source ip 10.9.20.11
Marcação de política do fluxo 1 (cometário).

policy condition uff2Condition from ldap source ip 10.9.21.11
Marcação de política do fluxo 2 (cometário).

policy action uff2Action from ldap maximum bandwidth 256K priority 1
Configuração de prioridade e banda mínima do fluxo 2 (cometário).

policy validity period AllTheTime from ldap days sunday monday tuesday wednesday thursday friday saturday months january february march april may june july august september october november December
É possível condicionar as configurações de QoS a períodos (data/mês/ano).

policy rule uff2 from ldap precedence 30002 condition uff2Condition action uff2A ction validity period AllTheTime

Linha responsável pela aplicação das configurações anteriores. O item Precedence permite priorizar uma rotina sobre a outra. Quanto maior o valor do Precedence, maior a prioridade na execução da rotina.

Após as configurações serem concluídas, foram utilizados comandos padrões para testar o êxito da configuração. Segue os resultados dos comandos:

OS7700C> show policy rule
Policy From Prec Enab Act Refl Log Save
uff2 ldap 30002 Yes Yes No No Yes
(L3): uff2Condition -> uff2Action
(VP): AllTheTime
 # Este comando verifica se existe alguma regra de QoS aplicada.

OS7700C> show policy condition
Condition Name From Src -> Dest
uff1Condition ldap
*IP : 10.9.20.11 -> Any

uff2Condition ldap
*IP : 10.9.21.11 -> Any
 # Este comando verifica se existem políticas de marcação.

OS7700C> show policy action
Bandwidth Max
Action Name From Disp Pri Share Min Max Depth Bufs
uff2Action ldap accept 1 No 256K
 # Este comando apresenta o tipo e a especificação da política de QoS ativada.

A configuração aceita pelo *Omniswitch* foi a do fluxo 2: limitação de banda a 256Kbps e prioridade baixa. A configuração do fluxo 1 não foi aceita devido ao *Omniswitch* não suportar o comando banda mínima. Assim sendo, o fluxo não ficou sem nenhuma configuração de comportamento de tráfego. O uso da concatenação do *SDH* permitiu a configuração de uma banda de saída com 4Mbps e 2Mbps, entre *Omniswitch* e placa *ISA*

Ethernet. Nesta simulação, a conexão *SDH* de saída do tráfego utilizada foi a de 4Mbps. Os resultados da transmissão dos fluxos estão mostrados a seguir na **Figura B**.

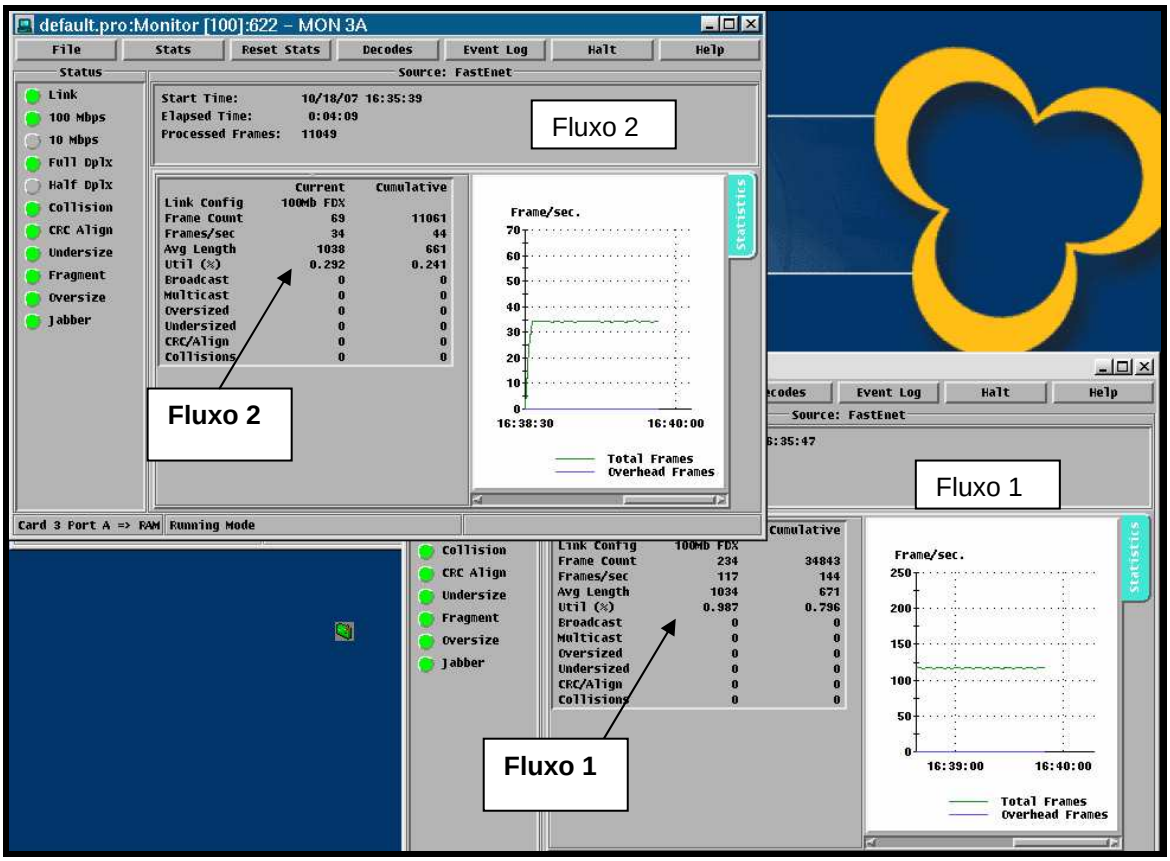


Figura B – Configuração de banda máxima.

O **fluxo 2** apresentou uma contenção de tráfego que permitiu apenas uma saída de tráfego do *Omniswitch* de 292Kbps. O valor está apenas 36Kbps acima do valor de banda máxima pré-determinado.

O **fluxo 1** utilizou a banda restante e apresentou uma banda 987Kbps (banda de saída equivalente a banda inserida na entrada pelo gerador de tráfego).

No ambiente de teste praticamente não existia tráfego concorrente, exceção feita aos protocolos de sinalização do *OSPF* e *Ethernet* (corresponde a menos de 2% do tráfego). Após a configuração ser retirada é possível verificar a eficiência da limitação de tráfego.

QoS Priority

Para testar o mecanismo de prioridade do *Omniswitch* foi aplicada uma nova configuração nos roteadores. Neste teste são criados dois fluxos com prioridades distintas. O fluxo 1 com prioridade alta e o fluxo 2 com prioridade baixa. O objetivo deste experimento é comprovar o funcionamento do mecanismo de priorização e também compreender o algoritmo utilizado. O *Interwatch*, neste caso, gerou dois fluxos simétricos nestes três valores de banda: 2,5 Mbps, 5Mbps e 6Mbps. Nesta simulação, a conexão *SDH* de saída do tráfego utilizada foi a de 4Mbps.

Foram necessárias novas configurações no *Omniswitch*, conforme descritas a seguir:

```
policy condition uff1Condition from ldap source ip 10.9.20.11 mask 255.255.255.0
# Marcação de política do fluxo 1 (cometário).

policy condition uff2Condition from ldap source ip 10.9.21.11 mask 255.255.255.0
# Marcação de política do fluxo 2 (cometário).

policy action uff1Action from ldap priority 7
# Selecionar prioridade do fluxo 1(cometário).

policy action uff2Action from ldap priority 1
# Selecionar prioridade do fluxo 2(cometário).

policy validity period AllTheTime from ldap days sunday monday tuesday wednesday
 thursday friday saturday months january february march april may june july augu
st september october november December

policy rule uff1 from ldap precedence 30001 condition uff1Condition action uff1A
ction validity period AllTheTime
# Aplicação das configurações do Fluxo 1. O item Precedence foi configurado com
mesmo grau de prioridade em ambos os fluxos.

policy rule uff2 from ldap precedence 30001 condition uff2Condition action uff2A
ction validity period AllTheTime
# Aplicação das configurações do Fluxo 2. O item Precedence foi configurado com
mesmo grau de prioridade em ambos os fluxos.
```

O fluxo 1 (maior prioridade) ocupou a maior fatia da banda nos três ensaios. Na **Tabela A** é apresentado o percentual de ocupação da saída de tráfego para cada fluxo.

		2,5 Mbps	**5Mbps**	**6Mbps**
Tráfego gerado	**Fluxo 1**	**56%**	**93%**	**99%**
	Fluxo 2	**44%**	**7%**	**1%**

Tabela A – Percentual de ocupação dos fluxos na saída do *Omniswitch.*

A banda de saída foi majoritariamente ocupada pelo fluxo 1. O percentual de ocupação do fluxo 1 aumentou com o crescimento dos fluxos gerados. No terceiro ensaio com fluxo de 6Mbps a ocupação chegou a 99% e o fluxo 2, com prioridade inferior, teve uma banda próxima a zero. Segundo o manual do fornecedor existem três algoritmos de escalonamento suportados pelo equipamento *Omniswitch* 7700. Os algoritmos são *Priority Weighted Round Robin, Weighted Round Robin* e *Strict Priority*.

O valor de banda próxima a zero do fluxo 2 (para fluxos de 6 Mbps) indica que o algoritmo em funcionamento é o *Strict Priority*. O algoritmo *Strict Priority* em situação de congestionamento caminha para um comportamento chamado de "*starvation*", visto neste ensaio. Este algoritmo sempre transmite pacotes com maior prioridade, sem nenhum mecanismo de ponderação ou peso (*weighted*). Os demais algoritmos não estavam disponíveis na versão de software atual do equipamento.

Para analisar a simetria de fluxos numa mesma fila de prioridade de tráfego foram configurados dois fluxos com a mesma prioridade. A marcação de *QoS* (*Policy Condition*) foi feita baseada nos endereços *IEEE 802.1q*. Desta forma, é testada marcação na camada 2 ou *Ethernet*. O gerador foi configurado para injetar 2 fluxos de 10Mbps (cada) e foi utilizado a

porta 4Mbps como saída para os fluxos. Ambos os fluxos foram configurados com a mesma prioridade, segue nova configuração:

policy condition uffnew1Condition from ldap destination vlan 20
 # Marcação de política do fluxo 1 utilizando o 802.1q.

policy condition uffnew2Condition from ldap destination vlan 21
 # Marcação de política do fluxo 2 utilizando o 802.1q.

policy action uffnew1Action from ldap priority 5
 # Selecionar prioridade do fluxo 1.

policy action uffnew2Action from ldap priority 5
 # Selecionar prioridade do fluxo 2.

Na **Figura C** é apresentada a coleta de cada fluxo com mesma priorização. É possível verificar que houve simetria entre os fluxos. A leitura da coletora foi em pacotes por segundo, mas no item marcado com circulo é possível observar o valor de Mbits/segundos.

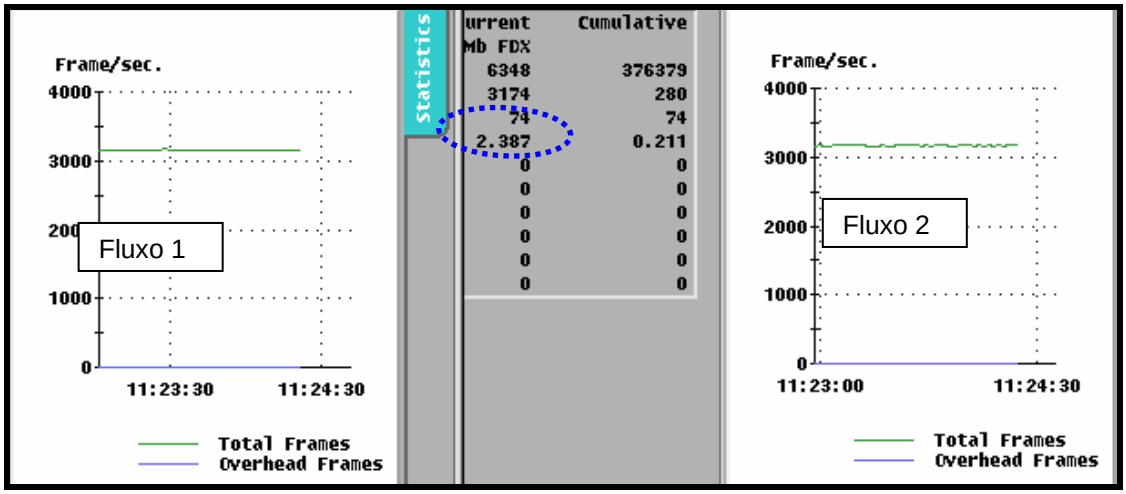


Figura C – Configuração com fluxos de prioridade iguais.

O fluxo 1 e o fluxo 2 apresentaram simetria. O fluxo 1 apresentou um *throughput* de 2,37 Mbps e o fluxo 2 teve um *throughput* de 2,38 Mbps. A resposta deste experimento é que o mecanismo de escalonamento de *QoS* do *Omniswitch* é justo para tráfegos na mesma fila de prioridade. Neste laboratório não foi possível novamente evidenciar que o protocolo de

escalonamento em funcionamento é o *Strict Priority*. Porque, neste caso, tanto o *Priority Weighted Round Robin* como *Strict Priority*, funcionariam da mesma forma.

2 - Testes de utilização das filas de *QoS* na Placa *ISA PREA*

O transporte dos quadros *Ethernet* no núcleo da rede é realizado através das placas *ISA PREA*, utilizando o encapsulamento *MPLS* em *VCs SDH*. O *MPLS* é utilizado para gerenciar fluxos de dados de pacotes, transportados em cima de uma infra-estrutura *SDH*. O *MPLS* opera no nível 2 do modelo OSI e utiliza o *SDH* como camada física. Os túneis são criados estaticamente pela solução do fornecedor.

A solução permite apenas 3 níveis de *QoS*. Sendo assim, faz-se necessário agrupar diferentes perfis de tráfego em apenas 3 grandes grupos. As três filas possíveis são: GA (banda garantida), RE (banda regulada) e BE *(Best Effort)*.

O conjunto *ISA PREA* (placas *ISA PREA* 2 e 3 e *Mux SDH*) foi configurado com três classes de QoS (*Outer Tunnel*) com 1Mbps (totalizando 3Mbps com a soma das três classes).

O *Interwatch* foi configurado para gerar 2 fluxos, cada um com 2Mbps e direcionados para filas de *QoS* distintas. Este teste visa basicamente verificar se a fila sem utilização é ocupada pelo tráfego excedente das filas ocupadas. O **fluxo 1** foi encaminhado para fila garantido e o **fluxo 2** para fila regulado da placa *ISA PREA*. Nenhum fluxo foi configurado para a fila *Best Effort* para verificar se em situações de congestionamentos as filas com baixa utilização são utilizadas para transbordo dos pacotes excedentes das filas saturadas.

A seguir é apresentada a configuração feita no *Omniswitch 7700* (7700A) para este teste. O *Omniswitch* precisa fazer a marcação do campo *IEEE 801.1p* que é utilizada pela placa *ISA PREA.* Na configuração de *QoS* do *Omniswitch* todos ficaram como se estivessem na mesma fila, apenas diferenciando na marcação de saída. A seguir é descrito a configuração realizada.

policy condition uff1Condition from ldap source ip 10.9.20.11 mask 255.255.255.0 destination ip 10.8.20.21 mask 255.255.255.0
 # Marcação de política do fluxo 1 .

policy condition uff1Condition from ldap source ip 10.9.21.11 mask 255.255.255.0 destination ip 10.8.21.21 mask 255.255.255.0
 # Marcação de política do fluxo 2 .

policy action uffnew1Action from ldap priority 4 802.1p 7
 # Selecionar prioridade iguais no contexto Omniswitch e marcação de saída (7) para perfilhamento no Outer Tunnel garantido no sistema (ISA PREA/SDH).

policy action uffnew2Action from ldap priority 4 802.1p 4
 # Selecionar prioridade iguais no contexto Omniswitch e marcação de saída (4) para perfilhamento no Outer Tunnel regulado no sistema (ISA PREA/SDH).

O **fluxo 1** e **o fluxo 2** apresentaram simetria e ocuparam apenas 1Mbps (banda configurada cada fila QoS). O **fluxo 1** apresentou um *throughput* de 1,094*Mbps* e o **fluxo 2** teve um *throughput* de 1,093*Mbps (estes valores estão baseados em medições instantâneas).* O **fluxo 1** foi encaminhado para fila garantido e o **fluxo 2** regulado. Na **Figura D** tem-se o resultado do *throughput* dos dois fluxos gerados pelo *InterWatch*.

Fluxo 1 – Garantido

	Current
Link Config	100Mb FDX
Frame Count	2907
Frames/sec	1454
Avg Length	74
Util (%)	1.093
Broadcast	0
Multicast	0
Oversized	0
Undersized	0
CRC/Align	0
Collisions	0

Fluxo 2 - Regulado

	Current
Link Config	100Mb FDX
Frame Count	2909
Frames/sec	1454
Avg Length	74
Util (%)	1.094
Broadcast	0
Multicast	0
Oversized	0
Undersized	0
CRC/Align	0
Collisions	0

Figura D – Ocupação das duas filas na placa *ISA PREA.*

A fila *Best Effort* não foi utilizada para transbordo dos pacotes excedentes. O resultado aponta que a configuração de banda na criação dos *Outers Tunnels* é estática, e o algoritmo utilizado segundo referência é o *Weighed Fair Queuing*. Não existe o aproveitamento de classes com banda não utilizada por outra com alta utilização.

3 - Tempo de convergência do *OSPF*

Os *Omniswitchs* percebem falhas nos enlaces através do protocolo de roteamento *OSPF* e optam por uma outra *VLAN* remota, que segue por outro enlace (ou caminho). As localidades devem possuir dois caminhos (*MPLS*) ou dois enlaces (borda). A placa *ISA PREA* não oferece suporte a protocolos de roteamento típicos IP (*OSPF, RIP e IS-IS*), ficando assim toda atividade concentrada no *Omniswitch*.

As simulações realizadas no capítulo 5 indicam um tempo de convergência da rede de 50 segundos. Este laboratório visa analisar este tempo com os equipamentos reais. Entretanto, a tendência do laboratório é apresentar tempos menores, já que a tabela *OSPF* dos equipamentos existentes na experiência é inferior ao da topologia simulada e da topologia operacional da rede. No laboratório existem apenas três equipamentos divulgando informações de rota *OSPF* e na simulação existiam onze equipamentos divulgando rotas (além dos equipamentos de borda).

Através do comando "*show ip route*" é possível observar todas as rotas divulgadas no *OSPF* no ambiente de laboratório. Ao todo são 13 rotas divulgadas pelos equipamentos utilizados no experimento. A seguir seguem as rotas divulgadas:

Dest Address	Subnet Mask	Gateway Addr	Age	Protocol
0.0.0.0	0.0.0.0	172.16.62.1	1d 7h	OSPF
10.7.50.1	255.255.255.255	172.16.62.1	1d 7h	OSPF
10.8.20.0	255.255.255.0	172.16.62.1	00:09:36	OSPF
10.8.21.0	255.255.255.0	172.16.62.1	00:08:46	OSPF
10.8.50.1	255.255.255.255	172.16.62.1	6d 7h	OSPF
10.9.20.0	255.255.255.0	10.9.20.1	00:16:23	LOCAL
10.9.21.0	255.255.255.0	10.9.21.1	00:16:23	LOCAL
10.9.50.1	255.255.255.255	10.9.50.1	35d 1h	LOCAL
10.9.74.0	255.255.255.0	10.9.74.1	1d 7h	LOCAL
10.9.75.0	255.255.255.0	10.9.75.1	1d 7h	LOCAL
127.0.0.1	255.255.255.255	127.0.0.1	35d 1h	LOCAL
172.16.60.0	255.255.255.252	172.16.62.1	2d 0h	OSPF
172.16.62.0	255.255.255.252	172.16.62.2	9d 5h	LOCAL

A **Figura E** apresenta o ponto de falha na topologia de testes e a direção dos fluxos de dados. A seta transparente representa o caminho principal, caminho este utilizado nos testes anteriores. Através de uma intervenção manual é gerada uma falha (o cabo é desconectado do equipamento) e espera-se que o tráfego utilize o caminho alternativo (conexão *Gigabit Ethernet*). O ensaio tem como intuito verificar o tempo de recuperação a falha numa estrutura similar ao do ambiente real.

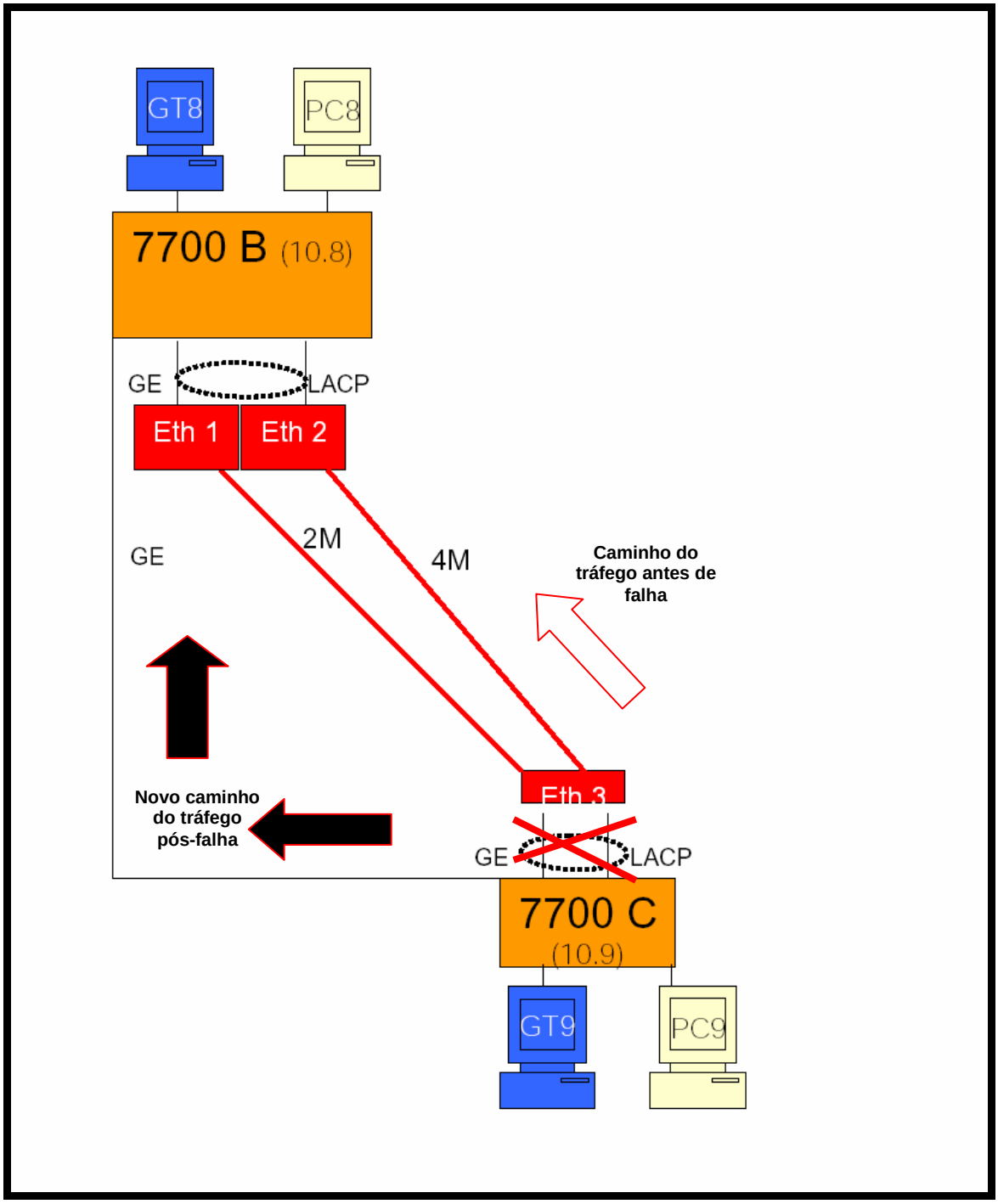


Figura E – Ponto de falha na topologia de teste.

Para testar o tempo de redundância a falha foram criados dois fluxos de dados com origem no *Omniswitch* 7700C e destino no 7700B. Uma outra conexão entre os dois *Omniswitch* foi necessária para funcionar como caminho redundante.

Para obrigar todo tráfego a passar prioritariamente pelo caminho da placa *ISA Ethernet*, foi necessário utilizar métricas artificiais (custo do *OSPF*). Após a falha nos enlaces *Gigabit Ethernet*, do *Omniswitch* 7700C com a placa *ISA Ethernet*, o equipamento verifica a mudança de estado da interface (*interface down*) e utiliza a tabela *OSPF* para escolha de um novo caminho.

Os fluxos 1 e 2 são direcionados para o 7700B. O comportamento dos fluxos de dados está na **Figura E**. Na figura E observa-se a falha e posteriormente a recuperação da comunicação.

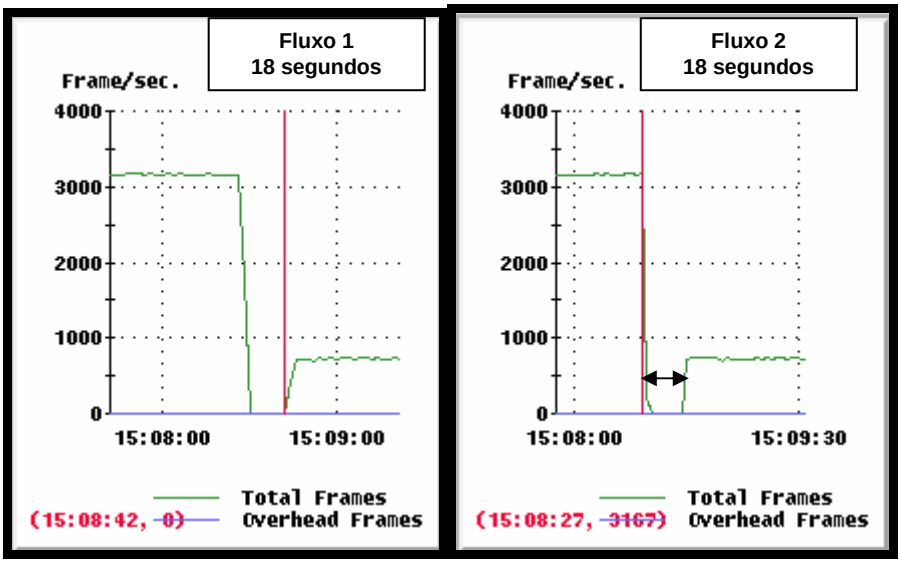


Figura E – Tempo de convergência pós-falha.

O fluxo 1 e o fluxo 2 convergiram em 18 segundos. O pequeno número de rotas *OSPF* propiciou este tempo pequeno de convergência.

O *Omniswitch* funcionando com todas as funcionalidades projetadas, com diferentes usuários conectados e vivenciando em um ambiente de operação, o tempo de recuperação a falhas tenderá a se aproximar dos valores verificados na simulação, ficando entre 30 segundos até 60 segundos.

4 - Tempos de convergência do *LACP*

Neste laboratório é testado o tempo do protocolo *LACP* (*Link Aggregation Control Protocol*).

O *LACP* é protocolo especificado pelo *IEEE802*.3ad que permite utilizar diversas portas físicas como se fosse uma única porta. Os pacotes enviados para um nó diretamente conectado são distribuídos por diferentes portas físicas. O *LACP* permite aumento de *throughput* de porta lógica, balanceamento de carga e manutenção de transmissão mesmo depois de falha em uma das portas físicas.

A manutenção da transmissão de dados da porta lógica nas portas físicas operante, mesmo após ocorrência de falha em portas físicas pertencente ao mesmo grupo *LACP*, é uma ferramenta que pode ser utilizada nas ligações *Omniswitch/placa ISA PREA*. Assim sendo, é importante a análise do funcionamento desta funcionalidade neste ambiente.

Esta experiência consiste basicamente em testar o funcionamento desta funcionalidade no ambiente do teste em dois pontos de ligação. São eles: interface local (falha1) e interface remota (falha2).

São utilizados os mesmos fluxos de dados configurados na experiência do item "*Tempo de convergência OSPF do Omniswitch*".

Na **Figura F** tem-se a topologia com o respectivo ponto de falha. A diferença da falha simulada neste experimento, em relação ao experimento anterior é que apenas um das portas *Gigabit Ethernet* é inutilizada.

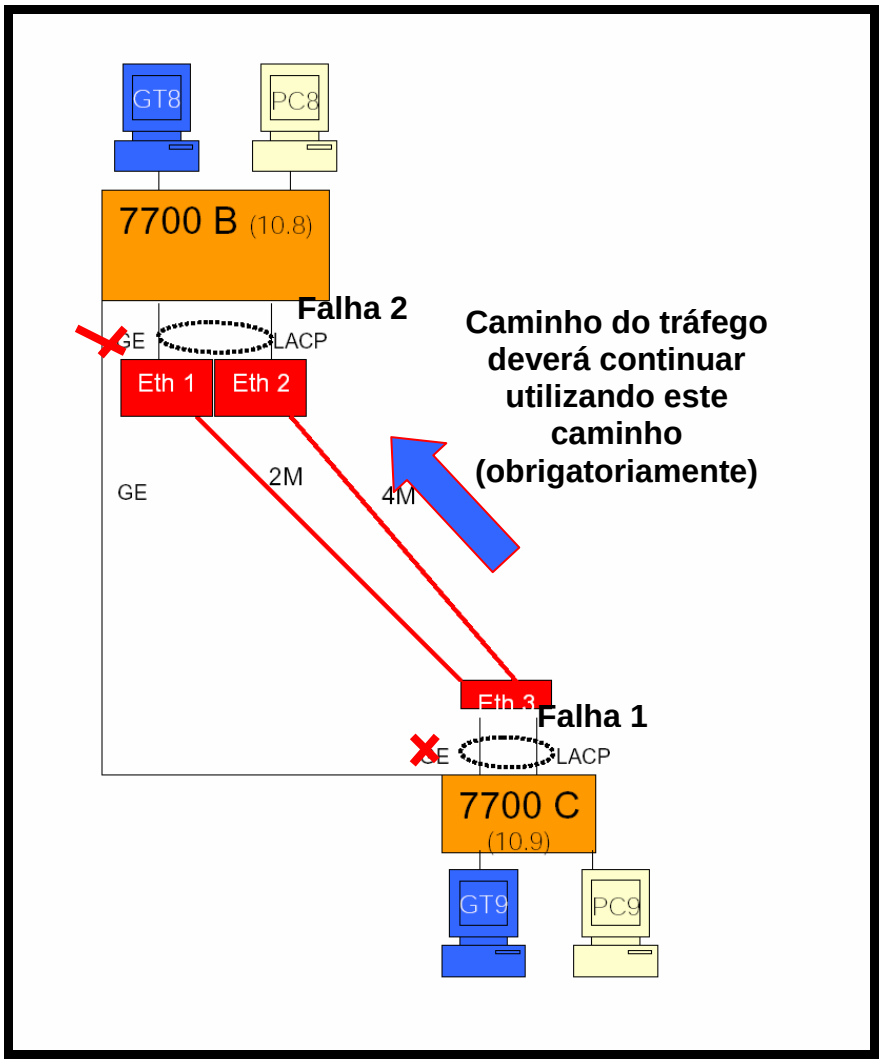


Figura F - Ponto de falha na topologia de teste (convergência *LACP*).

Na falha 1 o tempo de convergência foi de 1 segundo. O *LACP* demostrou ser eficiente neste contexto.

Na **Figura G** é verificado o tempo de convergência deste novo experimento (falha 2). Na figura observa-se o tempo de entre a falha e a recuperação da comunicação dos fluxos 1 e 2 do *Omniswitch* 7700C para o 7700B.

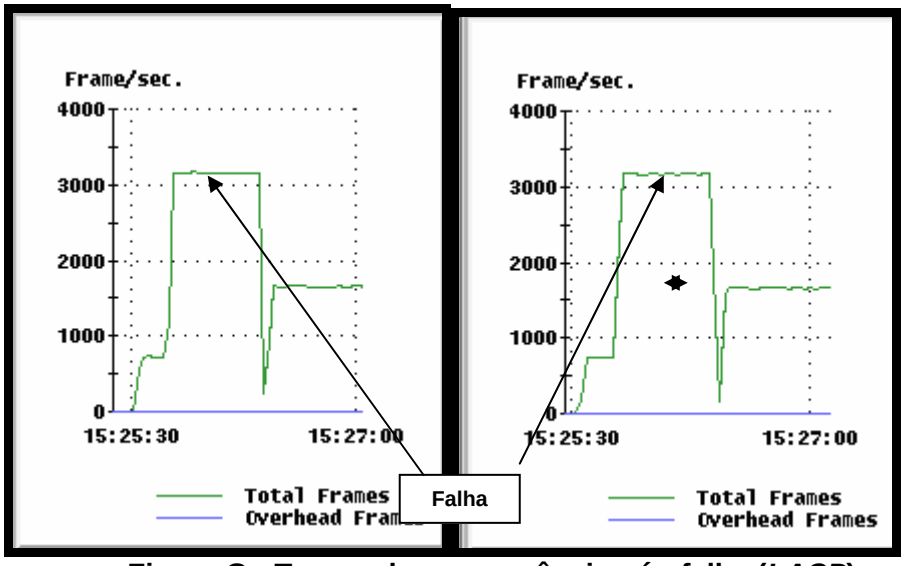


Figura G - Tempo de convergência pós-falha (*LACP*).

O tempo de recuperação a falha ficou também na casa de 1 segundo. Este tempo era esperado e está coerente com as referências analisadas. Os resultados mostraram que falhas nas interfaces *Ethernet* remotas são um pronto fraco deste desenho. Este comportamento traz desvantagens para rede operativa. A matriz *Ethernet* deve perceber a falha e comutar todo tráfego para a interface física ativa. O principal motivador deste problema é a conexão "indireta" das interfaces *Ethernet*. Para o *Omniswitch* local as interfaces *Gigabit Ethernet* não apresentam problemas, porque estas estão diretamente conectadas na placa *ISA Ethernet*. Este desenho topológico deve ser analisado com cautela em virtude deste problema.