Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Osvaldo da Silva Dantas Junior

Redes Metro Ethernet: Estudo de Caso Mundivox Telecomunicações

Rio de Janeiro

2010

Osvaldo da Silva Dantas Junior

Redes Metro Ethernet:
Estudo de Caso Mundivox Telecomunicações

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro – RJ

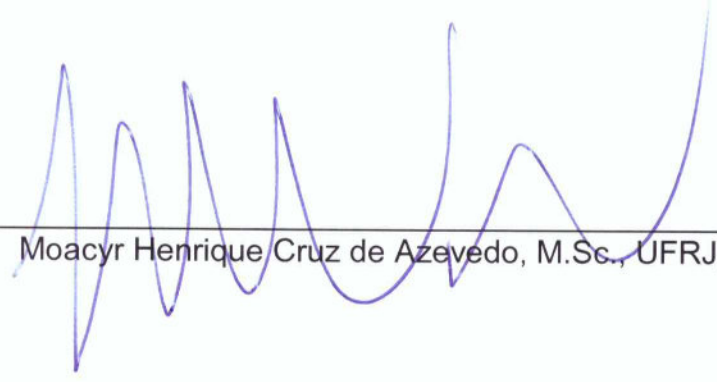
2010

Osvaldo da Silva Dantas Junior

Redes Metro Ethernet:
Estudo de Caso Mundivox Telecomunicações

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovado em agosto de 2010



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

RESUMO

Junior, Osvaldo da Silva Dantas de. **REDES METRO ETHERNET: Estudo de Caso Mundivox Telecomunicações**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Esta pesquisa apresenta uma tecnologia recente no mercado brasileiro e o modo como foi escolhida e implementada em uma empresa de telecomunicações. O mercado busca cada vez mais soluções de baixo custo e que garantam qualidade de serviço, proporcionando interconexão entre as redes corporativas geograficamente distribuídas assim como a Internet. As redes Metro Ethernet têm se mostrado uma escolha óbvia por oferecer simples administração, baixo custo e boa granularidade de banda.

ABSTRACT

Junior, Osvaldo da Silva Dantas de. **REDES METRO ETHERNET: Estudo de Caso Mundivox Telecomunicações**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

This research presents a recent technology in the Brazilian market and how it was chosen and implemented in a telecommunications company. The market increasingly seek low cost solutions and what guarantee quality of service, providing interconnectivity between geographically distributed enterprise networks and the Internet. Metro Ethernet Networks have been an obvious choice for offering simple administration, low cost and good granularity of bandwidth.

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

RELAÇÃO DE ABREVIATURAS E SIGLAS

ARP - Address Resolution Protocol
ATM - Asynchronous Transfer Mode
BPDU - Bridge Protocol Data Unit
CBR - Constant Bit Rate
CBS - Committed Burst Size
CE - Customer-Edge
CE-VLAN - Customer-Edge VLAN
CIR - Committed Information Rate
CoS - Class of Service
CSMA/CD - Carrier Sense Multple Access/Collision Detection
DIX - DEC, Intel, Xerox
DLCI - Data Link Connection Identifier
DWDM - Dense Wavelength Division Multiplexing
EBS - Excess Burst Size
EIR - Excess Information Rate
EoMPLS - Ethernet over Multi Protocol Label Switching
EVC - Ethernet Virtual Connection
ICMP - Internet Control Message Protocol
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IGMP - Internet Group Management Protocol
IP - Internet Protocol
ISO - International Organization for Stantardization
LAN - Local Area Networks
LLC - Logical Link Control MAC - Media Access Control
LSR - Label Switch Routers
LSP - Label Swith Path
L2TP - Layer 2 Transport Protocol
MAN - Metropolitan Area Networks
MPLS - Multiprotocol Label Switching
NNI - Network-Network Interface
NHLFE - Next Hop Label forwarding Entry
OSPF - Open Shortest-Path-First Protocol
PVC - Permanent Virtual Circuit
PDU - Protocol Unit Data
QoS - Quality of Service
RFC - Request For Comments
SDH - Synchronous Digital Hierarchy
SP - Service Provider
TCP - Transmission Control Protocol
ToS - Type of Service
UDP - User Datagram Protocol
UNI - User-to-Network Interface
VLAN - Virtual Local Area Network

SUMÁRIO

1. INTRODUÇÃO

1.1. OBJETIVOS

Este trabalho tem como foco mostrar como a tecnologia Metro Ethernet chegou ao Brasil e em pouco tempo vem ganhando espaço no mercado brasileiro.

Todas essas perspectivas sobre a tecnologia se baseiam em um tripé formado por sua escalabilidade, flexibilidade e confiabilidade, a um preço acessível. Ou seja, esta solução permite que as companhias adquiram banda de acordo com as suas necessidades, o que não ocorre com as tecnologias mais antigas, e possibilita que isso aconteça sem a aquisição de novos equipamentos e infra-estrutura.

A redução de custos é outra vantagem competitiva das Redes Metro Ethernet nas empresas, principalmente pela simplificação da solução e por ser aplicada diretamente sobre uma rede de fibra óptica. Diferentemente de tecnologias como Frame-Relay ou ATM, que têm excelente qualidade, mas com preços proibitivos, a solução Metro Ethernet reduz os custos com transporte de dados em até 50%, seja numa empresa de pequeno, médio ou grande porte. Em outras palavras, com o mesmo gasto, uma companhia poderá enviar o dobro de informações. **Qual foi a importância da tecnologia Metro Ethernet na expansão da rede Mundivox?**

1.2. Relevância

A demanda cada vez maior pela alta velocidade está forçando o mercado a implementar tecnologias que possam atender todo esse volume crescente de acesso à Internet. A tecnologia em ascensão no momento é chamada de Metro Ethernet, com velocidades altíssimas e com um padrão bem definido pelo órgão que a regulamenta.

As implementações da rede Metro Ethernet têm acontecido de maneira rápida e bem-sucedida, e quem hoje já a possui implementada oferece serviços diferenciados e vêem ganhando mercado no mundo da Internet.

A facilidade da rede Metro Ethernet de oferecer serviços em alta velocidade e com qualidade diferenciada vem caminhando lado a lado com a tendência do mercado à centralização dos ativos de rede em grandes *Data Centers*, onde detém maior controle de acesso, aumentando a escalabilidade, disponibilidade e reduzindo custos.

2. REFERENCIAL TEÓRICO

2.1. REDE METRO ETHERNET

2.1.1. Conceitos e definições

Hoje, mais de 95% do tráfego corporativo são através de interfaces Ethernet. Esse sucesso pode ser destacado em alguns aspectos como simplicidade, baixo preço e desempenho. Por outro lado, o mesmo não acontece com as redes MAN e WAN, com as operadoras oferecendo serviços baseados em ATM, Frame-Relay e linhas privativas, todos significantemente mais complicados e com custo mais elevado.

Atualmente os serviços mais importantes demandados pela área corporativa e que mais têm crescido são a interconexão das redes LAN geograficamente distribuída e a conectividade com a Internet. Isto se deve ao tráfego de dados comutados por pacotes estar crescendo exponencialmente. Com isso, utilizar como base tecnologias que otimizem a rede para tráfego de pacotes, ao invés de sobrepô-las com estrutura de comutação por circuitos, se torna quase uma necessidade.

Como usuários corporativos e residenciais estão familiarizados com a utilização da tecnologia Ethernet, eles buscam um serviço Ethernet universal, simples, de baixo custo e alta velocidade. Sendo assim, para o tráfego de pacotes, as operadoras optaram por prover serviços de transportes de quadros Ethernet em suas redes de longa distância. E uma das estratégias para isso é a Metro Ethernet.

Uma Rede Metro Ethernet (MEN – *Metropolitan Ethernet Network*) é definida basicamente como uma rede que interconecta LANs corporativas geograficamente separadas, interconectando-se ainda a uma rede WAN ou backbone operados pelo provedor de serviços, conforme ilustrado na Figura 1.

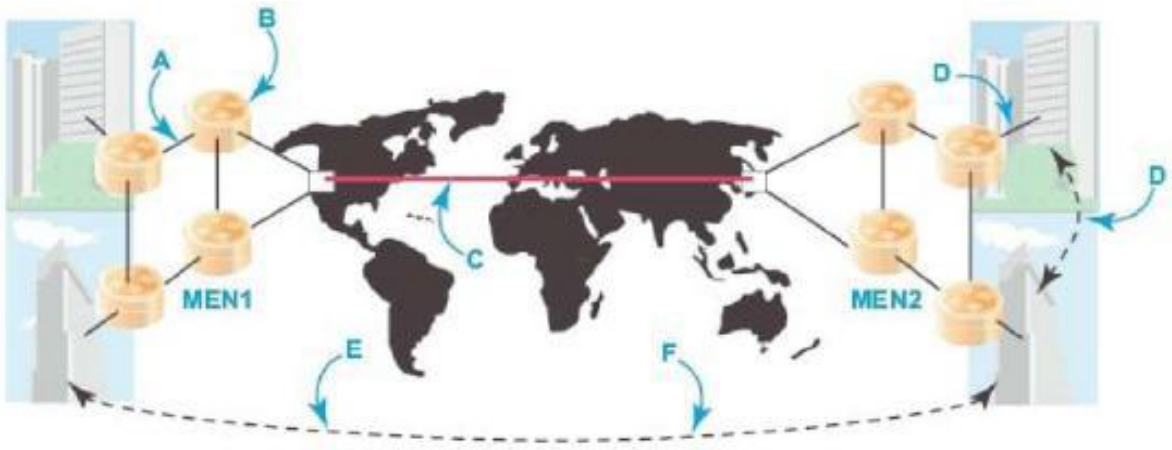


Figura 1 – Rede Metro Ethernet

As principais vantagens de uma rede Metro Ethernet são:

- O cliente lida com uma interface Ethernet comum e bem conhecida, integrando-se perfeitamente à LAN já instalada.
- Redução do custo operacional e de planejamento da rede, o qual é significativamente menor para redes comutadas tradicionais.
- Melhor granularidade e facilidade de aumento de banda, em comparação às redes de circuito comutado (E1/T1, E3/T3, SDH/SONET), permitindo, por exemplo, o aumento da banda do assinante de 1Mbps a 1Gbps em passos de 1Mbps.

2.1.2. Arquitetura

O Metro Ethernet Fórum utiliza um modelo genérico para descrever os componentes internos e externos de uma rede Metro Ethernet. Esta estrutura descreve as interações entre a rede Metro Ethernet através de interfaces bem definidas e seus pontos de referência. O modelo básico de referência de uma rede Metro Ethernet é mostrado na Figura 2.

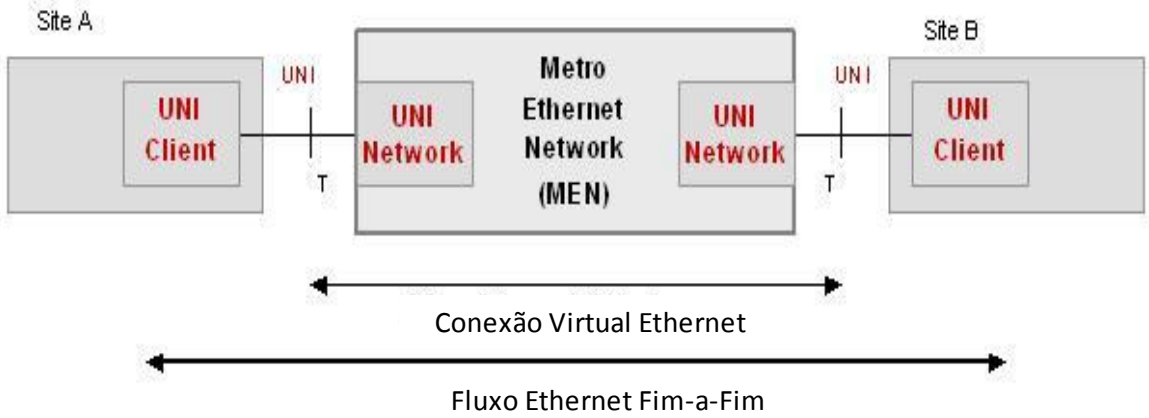


Figura 2 – Fluxo Ethernet Fim-a-Fim

O fluxo Ethernet (*Ethernet flow*) mostrado representa o tráfego de dados fim-a-fim entre dois equipamentos terminais, os quais originam e terminam os quadros Ethernet. A interface que interliga a rede de um cliente à rede de um provedor de serviços é denominada de UNI (*User Network Interface*). Do lado do cliente é chamada de UNI-C (*User Network Interface Client*) e do lado do provedor de serviços é denominada de UNI-N (*User Network Interface Network*). A figura 3 mostra um comparativo de serviços oferecido pelas operadoras em relação à rede Metro Ethernet e à rede tradicional. A simplicidade de trabalhar fim-a-fim com a mesma tecnologia facilita operação e gerencia de todo backbone.

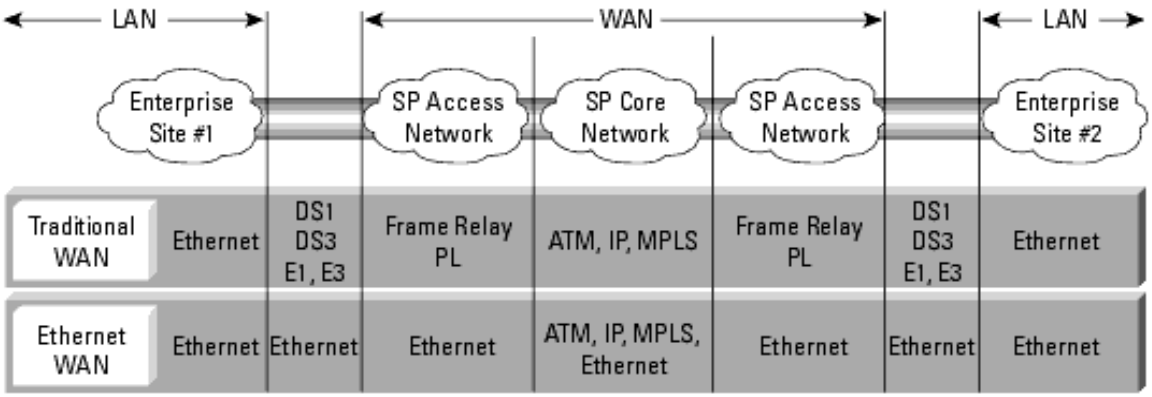


Figure 3 – Comparativo entre Redes Metro com Redes Tradicionais

2.1.3. Topologias de Redes Metro Ethernet

As principais topologias usadas em rede metro são:

2.1.3.1. Anel

Segue a tradição das redes SDH implementadas nos anos de 1990, com base, principalmente, no racional dos modelos de tráfego da época (em que havia menor necessidade de conectividade entre sites locais e a maior parte do tráfego de acesso era direcionada para os *POPs* principais) e na redução dos custos associados com a rede de fibra óptica.

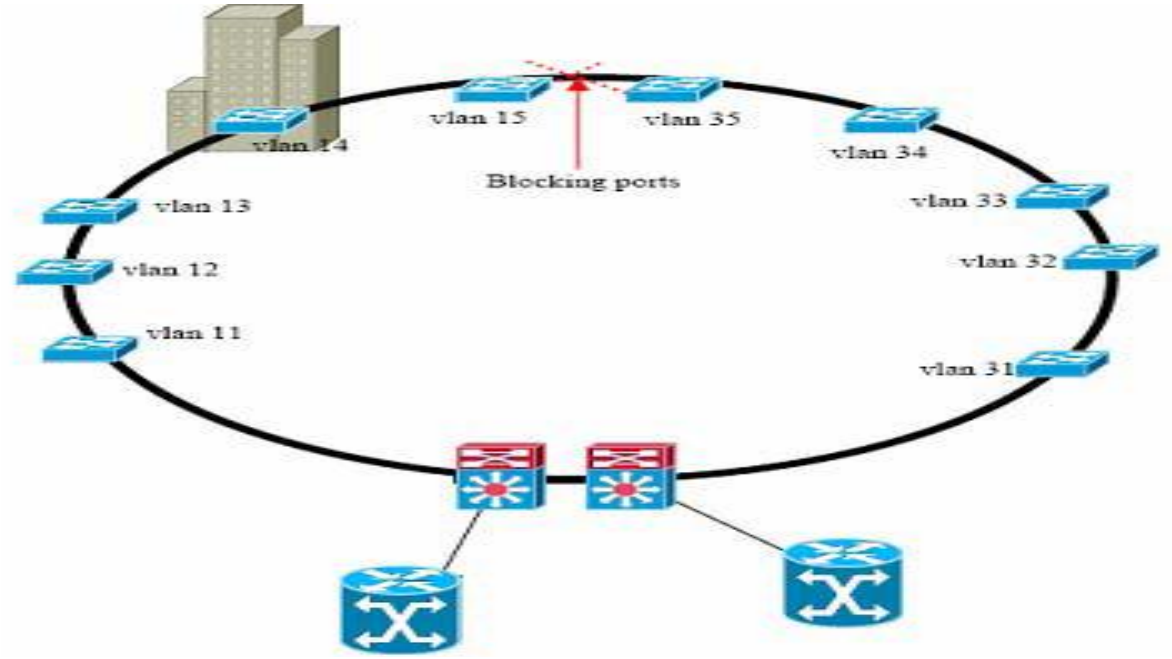


Figura 4 –Topologia ANEL

2.1.3.2. Mesh

Topologia *hub &* spoke, com conexão lógica entre todos os *sites*, é atualmente a forma mais utilizada, embora implique altos custos devido à intensa utilização de fibra óptica. Quanto às arquiteturas, é possível vislumbrá-las sob duas formas principais:

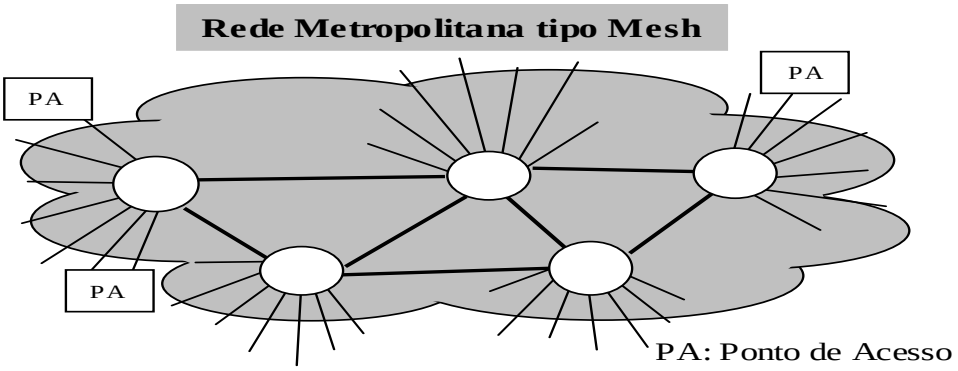


Figura 5 – Topologia *Mesh*

2.1.3.3. Pura

Formadas estritamente por switches Ethernet (ou seja, usando uma referência do modelo OSI – *Open System Interconnection* para descrição lógica de redes, operando somente em nível 2 – enlace). Solução adequada para redes pequenas, com reduzido número de clientes e *sites*.

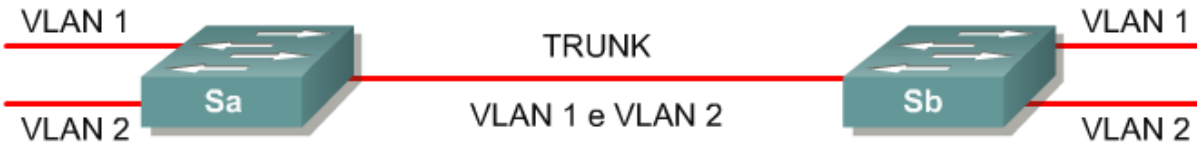


Figura 6 – Topologia Pura

2.1.3.4. Híbridas

Formadas por múltiplos domínios em nível 2 – enlace (Ethernet puro) conectados por um núcleo nível 3 – roteamento (IP/MPLS). Os quadros transportados de um domínio Ethernet para outro passam pelo núcleo, onde podem ser "tunelados" (envelopamento de informações visando otimizar controles na comunicação) via L2TP - *Layer 2 Transport Protocol* ou EoMPLS - *Ethernet over Multi Protocol Label Switching*. Para este último caso, o IETF – fórum de padronização de técnicas para o avanço das redes IP – está definindo uma especificação já conhecida no mercado

como VPLS – *Virtual Private LAN Service*. A arquitetura híbrida é interessante para grandes redes Metro Ethernet.

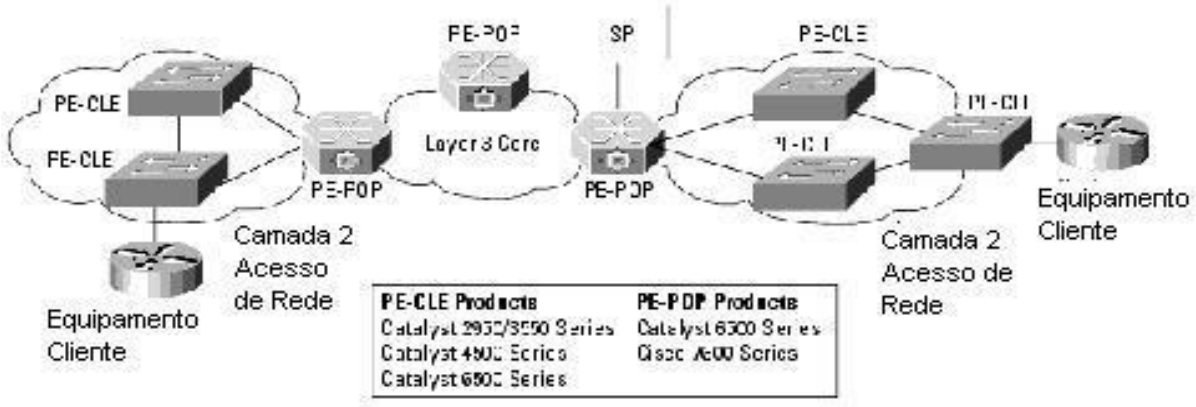


Figura 7 – Topologia Híbrida

2.1.4. Serviços Metro Ethernet

O serviço é assegurado pela operadora da MEN. Os serviços são definidos da perspectiva do cliente final, e podem ser suportados sobre uma variedade de tecnologias e protocolos de transporte como SONET, DWDM, MPLS, etc. De qualquer forma, do lado do cliente, a ligação no UNI é Ethernet. Um atributo chave de um serviço é a Conexão Virtual Ethernet (EVC). Um EVC é definido como uma associação entre duas ou mais UNI, sendo UNI uma interface Ethernet que demarca a fronteira entre o equipamento do cliente e a MEN do fornecedor de serviços. Uma EVC cumpre basicamente duas funções vitais: liga duas ou mais localizações do cliente, permitindo a troca de pacotes entre eles; e evita comunicações entre localizações que não façam parte da mesma EVC, o que possibilita a uma EVC fornecer segurança de dados e privacidade. A entrega de pacotes Ethernet numa EVC é regida por duas regras básicas. Primeiro, um pacote de serviço nunca poderá ser entregue no mesmo UNI que a enviou; segundo, pacotes de serviços têm de ser entregues com os endereços Ethernet e com o conteúdo inalterado. Isto contrasta

com as redes encaminhadas típicas, onde os cabeçalhos Ethernet são removidos e descartados. Com base nestas características, uma EVC pode ser usada para construir uma linha privada ou uma rede virtual privada de nível 2. O MEF definiu dois tipos de EVCs que suportam os tipos de serviços correspondentes (Figura 8):

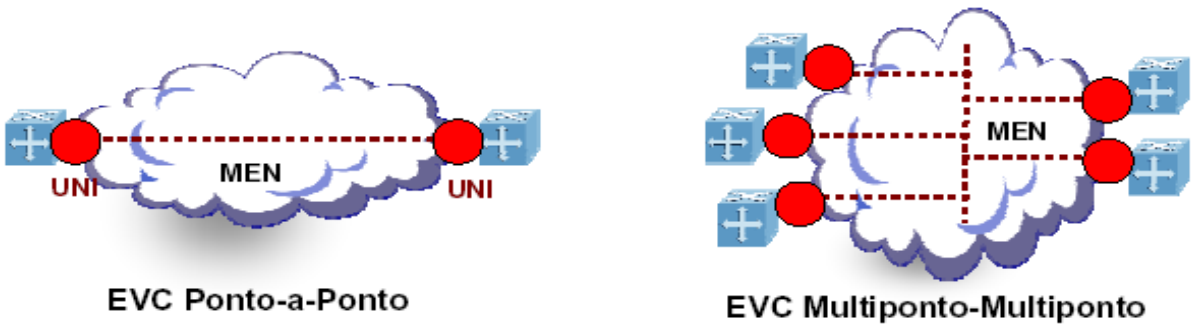


Figura 8 – Arquitetura Metro Ethernet Ponto-a-Ponto e Multiponto-Multiponto

De acordo com os tipos de EVC existem dois tipos de serviços, que são na realidade categorias, uma vez que serviços do mesmo tipo poderão ser bastante diferentes entre si dependendo dos atributos restantes que os caracterizam. Para definir completamente um serviço, um fornecedor terá que definir os UNIs e os atributos EVC associados ao serviço. Os dois tipos de serviço são *Ethernet Line* e *Ethernet LAN*. O tipo de serviço *Ethernet Line* (*E-Line*) fornece uma ligação virtual ponto-a-ponto entre dois UNIs, tal como ilustrado na Figura 9.

2.1.4.1. E-Line: Serviço Ponto-a-Ponto

O serviço *Ethernet Line* corresponde à comunicação ponto-a-ponto entre duas UNIs. Uma UNI poderá ainda receber mais de uma E-Line, desse modo, criando algo como quando se usam PVCs para conectar sites usando Frame-Relay. Pode ainda prover serviços análogos a uma linha privativa.

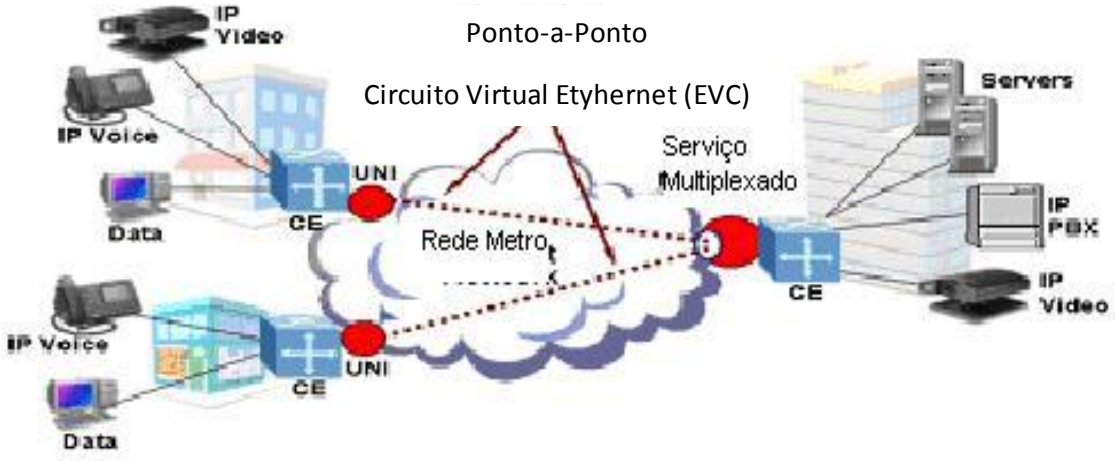


Figura 9 – Tipo de serviço E-Line

2.1.4.2. E-LAN: Serviço Multiponto

O serviço Ethernet LAN oferece conectividade multiponto entre duas ou mais UNIs. Quadros transmitidos poderão ser recebidos por duas ou mais outras UNIs. Sob a perspectiva do assinante, a MEN parece uma LAN. Ao incluir uma nova UNI, simplesmente conecta-se essa nova UNI ao mesmo EVC. Ele necessita de apenas uma EVC para conseguir conectividade *multi-site*.

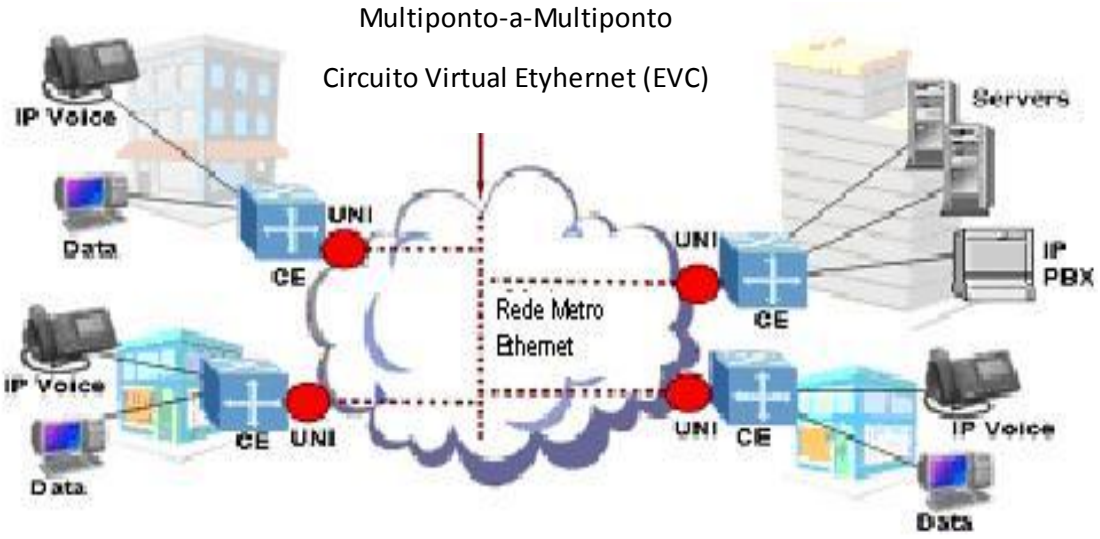


Figura 10 – Tipo de serviço E-Lan

2.1.4.3. Serviços Canônicos

A combinação de alguns atributos possibilita os “toques finais“ que qualificam, univocamente, os serviços canônicos. São eles:

- Multiplexação: possibilita que uma UNI esteja associada a múltiplos EVCs, como acontece em redes de comutação de pacotes, concretizando também o mapeamento entre VLANs e EVCs.
- Transparência: simplifica a operacionalização da rede através do uso do mesmo identificador de VLAN para pacotes ingressos e egressos do EVC.
- Empacotamento: quando mais de uma VLAN é mapeada para um EVC em uma UNI.
- Perfil de Banda: delimitação de “tetos“ em Mbps para pacotes ingressarem nas UNIs e EVCs e delas saírem, similarmente ao conceito de CIR/EIR em redes Frame-Relay.

Alguns fornecedores, como a Cisco Systems, por exemplo, criaram uma terminologia e classificação um pouco mais rica para identificar os serviços canônicos:

2.1.4.4. ERS – Ethernet Relay Service

Refere-se ao serviço básico análogo ao Frame-Relay (múltiplas conexões lógicas podem ser multiplexadas em uma única conexão física), em que roteadores são usados para estabelecimento de conexões entre dois sites. O serviço ERS não é transparente como o EWS, o controle de PDUs (exemplo BPDUs) do Customer Edge (CE) não são passados pelo Provider Edge (PE).

- Similar ao Frame-Relay. As VLANs são os VC Ids.
- Pseudowire – Caminho virtual estabelecido.
- ERS é "one-to-many" (um para muitos) serviços multiplexados.

- Serviços Multiplexados significam que múltiplos pseudowire utilizem uma única interface de acesso ou UNI.
- É Recomendado o uso de um roteador para bloquear controles de nível 2.

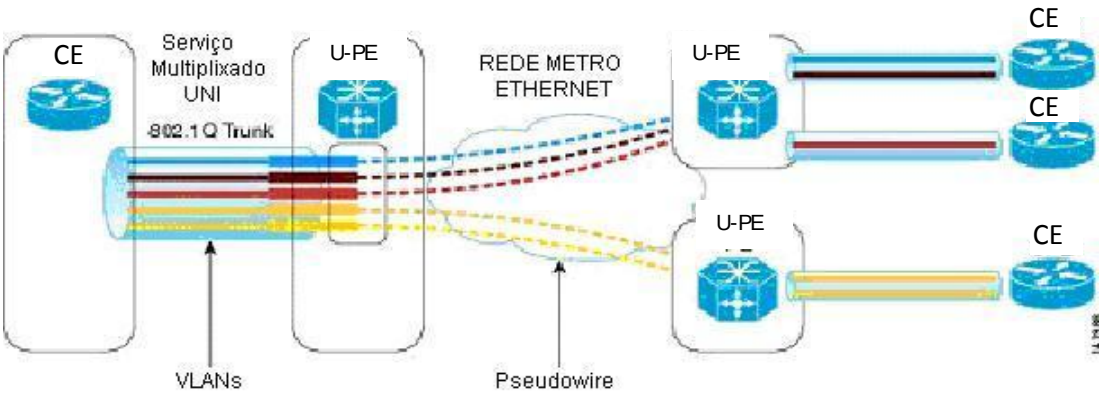


Figura 11 – Topologia Ethernet Relay Service

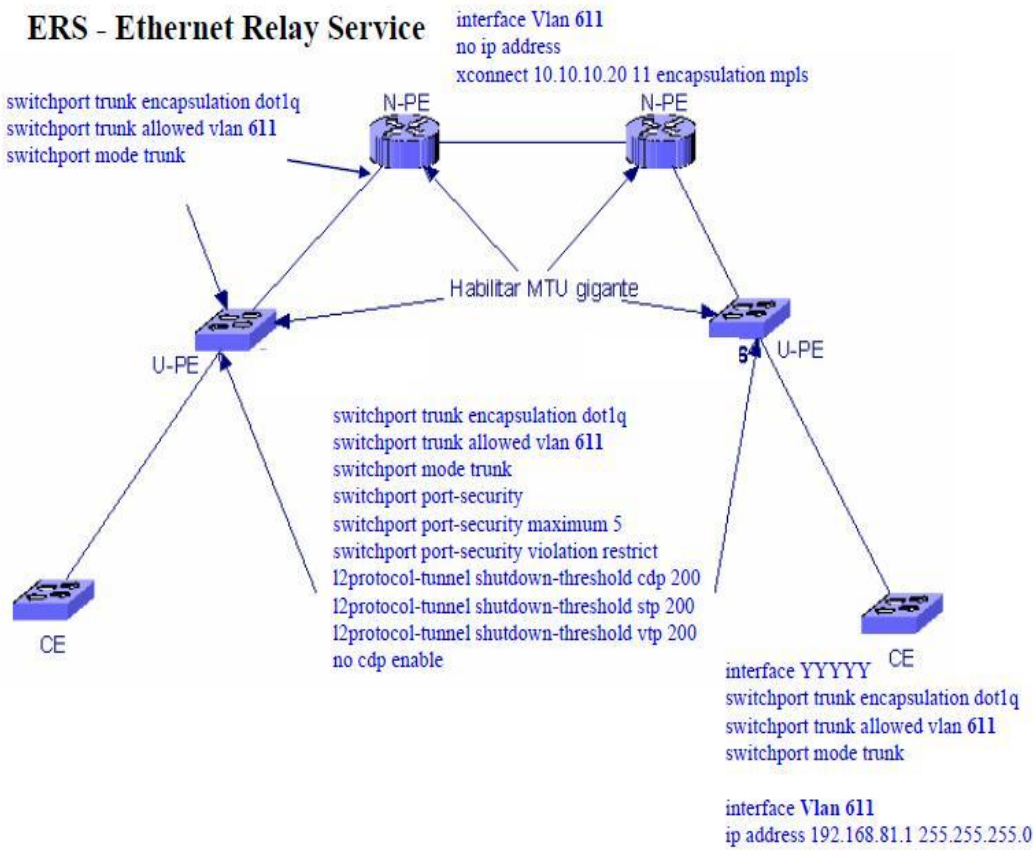


Figura 12 – Exemplo de configuração ERS

2.1.4.5. ERMS – Ethernet Relay Multipoint Service

Reflete importante extensão do ERS, em que conexões multiponto-multiponto são viabilizadas.

- Serviços ERS e ERMS podem coexistir na mesma UNI.
- Operação recomendada para ser feita por roteadores.
- Não é transparente. A VLAN do cliente é determinada pelo provedor.
- Necessário controle sobre a quantidade de MACs, broadcast, controles de nível 2, segurança e gerenciamento de banda.

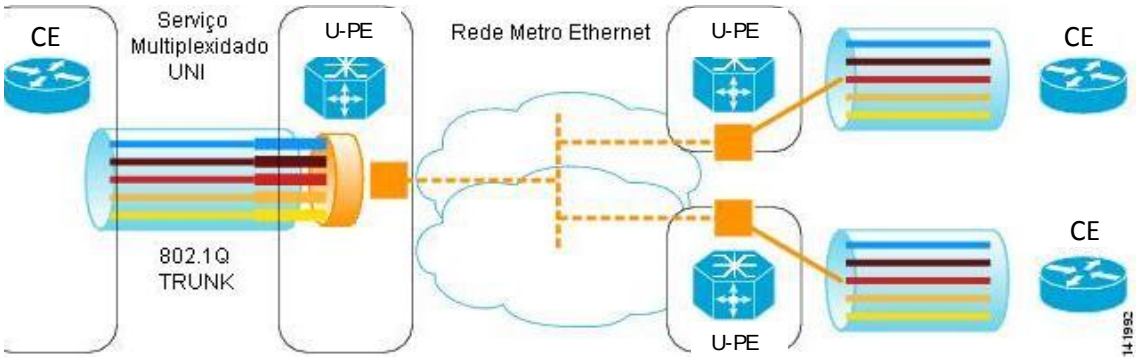


Figura 13 – Topologia Ethernet Relay Multipoint Service

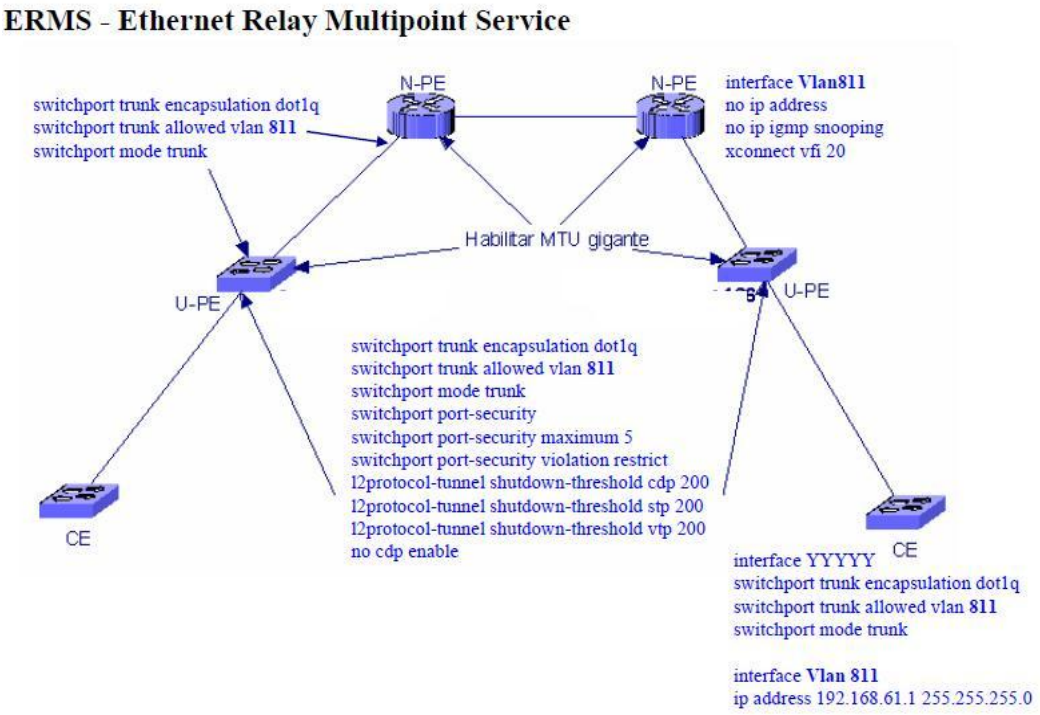


Figura 14 – Exemplo de configuração ERMS

2.1.4.6. EWS – Ethernet Wire Service

Refere-se ao serviço básico análogo às linhas privadas, onde roteadores (ou bridges) podem ser usados para estabelecimento de conexões ponto-a-ponto transparentes entre dois *sites*.

- Um EVC por porta.
- É transparente para BPDUs (Bridge Protocol Data Unit)

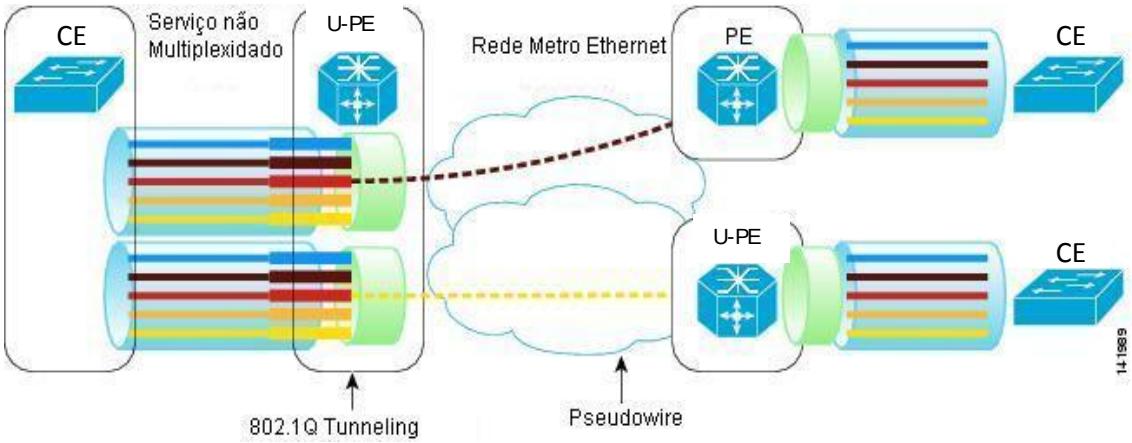


Figura 15 – Topologia Ethernet Wire Service

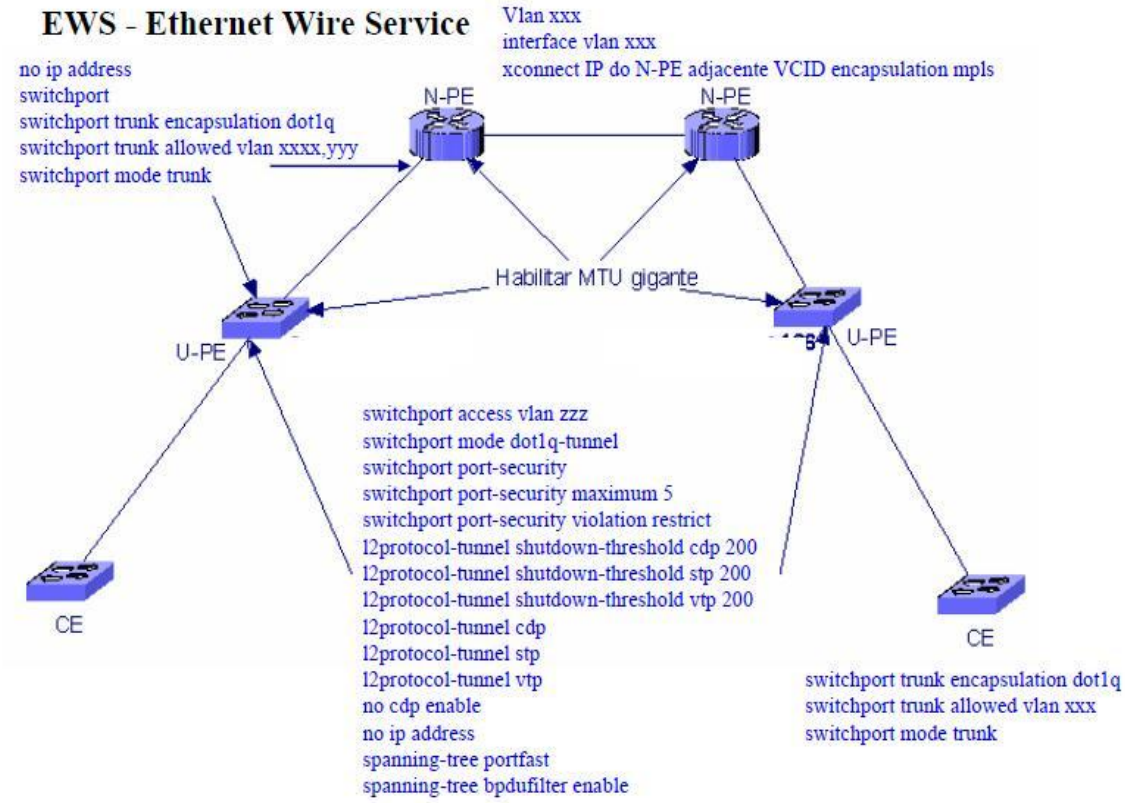


Figura 16 – Exemplo de configuração EWS

2.1.4.7. EMS – Ethernet Multipoint Service

O serviço *Ethernet Multipoint Service* (EMS), difere da EWS e ERS porque fornece um modelo de conectividade multiponto. A definição do serviço EMS ainda está em análise no âmbito do IETF, *Virtual Private LAN Service* (VPLS) grupo de trabalho. Embora o serviço EMS use um modelo multiponto, pode transmitir em *unicast* pacotes para destinos individuais, isto é, ele também suporta ligações ponto-a-ponto. Para o usuário final, a rede se parece com um *switch Ethernet* gigante onde cada cliente tem sua própria *VLAN* ou domínio de *broadcast*, ao invés de link fim-a-fim *pseudowire*.

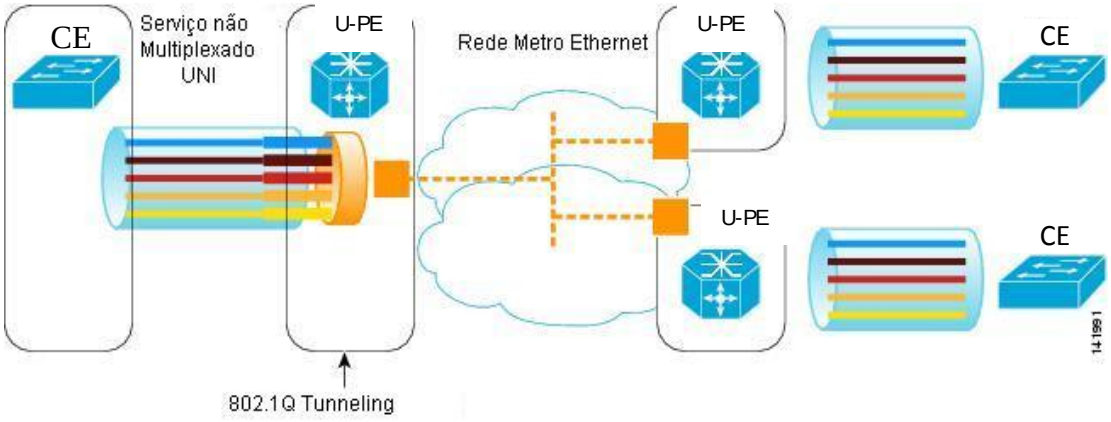


Figura 17 – Topologia Ethernet Multipoint Service

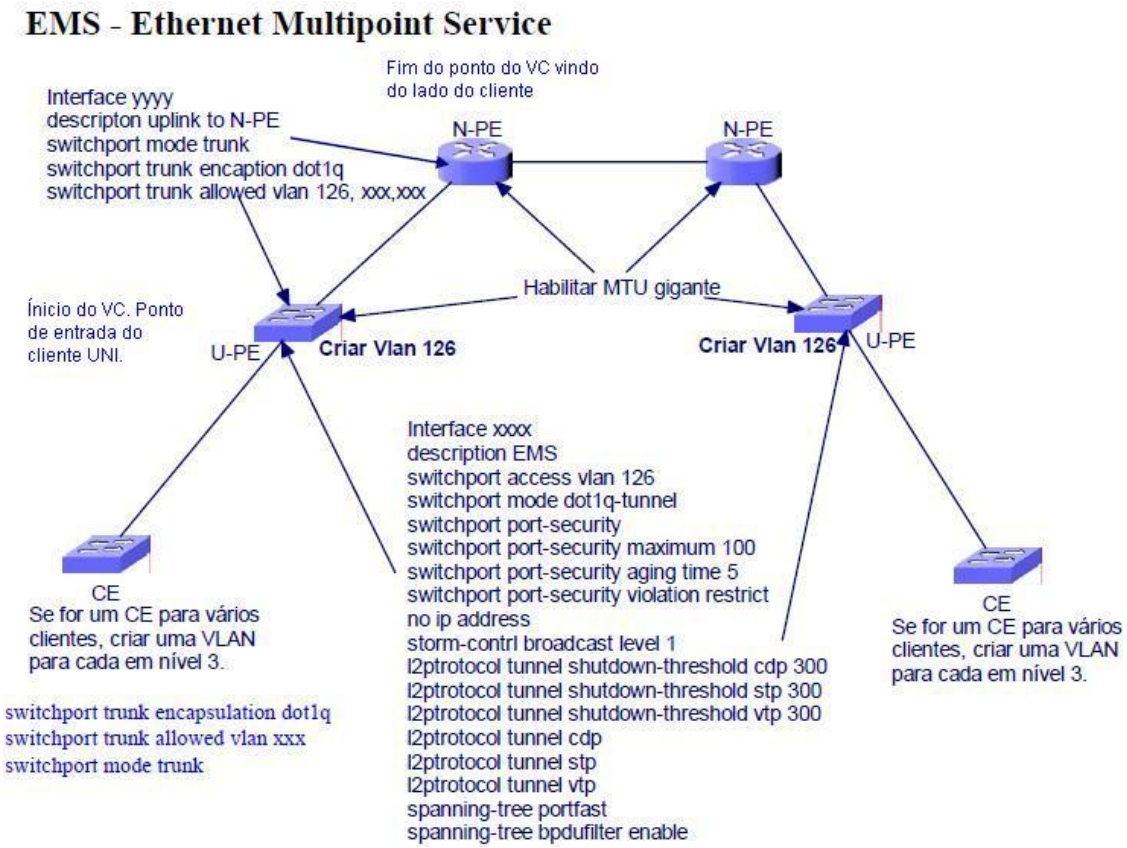


Figura 18 – Exemplo de configuração do serviço EMS

2.1.4.8. Serviços Principais Oferecidos na Prática

Na prática, a partir dos serviços canônicos surgiram e popularizaram-se três serviços principais oferecidos, no varejo, pelas operadoras que utilizam o Metro Ethernet para fornecer acesso e agregação:

- EPL – Ethernet Private Line: serviço dedicado fim-a-fim, com variações (por exemplo, com/sem *SLAs*). Taxas de transmissão variam entre 10 Mbps a 10 Gbps. Utilizado para conexão direta entre *sites*.
- DIA – Dedicated Internet Access: acesso Internet dedicado, interligando a LAN Ethernet da empresa até o *POP* de *ISP* que oferece o serviço. Nos mercados mais sofisticados os links são oferecidos a partir de 1 Mbps, com opções adicionais oscilando entre 5 Mbps e 10 Mbps.
- TLS – Transparent LAN Service: serviço de conectividade entre LANs, desenhado para interligar edifícios ou escritórios de empresas distantes geograficamente em taxa de transmissão similar àquela experimentada na rede local. Normalmente, os diferentes tráfegos são protegidos por mecanismos de segurança (separação) e a topologia pode ser desenhada visando aumentar a disponibilidade.

2.1.5. Protocolos de Camada 2

2.1.5.1. Ethernet

Robert Metcalfe e seus colegas na Xerox fizeram o seu projeto há mais de trinta anos. O primeiro padrão Ethernet foi publicado em 1980 por um consórcio entre a *Digital Equipment Company*, a Intel, e a Xerox chamado de DIX. Metcalfe quis que a Ethernet fosse um padrão compartilhado que beneficiasse a todos e foi então lançada como padrão aberto. Em 1985 o comitê de padronização de Redes Locais e Metropolitanas do Institute of Electrical and Electronics Engineers (IEEE) publicou padrões para redes locais. Esses padrões começam com o número 802. O padrão para Ethernet é 802.3. O IEEE procurou assegurar que os padrões fossem compatíveis com o modelo da International Standards Organization (ISO)/OSI. Para

fazer isso, o padrão IEEE 802.3 teria que satisfazer às necessidades da camada 1 e da parte inferior da camada 2 do modelo OSI. Como resultado, no 802.3 foram realizadas algumas pequenas modificações em relação ao padrão Ethernet original.

O padrão Ethernet original tem sido atualizado várias vezes com a finalidade de acomodar novos meios físicos e taxas mais altas de transmissão. Essas atualizações proporcionam padrões para as tecnologias emergentes e mantêm compatibilidade entre as variações da Ethernet.

A Figura 19 mapeia uma variedade de tecnologias Ethernet para a metade inferior da camada 2 do modelo OSI e toda a camada 1. A camada 1 da Ethernet envolve as interfaces entre meios físicos, sinais, fluxo de bits que se propagam nos meios físicos, componentes que inserem sinais nos meios e várias topologias. A camada 1 da Ethernet realiza um papel importante na comunicação existente entre dispositivos, mas cada uma de suas funções tem limitações. A camada 2 trata dessas limitações.

	802.3	802.4	802.5	802.6	802.11	802.12	802.16
MAC	CSMA/CD ethernet	Token bus	Token ring	DQDB	CSMA (WLAN)	prioridade	WLAN Banda Larga
Física	Coaxial Fios* Fibra	Coaxial	Fios*	Fibra	Sem fio	Fios*	Sem fio

Figura 19 – Padrões IEEE 802.X

As subcamadas de enlace de dados contribuem significativamente para a compatibilidade da tecnologia e a comunicação entre computadores. A subcamada MAC trata dos componentes físicos que serão usados para comunicar as informações. A subcamada LLC (*Logical Link Control*) permanece relativamente independente do equipamento físico que será usado para o processo de comunicação.

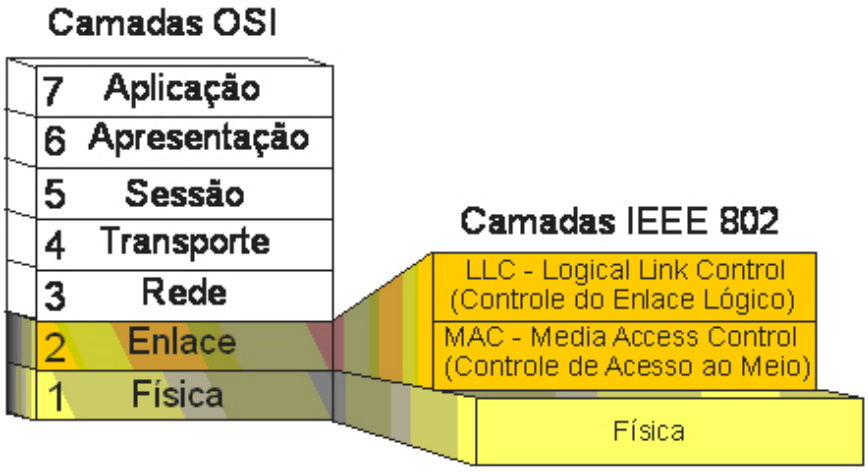


Figura 20 – Relação das camadas OSI e camadas IEEE 802

2.1.5.2. Frame Ethernet 802.3

O frame Ethernet 802.3 é composto pelos seguintes campos: preâmbulo, endereço de destino, endereço de origem, comprimento, dado, tipo e FCS (Seqüência de Checagem do Frame). A figura 21 mostra o formato do quadro, cada campo do cabeçalho é descrito a seguir:

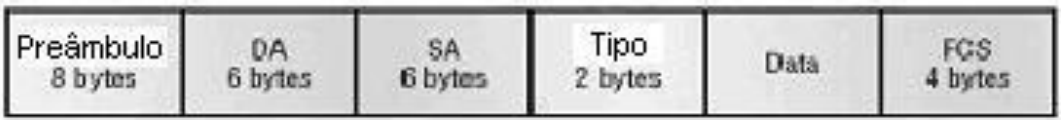


Figura 21 – Formato do quadro Ethernet 802.3

- Preâmbulo: há uma variância entre 0 e 1, para sincronizar o relógio interno do remetente. Consiste de 64 bits ou 7 bytes;
- Endereço de Destino (DA): este campo identifica qual computador receberá o quadro, que pode ser um endereço individual ou um grupo de endereços. Consiste de 6 bytes ou 48 bits;
- Endereço de Origem (SA): é usado para identificar o computador que emite a mensagem. Consiste de 6 bytes ou 48 bits;
- Tipo: é usado para identificar o protocolo da camada de rede. Consiste de 16 bits;

- Data: contém as informações a serem transmitidas, ou seja, os dados do usuário. O tamanho pode variar de 46 até 1500 bytes;
- *Frame Check Sequence* (*FCS*): é um campo usado para armazenar CRC (*Cyclic Redundancy Check*). Consiste de 4 bytes ou 32 bits.

2.1.5.3. VLAN

Uma VLAN é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local.

As VLANs segmentam logicamente as redes comutadas com base nas funções profissionais, departamentos ou equipes de projetos, independentemente da localização física dos usuários ou das conexões físicas da rede. Todas as estações de trabalho e servidores utilizados por um grupo de trabalho em particular compartilham a mesma VLAN, independentemente da sua conexão ou localização física. A configuração ou reconfiguração de VLANs é realizada através de software. Portanto, a configuração de uma VLAN não requer o deslocamento ou conexão física dos equipamentos da rede. A comunicação de uma estação de trabalho em um grupo VLAN é restrita aos servidores de arquivo no mesmo grupo VLAN. As VLANs segmentam a rede logicamente em diferentes domínios de broadcast, de modo que os pacotes sejam comutados somente entre portas designadas à mesma VLAN.

As VLANs são criadas para proporcionarem serviços de segmentação tradicionalmente proporcionados por roteadores físicos nas configurações de rede local. As VLANs tratam das questões de escalabilidade, segurança e gerenciamento da rede. Os switches não processam tráfego com bridges entre VLANs porque isso viola a integridade dos domínios de broadcast das VLANs. O tráfego deve ser roteado entre as VLANs. O protocolo predominante é o IEEE 802.1Q. Antes da

introdução do 802.1Q, o protocolo ISL da Cisco, uma variante do IEEE 802.1Q, foi um dos vários protocolos proprietários que existiram.

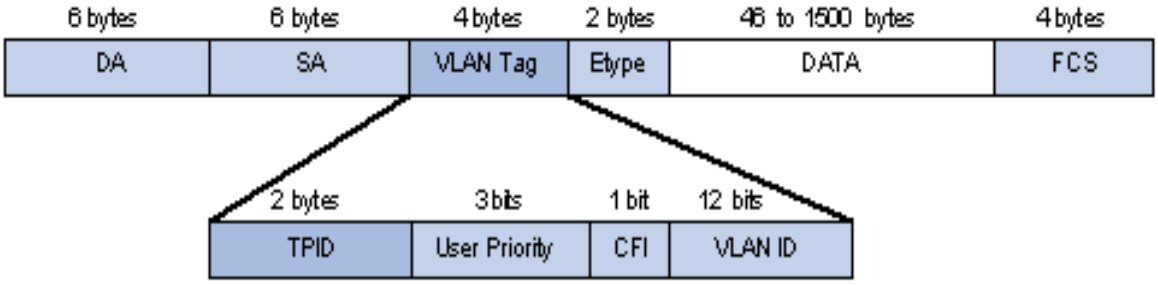


Figura 22 – Cabeçalho 802.1Q.

2.1.5.4. Protocolo Spanning Tree ou 802.1D

A primeira versão do *Spanning Tree Protocol* foi criada em 1985 pela empresa DEC (Digital Equipment Corporation). Em 1990, o IEEE criou sua própria versão, o 802.1D, chamado de STP. O objetivo é evitar que loops ocorram na camada 2 - Enlace de Dados - realizado por meio do monitoramento de todos os links da rede [5].

O conceito para se alcançar essa tarefa consiste na transmissão de mensagens especiais entre os switches para que se possa calcular o *Spanning Tree*. Essas mensagens trocas entre switch são chamadas de BPDUs ou mensagens de configuração, os quais contêm informações de configuração suficientes para que o switch possa efetuar as seguintes etapas:

- Eleger um único switch, entre todos da *LAN*, para se tornar o *Root Switch*;
- Calcular a distância do caminho mais curto para o *Root Switch*;
- Eleger o *Designated Switch* que fica próximo ao switch principal e enviar-lhe pacotes;
- Escolher uma porta, conhecida como Designated Port, que utiliza o melhor caminho para o *Root Switch*;

- Selecionar as portas que se incluem no *Spanning Tree*.

O *Spanning Tree* utiliza dois campos para montar uma topologia livre de loops, são eles: BID (*Bridge ID*) e *Path Cost*.

- *Bridge* ID: esses são únicos para cada switch, cujo tamanho equivale a 8 bytes, dividido em dois sub-campos: *Brigde Priotiy* e MAC, conforme ilustrado na figura 23.

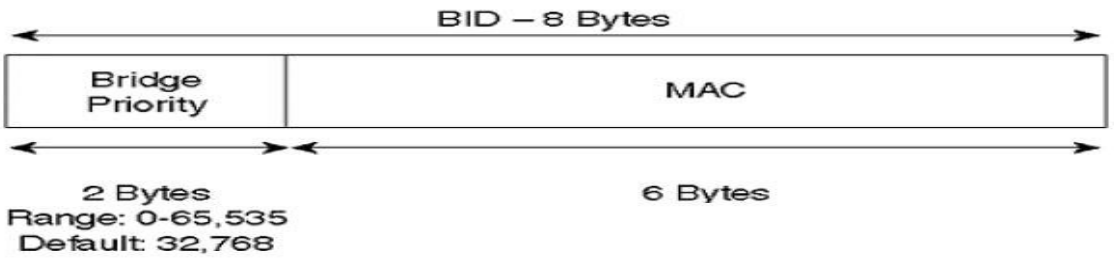


Figura 23 – Formato do *Bridge ID* IEEE.

- *Bridge Priority*: primeiro parâmetro para escolha do switch principal. Prioriza-se o menor valor e, esse varia 0 a 65535, com valor padrão equivalente a 32768, alterável para garantir que determinado switch vença a eleição;
- MAC: refere-se ao próprio endereço físico do switch, caso todos os switches possuam o mesmo valor *bridge priority*, utiliza-se para critério de desempate esse campo.

Em virtude disso, primeiramente, a precedência de escolha é para o menor *bridge priority*. Caso sejam iguais, o menor *MAC-address* será o escolhido.

- Path Cost: o *Spanning Tree* utiliza o conceito custo de link para escolha do melhor caminho para o switch principal e, esse está associado à largura do link. A tabela 1 lista os custos dos links de acordo com o IEEE [7].

Tabela 1 – Custo dos diferentes tipos de *Ethernet.*

Bandwidth	Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

A figura 24 nos mostra uma topologia STP com a bridge raiz e duas bridges não raiz. Observa-se que as bridges não raiz possuem uma porta raiz, porque está ligado diretamente a bridge raiz. Outro detalhe é que uma delas possui uma porta designada, pelo fato do custo ser menor e a outra não designada porque o custo é maior. A tabela 2 explica os papéis das portas STP, seu estado e a descrição de sua função.

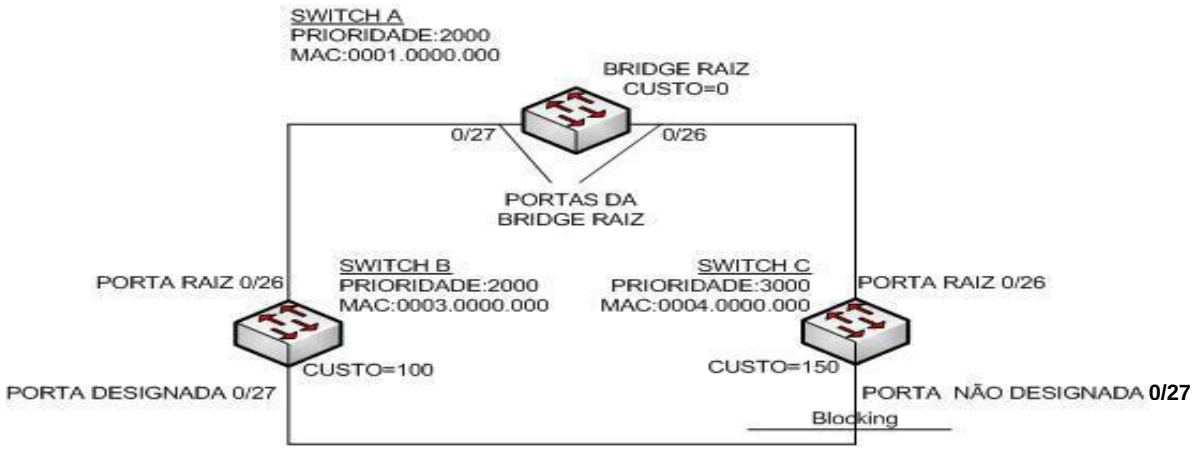


Figura 24 – Topologia da árvore STP

Tabela 2 – Papéis das portas STP

Porta	Estado	Descrição
Portas da bridge raiz	*Forwarding*	A bridge raiz é o núcleo da rede e todos os segmentos estão conectados a ela, portanto todas as portas estão no estado de forwarding.
Porta raiz da bridge não raiz	*Forwarding*	Recebe a BPDU (Bridge Protocol Data Units) da bridge raiz.
Porta designada	*Forwarding*	Encaminha a BPDU da bridge raiz para o seu segmento de LAN.
Porta não designada	*Blocking*	Não é usada para receber nem encaminhar quadros.

A eleição da bridge raiz, porta raiz, porta designada acontece quando um switch é ligado e começa a enviar mensagens BPDUs para trocar com outros switches, reivindicando ser a bridge raiz.

Essas mensagens especificam:

- O ID da bridge raiz que é a prioridade da bridge (0 - 65535) + MAC dessa bridge;
- O Custo para se alcançar à raiz a partir dessa bridge, quanto menor o custo menor o caminho, o custo fica na faixa de 0 a 65.535;
- O ID de bridge do emissor dessa BPDU, independente se for raiz ou não;

A BPDU define os tempos usados por todas as bridges/switches:

- *Hello time* (intervalo de tempo): O tempo que a raiz aguarda antes de encaminhar as *BPDUs hello* periódicas, as quais são encaminhadas por vários switches e bridges em seqüência. O padrão é 2 segundos.
- *MaxAge* (tempo máximo): O tempo máximo que qualquer bridge deve esperar, caso não receba mais os *hellos*, antes de tentar mudar a topologia STP, padrão é 20 segundos.

- *Forward Delay* (atraso de encaminhamento): Tempo em que uma interface demora a passar do estado *Blocking* para o estado de *Forwarding*. O padrão é 15 segundos.

Na tabela 3 são mostrados os estados intermediários das portas. Esses estados referem-se a uma mudança, partindo do estado de *blocking* até o estado *forwarding*.

Tabela 3 – Estados intermediários das portas no STP

Estado	Encaminha quadros de dados?	Aprende MACs com base nos quadros recebidos?	Estado transitório ou estável?
Blocking (Bloqueado)	Não	Não	Estável
Listening (Escutando)	Não	Não	Transitório
Learning (Aprendendo)	Não	Sim	Transitório
Forwarding (Encaminhando)	Sim	Sim	Estável

O processo de convergência STP, só ocorre quando há modificações na topologia da rede ou acontece alguma falha.

O protocolo STP sofreu alterações ao longo dos anos, que foram publicados em 1998 e 2004, incorporando várias extensões ao protocolo *spanning tree*. Embora o objetivo da norma seja promover a interoperabilidade dos equipamentos de diferentes fornecedores, diferentes implementações de um padrão não são garantidas para o funcionamento, por exemplo, devido a diferenças nas definições de configurações padrão do temporizador. Serão vistos as evoluções do STP e suas respectivas características.

2.1.5.5. Protocolo RSTP

O IEEE define o STP no padrão IEEE 802.1D. Sua evolução ou aprimoramento é RSTP (*Rapid Spanning Tree Protocol*) definido no padrão IEEE 802.1w. O RSTP funciona da mesma forma que o STP em vários aspectos como:

- Elege o switch raiz através do ID que é a concatenação da prioridade com o endereço MAC.
- Elege a porta raiz e portas designadas em switches não-raiz, com as mesmas regras.
- Cada porta fica no estado de *forwarding* ou *blocking* embora o RSTP chame o estado de *blocking* de *discarding*.

O IEEE aperfeiçoou o STP porque sua convergência demora um tempo relativamente alto, 50 segundos na configuração padrão. O tempo de convergência do RSTP é geralmente 10 segundos, mas pode ser reduzida para 2, ou até para 1 segundo, dependendo do caso.

Podem-se fazer enlaces com switches que estejam executando RSTP e STP sem nenhum problema, o switch que estiver executando o RSTP funcionará com STP nesse enlace e, adicionalmente, poderá ter outros enlaces com switches que esteja executando RSTP, sendo que com esses funcionarão em RSTP. A figura 25 mostra nosso exemplo em passos para melhor compreensão.

- Passo 1: uma rede sem enlaces redundantes.
- Passo 2: administrador da rede adiciona novo enlace entre os switchs “A” e “C”.

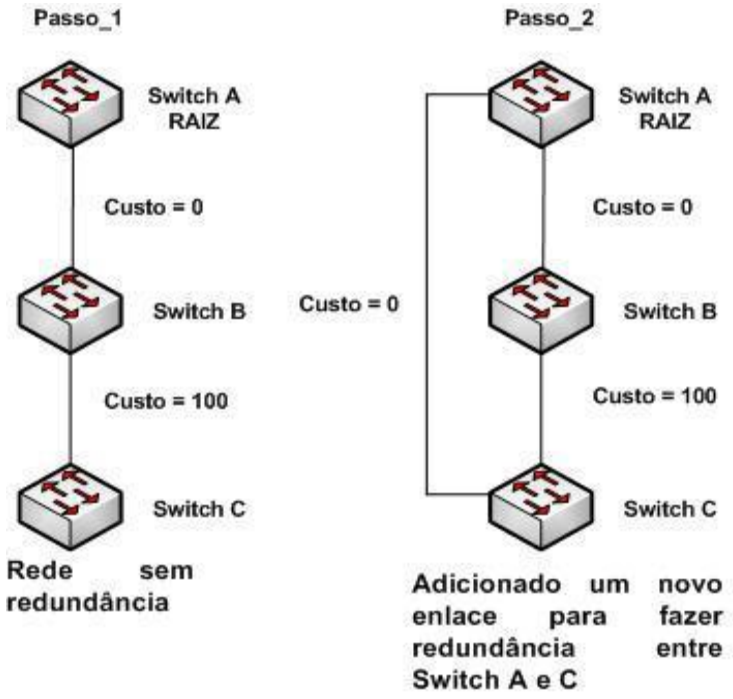


Figura 25a – Passos 1 e 2 durante a convergência RSTP

- Passo 3: switch “C” percebe que agora está recebendo BPDUs com custo menor vindos desse novo enlace, assim bloqueia todas a suas portas tipo link, ou seja, as portas que são ligadas a outros switches. Esse procedimento é feito para que não haja laços (loops) na rede. Assim, entra em contato com switch “A” para negociar sua nova porta raiz. Usando uma mensagem proposta-acordo (*proposal-agreement*) o switch “C” negocia uma transição rápida com switch “A”,. Assim que “A” concordar esse novo enlace entra em estado de *forwarding* e a ligação entre os switch “C” e “B” fica no estado de *discarding*, uma vez que a melhor BPDU vem do switch “A”.

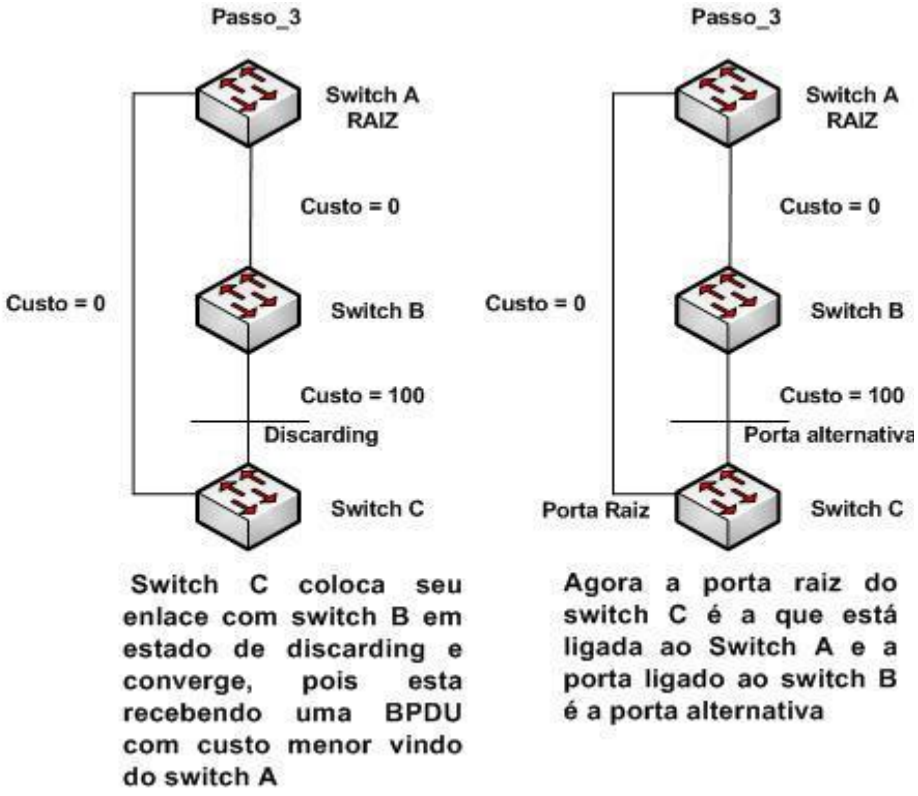


Figura 25b – Passo 3 durante a convergência RSTP

2.1.5.6. Protocolo PVST e PVST+

O protocolo PVST (Per Vlan Spanning Tree) é proprietário da Cisco System e baseado no IEEE 802.1D, basicamente o algoritmo do *Spanning Tree* é feito em cada Vlan.

PVST só funciona com o protocolo proprietário ISL devido à sua árvore s*panning tree* incorporar o *brigde ID*. Com a alta penetração do padrão IEEE 802.1Q VLAN *trunking* e a dependência do PVST pelo padrão proprietário ISL, a Cisco definiu um padrão diferente chamado PVST+ que suporta também o padrão 802.1Q.

PVST e PVST+ permitem balanceamento de carga, escolhendo *trunks* diferentes para diferentes VLANS. Na figura 26 o switch D1 é *root* para as VLANs de 501 à 1000; o switch D2 é *root* para as VLANs de 1 à 500, possuindo um balanceamento nos links redundantes.

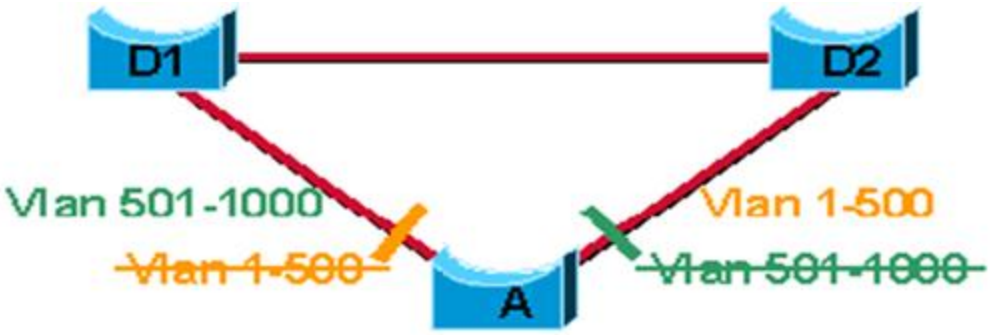


Figura 26 – Topologia de balanceamento PVST

2.1.5.7. Protocolo MSTP ou IEEE 802.1s

O Protocolo Múltiplo de Spanning Tree, originalmente definido no IEEE 801.s e posteriormente migrado para o IEEE 802.1Q-2003, define uma extensão para o RSTP. Este protocolo múltiplo de *spanning tree* "por vlan" define um *spanning tree* para cada grupo de VLAN e *bloqueia* não todas, mas um dos possíveis caminhos para cada *spanning tree*.

MSTP permite a formação de regiões MST que podem executar várias instâncias do MST (MSTI). Múltiplas regiões e de outras pontes STP estão interligadas através de um único e comum *Spanning Tree* (CST).

Ao contrário de algumas propriedades de implementação do *spanning tree* “por-vlan”, MSTP inclui todas as informações de *spanning tree* em um formato BPDU único, reduzindo o número de BPDUs necessários em uma rede de comunicação que abrange informações de árvore para cada VLAN. Também garante a compatibilidade com RSTP (e, em efeito, STP clássico também). MSTP faz isso através da codificação das regiões de informação adicional após o padrão RSTP BPDU, bem como um número de mensagens MSTI (de 0 a 64 instâncias, embora, na prática, muitas pontes suportem menos instâncias).

2.1.6. Protocolo 802.1 Tunneling

A utilização de VLANs é uma forma simples e segura de assegurar isolamento de tráfego dentro da rede. O padrão 802.1Q define o seu funcionamento, sendo que a cada VLAN é atribuído um identificador (VLAN-ID). Este conceito já é largamente utilizado pelas LANs existentes. Esta seria uma alternativa natural para as redes Metro Ethernet proverem isolamento de tráfego entre os diversos clientes. Porém, a utilização do 802.1Q em redes Metro Ethernet esbarra no problema da quantidade e administração dos VLAN-IDs. O operador de serviços não tem como gerenciar e assegurar que cada cliente utilize um VLAN-ID diferente dentro da rede metropolitana. Outra questão é que o número máximo de VLAN-IDs é de 4096, sendo este número limitado para as dimensões de uma rede metropolitana, além do fato de limitar o cliente na criação de suas próprias VLANs internas, o que não é aceitável.

Para solucionar esta questão, foi criado o conceito de tunelamento de *VLANs* (802.1ad – *Provider Bridge*, *Stacked* VLAN, VLAN *Tunneling*, *QinQ*). O tunelamento de VLAN é um mecanismo simples, no qual uma VLAN (*C-VLAN* – Cliente *VLAN*) é encapsulada (tunelada) dentro de outra VLAN (*S-VLAN – Service VLAN*), conforme a figura 27. Este tunelamento permite uma completa separação do tráfego do cliente. Desta forma, o cliente tem total liberdade de gerenciar suas C-VLANs. O provedor tem à sua disposição até 4096 S-VLANs, suportando até 4k clientes/serviços.

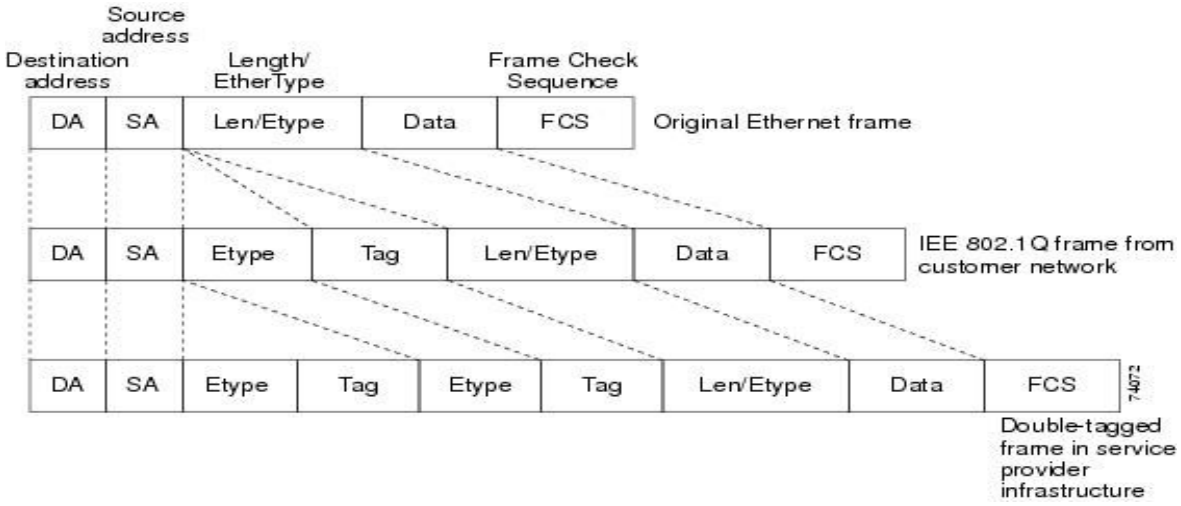


Figura 27 – Exemplo de tunelamento

O formato do cabeçalho do 802.1ad é similar ao do 802.1Q, conforme mostrado na figura 28. A implementação da S-VLAN se dá acrescentando 4 bytes ao cabeçalho Ethernet: após os campos de MAC de origem e destino, são inseridos 2 bytes correspondentes ao *EtherType* de S-VLAN (88A8 Hexadecimal) e dois bytes correspondentes ao TCI (*Tag Control Information*). Diferentemente do 802.1Q, o bit 4 do primeiro byte do campo TCI passa a ser chamado de DEI (*Drop Eligeble Indicator*). A combinação dos 3 bits de prioridade mais o bit DEI formam o conceito de PCP (*Priority Code Point*), que é utilizado dentro da rede como parâmetro de descarte ou não de pacotes.

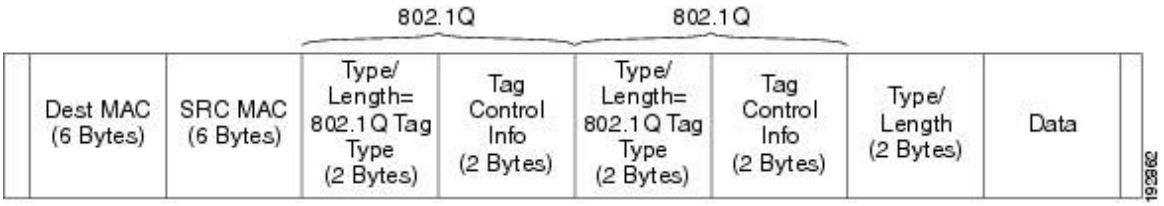


Figura 28 – Formato do quadro 802.1Q

Devido à inserção ou remoção destes 4 bytes do cabeçalho, o 802.1ad exige o recálculo do *checksum* do campo CRC do quadro Ethernet.

2.2. ITENS DE SEGURANÇA USADOS EM REDE METRO ETHERNET

2.2.1. Desabilitando Serviços ERS x EWS

O serviço de ERS não é transparente como o EWS, e por isso não é permitido o tráfego de PDUs (exemplo BPDUs) sendo bloqueado no switch U-PE da operadora. Vê-se a seguir como é bloqueado o tráfego de PDUs na interface UNI da operadora:

```
ERS UNI Configuração Global:
mac access-list extended Block-Invalid-ERS-Frames
deny any 0180.c200.000 00000.000.000f → Bloquea o tráfego STP
deny any host 0180.c200.0010
deny any host 0100.0c00.0000
deny any host 0100.0ccc.cccc
deny any host 0100.0ccc.cccd
deny any host 0100.0ccd.cdce
deny any host 0100.0ccd.cdd0
deny any  000b.fd80.6500 0000.0000.000f
permity  any any
!
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 30
no keepalive
mac access-group Block-Invalid-ERS-Frames in
no cdp enable.
!
```

O serviço EWS é transparente para o cliente permitindo o tráfego de PDUs na interface UNI. A seguir vê-se a configuração de lista de acesso na interface UNI:

```
EWS UNI Configuração Global:
mac access-list extended Block-Invalid-EWS-Frames
permit any host 0180.c200.0000 → Permite o tráfego do
      protocolo STP
deny any 0180.c200.000 00000.000.000f
deny any host 0180.c200.0010
deny any host 0100.0c00.0000
deny any host 0100.0ccc.cccc
deny any host 0100.0ccc.cccd
deny any host 0100.0ccd.cdce
deny any host 0100.0ccd.cdd0
deny any  000b.fd80.6500 0000.0000.000f
permity  any any
!
```

```
interface FastEthernet0/1
switchport  access vlan 15
switchport mode dot1q-tunnel
no keepalive
l2protocol-tunnel CDP
l2protocol-tunnel VTP
no cdp enable
!
```

2.2.2. Soluções para MAC Ataque

O ataque através do uso do endereçamento MAC se dá na intenção de transformar o switch em um repetidor (HUB). Quando isso ocorre o switch, agora HUB, passa a mandar os frames que entram no equipamento para todas as interfaces, ao invés de mandar apenas para a interface destino.

A solução para evitar esse tipo de ataque é limitando o numero de MACs por interface UNI, tendo como opção duas penalidades. São elas:

- Restrict: a porta continua em estado “UP” após a violação, mas os pacotes violados serão descartados. Abaixo vê-se um exemplo dessa configuração:

```
!
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20
switchport port-security → Habilitando modo de segurança
switchport port-security maximum 20 → Limitando a interface
       para, no máximo, 20 MACs
switchport port-security violation restric → Após esse número,
       descartar todos os frames.
!
```

- Shutdown: a porta é desabilitada após a violação, essa configuração é padrão, se for habilitado o modo de segurança. Abaixo vê-se um exemplo dessa configuração:

```
!
interface FastEthernet0/1
switchport trunk encapsulation dot1q
```

```
switchport trunk allowed vlan 10,20
switchport port-security → Habilitando modo de segurança
switchport port-security maximum 20 → Limitando a interface
       para, no maximo, 20 MACs
!
```

2.3. NÍVEIS DE QoS

2.3.1. Conceitos e Definições

A qualidade de serviços é obtida pela combinação de técnicas que tem por objetivo garantir níveis de confiabilidade compatíveis com as necessidades dos clientes. Da perspectiva da rede do cliente, o QoS é visto como uma especificação técnica e operacional de nível de serviço (SLS - *Service Level Specification*), o qual comercialmente é denominado de SLA (*Service Level Agreement*).

Uma das características do protocolo Ethernet é prover a cada usuário um acesso compartilhado e semelhante à rede, de forma que haja uma mínima implementação nos equipamentos da mesma. Isso é bom para uma ambiente LAN; porém para usar o Ethernet para prover serviços diferenciados, os provedores de serviços precisam, de alguma maneira, separar o tráfego dos clientes em redes privadas.

Em redes LAN, isso não é novidade, o tráfego entre departamentos é separado através do uso de LANs virtuais (VLANs). Cada VLAN é identificada por um *tag* (12 bits), adicionado após o cabeçalho MAC, como definido pelo padrão IEEE 802.1Q. Em uma rede Metro Ethernet, o provedor de serviços também tem a necessidade de separar o tráfego de seus clientes em redes separadas.

Vários padrões têm sido propostos para permitir uma melhor hierarquização do tráfego dentro das redes Metro Ethernet, assim como facilitar a atribuição de QoS.

2.3.2. Parâmetros de Tráfego

O parâmetro de tráfego especifica o limite da taxa média de quadros de serviços Ethernet que podem entrar na rede do provedor de serviços através de uma UNI. O MEF tem definido três atributos de parâmetro de tráfego, conforme mostrados na figura 29 e descritos a seguir.

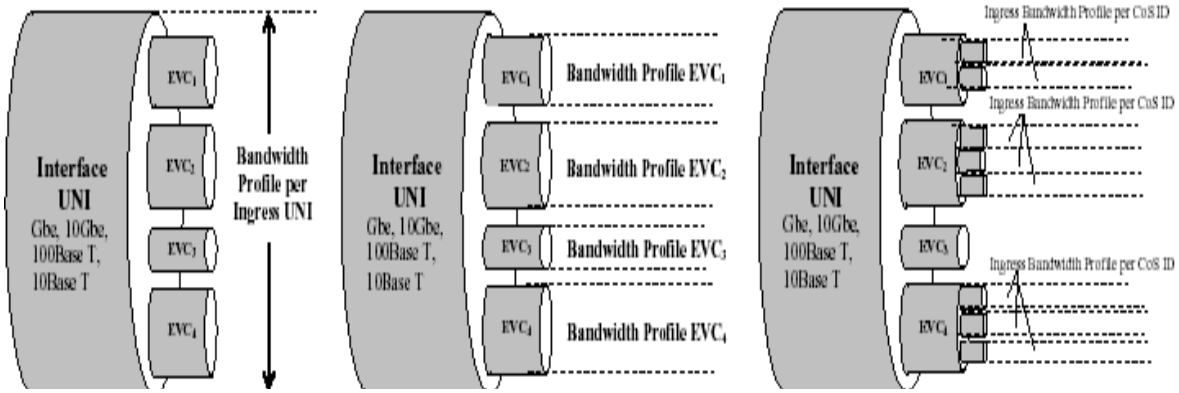


Figura 29 – Atributos de parâmetro de tráfego

- Perfil por UNI: aplica-se para todos os quadros de serviço que entram na rede do provedor através da UNI.
- Perfil por EVC: aplica-se para todos os quadros de serviço que passam por um determinado EVC dentro da UNI.
- Perfil pelo identificador CoS: aplica-se a todos os quadros de serviço dentro de um EVC identificados pelos bits de prioridade da marcação (*tag*) de VLAN IEEE 802.1p do cliente.

Cada atributo de *Bandwidth Profile* definidos acima, consiste de quatro parâmetros de tráfego que definem a vazão (*throughput*), fornecida pelo serviço. Os parâmetros de tráfego são os seguintes:

- CIR (*Committed Information Rate*): taxa média garantida e de acordo com os objetivos de desempenho contratados (por exemplo: *jitter*, atraso, etc.) e especificados em um SLA (*Service Level Agreement*).

- CBS (*Committed Burst Size*): definido como o número máximo de bytes permitidos para os quadros de serviços que entram, sendo ainda contados dentro do CIR.
- EIR (*Excess Information Rate*): taxa média, excedente ao CIR, para a qual os quadros de serviços são entregues sem nenhuma garantia de desempenho.
- EBS (*Excess Burst Size*): definido como o número máximo de bytes permitidos para os quadros de serviços que entram, sendo ainda contados dentro do EIR.

Um meio prático de descrever ou marcar os quadros de serviços quando sua taxa média está conforme ou não ao perfil definido é através do uso de cores. Os quadros de serviço verdes são os que estão de acordo com o SLA contratado e geralmente não podem ser descartados. Os quadros de serviço amarelos são os que não estão de acordo com o SLA contratado, mas que tipicamente não são imediatamente descartados. Os quadros de serviços vermelhos também não estão de acordo com os objetivos de desempenho contratados e são imediatamente descartados.

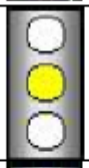
Conformance	Color	Service Frame Delivery
CIR Conformant		Service Frames green and delivered per the performance objectives specified in the SLA/SLS.
EIR Conformant		Service Frames are yellow and may be delivered but with no performance assurances.
None		Service Frames are red and dropped.

Figura 30 – Marcação dos quadros de serviço através de cores

A especificação do valor do CBS vai depender do tipo de aplicação ou tráfego que se deseja suportar. Por exemplo, para serviços destinados a suportar picos de transferência de dados TCP, o CBS deve ser muito maior que em aplicações VoIP, onde a taxa é mais constante.

As redes Metro Ethernet devem oferecer diferentes classes de serviço (CoS) para os clientes, identificados por meio de:

- Porta Física: nesse caso uma única classe de serviço pode ser fornecida.
- CE-VLAN CoS (802.1p): a classe de serviço é identificada pelos bits de prioridade do *tag* de VLAN do cliente. Nesse caso o SLA deve especificar o *Bandwidth Profile* e os parâmetros de desempenho para cada classe de serviço.
- DiffServ / IP TOS: o segundo byte do cabeçalho IP pode ser usado para definir classes de serviço. Para o caso do TOS, até 8 classes podem ser definidas. No caso do *Diffserv* capacidades mais robustas de QoS podem ser fornecidas através do padronizados PHBs (*Per-Hop Behaviors*).

O provedor de serviços vai utilizar um desses identificadores para, por exemplo, separar um tráfego que estará sujeito a um determinado CIR.

3. REDES MPLS

3.1. CONCEITOS

O MPLS, ou *MultiProtocol Label Switching*, foi originalmente desenvolvido pela IETF-Internet Engineering Task Force através da RFC-3031 e opera numa camada OSI intermediária às definições tradicionais do camada 2 (Enlace) e camada 3 (Rede), e se tornou recorrente ser referenciado como um protocolo de "camada 2,5".

Figura 31 – Formato do Rótulo MPLS.

O *label* é um identificador curto, de tamanho fixo e significado local. Todo pacote, ao entrar em uma rede MPLS, recebe um label. Este pode ser pensado como uma forma abreviada para o cabeçalho do pacote. Desta forma, os roteadores somente analisam os labels para poder encaminhar o pacote. O cabeçalho MPLS deve ser posicionado depois de qualquer cabeçalho da camada 2 e antes do cabeçalho da camada 3. Abaixo vê-se as descrições dos campos do cabeçalho MPLS.

- campo *Label/Tag* (20 bits) carrega o valor atual do rótulo MPLS;
- campo *EXP/COS* (3 bits) pode afetar o enfileiramento e algoritmos de descarte aplicados ao pacote enquanto ele é transmitido pela rede;
- campo *Stack/S* (1 bit) suporta uma pilha hierárquica de rótulos;
- campo *TTL* (8 bits) fornece funcionalidades de TTL IP convencional, especificando um limite de quantos saltos o pacote pode atravessar.

Como o MPLS foi concebido para permitir um serviço unificado de transporte de dados para aplicações baseadas em comutação de pacotes ou comutação circuitos, ele pode ser usado para transportar vários tipos de tráfego, como pacotes IP, ATM, SONET, ou mesmo frames Ethernet.

3.2. CARACTERÍSTICAS

O MPLS, é uma tecnologia de encaminhamento de pacotes baseada em rótulos (*labels*) que funciona, basicamente, com a adição de um rótulo nos pacotes de tráfego à entrada do *backbone* (chamados de roteadores de borda) e, a partir daí, todo o encaminhamento pelo backbone passa a ser feito com base neste rótulo. Comparativamente ao encaminhamento IP, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de roteamento.

Este protocolo permite a criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "*labels*" (usadas para roteamento) exclusivas de cada VPN.

Além disso, é possível realizar QoS (*Quality of Service*) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo.

Os produtos que as operadoras utilizam baseados em MPLS permitem que elas possam agregar valor aos seus produtos, pois passam a não oferecer apenas banda, mas um tráfego diferenciado com: Multimídia (Voz, Vídeo e Dados) e aplicações críticas, com garantias aplicáveis de QoS, através das seguintes classes de serviço:

- *Multimídia*: priorização de tráfego dos pacotes multimídia (ex.: vídeo conferência, etc.).

- *Voz*: priorização de tráfego dos pacotes de voz (ex.: interligação de PABX, telefonia IP, etc.).
- *Dados Expressos*: priorização de tráfego de dados de aplicações críticas (ex.: SAP, etc.).
- *Dados*: tráfego de dados sem priorização (*Best Effort*).

Os produtos baseados em MPLS, oferecidos pelas operadoras, permitem que possam ser utilizados nas seguintes situações:

- Acesso corporativo a servidores de aplicações centralizadas como sistemas corporativos, e-mail e Intranet;
- Formação de redes para compartilhamento de arquivos;
- Integração de sistemas de telefonia;
- Formação de sistemas de videoconferência;
- Acesso remoto aos sistemas corporativos.

3.3. FUNCIONAMENTO DO MPLS

O MPLS funciona da seguinte forma: cada pacote recebe um rótulo (*label*) de um determinado roteador LER (*Label Edge Router*). Os pacotes são encaminhados de um caminho comutado por rótulos LSP (*Label Switch Path*), formado por roteadores de comutação por rótulos LSRs (*Label Switch Routers*), e cada LSR toma decisões de encaminhamento baseado apenas no rótulo do pacote. Em cada salto, o LSR retira o rótulo existente e aplica um novo que diz ao próximo salto como encaminhar o pacote como descrito na (figura 32). Esse processo é muito parecido com o que acontece nas redes ATM com os VCs e VPs. [9].

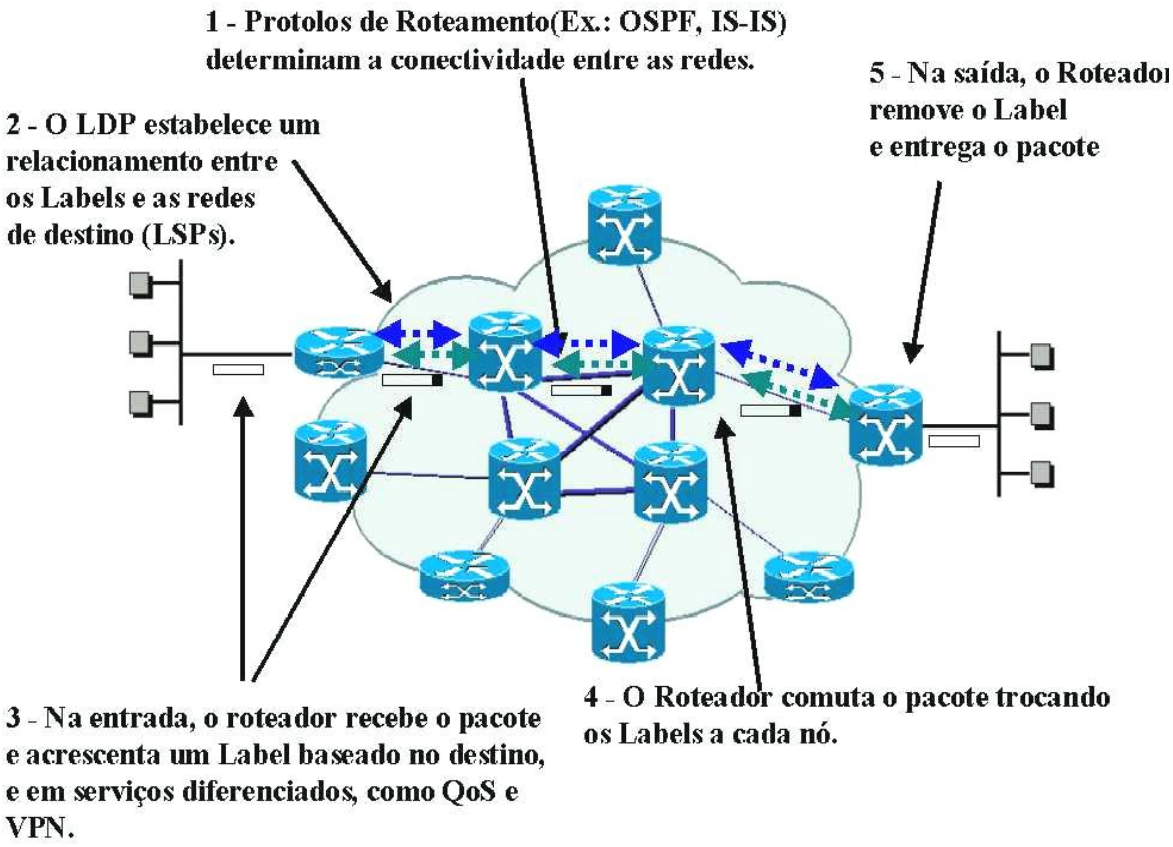


Figura 32 – Funcionamento MPLS [9]

A RFC 3031, "*Multiprotocol Label Switching Architecture*", define um rótulo como "um identificador curto de tamanho fixo e fisicamente contíguo, usado para identificar uma FEC (*Forwarding Equivalency Class*), normalmente com significado local". O cabeçalho MPLS deve ser posicionado depois de qualquer cabeçalho de camada 2 e antes de um cabeçalho de camada 3. Seu tamanho é definido em 32 bits. O rótulo que associa pacotes às respectivas conexões é algo semelhante ao VPI/VCI no ATM e ao DLCI no Frame-Relay. No nível mais simples, um rótulo pode ser pensado como nada mais que uma forma abreviada para o cabeçalho do pacote, de forma a indicar ao pacote a decisão de remessa que um roteador faria. [9].

O grupo de trabalho IETF decidiu que, quando possível, o MPLS deveria usar formatos existentes de rótulos. Por essa razão o MPLS suporta três tipos diferentes. Em hardware ATM, usa os bem definidos rótulos VCI e VPI. Em Frame-Relay,

utiliza-se o rótulo DLCI, e em qualquer outro lugar utiliza-se um novo e genérico rótulo conhecido como *Shim Shim* Header [9] (figura 33), que se posiciona entre as camadas 2 e 3. Como o MPLS permite criar novos formatos de rótulos sem ter que trocar os protocolos de roteamento, é relativamente simples estender a tecnologia para formas de transporte óptico emergentes, como DWDM e comutação óptica:

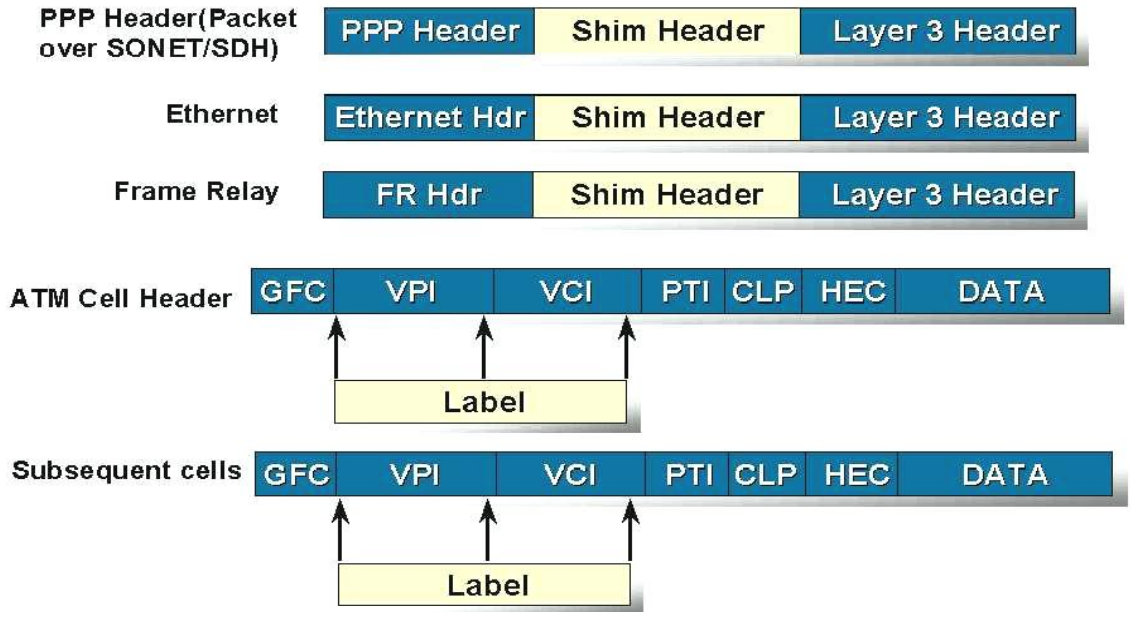


Figura 33 – *Shim* Header [9]

- Pilha de Rótulos (Label Stack)

A comutação de rótulos foi projetada para ser usada em redes de grande porte, e o MPLS suporta comutação de rótulos com operações hierárquicas, baseadas na habilidade do pacote carregar mais de um rótulo. O empilhamento de rótulos permite que LSRs designados troquem informações entre si e ajam como nós de borda para um grande domínio de redes e outros LSRs. Estes outros LSRs são nós internos ao domínio, e não se preocupam com rotas inter-domíno, nem com os rótulos associados a essas rotas.

O processamento de um pacote rotulado é completamente independente do nível de hierarquia, ou seja, o nível do rótulo é irrelevante para o LSR. O processamento é sempre baseado no rótulo do topo, abstraindo-se dos outros rótulos que podem haver abaixo deste. A figura 34 mostra um exemplo de Pilha de Rótulo. [9]

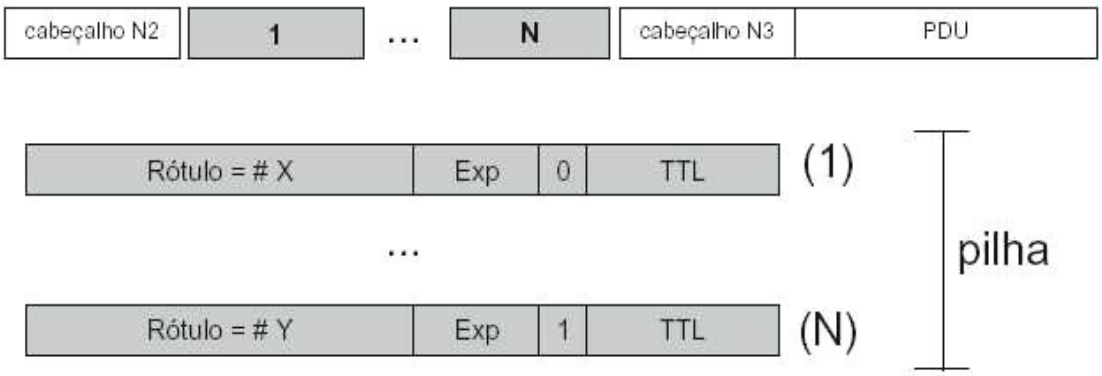


Figura 34 – Pilha de Rótulo [9]

- FEC (Classe de Equivalência de Envio)

Uma FEC consiste em um conjunto de pacotes que serão encaminhados da mesma maneira em uma rede MPLS. Pacotes de um mesmo fluxo de dados geralmente pertencem à mesma FEC. Requisitos de QoS também podem ser definidos com a designação de FECs. A FEC é representada por um rótulo e cada LSP é associado a uma FEC. Ao receber um pacote o LER verifica a qual FEC ele pertence e o encaminha através do LSP correspondente. Portanto, há uma associação pacote-rótulo-FEC-LSP. A associação pacote-FEC acontece apenas uma vez, quando o pacote entra na rede MPLS. Isto proporciona grande flexibilidade e escalabilidade a este tipo de rede.

- LSR (Label Switch Routers)

LSRs são os roteadores de comutação por rótulos. Eles são equipamentos de comutação (por exemplo: roteadores IP, switches ATM) habilitados para MPLS,

devem ter algumas funcionalidades definidas pelo MPLS implementadas. São equipamentos situados no núcleo da rede MPLS, e sua função é encaminhar pacotes baseados apenas no rótulo de cada pacote.

Ao receber um pacote cada LSR troca o rótulo existente por outro, passando o pacote para o próximo roteador e assim por diante.

- LER (Label Edge Routers)

O LER é um roteador que fica na borda da rede, e é responsável por inserir ou remover pilhas inteiras de rótulos dos pacotes, dependendo se estes estão entrando ou saindo da rede, respectivamente. LERs realizam o FTN - *FEC-to-NHLFE* (redireciona pacotes ainda sem *labels* para o NHLFE - *Next Hop Label Forwarding Entry*, baseado na FEC). Também devem poder se conectar com redes de diferentes tipos, já que fazem a fronteira entre o domínio MPLS e as demais. LER é uma definição à parte do padrão MPLS, criado para facilitar a visão do domínio. Eles são, na verdade, LSRs que têm a capacidade de fazer fronteira com outras redes como Ethernet, Frame-Relay e ATM, ilustrado na figura 35.[9].

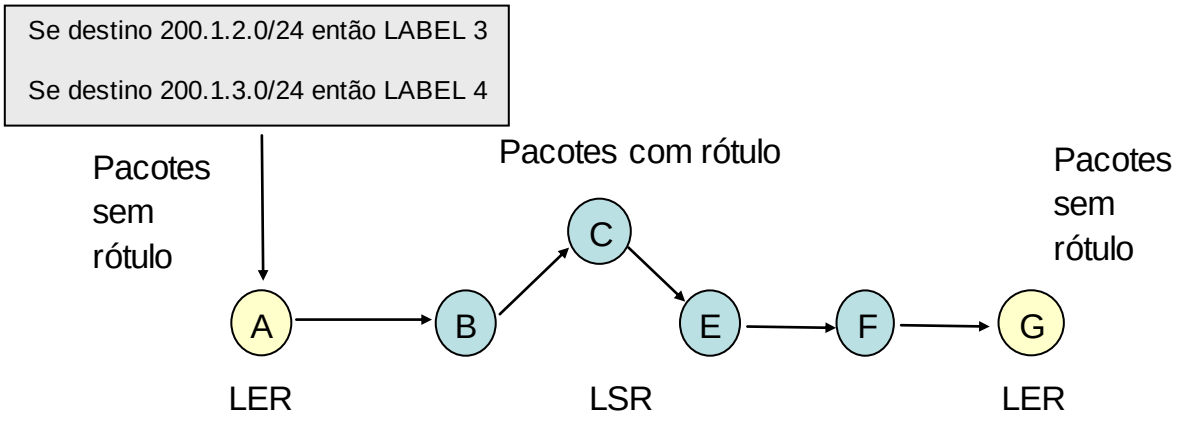


Figura 35 – Rede MPLS [9]

- LSP (Label Swith Path)

O LSP consiste em um caminho comutado por rótulo, ou seja, um caminho através de uma seqüência ordenada de LSRs, estabelecido entre uma origem e um destino. Um LSP é unidirecional, portanto é preciso ter dois LSPs para uma comunicação entre duas entidades.

Um LSP é um caminho através do qual transitarão pacotes de uma mesma classe e que compartilham o mesmo destino. Assim, uma rota deve ser estabelecida inicialmente. Isto é feito com protocolos de roteamento convencionais ou roteamento com restrições, quando o caminho fica definido, os pacotes pertencentes a ele não precisam mais ser roteados. Eles serão apenas comutados com base nos seus rótulos. Estes rótulos são distribuídos entre LSRs no momento do estabelecimento de LSPs, conforme mostrado na figura 36.

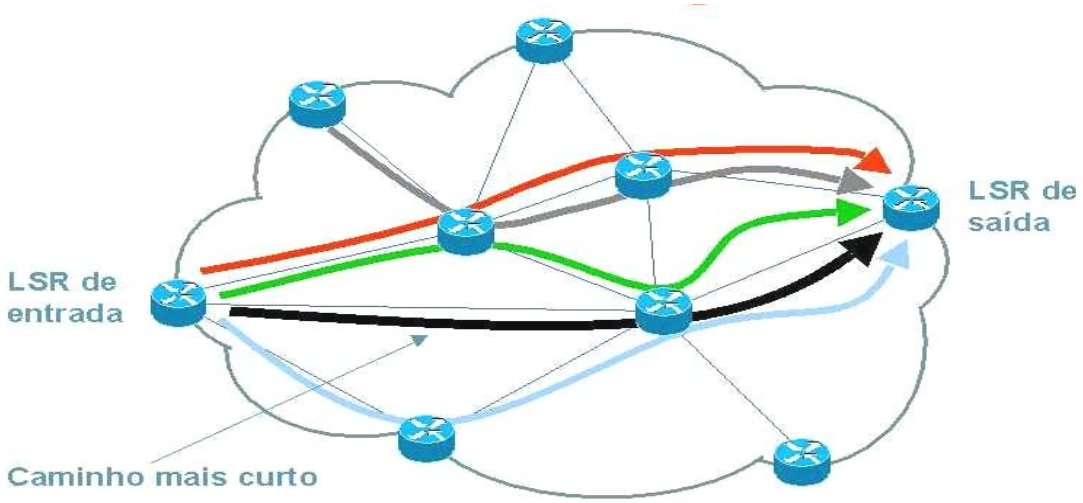


Figura 36 – LSP - Label Switching Paths

- LDP (Label Distribuition Protocol)

O LDP é uma especificação que permite a um LSR (Roteador de Comutação de Rótulos) distribuir rótulos. Quando um LSR atribui um rótulo a uma FEC (Classe de Equivalência de Envio), é preciso que ele deixe que seus pares saibam desse rótulo

e seu significado. O LDP é usado para este propósito. Já que um conjunto de rótulos do LSR de entrada ao LSR de saída em um domínio MPLS, define um caminho de comutação de rótulos (LSP), e que rótulos são mapeamentos de roteamento da camada de rede para os caminhos comutados da camada de enlace, o LDP ajuda no estabelecimento de um LSP através do uso de um conjunto de procedimentos para distribuir os rótulos entre os LSR.

LSRs utilizam rótulos para encaminhar tráfego. Um passo fundamental para a comutação de rótulos é que LSRs concordem em relação as quais rótulos eles devem usar para encaminhar o tráfego. Eles chegam a este entendimento utilizando o LDP.

O LDP é uma das partes mais importantes do MPLS. Mecanismos similares para troca de rótulos existiram em implementações proprietárias como o IFMP (*Ipsilon´s Flow Manegement Protocol*), ARIS (*Aggregate Route-based IP Switching)* da IBM), e TAG (*Tag Distribuition Protocol)* da Cisco.

LDP e rótulos são a base da comutação de rótulos e possui as seguintes características básicas:

- Oferece um mecanismo de "descoberta" de LSR para permitir que LSRs encontrem uns aos outros e estabeleçam comunicação;
- Define quatro classes de mensagens: *DISCOVERY*, *ADJACENCY*, *LABEL*, *ADVERTISEMENT* e *NOTIFICATION* (mensagens de notificação);
- Ele trabalha sobre TCP para proporcionar fidelidade de mensagens.

3.4. *ANY TRANSPORT OVER MPLS* - AToM

Any Transport over MPLS (AToM) é uma solução para o transporte de pacotes camada 2 sobre uma rede MPLS, permitindo que os prestadores de serviços utilizem a sua rede MPLS para fornecer conectividade entre sites de clientes existentes,

mantendo a camada 2 da rede. Em vez de separar redes com ambientes de gerenciamento de rede, provedores de serviços podem utilizar a rede MPLS para transportar todos os tipos de tráfego para diferentes clientes. O switch da Cisco Catalyst 3750 suporta EoMPLS Metro, um subconjunto de AToM que usa um mecanismo de encapsulamento para transportar tráfego Ethernet de camada 2 Ethernet. EoMPLS encapsula quadros Ethernet em pacotes MPLS e encaminha através da rede MPLS. Cada quadro é transportado como um único pacote, e os roteadores PEs ligadas ao *backbone* adicionam e removem etiquetas conforme apropriado para o encapsulamento de pacotes:

- O roteador PE de entrada recebe um quadro Ethernet e encapsula o pacote através da remoção do preâmbulo, o delimitador de início de quadro (SFD), e a seqüência de verificação de quadro (FCS). O restante do cabeçalho do pacote não é alterado.
- O roteador PE de ingresso acrescenta um *label* de conexão virtual (VC) ponto-a-ponto e um rótulo caminho ligado (LSP rótulo túnel) para MPLS normal de roteamento através do *backbone* MPLS.
- Os roteadores de núcleo da rede usam o rótulo LSP túnel para mover o pacote através do backbone MPLS e não fazem distinção do tráfego Ethernet de quaisquer outros tipos de pacotes no *backbone* MPLS.
- Na outra ponta do *backbone* MPLS o roteador de saída PE recebe o pacote e desencapsula o pacote através da remoção do rótulo se um túnel LSP está presente. O roteador PE também remove o rótulo de capital de risco do pacote.
- O roteador PE atualiza o cabeçalho, se necessário, e envia o pacote para a interface de destino apropriada.

O *backbone* MPLS utiliza os rótulos do túnel para o transporte de pacotes entre os roteadores PE. O roteador PE de saída usa o Label VC para selecionar a interface de saída para o pacote Ethernet. Túneis EoMPLS são unidirecionais; para ser bidirecional precisa ser configurado um túnel em cada sentido.

O VC ponto-a-ponto requer que se configure os parâmetros de VC nos dois roteadores PE. Apenas os roteadores PE de entrada e de saída do *backbone* MPLS vão saber sobre os caminhos dedicado ao transporte de tráfego da camada 2. Outros roteadores do *backbone* não possuem entradas na tabela para esses caminhos.

3.5. EoMPLS E 802.1Q TUNNELING

A característica do *IEEE 802.1Q Tunneling* permite que os provedores de serviço usem uma única VLAN para prestar serviço aos clientes que têm várias VLANs, preservando os IDs da VLAN do cliente e segregando o tráfego em VLANs diferentes.

A figura 37 é um exemplo de configuração onde o tráfego *IEEE 802.1Q Tunneling* é encaminhado através *EoMPLS* de uma rede MPLS. Para dar suporte 802.1Q tunelamento em uma topologia onde um dispositivo de camada 2 se conecta a uma rede MPLS através de um equipamento (roteador) que funciona como um PE, a porta LAN de entrada do PE que recebe o tráfego *802.1Q tunneling* (PE1) é configurada como porta túnel para aceitar o tráfego da VLAN 100. No roteador PE1 a interface é configurada para *port-based* de encaminhamento do EoMPLS, com o roteador PE2 como o endereço IP de destino. Quando os pacotes das Vlans de 10 a 50 chegam de CE1 eles são encapsulados em VLAN-100 e enviados para a porta de saída do PE1 que está conectado à rede MPLS. Na porta de saída, uma etiqueta

MPLS é adicionada ao cabeçalho do quadro antes que seja mapeado para um CV e enviadas para o PE MPLS seguinte (PE2).

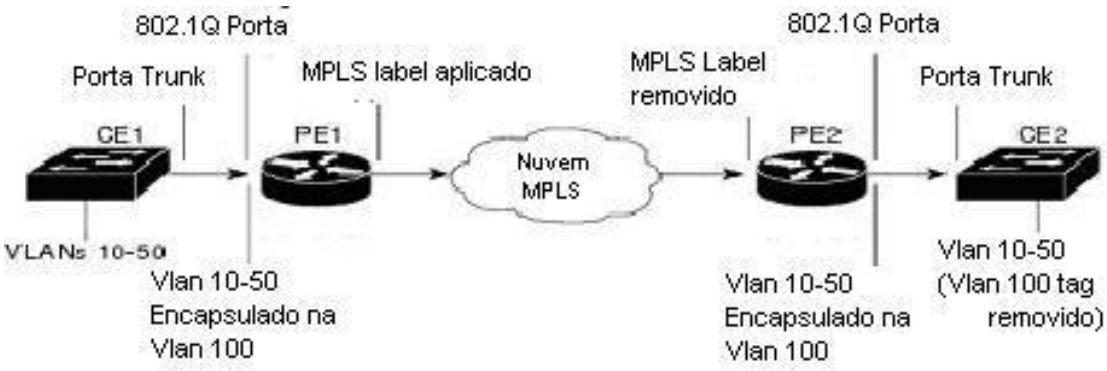


Figura 37 – Exemplo de Configuração 802.1Q

Ao entrar na rota MPLS L2transport ou o comando de configuração *XConnect* interface em cada uma VLAN para *EoMPLS VLAN-Based* ou uma porta Ethernet para *port-based EoMPLS*, pode-se configurar um túnel EoMPLS para encaminhar o tráfego baseado em um ou outro cliente ou a VLAN da porta Ethernet .

- Para encaminhar o tráfego 802.1Q túnel encapsulado através do núcleo MPLS para um destinatário específico do outro lado da rede MPLS, configura-se a porta como *port-based EoMPLS*.
- Para encaminhar o tráfego 802.1Q túnel encapsulado de um dispositivo de acesso a um roteador PE, configura-se a porta como *VLAN-based EoMPLS*.

O Protocolo Tunneling de camada 2 através de uma ligação EoMPLS permite que os protocolos CDP, STP, e VTP (PDUs) sejam tunelados através de uma rede MPLS. Para suportar o protocolo *tunneling* de camada 2, quando o dispositivo de camada 2 se conecta a uma rede MPLS através de um equipamento (roteador) que funciona como um PE, pode-se configurar a porta de entrada do PE que recebe o tráfego

como uma porta túnel. O tráfego do protocolo de camada 2 é encapsulado antes que seja transmitida através da rede MPLS.

O protocolo EoMPLS também tem suas limitações, que estão descritas abaixo:

- MTU - EoMPLS não suporta o pacote de fragmentação e remontagem. Por isso a unidade de transmissão máxima (MTU) de todos os elos intermediários entre os dois pontos devem ser suficientes para levar o maior quadro de camada 2 VLAN recebido. A entrada e saída dos roteadores PEs devem ter o mesmo valor MTU.
- Formato do Endereço - todos os endereços de *loopback* em roteadores PE devem ser configurado com máscaras de 32 bits para garantir o funcionamento adequado do encaminhamento MPLS. OSPF requer o uso de endereços de *loopback*.
- Formato do Pacote - EoMPLS suporta VLANs que estejam em conformidade com o padrão IEEE 802.1Q. Encapsulamento de ISL não é suportado entre os roteadores PE e CE.
- O número máximo de VLANs usando EoMPLS em um switch é 1005.
- Para suportar spanning tree (BPDUs) atravessando o *backbone EoMPLS*, deve ser desativado o *spanning tree* da VLAN do EoMPLS. Isso garante que as VLANs EoMPLS sejam enviadas apenas para interface *trunk* do switch to cliente.
- A VLAN nativa da interface *trunk* não pode ser uma VLAN EoMPLS

4. METODOLOGIA DE PESQUISA

4.1. TIPO DE PESQUISA

Quanto aos meios, esta pesquisa é:

a) ***Estudo de Caso*** que “é apenas uma das muitas maneiras de se fazer pesquisa em ciências sociais” [11]. Por se tratar de um estudo profundo, visando obter o máximo de informações que permitam um amplo conhecimento, o que seria impossível em outras pesquisas [12].

   A característica principal da pesquisa por estudo de caso é o fato de que quanto maior a quantidade de informação, melhor será a analise dos fatos.

b) ***Telemática,*** de acordo com a utilização de *WebSites* e bibliotecas *online* tais como UFRJ e PUC RIO.

4.2. COLETA E ANÁLISE DE DADOS

Segundo Gil [12], a coleta de dados em um estudo de caso é baseada em diversas fontes de evidências. Para efeito de elaboração dessa pesquisa, foram utilizados os seguintes procedimentos: entrevistas e técnica de observação participante.

As entrevistas focais, conforme classificação de Yin [11] ou focalizadas, de acordo com Gil, constituíram no principal meio de coleta de dados deste estudo. Ao mesmo tempo em que as entrevistas concedidas foram espontâneas, elas também foram parcialmente estruturadas, uma vez que precisaram ser guiadas por alguns pontos de interesse explorados pelo pesquisador. O roteiro utilizado durante a condução das entrevistas encontra-se disponível no Anexo I deste trabalho.

A coleta de dados ocorreu por meio de documentação direta, em entrevistas, abordando a implementação do projeto, seus problemas e seus benefícios. O roteiro de entrevista foi encaminhado aos Administradores de Redes, que no caso desta

pesquisa, foram dois responsáveis, e posteriormente serviram de roteiro de perguntas para uma série de entrevistas pessoais. Os mesmos administradores, posteriormente, também participaram através de novos formulários, que serviram de roteiro para perguntas direcionadas a entrevistas de cunho mais pessoal.

4.3. LIMITAÇÕES DO MÉTODO

A primeira limitação encontrada refere-se ao tipo de pesquisa utilizada, especialmente, quanto aos meios. De acordo com Yin [11], estudos de caso são generalizáveis a proposições teóricas e não a populações ou universos.

Já a segunda limitação relaciona-se com os procedimentos / técnicas utilizadas para coleta de dados. As entrevistas focais [11] ou focalizadas [12], além de contarem com a presença de um entrevistador, que pode inibir o entrevistado levando-o a emitir uma opinião diferente do que realmente pensa sobre determinado assunto, têm o inconveniente de captar as percepções dos entrevistados sobre os fatos, que podem não corresponder à realidade das organizações e sim à visão prática, ou até mesmo ao anseio dos entrevistados, comprometendo assim a análise. Para tentar minimizar o constrangimento causado pela presença do entrevistador, o pesquisador buscou, logo no início das entrevistas, garantir a confidencialidade das informações obtidas e deixar claro o caráter acadêmico da análise.

5. ANÁLISE DE CASO – MUNDIVOX TELECOMUNICAÇÕES

5.1 HISTÓRIA

A Mundivox Telecomunicações é uma empresa de telecomunicações com 10 anos de vida no mercado brasileiro, licenciada pela ANATEL para prover serviços de comunicação de redes. Dirigida por seu fundador e atual Presidente, Alberto Duran, a Mundivox possui uma equipe de executivos com sólida experiência em telecomunicações.

Com ajuda de parceiros tecnológicos, a Mundivox lançou no Rio de Janeiro, em novembro de 2000, sua rede de fibra ótica, um *Data Center* e um Centro de Operação de Rede de última geração. Atualmente, a Mundivox provê serviços de transmissão de dados para clientes corporativos e residenciais, destacando-se pelo acesso dedicado à Internet, redes privadas virtuais, hospedagem de páginas, e-mail e *co-location* ("compartilhamento de localização", entendida como espaço físico e infra-estrutura).

Com investimentos em tecnologia a Mundivox deixou o legado da Rede ATM para trás e iniciou o processo de migração do *backbone* para tecnologia IP. Após essa migração no seu *backbone*, a demanda por alta velocidade obrigou a Mundivox a rever toda sua rede de transporte. Para atender toda essa demanda de crescimento começou o processo de implementação da Rede Metro Ethernet na rede de transporte integrada com a atual rede SDH.

Com uma rede de quase 1000 km de rede de fibra ótica passada no Rio de Janeiro, ficou fácil essa integração com a Rede Metro Ethernet. A rede Metro começou no Centro do Rio até Botafogo na Zona Sul. Com um link de 1 Gbps redundante entre esses dois pontos, começaram as instalações de clientes de alta velocidade (10 Mbps a 100 Mbps).

O sucesso da Rede Metro foi muito rápido: em 6 meses foi criada uma grande estrutura de rede de fibra ótica ligando Centro, Botafogo, Tijuca e Barra da Tijuca, todas situadas na capital do Rio de Janeiro.

5.2. INFRA-ESTRUTURA DE REDE METRO ETHERNET

A Mundivox possui hoje duas Redes Metro Ethernet: a primeira abrange a região do Centro, Botafogo, Leblon e Tijuca. A segunda e mais recente, abrange a região do Centro para Barra da Tijuca. O tamanho da rede de fibra ótica para atender essa topologia gira em torno de 400 Km. Toda a rede Metro Ethernet foi implementada em anel ótico, usando equipamento da Cisco Systems. Os switches utilizados para essa topologia são da família 3500, 3700 e 6500. Na figura 38 vê-se a topologia da rede metro que liga CENTRO, BOTAFOGO, LEBLON e TIJUCA na ferramenta de gerenciamento de rede chamada “Cacti”.

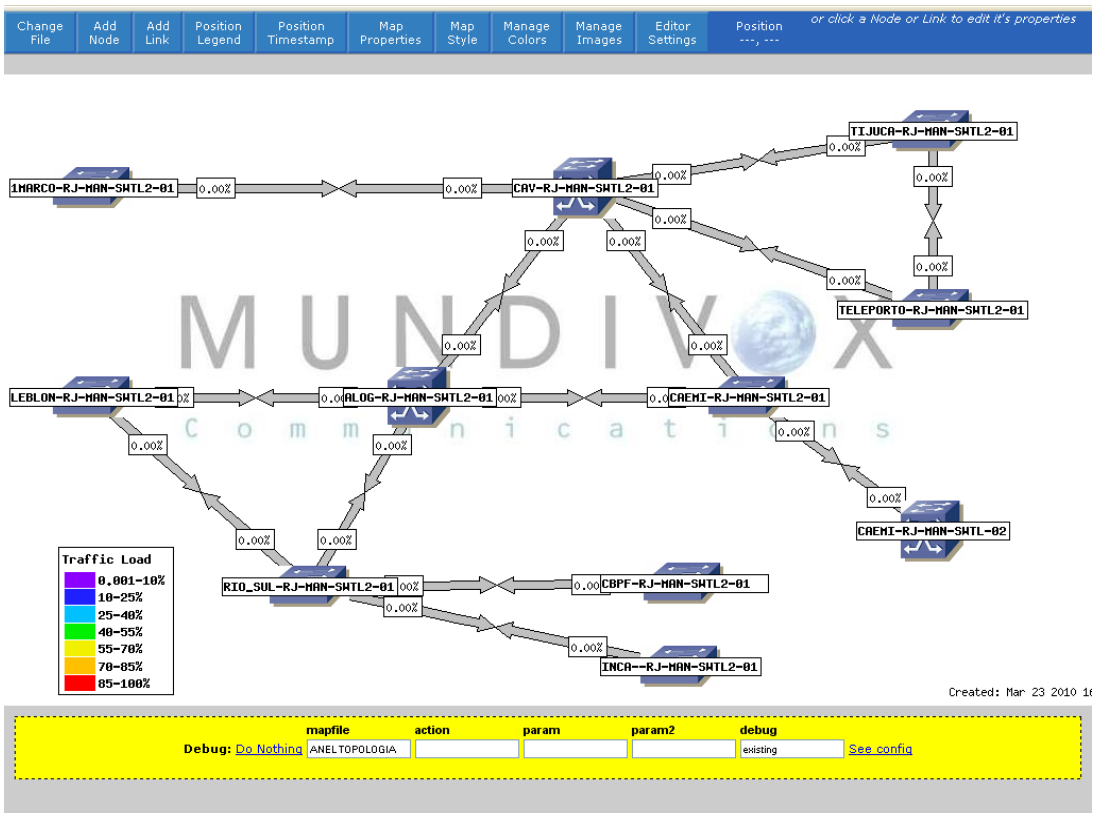


Figura 38 – a Gerencia do Cacti da Rede Metro Anel 1

A figura 39 mostra a topologia da Rede Metro Ethernet, que abrange a região do Centro para Barra da Tijuca. Essa topologia tem um diferencial: os equipamentos de switch de camada 2 são também de camada 3, realizando o roteamento dinâmico através do protocolo OSPF.

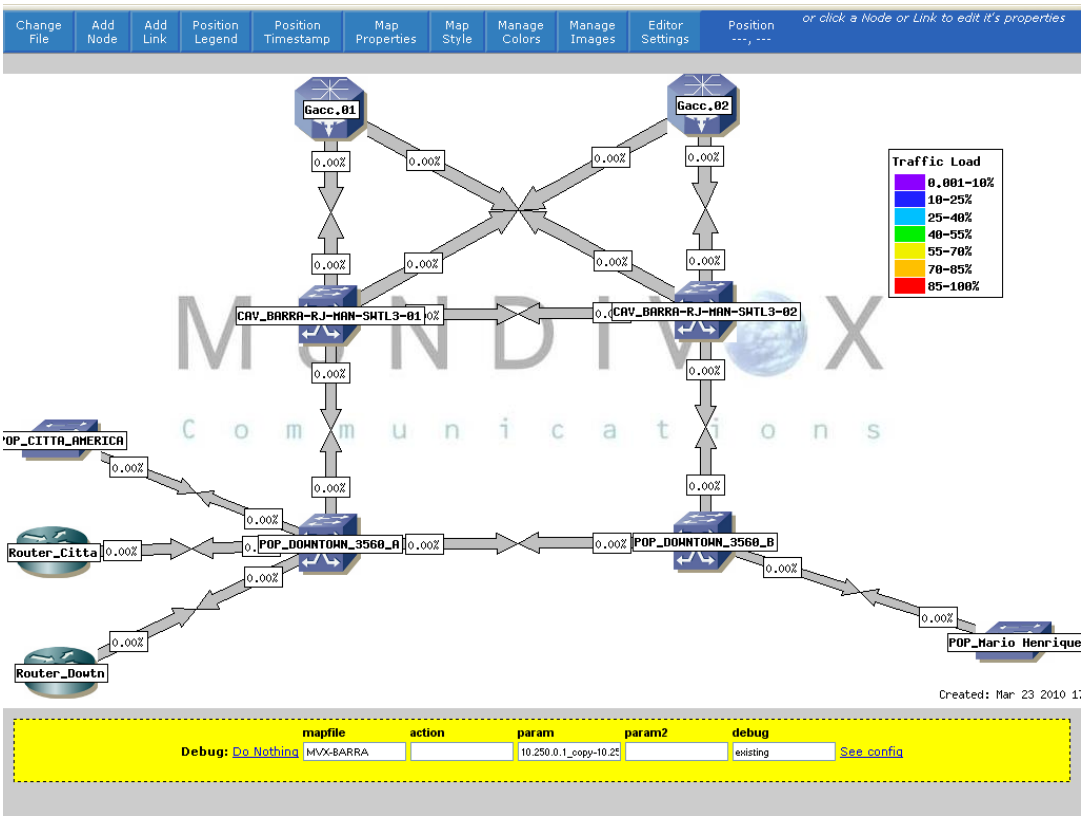


Figura 39 – Gerencia do Cacti da Rede Metro Anel 2

6. CONCLUSÃO

A tecnologia Ethernet amadureceu e hoje já representa uma importante solução de conectividade, que deve ser considerada para emprego tanto em expansões de redes como na criação de novas redes.

Através de um padrão bem estruturado e estudado, o Metro Ethernet consegue integrar-se perfeitamente às redes das operadoras já instaladas, além de trabalhar em perfeita harmonia com as novas redes Gigabit Ethernet, que utilizam Ethernet sobre fibra.

Observamos as técnicas de camada 2 envolvidas, como protocolo spanning-tree, os mecanismos de otimização de rede e os serviços que podem ser fornecidos ao mercado.

Pode-se observar que a integração de um backbone Metro Ethernet com outros backbones já existentes, como o IP/MPLS, torna possível fornecer serviços de camada 2 como VPNs, mesmo entre infra-estruturas não compatíveis, de forma tunelada, o que faz com que os pontos geograficamente dispersos se comportem como se pertencessem a um mesmo segmento de rede.

BIBLIOGRAFIA

[1] IETF Internet Draft, Layer Two Tunneling Protocol (Version 3) "L2TPv3", www.ietf.org/internet-drafts/draft-ietf-l2tpext-l2tp-base-03.txt, último acesso 15/03/2010

[2] IETF Internet Draft, Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks, www.ietf.org/internet-drafts/draft-martini-l2circuit-encap-mpls-04.txt, último acesso 20/03/2010

[3] IETF Internet Draft, Transport of Layer 2 Frames Over MPLS, www.ietf.org/internet-drafts/draft-martini-l2circuit-trans-mpls-10.txt, último acesso 19/03/2010

[4] BOYLES, T. HUCABY, D. Cisco CCNP Switching Exam Certification Guide Indianapolis: Cisco Press, 2001.576 p.

[5] LAMMLE, T. CCNA: Cisco Certified Network Associate: Study Guide. 6 ed. Indianapolis, Sybex 2007. 1012 p.

[6] http://www.metroethernetforum.org/, último acesso 02/05/2010

[7] BCMSN :Building Cisco MultiLayer Switched Networks. (Apostila do treinamento da empresa Cisco Systems)

[8] HALABI, S. Metro Ethernet. Indianápolis: Cisco Press, 2006 Metro Ethernet. (Apostila do treinamento da empresa Cisco Systems)

[9] MPLS: MultiProtocol Label Switching, Cisco Systems (Apostila de treinamento da empresa).

[10] MPLS QoS: MPLS Quality of Service. (Apostila do treinamento da empresa Mutirede Informática)

[11]http://www.unemat-net.br/prof/foto_p_downloads/cesar_-_metodo_do_estudo_de_caso_-_administracao.pdf, último acesso 01/03/2010

[12]http://www2.dbd.puc-rio.br/pergamum/tesesabertas/0116803_04_cap_04.pdf, ultimo acesso 05/04/2010