UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

LUANN HANNS HAMMERLE

SURVEY DA TECNOLOGIA MPLS E SUAS APLICAÇÕES

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2013

LUANN HANNS HAMMERLE

SURVEY DA TECNOLOGIA MPLS E SUAS APLICAÇÕES

Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática da Universidade Tecnológica Federal do Paraná, UTFPR.

Orientador: Prof. Joelson Vendramin

CURITIBA

2013

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Curitiba

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TERMO DE APROVAÇÃO

Título da Monografia

SURVEY DA TECNOLOGIA MPLS E SUAS APLICAÇÕES

por

Luann Hanns Hammerle

Monografia apresentada no dia 18 de outubro de 2013 ao Curso de Pós-graduação em Teleinformática e Redes de Computadores da Universidade Tecnológica Federal do Paraná, Campus Curitiba. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com nota 9,0 (NOVE INTEIROS)

Prof. Walter Godoy Junior

Prof. Joelson Tadeu Vendramin
Orientador

Visto da Coordenação:

Walter Godoy Junior
Coordenador do curso de Teleinformática
e redes de computadores

RESUMO

HAMMERLE, Luann Hanns. Survey da tecnologia MPLS. 2013. Monografia – Curso de Especialização em Teleinformática e Redes de Computadores – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

O MPLS (*Multi-Protocol Label Switching*) é uma tecnologia que cresceu muito nos últimos anos e ainda continua em constante expansão. Cada vez mais os provedores de serviço estão migrando seus equipamentos de rede para essa tecnologia. Com essa tecnologia a implementação de serviços com qualidade de serviço, redes privadas virtuais e engenharia de tráfego é facilitada. Essa monografia provê um *survey* sobre a tecnologia MPLS, assim como suas principais aplicações. O objetivo é auxiliar profissionais da área de telecomunicações no entendimento dessa tecnologia.

Palavras-chave: MPLS. QoS. Rótulo. VPN. LSR. LSP.

ABSTRACT

HAMMERLE, Luann Hanns. Survey da tecnologia MPLS. 2013. Monografia – Curso de Especialização em Teleinformática e Redes de Computadores – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

MPLS (Multi-Protocol Label Switching) is a technology that has grown in recent years and is still in constant expansion. Increasingly, service providers are migrating their network equipment for this technology. With this technology the implementation of services with quality of service, virtual private networks and traffic engineering is improved. This work will provide a survey on MPLS technology, as well as its main applications. The goal is to help telecommunications professionals to understanding this technology.

Keywords: MPLS. QoS. Label. VPN. LSR. LSP.

LISTA DE ABREVIAÇÕES E SIGLAS

AF	*Assured Forwarding*
ASICs	*Application Specific Integrated Circuit*
ATM	*Asynchronous Transfer Mode*
AToM	*Any Transport over MPLS*
BGP	*Border Gateway Protocol*
C	*Customer*
CBR	*Constraint-Based Routing*
CE	*Customer Edge*
CLR	Conservative Label Retention
CPU	*Central Processing Unit*
CS	*Class Selector*
DiffServ	*Differencial Service*
DoD	Downstream-on-Demand
DSCP	*Differentiated Services Code Point*
eBGP	*External Border Gateway Protocol*
EF	*Expedited Forwarding*
ERO	*Explicit Route Object*
EXP	*Experimental*
FEC	*Forwarding Equivalence Class*
FRR	*Fast ReRouting*
FTP	*File Transfer Protocol*
GMPLS	*Generalized Multiprotocol Label Switching*
HTTP	*Hyper Text Transfer Protocol*
iBGP	*Internal Border Gateway Protocol*
IETF	*Internet Engineering Task Force*
IGP	*Interior Gateway Protocol*
IntServ	*Integrated Services*
IP	*Internet Protocol*
LAN	*Local Area Network*
LDP	*Label Distribution Protocol*
LFIB	*Label Forwarding Information Base*
LIB	*Label Information Base*
LLR	*Liberal Label Retention*
LSP	*Label Switching Path*
LSR	*Label Switching Router*
MP-BGP	*Multiprotocol Border Gateway Protocol*
MPLS	*Multi Protocol Label Switching*
MPLS-TE	*Multi Protocol Label Switching Traffic Engineering*
MPLS-TP	*Multi Protocol Label Switching Transport Profile*
NSA	Número do Sistema Autônomo

OSPF	*Open Shortest Path First*
P	*Provider*
PE	*Provider Edge*
PHP	*Penultimate Hop Popping*
QoS	*Quality of service*
RD	*Route Distinguisher*
RESV	*Reservation*
RIP	*Routing Information Protocol*
RSVP	*Resource Reservation Protocol*
RSVP-TE	*Resource Reservation Protocol Traffic Engineering*
RT	*Route target*
TC	*Traffic Class*
TDP	*Tag Distribution Protocol*
ToS	*Type of Service*
TTL	*Time to Live*
UD	*Unsolicited Downstream*
VC	Virtual Circuit
VLAN	*Virtual Local Area Network*
VPLS	*Virtual Private Lan Service*
VPN	*Virtual Private Network*
VRF	*Virtual routing and forwarding*
WAN	*World Area Network*

SUMÁRIO

1 APRESENTAÇÃO

1.1 INTRODUÇÃO

Com a constante evolução da Internet e da necessidade de melhorar a comunicação entre os equipamentos da rede, o MPLS (*Multi Protocol Label Switching)* foi criado. O MPLS é um protocolo de rede que faz o roteamento dos pacotes através de rótulos inseridos no cabeçalho e não mais pelo endereço IP (*Internet Protocol)* de destino [GHEIN, 2007].

Esse protocolo começou a ser amplamente utilizado no final da década de 90. Um dos motivos para sua criação foi a otimização da velocidade de processamento dos pacotes entre os roteadores. Isso acontece pois quando o roteamento baseado em IP faz a pesquisa da tabela de rotas, há preocupação de qual é o prefixo que tem o maior número de bits igual ao do endereço de destino do pacote IP que está sendo roteado. Ou seja, nessa pesquisa a tabela pode conter várias entradas de rotas e prefixos que o pacote IP se encaixa, mas somente a rota com maior precisão será utilizada. Já na pesquisa da tabela de roteamento do MPLS (*labels*), o campo procurado sempre possui um valor fixo, por isso não existe maior ou menor precisão de dados e sempre será encontrado o valor procurado. Dessa forma a procura na tabela do MPLS é mais rápida do que a do IP, tornando o processamento dos pacotes mais rápido no MPLS. [Bhandure, 2013]

Um dos protocolos que antecederam o MPLS que também utilizava o roteamento por rótulo é o *ATM (Asynchronous Transfer Mode)* [GHEIN, 2007]. Esse protocolo de roteamento para WAN (*World Area Network)* foi o mais popular antes do MPLS. Mas, com a popularidade da Internet, o protocolo IP se tornou o protocolo mais utilizado. Muitos dos provedores de serviço tentaram fazer a integração do IP com o ATM, o que não era uma tarefa tão simples. Uma melhor integração do IP sobre o ATM foi uma das principais razões para a invenção do MPLS.

1.2 OBJETIVO GERAL

O objetivo geral do presente trabalho é realizar um *survey* da tecnologia MPLS e suas aplicações.

1.3 OBJETIVO ESPECÍFICO

Os objetivos específicos do presente trabalho são:

1) Apresentar os conceitos básicos do MPLS;

2) Demonstrar as aplicações VPN de camada 2 e 3, os modelos de QoS e como esse é utilizado na rede MPLS e o funcionamento da Engenharia de tráfego referente a roteamento de tráfego.

1.4 JUSTIFICATIVA

Com a importância que o MPLS obteve nas últimas décadas, é necessário o entendimento desse protocolo pelos profissionais de telecomunicações.

A elaboração desse documento visa demonstrar detalhadamente os conceitos do MPLS e suas aplicações para que possa ser consultados por pessoas que desejam conhecer a tecnologia.

1.5 ORGANIZAÇÃO DO DOCUMENTO

A presente monografia está dividida em três capítulos. O capítulo 1 descreve a introdução, objetivos e justificativas do projeto. O capítulo 2 descreve os conceitos básicos sobre MPLS. O capítulo 3 descreve as aplicações da tecnologia MPLS. O capítulo 4 apresenta as conclusões e trabalhos futuros.

2 CONCEITOS BÁSICOS SOBRE *MPLS*

2.1 *MPLS*

Antigamente o roteamento nos equipamentos era feito pela CPU (*Central Processing Unit)*, o que poderia tornar esse processo lento. O MPLS aumentou a velocidade de processamento dos pacotes, por não precisar processar o endereço de destino IP e sim somente o rótulo anexado no pacote. Mas, hoje em dia, os roteadores processam os pacotes IP nas ASICs (*Application Specific Integrated Circuit)* o que faz com que o encaminhamento dos pacotes seja tão rápido quanto o feito pelo MPLS.

Para o MPLS o importante para o roteamento dos pacotes não é o protocolo que está encapsulado e sim o rótulo, mais conhecido como *label*, no cabeçalho. O *label* está descrito na próxima seção, juntamente com os elementos que formam a rede MPLS como: roteadores, protocolos de sinalização e controle de caminhos.

2.2 *LABELS*

O *label* é um dos campos do cabeçalho MPLS que informa ao roteador para onde o pacote precisa ser roteado. O cabeçalho é composto de 32 bits com as seguintes funções:

- Os primeiros 20 bits formam o valor do *label* e esse valor pode ser entre 0 e 1048575, entretanto os 16 primeiros valores são reservados para usos especiais, tais como, *Implicit Null Label*, *router alert label*, etc.
- Os três bits na sequência, são utilizados para QoS (*Quality of Service).* Na RFC 5462 esse campo foi renomeado de EXP (*Experimental*) para TC (*Traffic Class*);
- O bit 23 indica se o *label* é o último ou não da pilha de *labels*. Caso seja o último label, o bit assume o valor 1, sendo seu valor 0 para todos os demais *labels* da pilha.;
- Os últimos 8 bits indicam o TTL (*Time to Live)* do pacote. Esse campo é decrementado a cada salto. Quando esse campo atinge o valor 0, o

pacote é descartado. Seu objetivo é evitar que algum pacote entre em *loop* de roteamento.

O *label* MPLS é inserido entre o protocolo de camada 2 e o de camada3 (IP), conforme ilustra a Figura 1.

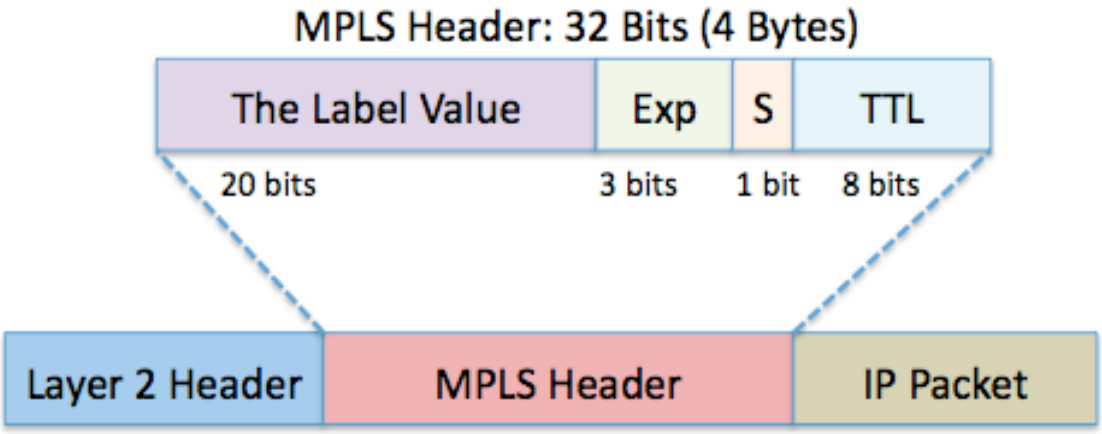


Figura 1: *Label* MPLS.
Fonte: http://blog.ine.com/

Os *labels* possuem significância local, com o objetivo principal de não ser necessária alguma entidade externa para controle dos mesmos.

Os roteadores MPLS podem precisar de mais de um *label* para rotear o pacote através da rede MPLS. Isso é utilizado para VPN (*Virtual Private Network)* MPLS e para transporte de pacotes que não sejam IP. Esses assuntos são abordados no capítulo 3.

2.3 *LABEL SWITCHING ROUTER* E *LABEL SWITCHING PATH*

Na rede MPLS há três tipos de roteadores que transportam *labels*. Esses roteadores são conhecidos como LSR (*Label Switching Router).*

O caminho que um pacote irá percorrer da origem ao destino é chamado de LSP (*Label Switching Path)*. Lembrando que LSP é um caminho unidirecional, ou seja, um pacote que sair de *New York* para *San Francisco*, por exemplo, pode seguir um caminho diferente do pacote que sair de *San Francisco* para *New York*, conforme ilustra a Figura 2.

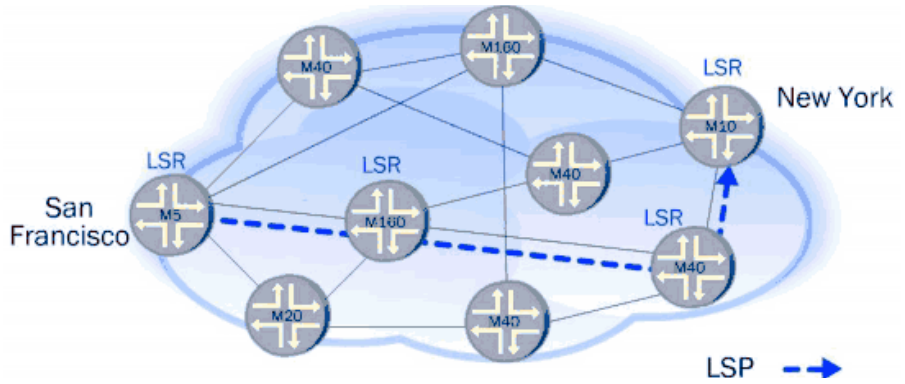


Figura 2: LSP

Fonte: Juniper Networks

Os três tipos de roteadores são:

- LSR de entrada: Recebe um pacote que não está com *label* e insere um *label* no cabeçalho. Esta operação recebe o nome de *"push"*.;
- LSR de saída: Recebe um pacote que já está com *label*, faz a retirada desse *label* (operação denominada *"pop"*) e encaminha para o destino;
- LSR Intermediários ou de trânsitos: São os roteadores que recebem e enviam os pacotes já com *labels*. Executando a operação de *"swap"* de *labels*.

Os tipos de roteadores podem ser melhor visualizados na Figura 3, onde o tráfego está saindo de San Francisco e chegando em New York.

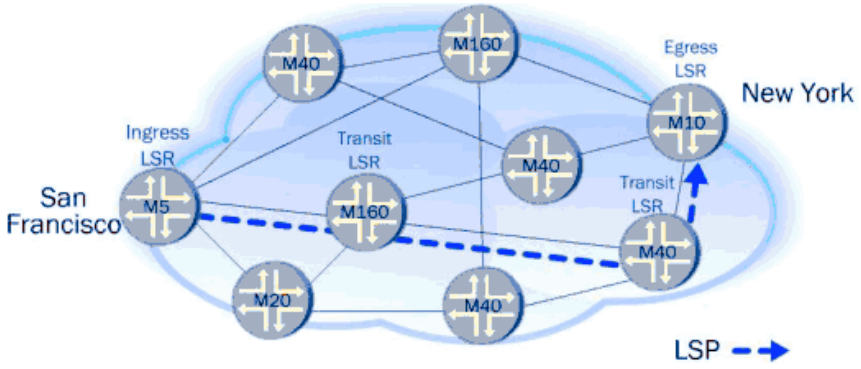


Figura 3: Tipos de roteadores

Fonte: Juniper Networks

A Figura 4 mostra como funciona o encaminhamento de pacotes dentro do LSP.

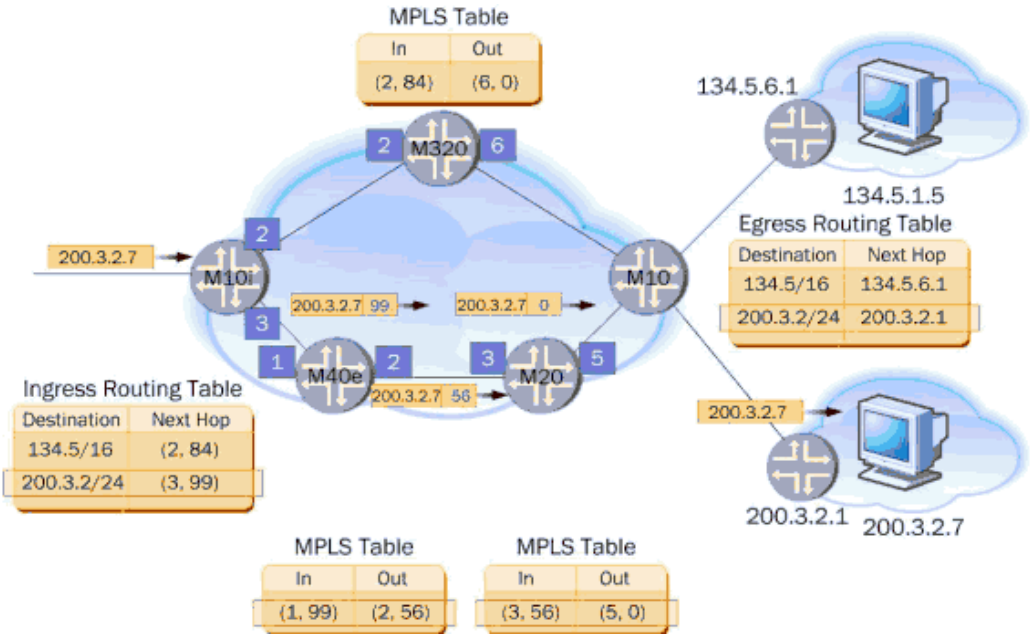


Figura 4: Encaminhamento de pacote na MPLS

Fonte: Juniper Networks

Quando o roteador de entrada da rede MPLS recebe o pacote destinado ao computador 200.3.2.7, ele encaminha esse pacote para a interface 3 com o *label* 99, conforme a sua tabela. Já o próximo roteador recebe o pacote e consulta a tabela MPLS, que informa que o pacote que chegar na interface 1 com o *label 99,* deverá ser roteado pela interface 2 com o label 56. Quando o pacote chega ao próximo roteador, esse faz a busca na tabela MPLS e encaminha o pacote para o roteador de saída da MPLS com o label valor 0, que indica que o label deve ser removido e que deve ser verificado o cabeçalho IP para fazer o encaminhamento do pacote. O roteador de saída da MPLS recebe o pacote, retira o label e faz o roteamento do pacote baseado na tabela de roteamento IP.

Na Figura 4, o último roteador está executando a ação *pop* no *label*. É possível que o penúltimo roteador da rede execute esta ação, retirando a carga do último roteador. Isso é conhecido como PHP (*Penultimate Hop Popping*) e traz o benefício de otimizar o funcionamento dos LSPs.

Quando muitos fluxos de dados passam pelo mesmo roteador de saída da MPLS e a ação de *pop* é executada nesse equipamento, pode ocorrer redução na

performance da rede nesse ponto. Pois o roteador de saída precisa retirar o *label* de todos os pacotes.

Se o PHP for utilizado, o processamento de retirada dos *labels* é distribuído entre os vários roteadores que fazem adjacência com o roteador de saída, melhorando a performance da rede.

2.4 *FORWARDING EQUIVALENCE CLASS*

FEC (*Forwarding Equivalence Class)* é um grupo de pacotes que são roteados pelo mesmo caminho e são marcados com o mesmo *label*. Se não houver diferenciação de QoS, eles são tratados da mesma maneira.

2.5 DISTRIBUIÇÃO DE *LABELS*

Há duas maneiras de distribuição de *labels*:

1. Colocar os *labels* juntamente com o protocolo de roteamento IP;
2. Ter um protocolo de sinalização de labels separado do protocolo de roteamento.

A grande vantagem de fazer a distribuição de *labels* juntamente com o protocolo de roteamento IP é que esses dois sempre estarão em sincronismo. Ou seja, se o prefixo para alguma rede não existir na tabela de roteamento, não existirá um *label* para a rede.

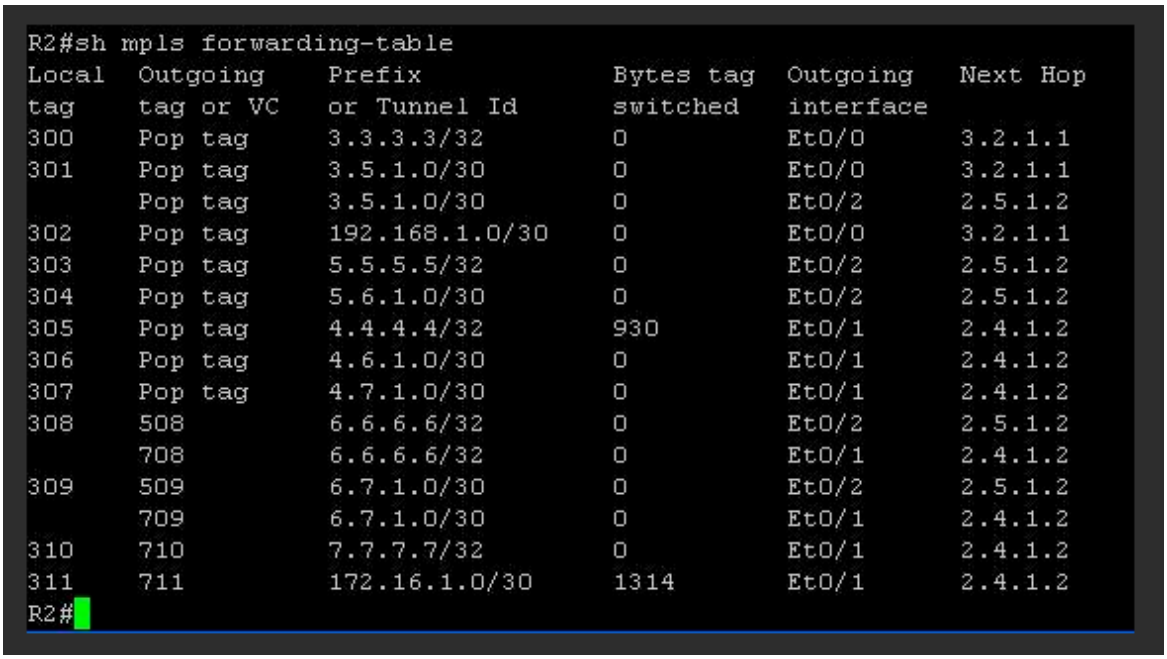
Já o segundo método exige um protocolo adicional nos roteadores, independente do protocolo utilizado no roteamento IP. Há vários protocolos de sinalização, entre eles:

- LDP (*Label Distribution Protocol)*;
- RSVP-TE (*Resource Reservation Protocol Traffic Engineering)*;

Na Figura 5, temos um exemplo da tabela de encaminhamento da rede MPLS baseada em *labels*. Para cada prefixo na tabela de roteamento, há um *label* associado na LIB (*Label Information Base*). Com a informação do próximo salto da tabela de roteamento e com o *label* associada da LIB é possível criar uma tabela

chamada LFIB (*Label Forwarding Information Base*) que será utilizada para decidir qual o destino que o pacote irá seguir baseado no *label* recebido. Assim, o roteador troca o *label* recebido, por um novo *label* conhecido no destino.

Na Figura 5 ainda podemos verificar a ação tomada pela LFIB quando um pacote chega ao roteador.



```
R2#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
300    Pop tag     3.3.3.3/32       0          Et0/0      3.2.1.1
301    Pop tag     3.5.1.0/30       0          Et0/0      3.2.1.1
       Pop tag     3.5.1.0/30       0          Et0/2      2.5.1.2
302    Pop tag     192.168.1.0/30   0          Et0/0      3.2.1.1
303    Pop tag     5.5.5.5/32       0          Et0/2      2.5.1.2
304    Pop tag     5.6.1.0/30       0          Et0/2      2.5.1.2
305    Pop tag     4.4.4.4/32       930        Et0/1      2.4.1.2
306    Pop tag     4.6.1.0/30       0          Et0/1      2.4.1.2
307    Pop tag     4.7.1.0/30       0          Et0/1      2.4.1.2
308    508         6.6.6.6/32       0          Et0/2      2.5.1.2
       708         6.6.6.6/32       0          Et0/1      2.4.1.2
309    509         6.7.1.0/30       0          Et0/2      2.5.1.2
       709         6.7.1.0/30       0          Et0/1      2.4.1.2
310    710         7.7.7.7/32       0          Et0/1      2.4.1.2
311    711         172.16.1.0/30    1314       Et0/1      2.4.1.2
R2#
```

Figura 5: Tabela MPLS

Fonte: http://ntwrklife.wordpress.com

Se um pacote chegar com o *label* 303, por exemplo, o roteador irá retirar o *label* do topo da pilha (303) executando a ação pop e encaminhará o pacote pela interface et0/2. Caso um pacote chegue com o *label* 311, esse *label* é retirado, e é colocado o *label* 711, executando a ação *swap* e o pacote é encaminhado para a interface et0/1.

Outro exemplo seria a ação *untagged*, que seria retirar todos os *labels* da pilha para encaminhar o pacote para a rede IP.

Também pode-se citar a ação *aggregate*, que faz com que o roteador retire o *label* existente no pacote MPLS. Com o endereço IP de destino, ele faz uma busca na tabela de roteamento para verificar o IP do próximo salto. Nesse caso é necessário a verificação nessa tabela, pois não há próximo passo definido na LFIB, pois são rotas sumarizadas onde cada destino pode possuir um *default gateway* diferente.

2.6 PROTOCOLOS DE SINALIZAÇÃO

Os protocolos de sinalização mais conhecidos no MPLS são o LDP e o RSVP. O LDP é muito utilizado para aplicações VPN. Já o RSVP-TE *(Resource Reservation Protocol Traffic Engineering)* funciona com roteamento explícito que é necessário para engenharia de tráfego. Esses dois protocolos são detalhados na sequência.

Ainda existe um outro protocolo de sinalização utilizado pelo MPLS, que é o CR-LDP (*Constraint-based Routing Label Distribution Protocol*). Esse protocolo evoluiu de maneira inversa ao RSVP, ou seja, o protocolo LDP que fazia simplesmente a distribuição de *labels*, foi estendido para suportar engenharia de tráfego. A principal diferença com relação ao RSVP-TE é que o CR-LDP é do tipo *Hard State*, isto é, uma vez estabelecido o circuito virtual, ele não será desfeito até que um pedido de desconexão seja enviado, ao passo que o RSVP-TE é do tipo *Soft State* pois mensagens de verificação do estado operacional do circuito virtual são trocadas periodicamente [Fialho,2007].

Entretanto, em virtude da baixa utilização do CR-LDP, o grupo de trabalho sobre MPLS do IETF (*Internet Engineering Task Force*) decidiu não direcionar novos esforços ao mesmo, concentrando seus trabalhos no desenvolvimento do RSVP-TE como o protocolo de sinalização para aplicações que requeiram engenharia de tráfego no MPLS [Fialho, 2007].

2.6.1 LDP

Para cada prefixo IP na tabela de roteamento, cada LSR cria um banco de *labels* local, designando um label para cada prefixo. Então o LSR distribui a informação dos *labels* para todos os vizinhos LDP. Essa informação recebida se torna uma informação remota. Então os vizinhos guardam a informação de *labels* remota e local.

O roteador 4 da Figura 6, anuncia para o vizinho (roteador 3) o *label* 33 para chegar a rede 10.0.0.0/8 que está conectado a ele. O roteador 3 armazena essa informação e envia o anúncio da rede para o roteador 2, através do *label* 17. E assim por diante até chegar no roteador 1.

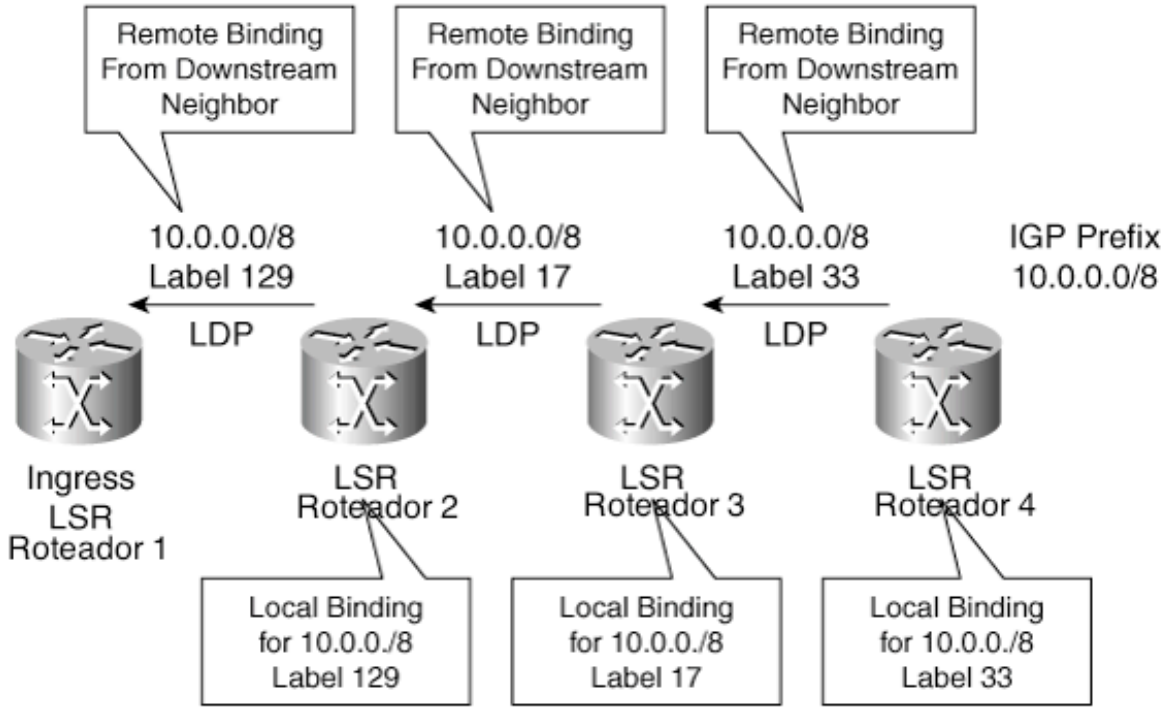


Figura 6: Anúncio LDP

Fonte: http://blog.ine.com/

Quando um pacote IP com destino a rede 10.0.0.0/8 chega ao roteador 1, como mostrado na Figura 7, esse sabe que deve encaminhar o pacote para o roteador 2 com o *label* 129. Assim o tráfego vai fluindo entre os roteadores e a cada segmento o *label* é alterado até chegar no roteador de destino.

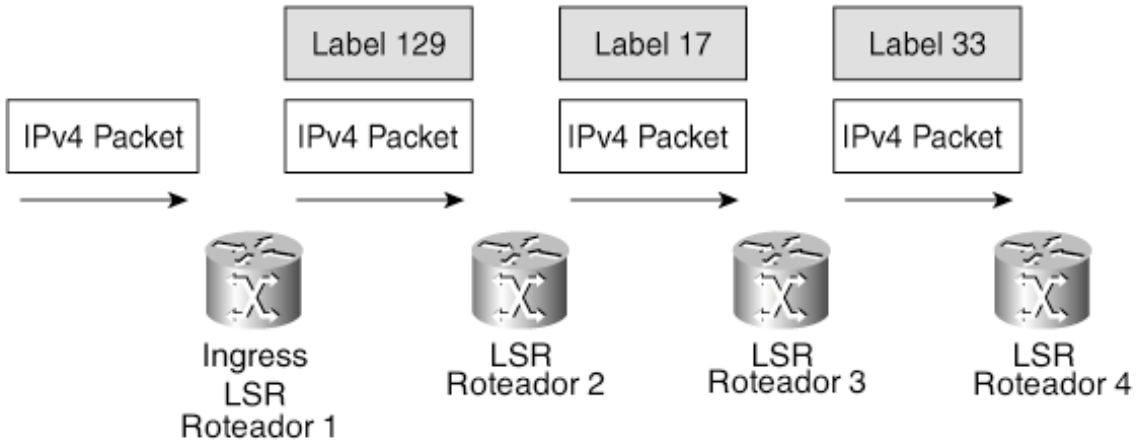


Figura 7. *Label* MPLS.

Fonte: http://blog.ine.com/

Um LSR pode utilizar diferentes modos de distribuição e retenção de *labels* para outros roteadores. Também existem várias formas de como os LSRs controlam a criação e a remoção dos LSPs.

2.6.1.1 MODO DE DISTRIBUIÇÃO DE *LABELS*

Há dois modos de distribuição de *labels*: o primeiro é o DoD *(Downstream-on-Demand)* e o UD *(Unsolicited Downstream)*.

No modo DoD cada LSR faz a requisição para o roteador de próximo salto, requisitando um *label* para a FEC. Cada LSR recebe um *label* por FEC.

Já no modo UD, cada LSR distribui as informações com os *labels* para os LSR vizinhos, sem que esses roteadores façam a requisição desses *labels.*

2.6.1.2 MODO DE RETENÇÃO DE *LABELS*

Nesse modelo também possuímos dois modos: sendo o primeiro o LLR (*Liberal Label Retention*) e o CLR (*Conservative Label Retention*).

No primeiro modo (LRR) todas as informações de *labels* enviadas pelos vizinhos são colocadas na tabela de *labels,* diferentemente do segundo modo (CLR) que inclui na tabela somente os *labels* que são associados com o próximo passo do LSR para uma FEC em particular.

2.6.1.3 CONTROLE DE LSPs

Existem dois modelos de controle de LSPs, os quais são conhecidos como controle independente de LSP e controle ordenado de LSP.

No modo independente, cada LSR é livre para estabelecer seus próprios mapeamentos de rótulos, e anunciá-los a seus vizinhos. No modo ordenado, apenas um roteador de borda da MPLS (saída para a rede em questão) pode iniciar a criação de um LSP. Esta abordagem auxilia na prevenção de *loops*, mas tem a desvantagem de tornar mais lenta a criação dos LSPs.

2.6.2 RSVP-TE

O RSVP foi concebido inicialmente para suportar a reserva de recursos em redes IP, no modelo de QoS Intserv *(Integrated Services)*, mas não foi muito utilizado. A razão disso é explicada na seção 3.4.

Uma extensão do RSVP foi criada para permitir o estabelecimento de LSPs no MPLS, chamada de RSVP-TE. O funcionamento do RSVP e de sua extensão são similares.

O RSVP-TE tem como objetivos designar *labels*, estabelecer LSPs, permitir a engenharia de tráfego e o QoS.

As Figuras 8 e 9 mostram o funcionamento do RSVP-TE.

Uma mensagem chamada *path message* é enviada pelo roteador de entrada da rede MPLS para os roteadores P. O roteador de saída da rede MPLS envia uma mensagem RESV no mesmo caminho, mas na posição oposta. A mensagem RESV atribui valores específicos nos *labels*.

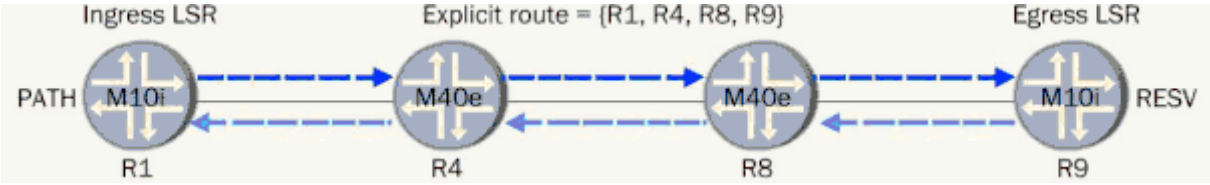


Figura 8: RSVP

Fonte: Juniper Networks

A *path message* contém o ERO (*Explicit Route Object*) que indica o caminho que o LSP deve seguir, que no caso da Figura 7 é do R1 para o R9 passando pelos roteadores R4 e R8.

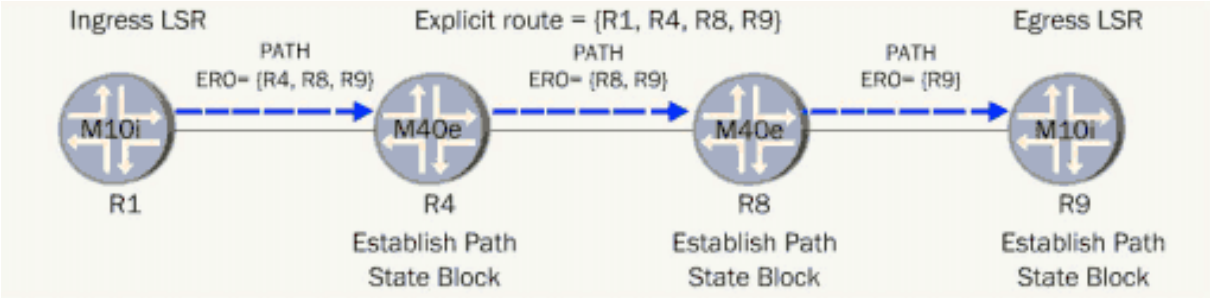


Figura 9: *Explicit Route Object*

Fonte: Juniper Networks

3 APLICAÇÕES MPLS

3.1 MODELOS DE VPN MPLS

Uma VPN MPLS emula uma rede privada sobre uma infraestrutura de rede pública. Uma rede privada exige que todos os locais possam se interligar, e ao mesmo tempo devem estar completamente isolados das outras VPNs. Uma VPN normalmente pertence a uma empresa e tem vários locais interconectados através da infraestrutura comum do provedor de serviços.

A diferença da MPLS VPN para a VPN utilizada para fechar túneis criptografados na Internet é que a VPN estabelecida pelo MPLS possui os diferenciais desse protocolo, como por exemplo o QoS, o roteamento feito por *labels* e flexibilidade de roteamento, atributos que a VPN tradicional não possui.

Os provedores de serviços podem implantar dois modelos de serviços: VPN *Overlay Model* e VPN *Peer-to-Peer*, os quais estão descritos nas próximas seções.

3.1.1 VPN *OVERLAY MODEL*

No modelo VPN *overlay*, o provedor de serviços fornece um serviço de ligação ponto-a-ponto ou de circuito virtual através de sua rede, entre os roteadores do cliente. Os roteadores dos clientes criam uma conexão direta pelo link ou um circuito virtual entre eles, através da infraestrutura do provedor de serviços. Os roteadores e *switches* do provedor de serviços carregam os dados dos clientes através de sua rede, mas nenhuma interconexão de roteamento ocorre entre o roteador cliente e o roteador do provedor de serviços. O resultado disso é que os roteadores do provedor de serviços nunca enxergam as rotas dos clientes [GHEIN, 2007].

Na Figura 10 é mostrado um exemplo desse modelo, onde a rede do provedor de serviços possui *switches Frame Relay* que estabelecem circuitos virtuais entre os roteadores dos clientes na borda da rede *Frame Relay*. Esse modelo não é utilizado pelo MPLS. Ele era uma alternativa que os provedores de serviço possuíam antes do advento do MPLS.

Do ponto de vista do cliente, os roteadores parecem estar diretamente conectados.

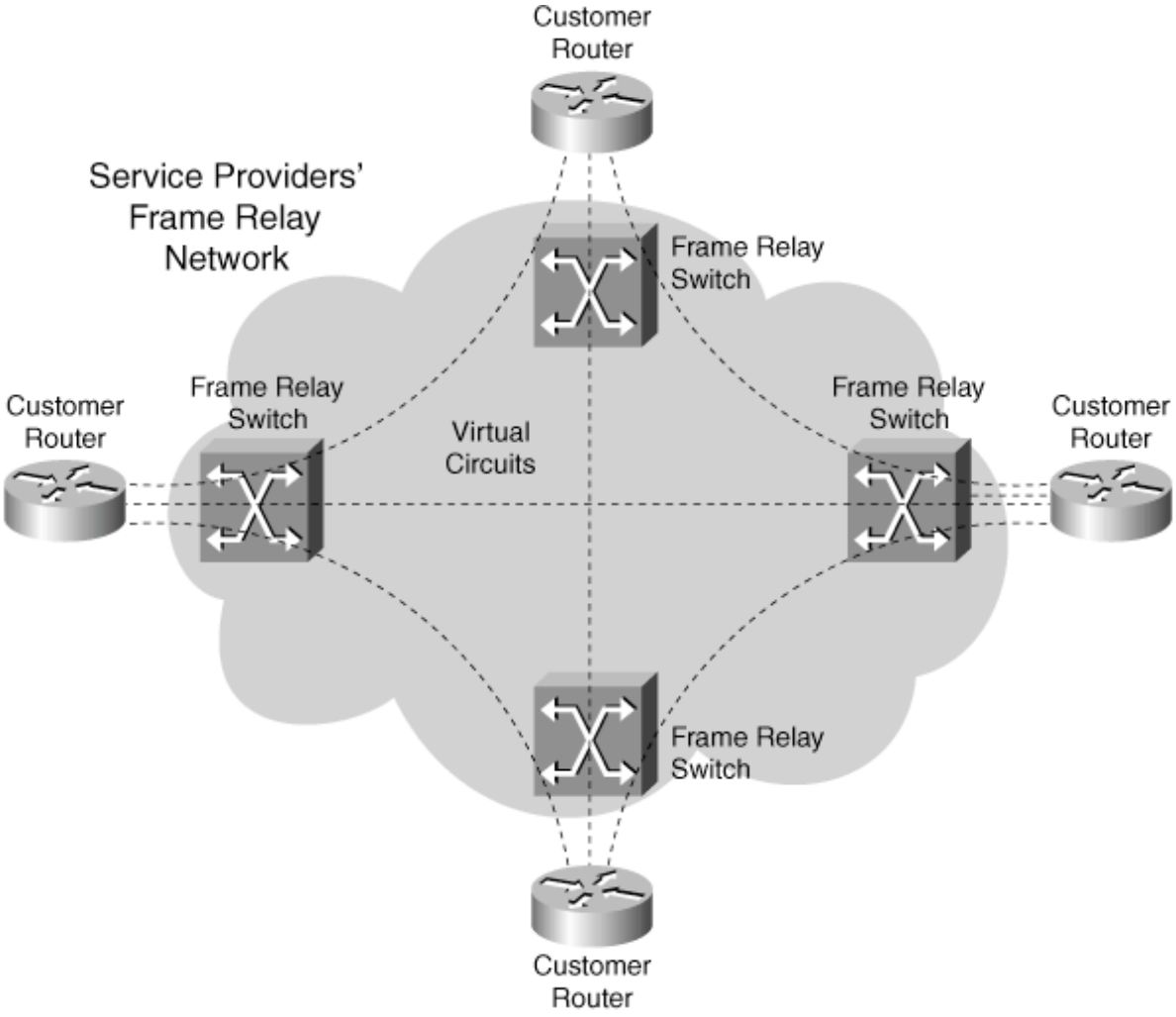


Figura 10: VPN *Overlay Model*

Fonte: http://www.lume.ufrgs.br

3.1.2 VPN PEER-TO-PEER MODEL

No modelo VPN *peer-to-peer*, os roteadores do provedor de serviços carregam os dados do cliente em toda a rede e também participam do roteamento dos pacotes. Em outras palavras, os roteadores do provedor de serviços conectam-se diretamente com os roteadores dos clientes em nível de camada 3. O resultado disso é que existe um protocolo de roteamento entre os roteadores do cliente e do provedor [GHEIN, 2007].

Na Figura 11 é mostrado um exemplo desse modelo, onde cada roteador CE faz adjacência somente com o roteador PE. Não há mais necessidade de criar vários circuitos virtuais entre todos os *sites* do cliente. A MPLS VPN utiliza esse modelo.

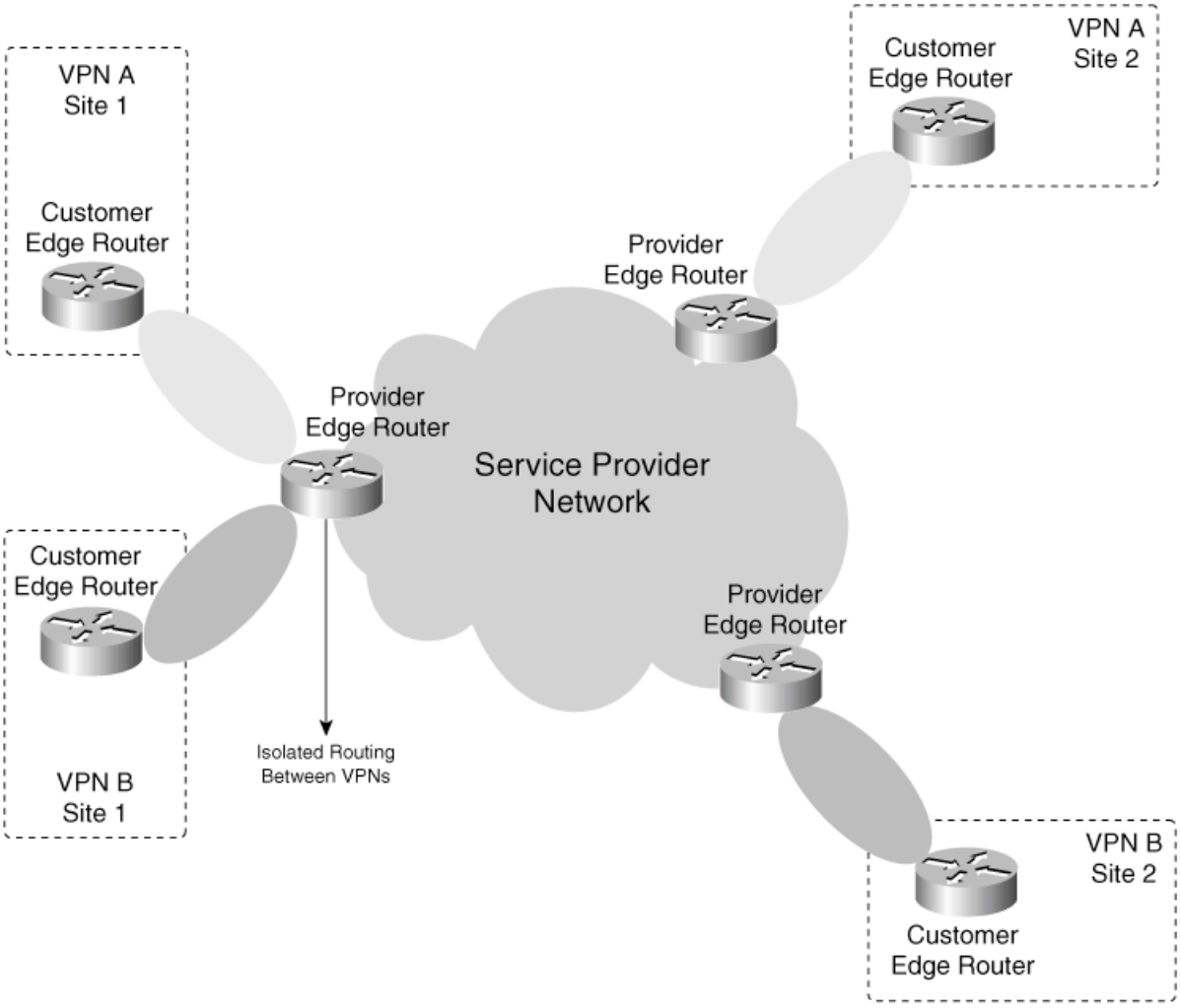


Figura 11: VPN Peer-to-Peer Model

Fonte: http://www.lume.ufrgs.br

Antes de existir o MPLS, para implementar o modelo de VPN *Peer-to-Peer* era necessário criar as rotas IP entre os roteadores do cliente e do provedor e para obter o isolamento era necessário a criação de filtros de pacotes (listas de acesso). Assim era muito mais comum o modelo implantado ser o *Overlay*. Contudo, o advento das VPNs MPLS permitiu que a implantação do modelo VPN *Peer-to-Peer* fosse muito mais fácil. Adicionar ou remover *sites* é agora mais fácil de configurar e assim demanda menos tempo e esforço [GHEIN, 2007]. Isso é melhor explicado na seção 3.2 que trata das VPN MPLS.

3.1.3 NOMENCLATURA DE ROTEADORES NA MPLS

As Figuras 12 e 13 mostram as nomenclaturas de roteadores utilizadas nas VPNs MPLS.

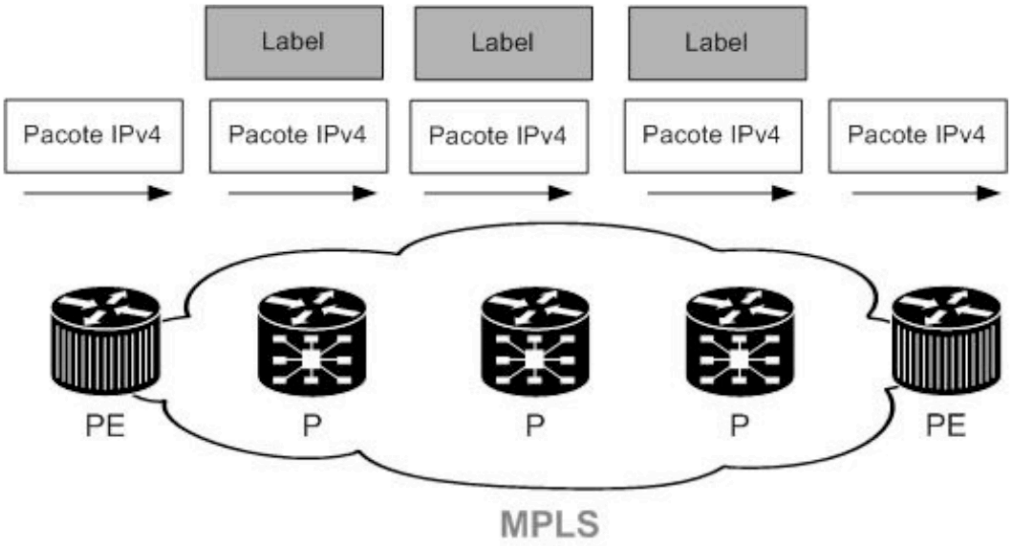


Figura 12: Roteadores da operadora

Fonte: http://www.rotadefault.com.br/

O roteador PE (*Provider Edge*) é o roteador de borda da rede MPLS, pertencente à provedora de serviço e está conectado em camada 3 ao roteador do cliente.

O roteador P (*Provider*) é o equipamento que pertence à provedora de serviço, mas que não está diretamente conectado aos roteadores dos clientes. Eles ficam na “nuvem“ MPLS, conectados a outros roteadores P e a roteadores PE.

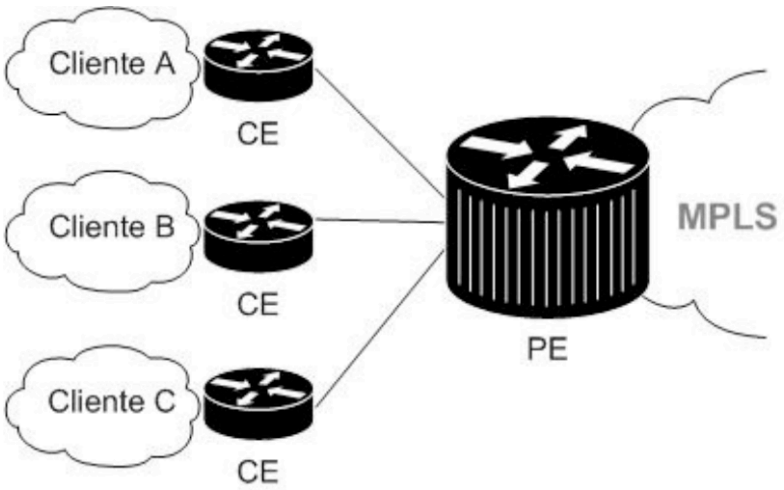


Figura 13: Roteadores do cliente

Fonte: http://www.rotadefault.com.br/

Na implementação MPLS VPN, os dois roteadores precisam estar com o MPLS habilitado e com isso fazer o roteamento com base em *labels*.

O roteador CE (*Customer Edge*) é o roteador pertencente ao cliente, e está conectado em camada 3 ao roteador PE. O roteador C (*Customer*) pertence ao cliente e não possui uma conexão direta com o roteador CE. Os roteador CE e C não precisam estar com o MPLS habilitado.

Os roteadores P tem uma tabela baseada em *label* e irão encaminhar os *labels* conforme a tabela, não tendo necessidade de conhecer o IP da rede de destino e origem ou ainda se o tráfego pertence a clientes diferentes. Quem possui essas definições são os roteadores PE que além da tabela de *labels*, mantêm a tabela de roteamento IP.

3.2 MPLS VPN CAMADA 3

Essa aplicação cresceu exponencialmente nos últimos anos e ainda continua crescendo. Muitos provedores de serviços implementaram essa aplicação para substituir as tecnologias *Frame relay* e ATM que foram muito popular antes do MPLS.

3.2.1 *VIRTUAL ROUTING AND FORWARDING*

Na rede MPLS o tráfego de diferentes clientes é tratado separadamente, como se cada cliente fechasse um túnel VPN com todas as pontas. O tráfego de dados de um cliente não será acessível para outro, a não ser que essa comunicação seja desejada. A operadora consegue separar o tráfego de diferentes clientes (VPNs) através de VRFs (*Virtual Routing and Forwarding*). Com isso não é necessário a criptografia ou autenticação dos dados.

VRF é uma tecnologia que permite que várias instâncias de tabelas de roteamento existam em um roteador e funcionem simultaneamente. Isso evita que várias tabelas de roteamento sejam segmentadas em diferentes equipamentos.

A VRF funciona como um roteador virtual, mas como um roteador virtual pode ter várias tabelas de roteamento, a instância VRF utiliza somente uma. Além disso a VRF requer uma tabela de encaminhamento que designe um próximo salto para cada pacote, uma lista de equipamentos que podem encaminhar pacotes e uma lista

de regras e protocolos de roteamento que informam como os pacotes serão encaminhados. Essas tabelas previnem o tráfego de ser encaminhado para fora de uma VRF específica e também evitam que um tráfego de fora entre pelo caminho da VRF [Rouse, 2007].

Um único roteador PE pode possuir várias tabelas de roteamento, cada uma referente a um cliente diferente.

Uma interface do roteador PE pode pertencer somente a uma VRF e várias interfaces desse equipamento podem pertencer à mesma VRF.

A Figura 14 mostra um exemplo de um roteador PE conectado a dois clientes distintos, e cada interface do roteador PE está em uma VRF diferente.

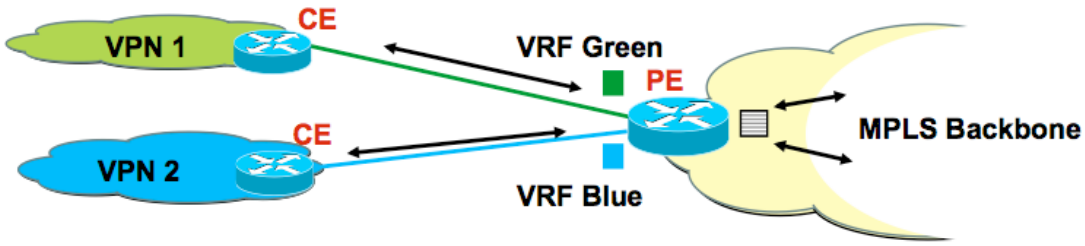


Figura 14: VRF

Fonte: http://www.sanog.org/

Os prefixos VPNs são exportados para os roteadores através do protocolo de roteamento MP-BGP (*MultiProtocol Border Gateway Protocol)*. O problema é que quando os prefixos dos clientes são propagados através do provedor de serviço, podem ocorrer sobreposição de rotas, ou seja, um roteador PE que recebe atualizações de seus vizinhos, poderá receber rotas conflitantes ou repetidas, que pertencem a VPNs diferentes.

Para identificar rotas pertencentes a VPNs diferentes (e evitar que o MP-BGP selecione uma e descarte as outras), foi criada as RDs (*Route Distinguisher*).

A RD funciona aplicando um identificador ao prefixo do cliente para fazer a distinção do tráfego dos diferentes clientes e possui um campo de 64 bits. A combinação do prefixo IP com a RD é chamado de vpnv4. Cada VRF precisa possuir um RD associado a ela.

Dois exemplos de identificadores utilizados são o NSA (Número do Sistema autônomo) e o número gerado pelo servidor de serviço para identificar a VRF. Sendo esses dois separados por dois pontos. Na Figura 15 é mostrado um exemplo de configuração de duas VPNs em um mesmo equipamento.

Lembrando que as configurações de RDs e RTs (*Route target*) são aplicadas somente nos roteadores PE.

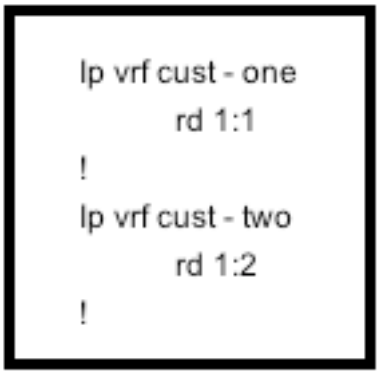


Figura 15: *Route Distinguisher*
Fonte: Autoria própria

A RD faz o papel de somente identificar a qual VPN cada prefixo/rota pertence. Se diferentes clientes pertencentes a diferentes VPNs precisarem se comunicar, é necessária a utilização de RT.

A RT precisa ser configurada para exportar e importar rotas entre roteadores para a mesma VPN, ou seja, é preciso criar a configuração conforme mostra a Figura 16.

Figura 16: *Route Target*
Fonte: Autoria própria

Assim todos os roteadores *cust-one* e *cust-two* irão possuir as rotas referentes a sua VRF somente.

Caso seja necessário que duas VPNs se comuniquem entre si, é necessário criar uma outra RT.

Na Figura 17, por exemplo, se o site A *cust-one* quiser se comunicar com o site A *cust-two*, será criada a RT 100:1, que precisa ser importada e exportada entre esses sites. Lembrando que a RT deve ser configurada em ambos os roteadores.

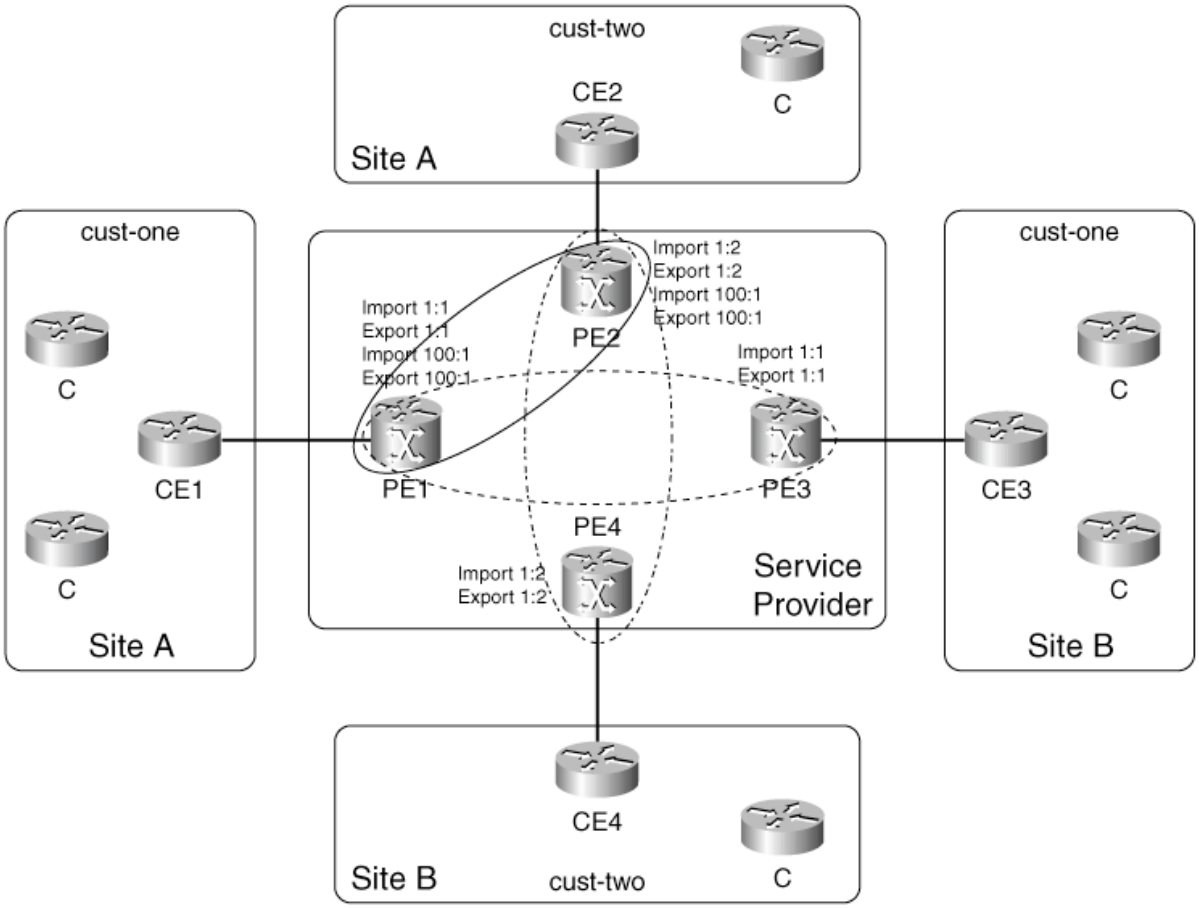


Figura 17: Comunicação entre VPNs

Fonte: [GHEIN, 2007]

Dessa forma, a configuração no PE1 e no PE2 ficam conforme mostra a Figura 18.

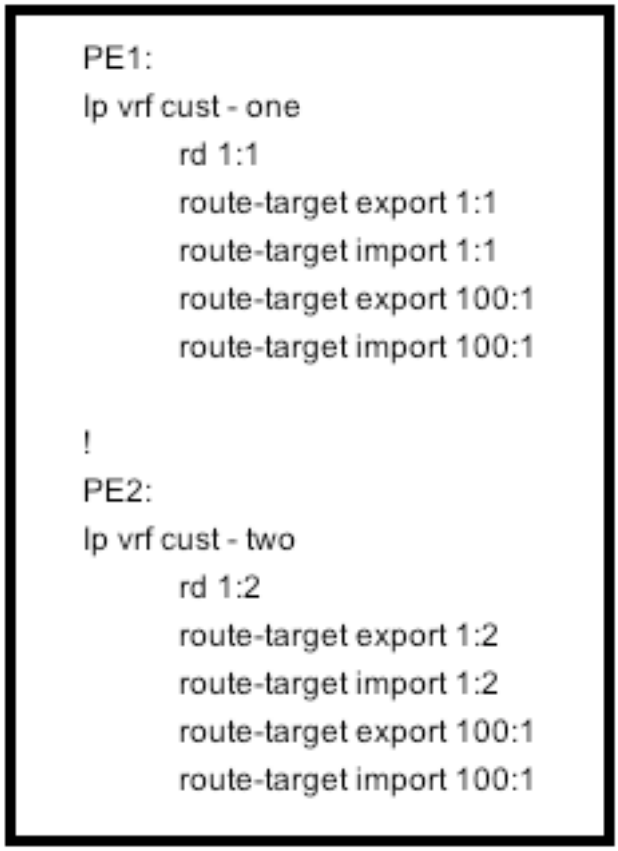


Figura 18: Configuração de RD e RT
Fonte: Autoria própria

Os RT *import* e *export* podem ser substituídos pelo comando *both*, assim o exemplo do roteador PE1 ficaria conforme a Figura 19.

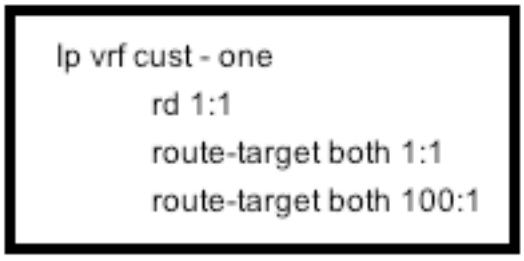


Figura 19: Comando *both* na RT
Fonte: Autoria própria

3.2.2 PROPAGAÇÃO DE ROTAS NA MPLS

Nessa seção é tratada como as rotas dos clientes são propagadas da origem até o destino.

Como as rotas de todos os clientes são transportadas pelos roteadores PE, é necessário um protocolo de roteamento estável que suporte inúmeras rotas na tabela de roteamento. O protocolo mais estável e muito utilizado na Internet é o BGP (*Border Gateway Protocol).*

Como explicado na seção 3.2.1, os prefixos dos clientes são transportados com um identificador único (RD), logo eles podem ser transportados sem o problema de sobreposição de redes iguais para clientes diferentes através da rede MPLS.

A Figura 20 mostra um resumo de como as rotas são propagadas, de um roteador de um site A chegando a outro site B.

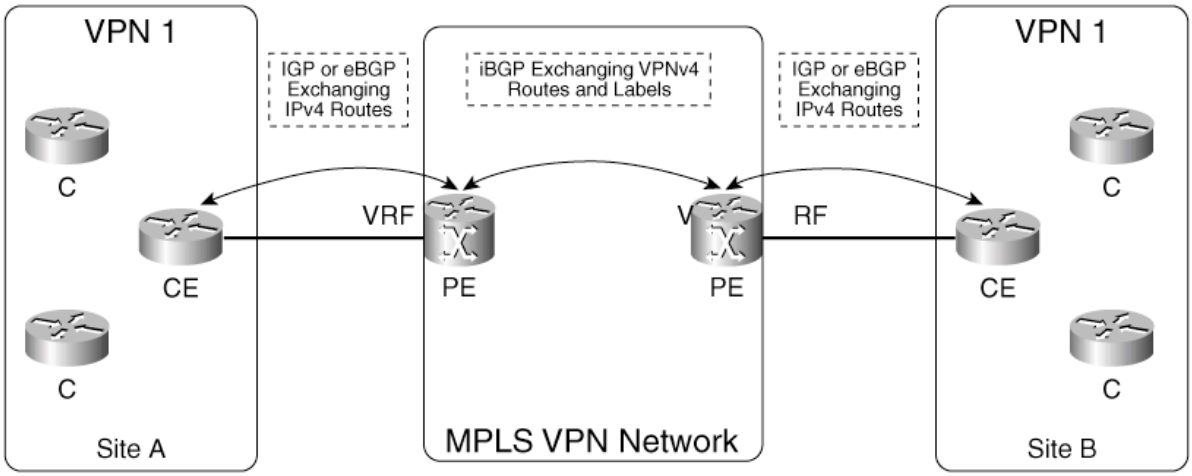


Figura 20: Propagação MPLS

Fonte: http://mpls-tp.com/

Como se pode perceber na figura, os roteadores CE e PE fazem as trocas de prefixos para adicionar às suas tabelas de roteamento. Essas trocas normalmente são feitas por um protocolo IGP (*Interior Gateway Protocol)*, como por exemplo o RIP (*Routing Information Protocol*) ou OSPF (*Open Shortest Path First*), ou pelo eBGP (*External Border Gateway Protocol*), mas também podem ser utilizadas rotas estáticas.

Dentro da rede MPLS os roteadores PE trocam informações através do protocolo iBGP (*Internal Border Gateway Protocol*).

A Figura 21 mostra detalhadamente o anúncio de uma rota desde o roteador CE do Site A até o roteador CE do Site B.

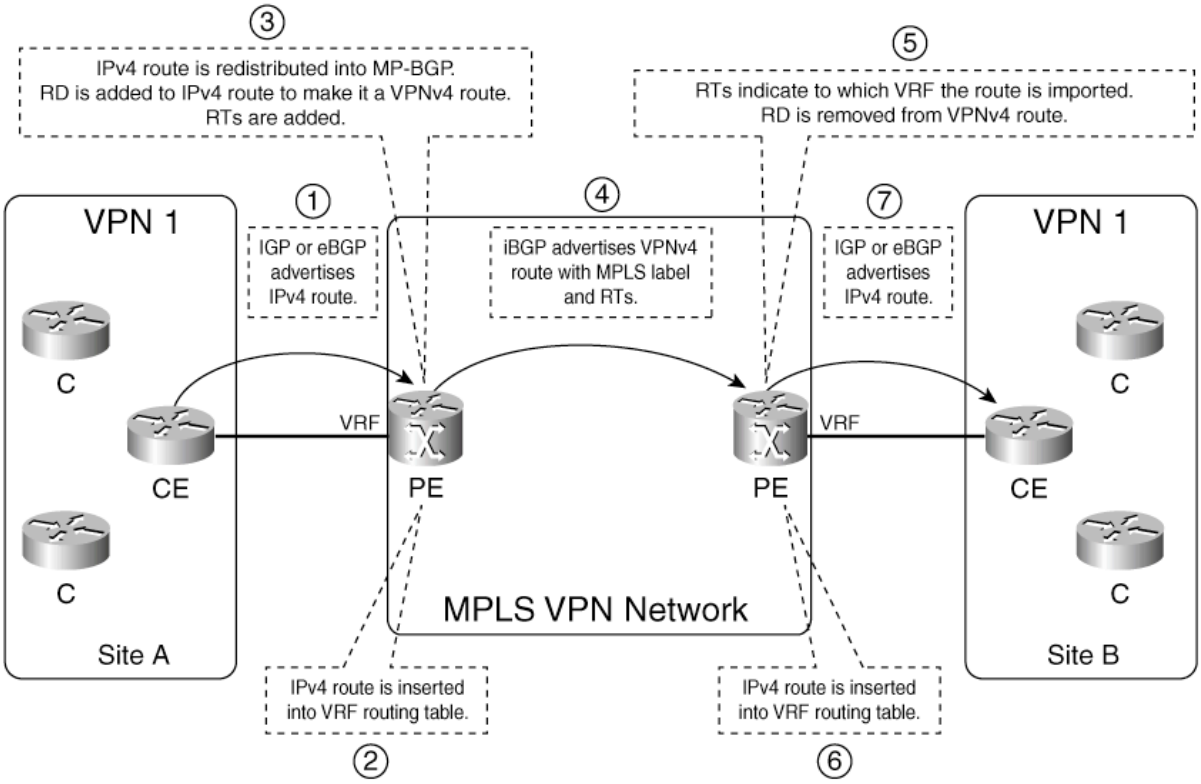


Figura 21: Propagação MPLS detalhada

Fonte: http://mpls-tp.com/

Os sete passos necessários para que um prefixo no Site A seja anunciado para o Site B são:

- Passo 1: o roteador CE do Site A anuncia o prefixo para o roteador PE que está diretamente conectado a ele e que pertence à operadora;
- Passo 2: a rota IPv4 é inserida na VRF pertencente à interface à qual o roteador CE está conectado;
- Passo 3: as rotas IPv4 aprendidas pelo protocolo de roteamento IGP ou eBGP são importadas para o MP-BGP. O identificador único RD é adicionado ao prefixo aprendido para formar o prefixo VPNv4. O identificador RT também é adicionado a VRF;
- Passo 4: o iBGP anuncia o prefixo VPNv4 que é anunciado pela MPLS através de *labels* e RT;
- Passo 5: no roteador PE de destino, o prefixo VPNv4 é associado a VRF correta e o identificador RD é retirado da VPNv4;

- Passo 6: o roteador PE insere a rota IPv4 na tabela de roteamento VRF;
- Passo 7: o prefixo IPv4 do roteador PE é anunciado para o roteador CE do Site B.

Vale lembrar que a importação/exportação de rotas pelos protocolos IGP e eBGP não são automáticas. Um comando precisa ser inserido no roteador para que as operações de importação e exportação sejam realizadas.

3.2.3 ENCAMINHAMENTO DE PACOTES NA MPLS VPN CAMADA 3

Na rede MPLS os pacotes IPv4 não podem ser encaminhados, pois os roteadores P não possuem a informação VRF de cada site. A rede MPLS resolve esse problema colocando *labels* nos pacotes.

Quando os pacotes passam pela MPLS estes possuem dois *labels*: um distribuído pelo LDP ou RSVP, que é o utilizado pelos roteadores P para fazer o encaminhamento dos pacotes na rede MPLS entre os roteadores PE. Esse *label* fica no topo da pilha. O outro é o *label* da VPN, que indica para qual roteador CE o roteador da provedora (PE) deve encaminhar o pacote. Esse *label* fica embaixo da pilha.

A Figura 22 mostra o anúncio da rota da VPNv4 e o *label* do roteador PE de entrada da MPLS para o roteador de saída. Nesse anúncio é informado ao roteador de entrada que para chegar ao cliente 1:1:10.10.100.1/32, deve ser enviado o *label* 30 para ele. Assim quando chegar o *label* 30, ele saberá de qual cliente o pacote é destinado. Esse *label* é referenciado como *label* VPN.

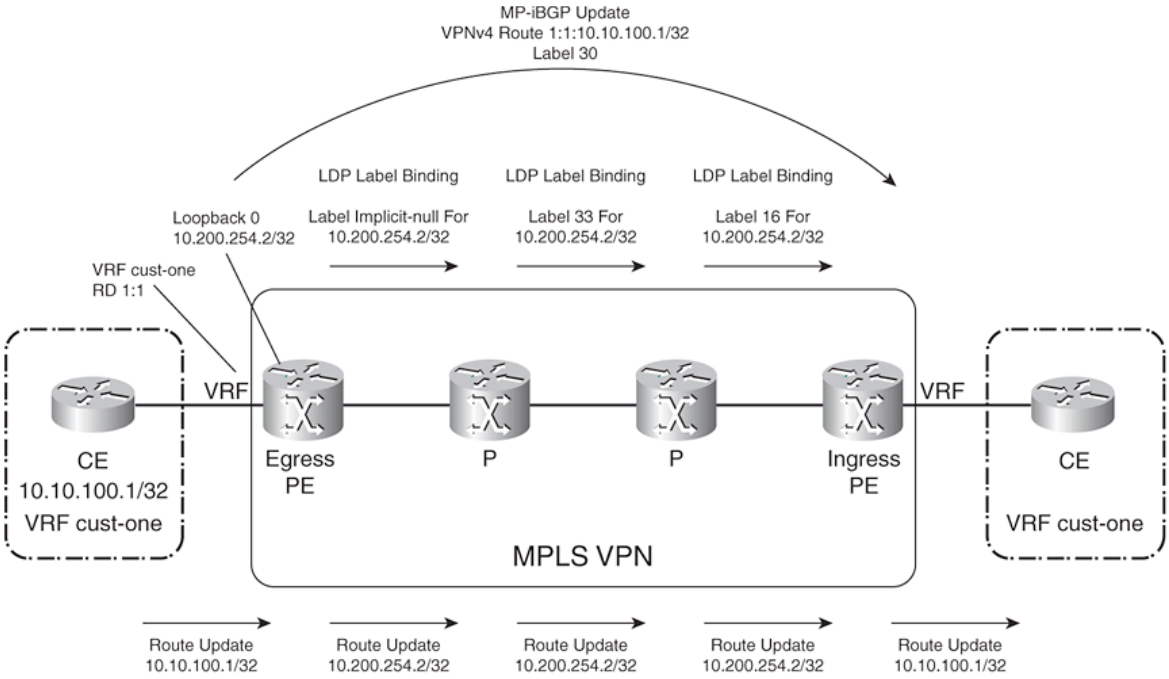


Figura 22: VPNv4

Fonte: [GHEIN, 2007]

Na Figura 23 um pacote está indo de um site para o outro do mesmo cliente. Quando um pacote IP chega ao roteador de entrada da rede MPLS, o roteador analisa o destino do pacote na tabela VRF. Quando esse roteador encontra a VRF correta, sabendo que cada interface está em uma VRF específica, a tabela de encaminhamento é examinada. Essa tabela indica que dois *labels* devem ser adicionados.

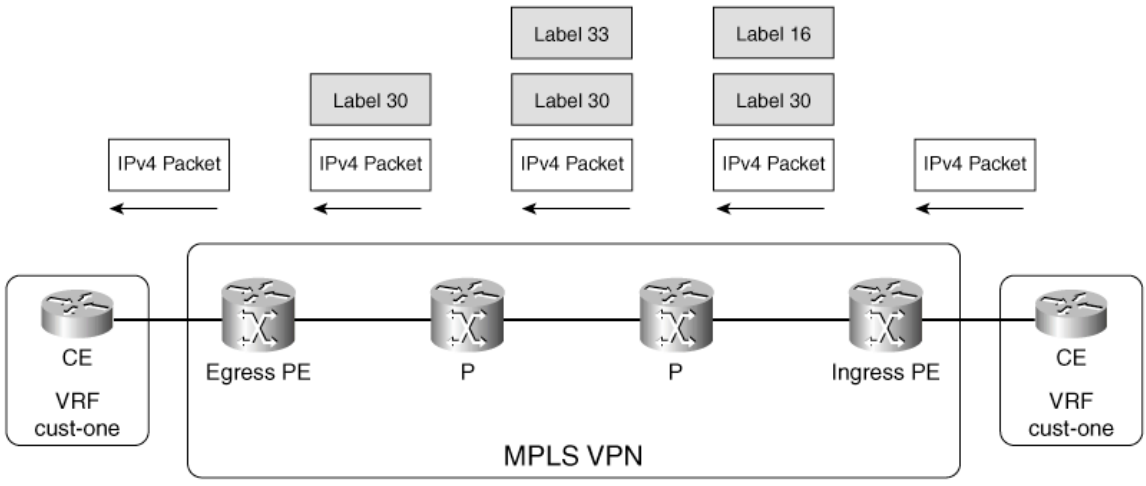


Figura 23: *Labels* na VPN

Fonte: [GHEIN, 2007]

Primeiro o roteador de entrada coloca o *label* 30, referente ao *label* VPN. Este se torna o *label* de baixo da pilha. Então o roteador PE coloca o *label* IGP em cima do *label* VPN. Este *label* está associado com a rota IGP para o endereço IP do vizinho BGP.

O pacote deixa, então, o roteador PE de entrada com dois *labels*. O *label* de cima (*label* IGP) é trocado em cada roteador do caminho (como já foi explicado no capítulo 2.3).

Finalmente o *label* IGP é retirado no último roteador P e o pacote chega ao roteador PE de saída somente com um *label*. Esse roteador verifica o *label* e faz a decisão de encaminhamento de pacote, retirando esse *label* e encaminhando o pacote IP para o roteador CE de destino.

3.3 MPLS VPN CAMADA 2

Depois da criação da rede MPLS, muitos provedores de serviços ainda possuíam clientes que alugavam seus meios físicos para conectar seus escritórios. Esses meios físicos eram estruturas ATM e *Frame Relay*, os quais os clientes utilizavam com um meio de transporte da camada 2. Sendo assim, não havia interação entre os equipamentos da operadora e do cliente em camada 3.

Esses clientes possuíam roteadores em cada escritório e esses locais eram interconectados pela estrutura locada pela operadora. Portanto, essa estrutura não podia ser abolida, pois ainda gerava muito dinheiro para as operadoras.

Os clientes não queriam migrar para as VPNs MPLS, pois eles ainda queriam ter o total controle sobre suas redes e ainda possuíam equipamentos legados que operavam com protocolos que não podiam ser transportados sobre IP.

Como havia a VPN MPLS que criava VPNs em camada 3, foi necessária a criação de VPNs de camada 2 na rede MPLS, as quais podiam transportar o tráfego dessa camada. Assim, elimina-se a necessidade de manter duas estruturas paralelas funcionando (MPLS e ATM ou MPLS e *Frame Relay*).

A Figura 24 mostra que um pseudo-tunel é criado na rede MPLS, emulando um túnel entre os clientes.

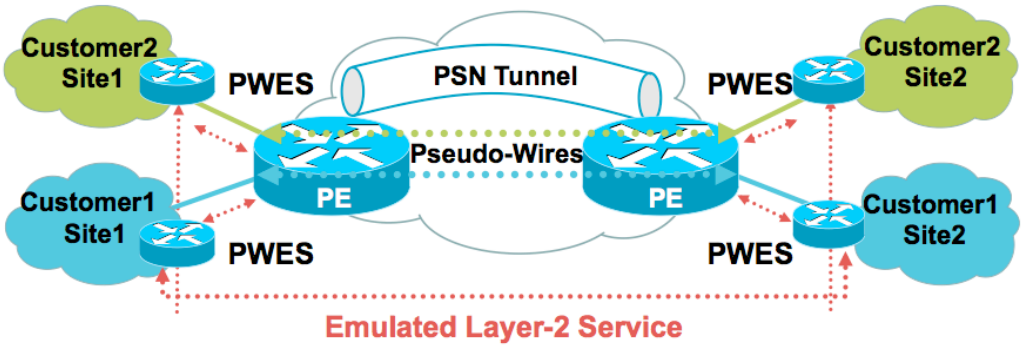


Figura 24: Túnel MPLS

Fonte: http://www.blackhat.com/

3.3.1 ANY TRANSPORT OVER MPLS

Nas VPN de camada 2 ponto a ponto também conhecidas com AToM (*Any Transport over MPLS)*, o roteamento através da rede MPLS é praticamente o mesmo. Os roteadores P ainda continuam encaminhando os pacotes com base em *labels*.

Dois *labels* são colocados no quadro *Ethernet*. O *label* de cima ou *tunnel label* identifica o túnel (LSP) que o quadro pertence. O *label* de baixo é o *label* VC *(Virtual Circuit)* e identifica o túnel virtual. Em outas palavras, o roteador de saída da MPLS consulta o *label* VC, e utiliza esse *label* para determinar qual o circuito adjacente (porta *Ethernet* ou sub-interface) que o pacote deve ser encaminhado. Cada sessão LDP sinaliza cada VC ou pseudo-túnel entre um par de roteadores PE e anuncia o *label* VC.

Estabelecida a sessão, os dois *switches* ou roteadores CE ficarão diretamente conectados via camada 2, ou seja, a rede da operadora é totalmente transparente para o cliente.

Como se pode ver na Figura 25, quando um pacote entra na rede MPLS o roteador PE1 insere os dois *labels* mencionados anteriormente e encaminha o pacote para os roteadores P. O último roteador P retira o *label* referente ao circuito virtual e encaminha para o PE de destino. Esse roteador com base no *label* encaminha o quadro *Ethernet* para o usuário de destino.

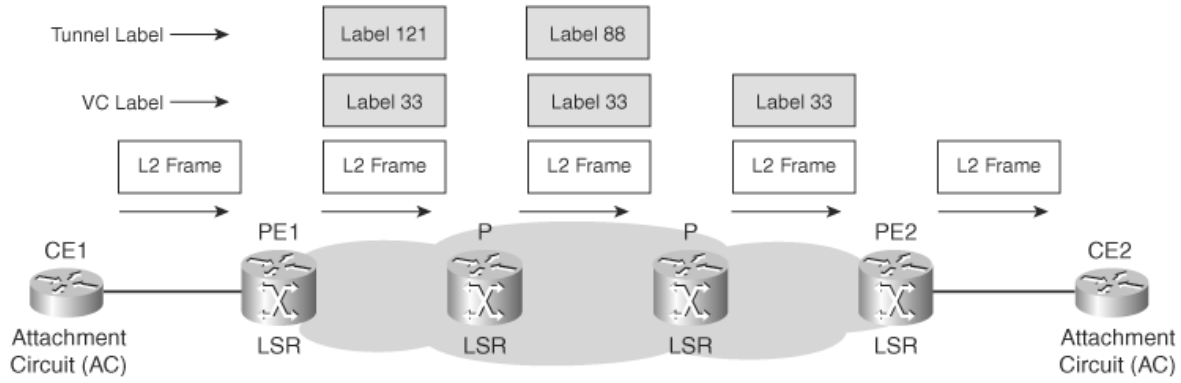


Figura 25: Labels MPLS VPN camada 2
Fonte: http://www.datacentertalk.com/

Como há clientes que possuem vários sites distintos, há a necessidade da criação de túneis de camada 2 entre mais de dois sites. Como o AToM fornece um pseudo-túnel de camada 2 ponto a ponto, houve a necessidade da criação da VPLS (*Virtual Private Lan Service*).

3.3.2 VPLS

Uma VPLS (*Virtual Private Lan Service*) é utilizada para emular uma rede local sobre uma rede MPLS. Na visão do cliente toda a rede do provedor é vista como um grande switch, e toda comunicação entre os pontos interligados é feita a nível 2 da camada OSI. O provedor de serviços analisará o pacote apenas até a camada de enlace, ignorando completamente as informações no cabeçalho da camada de rede [Valente, 2010].

A rede VPLS funciona como um *switch*, e para realizar tal função possui algumas características do mesmo:

- Comutação de pacotes baseados no cabeçalho da camada 2;
- *Broadcast* de pacotes com MAC destino desconhecido;
- Replicação de *broadcast* e *multicast*;
- Prevenção de *loops*;
- Aprendizagem de endereços MAC;

E algumas restrições:

- A rede MPLS deve estar funcionando entre os PEs;
- Os PEs participantes devem possuir as rotas dos PEs remotos;
- A rede VPLS aplica o conceito de *split-horizon* nos PEs, ou seja, nada recebido de um *pseudowire* volta para o mesmo;
- A rede VPLS deve formar uma rede *full-mesh* entre os PEs participantes;

A forma que os *labels* são inseridos nos *quadros* Ethernet são os mesmos do AToM.

O quadro transportado é o *Ethernet* sem o 802.1Q tag. Este tag é retirado antes que o quadro seja encaminhado para a rede MPLS. O roteador PE constrói a tabela MAC como um *switch Ethernet* padrão. Esta tabela MAC encaminha quadros *Ethernet* para e de uma porta física ethernet para e de tuneis virtuais.

A VPLS requer uma rede *full mash* de pseudo túnel entre os roteadores PE para cada instância VPLS. Quando se configura a instância VPLS no roteador PE, precisa-se também especificar o vizinho VPLS do roteador PE. O que significa que é preciso especificar todos os roteadores PE remotos para este roteador PE para qual tem a instância VPLS. O roteador PE então estabelece uma sessão LDP entre eles de forma que fique uma rede *full mash*. Se uma instância VPLS é associada a uma interface VLAN (*Virtual Local Area Network)* no roteador PE local, um VC ID local é associado à instância VPLS. O VC ID é o identificador VPN (VPN ID) que é preciso associá-lo na configuração a instância VPLS. Cada pseudo-túnel entre um par de roteadores PE para a instância VPLS possui o VC ID. Entretanto, o *label* VC local que o roteador associa para a instância VPLS é diferente para cada pseudo-túnel. A Figura 26 mostra essa sinalização.

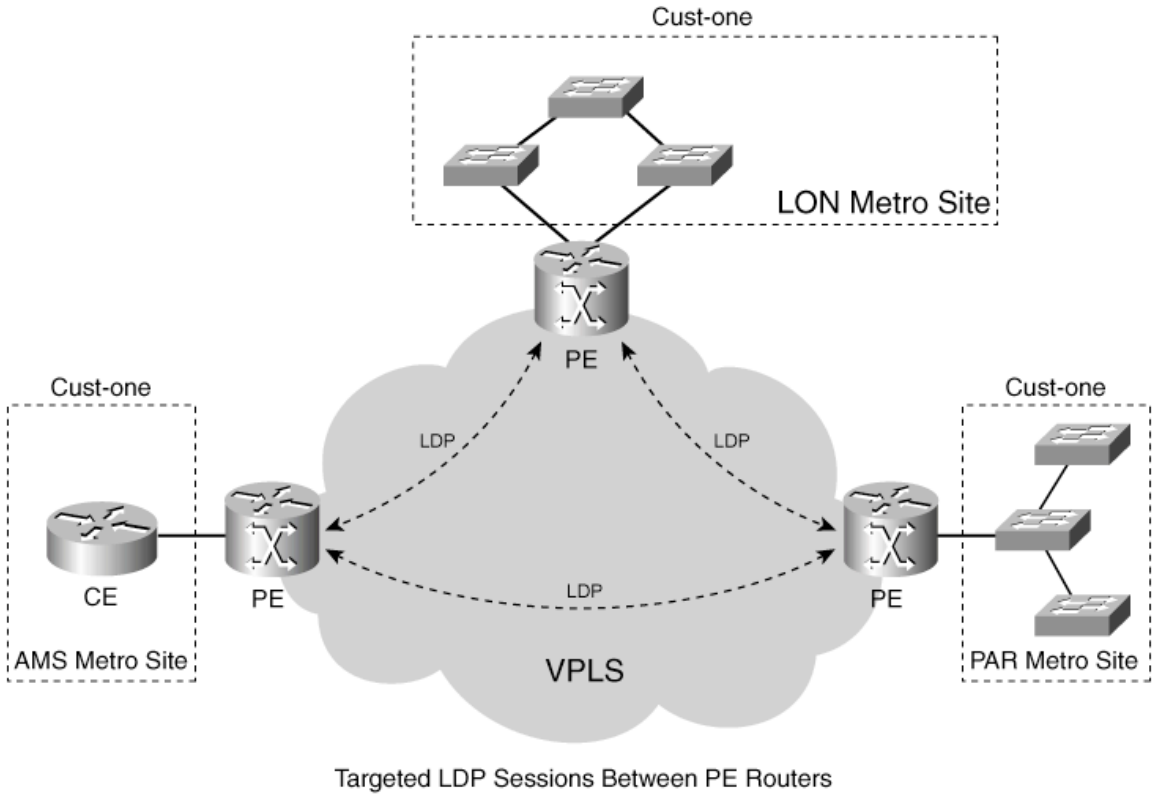


Figura 26: Sinalização VPLS

Fonte: [GHEIN, 2007]

3.4 QUALIDADE DE SERVIÇO

Antigamente, a Internet trabalhava apenas com uma classe de serviço. Não havia nenhum compromisso de segurança de entrega dos pacotes ou prioridade.

Algumas aplicações são elásticas, ou seja, tolerantes a perdas e atrasos. Essas aplicações podem se adaptar a congestionamentos de rede.

Quando se começou a utilizar aplicações através da rede, essas não eram elásticas, ou seja, se um pacote atrasasse ou não chegasse ao destino não havia problema, pois esse pacote era reenviado novamente pela origem e eles eram reordenados no destino. Quando se começou a utilização de aplicações elásticas (aplicações afetadas com o atraso de pacotes) como voz e vídeo surgiu a necessidade da criação de QoS (Quality of Service) na rede para que fosse possível fazer a priorização desse deste tráfego.

Alguns exemplos de aplicações prioritárias (inelásticas) são voz e vídeo. Enquanto HTTP (*Hyper Text Transfer Protocol*) e FTP (*File Transfer Protocol)* são aplicações não prioritárias (elásticas).

O IETF (*Internet Engineering Task Force*) desenvolveu duas maneiras de implementar o QoS que são: Intserv e Diffserv (*Differencial Service)*.

O Intserv utiliza o protocolo RSVP como protocolo de sinalização. Ele garante que o fluxo terá plenas condições de atravessar a rede com qualidade porque requisita e aloca recursos em todos os roteadores, antes mesmo de começar a transmitir os dados. Dessa forma, a comunicação só acontece se todos os nós responderem positivamente à requisição de recurso. Se não houver recurso disponível, não haverá comunicação.

- Uma rede que implementa Intserv precisa garantir que seus roteadores sejam capazes de executar as seguintes tarefas:Controle de admissão: determina que um fluxo pode ser encaminhado com o grau de qualidade requerido sem interferir em fluxos que já estejam em curso;
- Classificação: reconhece pacotes que necessitam de níveis específicos de QoS.
- Policiamento: Age, inclusive descartando pacotes, quando o tráfego não está em conformidade com o especificado.;
- Enfileramento e escalonamento: encaminha os pacotes de acordo com os requisitos de QoS.

O modelo Intserv possui uma desvantagem: o RSVP requer muita memória nos roteadores, pois é necessário manter o estado de diversas conexões simultaneamente. A dificuldade em escalar para redes muito grandes tornando-o impraticável na Internet.

Já o Diffserv foi criado pela necessidade de um método relativamente simples prover tratamento adequado para os fluxos das diferentes aplicações de rede. Era preciso diferenciar os fluxos em classes de serviço distintas e tratar os pacotes de acordo com suas necessidades.

Os roteadores que implementam Diffserv precisam possuir quatro blocos lógicos, ilustrados na figura 27:

- Classificador: seleciona um pacote do fluxo baseado no conteúdo de alguma porção do cabeçalho;

- Medidor: Verifica se os parâmetros do tráfego estão de acordo e passa os resultados para o marcador e modelador;
- Marcador: Escreve (ou rescreve) o campo DSCP (*Differentiated Services Code Point*);
- Modelador: atrasa ou descarta alguns pacotes para que o tráfego fique em conformidade com o projeto.

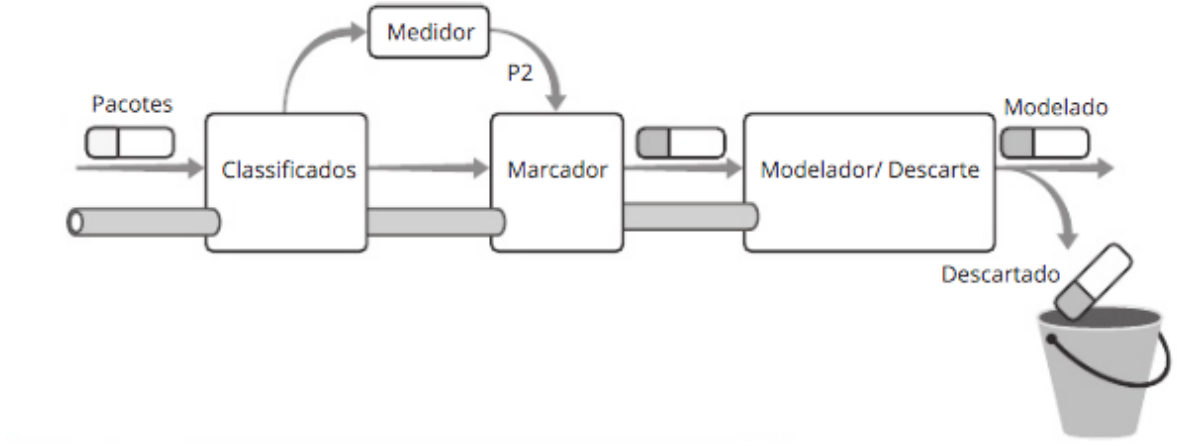


Figura 27: DiffServ
Fonte: [Maluf, 2013]

Mecanismos de condicionamento de tráfego:

- Policiamento (*Policing)*: O policiamento consiste em descartar todo o tráfego que excede determinada taxa.
- Modelagem (*Shaping)*: A modelagem tenta não descartar o tráfego excedente, enfileirando e distribuindo as rajadas de dados que excedem determinado limite, amortecendo o efeito da rajada no enlace.

Para alcançar o objetivo de encaminhar pacotes de diferentes classes e, portanto com diferentes prioridades, são necessárias duas ações principais:

1. Marcação de pacotes, utilizando o campo ToS (*Type of Service*) do cabeçalho IP.
2. PHP (*Per Hop Behavior)*, que define um comportamento diferente a cada salto do pacote, ou seja, a cada roteador.

A grande vantagem do Diffserv em relação ao Intserv é que o primeiro não utiliza nenhum protocolo adicional nos roteadores. Já no caso do Intserv todos os roteadores e host da rede precisam utilizar o protocolo de sinalização RSVP. Outra vantagem seria que o Diffserv possui um conceito de classes, enquanto o Intserv mantém o controle de sessões. O que torna o Diffserv muito mais utilizado nas redes de hoje.

Na Figura 28, o campo em vermelho no cabeçalho IP indica o *Type of Service*.

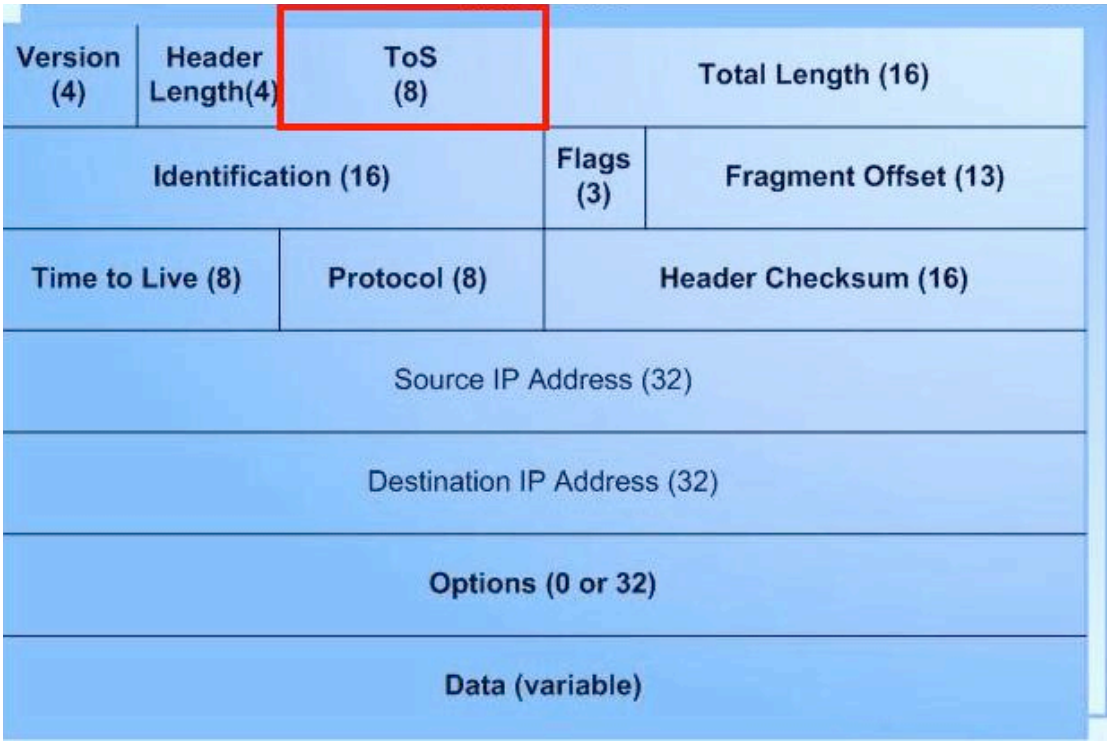


Figura 28: Pacote IP

Fonte: http://ciscoredes.com.br

Na figura 29, mostra que os três primeiros bits são destinados a classe de QoS. Com esses 3 bits só poderiam existir no máximo oito classes de serviço, com a crescente demanda de utilização de fluxos prioritários na rede era necessário mais classes.

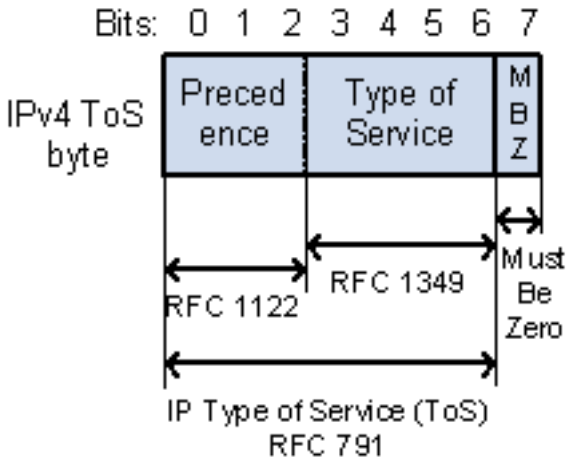


Figura 29: ToS

Fonte: http://www.h3c.com/

Com isso a IETF redefiniu o campo *Type of Service* e o último bit (MBZ – Must Be Zero), criando um novo campo chamado de DSCP, o qual aumentava o número de classes de QoS disponíveis. Esse novo campo é mostrado na Figura 30.

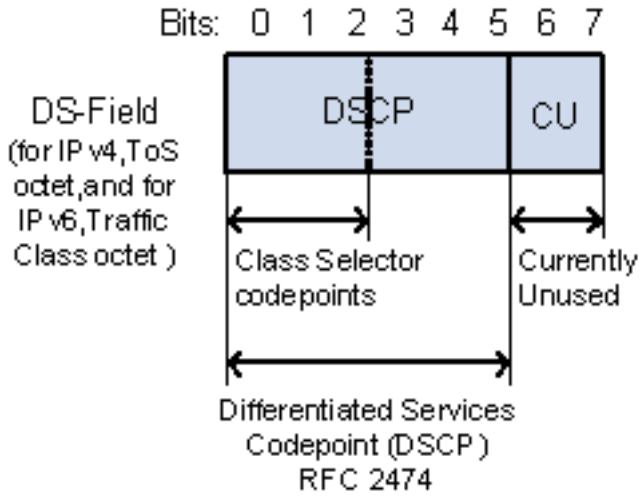


Figura 30: DSCP

Fonte: http://www.h3c.com/

Existem várias classes de encaminhamento de pacotes no Diffserv. Uma das classes é a EF (*Expedited Forwarding)*, que possui baixa perda, baixa latência, baixo *jitter* e largura de banda garantida. Outra classe, que é a AF (*Assured Forwarding)* define vários encaminhamentos para serviços diferentes. Dentro da classe AF, há quatro subclasses definidas, cada uma com três níveis de descarte de pacotes.

Os três primeiros bits do campo DSCP indicam a classe de serviço (AF), os dois bits seguintes indicam o nível de descarte de pacote e os últimos dois bits são reservados.

Quanto maior o nível de descarte de pacotes, maior a chance desse pacote ser descartado quando ocorrer congestionamentos na rede.

A Tabela 1 mostra o nível de descarte dos pacote das classes AF:

Prioridade de tratamento

	Classe 1	Classe 2	Classe 3	Classe 4
Precedência De Descarte ↓	001010 (AF11)	010010 (AF21)	011010 (AF31)	100010 (AF41)
	001100 (AF12)	010100 (AF22)	011100 (AF32)	100100 (AF42)
	001110 (AF13)	010110 (AF23)	011110 (AF33)	100110 (AF43)

Tabela 1: Classes QOS

Fonte: http://gredes.ifto.edu.br/

A classe EF é representada pelo campo 101110.

Além dessas classes também existe a classe *Best Effort*, que possui menor prioridade e cujos pacotes serão encaminhados depois de todas as outras classes, se houverem recursos para isso. E também a classe CS (*Class Selector),* que determina o valor da prioridade de modo linear.

3.4.1 QoS NA REDE MPLS

No MPLS o campo EXP/TC representa os bits de QoS, como já foi explicado na seção 2.2. Quando um pacote IP passa pelo roteador MPLS, os três primeiros bits do campo *precedence* são copiados para o campo EXP/TC do cabeçalho MPLS. Isso é uma grande desvantagem do MPLS, pois não é possível transportar toda a informação contida no campo ToS do cabeçalho IP (8 bits). Consequentemente o MPLS possui menos classes de serviço que o IP. Também é possível configurar o roteador para que esse campo não seja copiado e que seja colocado no campo EXP um valor diferente.

Existem algumas regras para imposição, troca e retirada de *labels* referente ao campo EXP.

Como podemos ver na Figura 31 e 32, mostram a imposição de *labels* que indica a reflexão do campo *Precedence* para o campo EXP/TC.

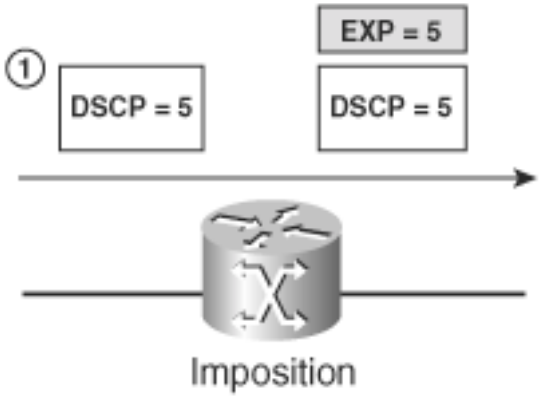


Figura 31: Reflexão do campo *Precedence I*

Fonte: [GHEIN, 2007]

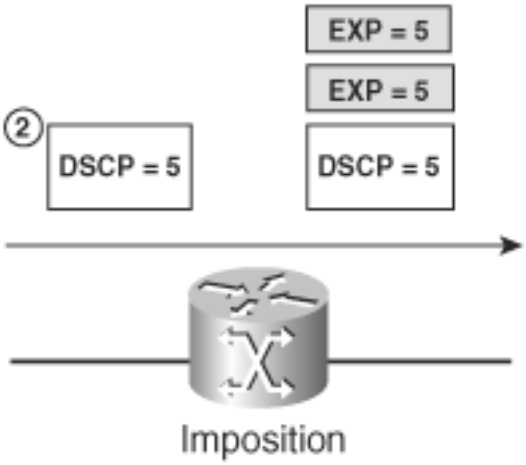


Figura 32: Reflexão do campo *Precedence II*

Fonte: [GHEIN, 2007]

Na Figura 33 podemos constatar que os bits EXP/TC do *label* de cima da pilha são copiados para todos os *labels* trocados e inseridos na pilha (*swap* e *push)*.

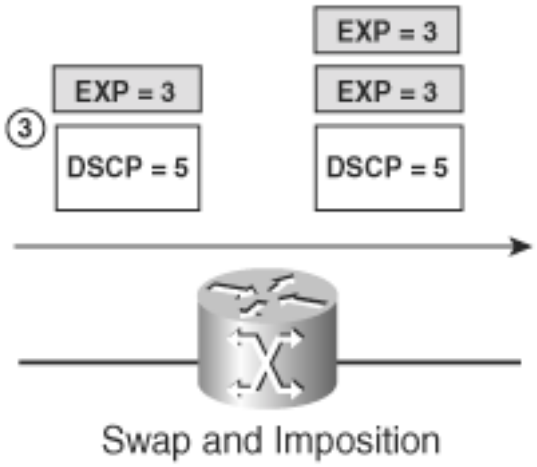


Figura 33: Copia do campo EXP I

Fonte: [GHEIN, 2007]

As Figuras 34 e 35, mostram o mesmo procedimento da Figura 33 com o acréscimo que o *label* de baixo da pilha permanece inalterado.

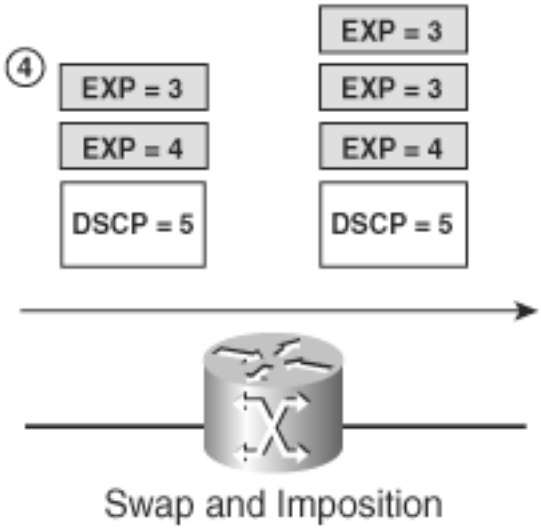


Figura 34: Copia do campo EXP II

Fonte: [GHEIN, 2007]

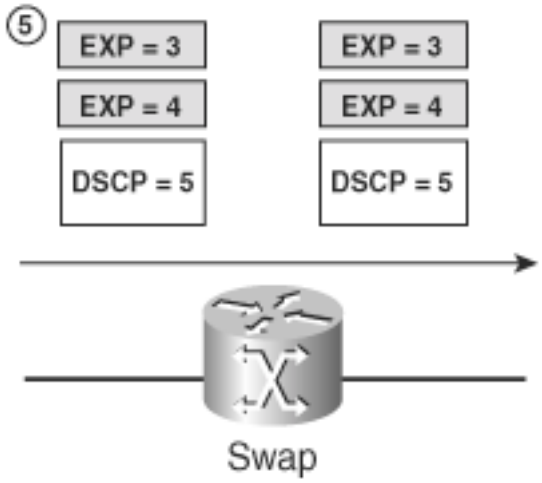


Figura 35: Copia do campo EXP III
Fonte: [GHEIN, 2007]

A Figura 36 indica que o campo EXP/TC do *label* retirado, não é copiado para os *labels* que continuam na pilha.

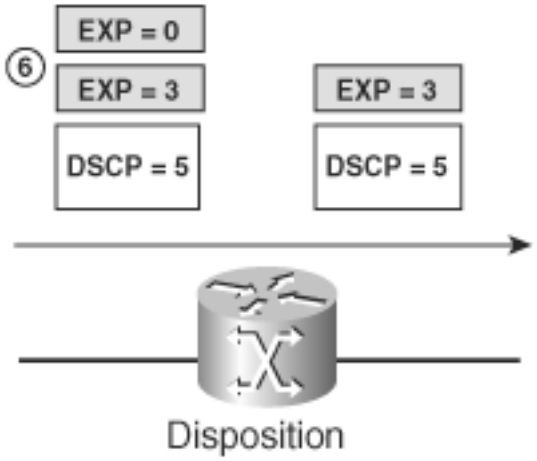


Figura 36: Retirada de *label*
Fonte: [GHEIN, 2007]

A Figura 37 indica que o campo EXP/TC do último *label* retirado, não é copiado para o campo *Precedence* do pacote IP.

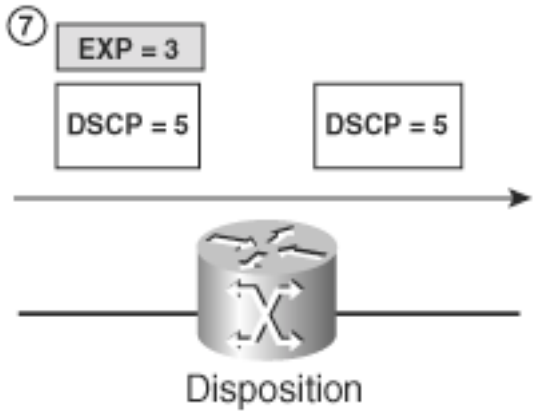


Figura 37: Retirada do último *label*
Fonte: [GHEIN, 2007]

No MPLS existem três modelos de tunelamento: O *Pipe Model, Short Pipe Model* e o *Uniform Model.*

O modelo *Pipe* e *Short Pipe* são quase os mesmos: Eles não mudam o ToS do campo IP do cliente. Eles podem mudar o campo EXP/TC do caminho, mas o campo DSCP do pacote IP permanece o mesmo. A diferença dos dois modelos, mostrada na Figura 38, está no roteador PE de saída da MPLS. Enquanto o modelo *Pipe* faz o encaminhamento e descarte de pacotes baseados no campo EXP/TC, o *Short Pipe* faz isso baseado no campo ToS do pacote IP.

Já no modelo *Uniform* não há garantia que o campo ToS do cliente permaneça inalterado, mas o campo EXP/TC e o campo ToS irão sempre ser iguais. Isso significa que quando o provedor de serviços mudar o campo EXP, esse campo será copiado depois para o campo ToS no roteador de saída, conforme a Figura 30.

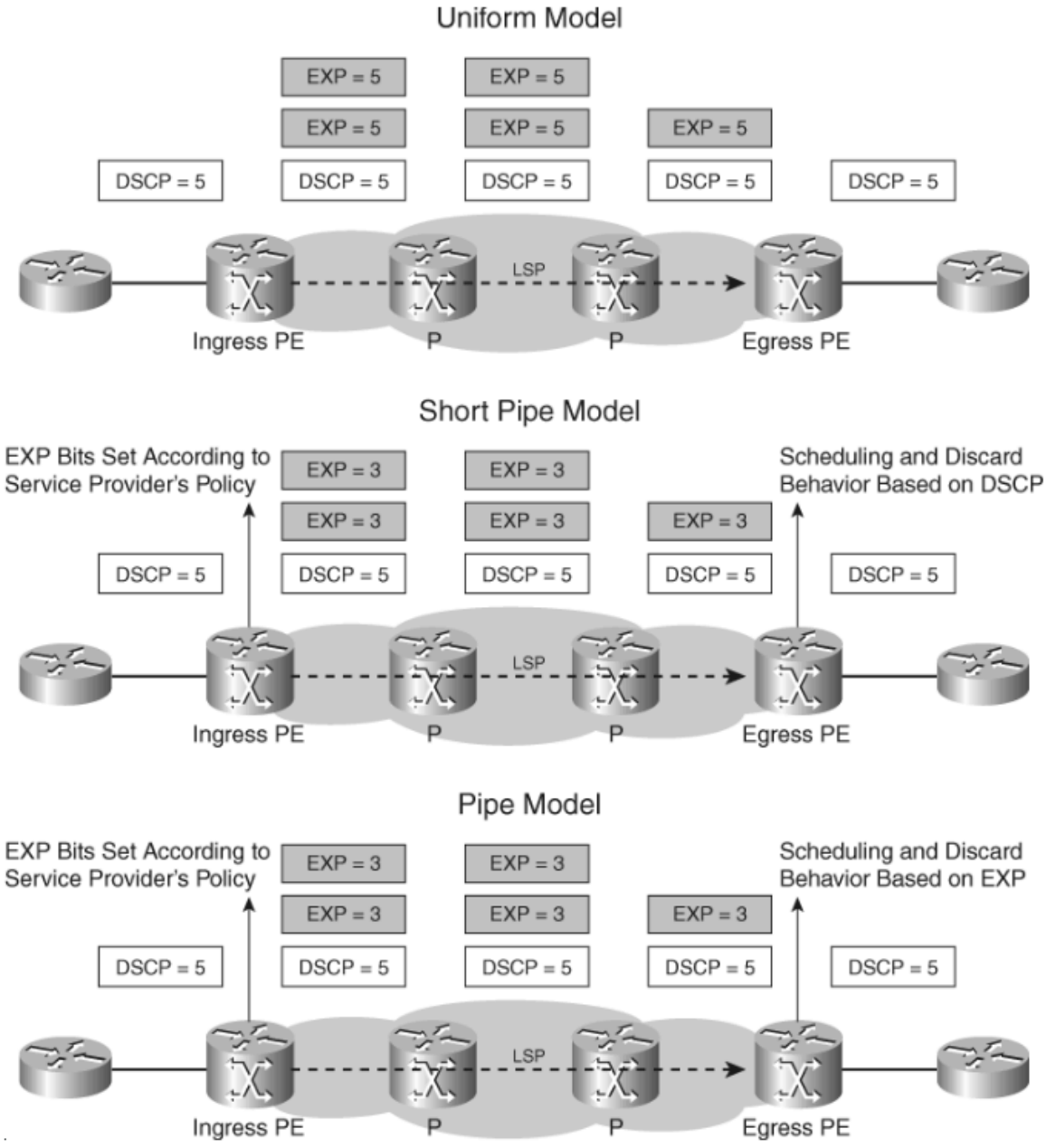


Figura 38: Regras de *labels* na MPLS

Fonte: [GHEIN, 2007]

3.5 ENGENHARIA DE TRÁFEGO

As redes IP não possuem a capacidade de otimização na manipulação de tráfego. Ou seja, sempre que um tráfego é enviado através da rede IP, ele percorre o caminho com a menor métrica, o que pode ocasionar congestionamentos na rede enquanto rotas alternativas estão sem utilização.

A Figura 39 mostra um problema de congestionamento, causado por esta característica da rede IP, onde o roteador RtrA, envia um fluxo de 60Mb para o

roteador RtrE. O caminho escolhido pelo protocolo de roteamento passa através do roteador RtrB (pois este possui a menor métrica). O problema é que a largura de banda do *link* entre RtrB e o RtrE é de apenas 34Mbps, ou seja, 26Mb do fluxo enviado será descartado.

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	25
E	B	25
F	B	40
G	B	40

- **RtrA tem 30Mb de tráfego para o RtrF e 30Mb de tráfego para o RtrG**
- **(43%) perda de pacotes entre RtrB->RtrE!**
- **Mudando a rota para A->C->D->E não soluciona o problema**

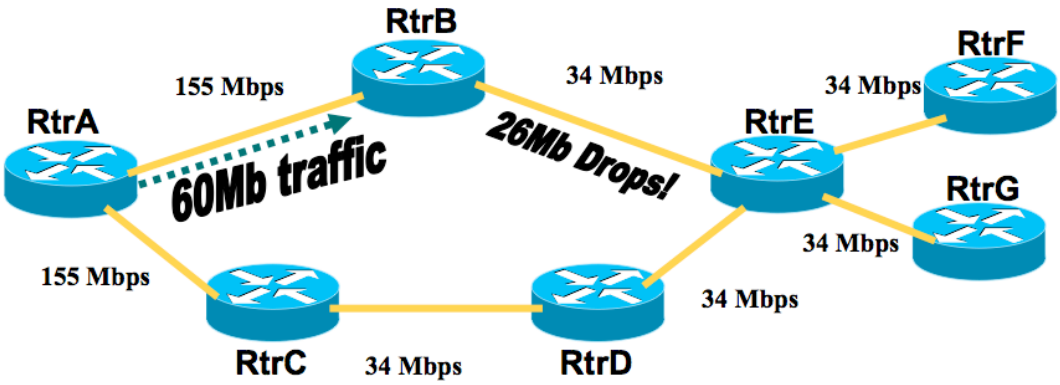


Figura 39: Congestionamento

Fonte: http://www.lsi.usp.br

Ao invés de adicionar largura de banda para gerenciar o aumento do tráfego, a engenharia de tráfego MPLS utiliza a largura de banda existente de forma mais eficiente. Permitindo, assim, que pacotes possam ser encaminhados por rotas explícitas e com uma largura de banda específica garantida. Isto é permitido pelo RSVP-TE, e é a chave da engenharia de tráfego MPLS. O RSVP-TE gera caminhos do tráfego de dados dentro de uma rede MPLS, permitindo que o tráfego seja encaminhado a rotas desejadas [ROCHA, 2011].

Na Figura 40, podemos perceber que com a implementação da engenharia de tráfego, o fluxo de dados (60Mb) é divido entre dois caminhos, assim não havendo descartes de pacotes.

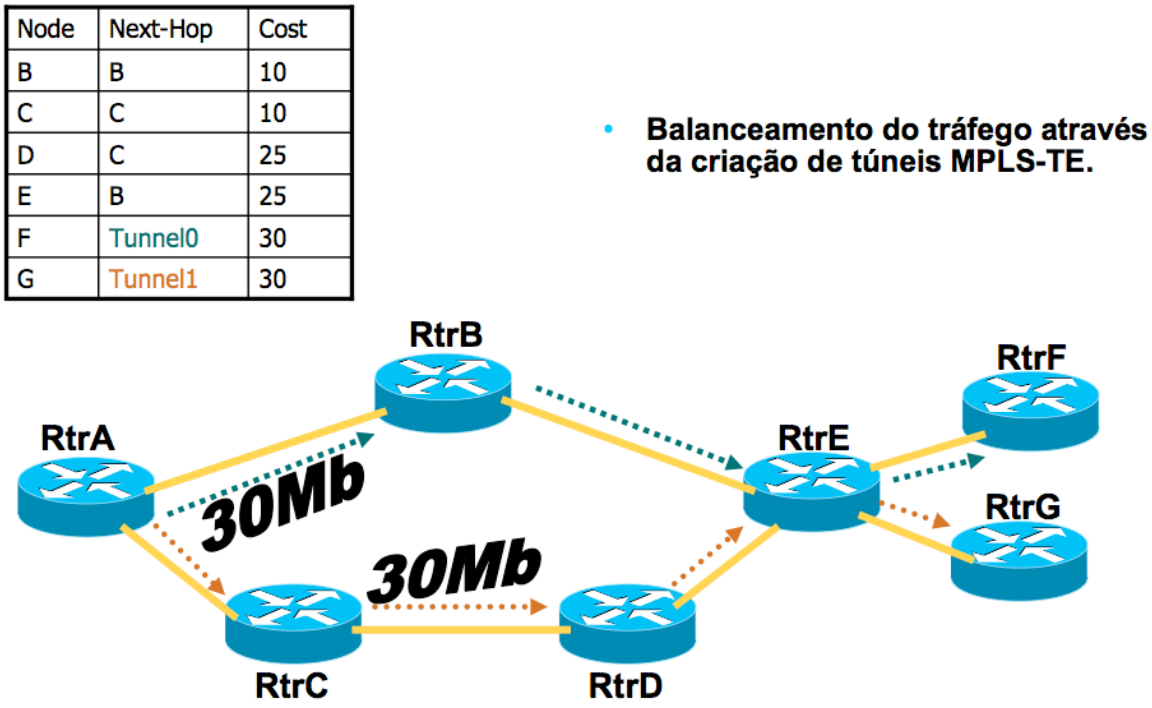


Figura 40: Engenharia de Tráfego

Fonte: http://www.lsi.usp.br

Uma outra vantagem de utilizar a engenharia de tráfego com MPLS é a possibilidade do uso de FRR (*Fast ReRouting)*, que permite mudar o roteamento do tráfego rotulado em torno de um *link* ou roteador que se tornou indisponível. Este *re-routing* do tráfego ocorre em menos de 50 ms, que é rápido mesmo para os padrões de hoje em comparação com outros protocolos de redundância [LINHARES, 2010].

No caso do OSPF, por exemplo, o tempo de convergência é em torno de 14 segundos, segundos [Pun, 2001].

3.5.1 FRR

O mecanismo de FRR é um mecanismo de proteção. Ele é definido através de túneis *backup*, que serão utilizados para proteção em situações de falha do túnel principal na arquitetura MPLS TE. A proteção local proporciona diversas vantagens tais como: recuperação de falhas mais rápida, escalabilidade e o consumo de menos recursos da rede [Gondim, 2011].

A proteção local pode ser dividida em:

- *Link Protection* (Proteção do enlace)
- *Node Protection* (Proteção do Nó)

A Figura 41, exibe a proteção local entre R3 e R5 e também a proteção de nó no equipamento R5.

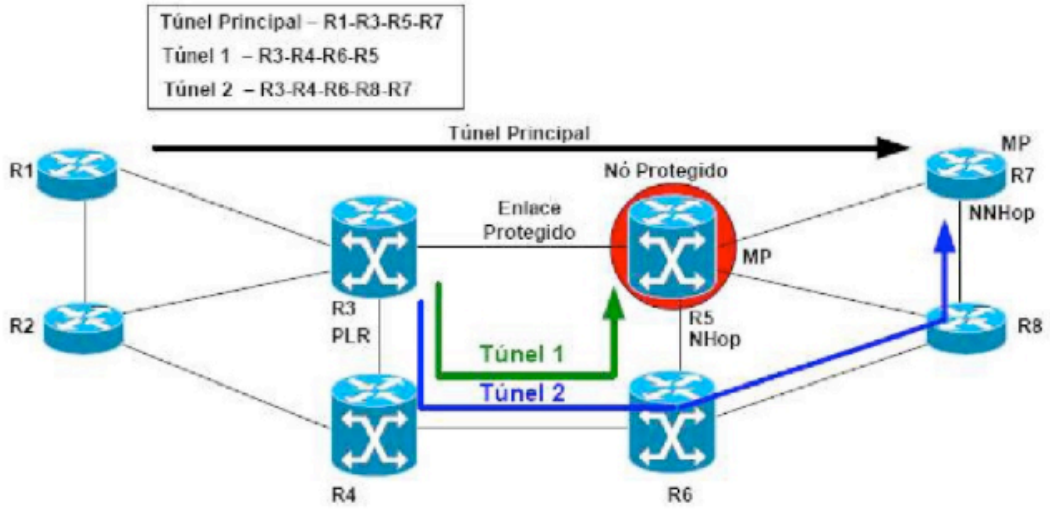


Figura 41:FRR

Fonte: [GONDIM, 2011]

O enlace R3-R5 é considerado o enlace crítico sobre o qual o túnel primário é estabelecido.

Para a proteção do enlace crítico, um túnel *backup* entre os roteadores R3 e R5 é estabelecido, passando pelos roteadores R4 e R6.

Já para a proteção do nó, o túnel backup será entre o roteador R3 e o R7, com o túnel sendo formado através dos roteadores R4,R6 e R8.

A proteção do enlace conta com o fato de que, embora o enlace protegido tenha sido rompido, o roteador na outra ponta desse enlace protegido ainda está ativo, portanto a proteção do enlace permite a proteção de uma falha do enlace, mas não contra uma falha de nó

A proteção do nó é semelhante à proteção do enlace, ou seja, em caso de falha do roteador R5, o tráfego será transmitido através do Túnel 2, até que o roteador R5 seja reestabelecido.

4 CONCLUSÃO

Antes do MPLS surgir, o protocolo ATM, que era predominante na Internet, possuía dificuldade de integração com o protocolo IP. Esse motivo somado com a exigência de velocidade de transmissões cada vez mais rápidas exigidas por clientes, o MPLS surge como um multiprotocolo, solucionando o problema de interoperabilidade e otimizando a velocidade de transmissões dos pacotes.

O MPLS possuí facilidade de interoperabilidade com diversos protocolos através das aplicações de MPLS VPN e da otimização da transmissão de dados possibilitada pelo roteamento baseado em *labels*. Também podemos citar outras características importantes desse protocolo como a possibilidade de implementação de engenharia de tráfego, sendo possível manipulação dos fluxos de dados por diferentes caminhos e o suporte a qualidade de serviço. Tudo isso sem ser necessário alterar a infraestrutura já existente.

Todas essas características mostram que o MPLS é um multiprocolo que melhora a qualidade de transmissão (QoS), a segurança (VPN) e planejamento dos fluxos de dados (Engenharia de Tráfego).

Uma extensão do MPLS é conhecida como GMPLS (*Generalized Multiprotocol Label Switching*) permitindo que o MPLS seja utilizado não somente em caminhos baseados em pacotes, mas também em caminhos que possuem equipamentos que não suportem pacotes, como *switches* ópticos e multiplexadores TDM.

Como o MPLS se tornou uma arquitetura de sucesso, outras extensões estão sendo criadas e testadas para expandir seu funcionamento para outras redes. Dentre estas, pode-se citar a MPLS-TP (*Multi Protocol Label Switching Transport Profile*) que é uma versão simplificada do MPLS tradicional e que é usada principalmente para oferecer transporte orientado à conexão para serviços baseados em pacotes sobre redes ópticas aproveitando a tecnologia MPLS. A chave para essa tecnologia é a definição e implementação de funcionalidades de operação, administração, monitoramento e resiliência para garantir as características necessárias para uma rede de transporte classe operadora – operações escaláveis, alta disponibilidade, monitoramento de desempenho e suporte a multi-domínios. O

MPLS-TP utiliza o GMPLS para o plano de controle, o qual é o responsável pela troca de informação em camada 3.

Isso mostra que o MPLS é muito aceito nos dias de hoje e que está servindo como referência para novas tecnologias. Além disso esse protocolo está cada vez mais sendo difundido, isso é observado pelo GMPLS que tem como foco as redes que não são baseadas em pacotes.

REFERÊNCIAS

[FELIPPETTI, 2008] Marco Aurélio. CCNA 4.1: Guia completo de estudo. Florianópolis: Visual Books, 2008. 480 p.

[INÁCIO, 2010] Fabricio Couto. MPLS – Multiprotocol Label Switching. Disponível em: < http://www.gta.ufrj.br/grad/02_1/mpls/apres.html > Acesso em 30 nov. 2010.

[KUROSE, 2006] James F.; ROSS, Keith W. Redes de computadores e a internet: uma abordagem top-down. 3. ed. São Paulo, SP: Pearson Addison-Wesley, 2006. xx, 634 p.

[GHEIN, 2007] Luc De; MPLS Fundamentals. Indianapolis, EUA; Cisco Press, 2007. 626 p.

[MORGAN, 2008] Brian; LOVERING, Neil. CCNP ISCW: Official Exam Certification Guide. Indianapolis, USA: Cisco Press, 2008. 682 p.

[RUELA, 2010] Ruela. Redes IP e Tecnologias de Nível 2 – Arquiteturas/MPLS. Disponível em: < http://paginas.fe.up.pt/~jruela/redes/teoricas/8_mpls_v1011_mieec_2slides.pdf > Acesso em 17 a 30 set. 2013.

[ROCHA, 2011] Adriano Santos. Estudo Básico do MPLS (Multi Protocol Label Switching) – II. Disponível em: < http://www.teleco.com.br/tutoriais/tutorialmplseb2/pagina_2.asp > Acesso em 17 a 30 set. 2013.

[LINHARES, 2010] Fhilipe Guimarães. Avaliação de desempenho de VPNs sobre redes MPLS-Linux. Disponível em: < http://www.lume.ufrgs.br/bitstream/handle/10183/28311/000767714.pdf?sequence=1 > Acesso em 17 a 30 set. 2013.

[MONFREDINHO, 2011] Andre Luiz. MPLS. Disponível em: < http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/398/1/CT_GESER_1_2011_06.pdf > Acesso em 17 a 30 set. 2013.

[DIEGO, 2011] Introdução ao MPLS (Multi Protocol Label Switching) – parte 1. Disponível em: < http://www.rotadefault.com.br/2011/10/20/introducao-ao-mpls-multi-protocol-label-switching-–-parte-1/ > Acesso em 17 a 30 set. 2013.

[DASGUPTA, 2010] Santanu. *Introduction to* MPLS. Disponível em: < http://www.sanog.org/resources/sanog17/sanog17-mpls-intro-santanu.pdf > Acesso em 17 a 30 set. 2013.

[REY, 2006] Enno. MPLS *and* VPLS *Security*. Disponível em: < http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rey-up.pdf > Acesso em 17 a 30 set. 2013.

[BEZZERA, 2008] Jossenilson de Melo. A Tecnologia MPLS e seus Serviços. Disponível em: < http://dietinf.ifrn.edu.br/lib/exe/fetch.php?media=corpodocente:alfredo:ir_-mpls_-_monografia_jossenilson.pdf > Acesso em 17 a 30 set. 2013.

[YASUDA, 2004] Luis M.; Chiaverini, Andre Omar. MPLS – Engenharia de Tráfego. Disponível em: < http://www.lsi.usp.br/~rav/rav-fev-2004/apres-alunos/02-MPLS.pdf > Acesso em 17 a 30 set. 2013.

[FILHO, 2006] Jorge Lima de Oliveira. Tecnologias Diffserv como suporte para a qualidade de serviço (QoS) de aplicações Multimídia – Aspectos de Configuração e Integração. Disponível em: < http://gredes.ifto.edu.br/wp-content/uploads/Dissertacao-Mestrado-Jorge-Lima-Texto-completo.pdf > Acesso em 17 a 30 set. 2013.

[BHANDURE, 2013] Madhulika. Comparative Analysis of Mpls and Non -Mpls Network. Disponível em: < http://www.docstoc.com/docs/159648749/L347176 > Acesso em 1 a 12 out. 2013.

[ROUSE, 2007] Margaret. Virtual routing and forwarding (VRF). Disponível em: < http://searchenterprisewan.techtarget.com/definition/virtual-routing-and-forwarding > Acesso em 1 a 12 out. 2013.

[VALENTE, 2010] Daniel. Introdução a tecnologia VPLS (Virtual Private LAN Service). Disponível em: < http://blog.ccna.com.br/2010/11/01/introducao-a-tecnologia-vpls-virtual-private-lan-service/ > Acesso em 1 a 12 out. 2013.

[TAFT,2004] Bruno Prestes. MultiProtocol Label Switching. Disponível em: < http://www.gta.ufrj.br/grad/04_2/MPLS/ > Acesso em 1 a 12 out. 2013.

[FANTIN, 2013] Junovan. QoS (Qualidade de Serviço). Disponível em: < http://www.junovan.com.br/home/network/291-qos-qualidade-de-serviço > Acesso em 1 a 12 out. 2013.

[PUN,2001] Humbert. Convergence Behavior of RIP and OSPF Network Protocols 2001. Disponível em: < http://www2.ensc.sfu.ca/~ljilja/cnl/pdf/hubert.pdf > Acesso em 1 a 12 out. 2013.

[MALUF,2013] Thiago. Serviço fone@RNP. Disponível em: < http://pt.scribd.com/doc/123378983/148/IntServ-—-Integrated-Services#page=216 > Acesso em 1 a 12 out. 2013.

[JUNIPER, 2005] Juniper Networks. mpls_curso_jnpr_se021204. Disponível em: < http://www.wztech.com.br/cursos/mpls/ > Acesso em 17 a 30 set. 2013.

[GONDIM, 2011] Marcos. Redes MPLS Engenharia de Tráfego (TE). Disponível em: < http://pt.scribd.com/doc/51222645/7-TE-MPLS> Acesso em 17 a 30 set. 2013.