Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e

Pesquisas Computacionais

Rodrigo Fernandes da Costa Cardoso

APLICAÇÕES EM TEMPO REAL SOBRE REDES MPLS

Rio de Janeiro

2013

Rodrigo Fernandes da Costa Cardoso

APLICAÇÕES EM TEMPO REAL SOBRE REDES MPLS

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 Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

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

Rio de Janeiro

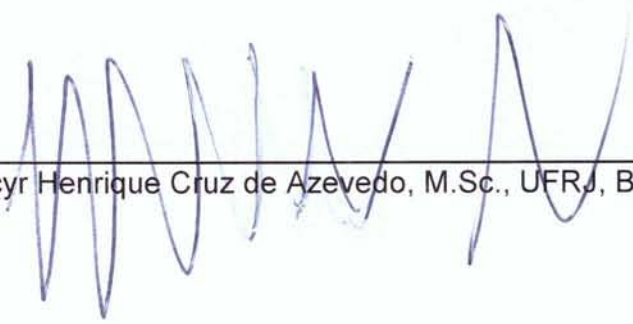
2013

Rodrigo Fernandes da Costa Cardoso

APLICAÇÕES EM TEMPO REAL SOBRE REDES MPLS

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 Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



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

Dedico esta monografia aos meus pais, minha avó, meu irmão e minha namorada que sempre me deram muito apoio nos momentos difíceis da minha vida, nunca mediram esforços para me ajudar, pela compreensão e por estarem sempre ao meu lado.

AGRADECIMENTOS

Agradeço a minha namorada Bruna pelo apoio, compreensão e incentivo que me foi dado para a conclusão desta especialização.

Aos meus pais, pelo apoio em mais esta etapa e objetivo de minha vida.

Ao professor Moacyr Henrique Cruz de Azevedo pela dedicação prestada na orientação deste trabalho.

A todos meus amigos e colegas que colaboraram direta ou indiretamente para a realização deste trabalho.

RESUMO

CARDOSO, Rodrigo Fernandes da Costa. **APLICAÇÕES EM TEMPO REAL SOBRE REDES MPLS**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

O objetivo central deste trabalho é apresentar as principais características de aplicações em tempo real (VoIP, Vídeo Conferência) trabalhando em conjunto com a tecnologia de rede MPLS (*Multiprotocol Label Switching*). Inicialmente serão apresentados alguns conceitos básicos e características dessas tecnologias, juntamente com os principais serviços disponibilizados em MPLS, como a criação de VPN (*Virtual Private Network*) e a implementação de QoS (*Quality of Service*). Por fim, serão mostrados alguns exemplos de configurações de MPLS em equipamentos Cisco.

ABSTRACT

CARDOSO, Rodrigo Fernandes da Costa. **APLICAÇÕES EM TEMPO REAL SOBRE REDES MPLS**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

The main objective of this essay is to do present the main features of real-time applications (VoIP, Video Conference) working with network technology MPLS (Multiprotocol Label Switching). First will be presented some basic concepts and features of these technologies with the main services available in MPLS as VPN (Virtual Private Network) implementation under a QoS (Quality of Service) facility. Finally will discuss MPLS technology configuration examples working on Cisco devices.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ATM	Asynchronous Transfer Mode
CBWFQ	Class Based Weighted Fair Queuing
CE	Customer Edge Router
CSR	Cell Switching Routers
DiffServ	Differentiated Services
DLCI	Data Link Connection Identifier
FEC	Forwarding Equivalency Class
FTN	FEC to NHLFE
IETF	Internet Engineering Task Force
ILM	Incoming Label Mapping
IntServ	Integrated Services
IP	Internet Protocol
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
LDP	Label Distribuition Protocol
LER	Label Edge Router
LIB	Label Information Base
LSP	Label Switch Path
LSR	Label Switch Router
MPLS	MultiProtocol Label Switching
NAS	Network Access Server
NHLFE	Next Hop Label Forwarding Entry
PE	Provider Edge Router
PPTP	Point-ti-Point Tunneling Protocol
QoS	Quality of Service
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TTL	Time To Live
VCI	Virtual Channel Identifier
VoIP	Voice over IP
VPDN	Virtual Private Dial Network
VPI	Virtual Path Identifier
VPN	Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

Em virtude do crescimento e popularização da Internet, do acesso à banda larga e dos avanços da tecnologia das máquinas micro processadas, aplicações em tempo real (ex.: VoIP (*Voice over IP*), Vídeo Conferência, *live streaming*) vêm se tornando cada vez mais usuais no contexto atual da comunicação em redes de computadores.

Na informática, aplicações em tempo real se referem a sistemas onde o tempo de operação é muito curto e a tarefa de processar grandes quantidades de dados, inclusive o tratamento simultâneo de sinais de áudio e vídeo, é muito extensa e deve ser executada de qualquer forma.

Com esse aumento progressivo das redes de computadores, tanto em número de usuários como na variedade de aplicações que utilizam, ficou clara a exigência de criar novas formas para atender todas as necessidades dos usuários, notadamente serviços baseados em protocolo IP (*Internet Protocol*) com largura de banda flexível. O MPLS (*Multiprotocol Label Switching*) surge como a principal tecnologia capaz de viabilizar múltiplos serviços de rede sobre uma infraestrutura compartilhada, permitindo o provisionamento rápido de serviços por ser facilmente escalonável, além de oferecer as potencialidades de engenharia de tráfego às redes baseadas em pacotes, criação de VPN's (*Virtual Private Network*) e garantia de QoS (*Quality of Service*) sobre IP, a qual é imprescindível para aplicações em tempo real que utilizam esse protocolo e apresentam algumas limitações em sua implementação por serem originalmente simples.

2 TECNOLOGIA MPLS

2.1 HISTÓRICO

Nas tradicionais redes sem conexão, como é o caso da Internet, cada pacote é tratado e encaminhado independentemente em cada roteador, no qual esse processo é baseado no endereço de destino carregado no cabeçalho do pacote.

Os roteadores IP, que são amplamente utilizados na Internet, possuem um algoritmo de roteamento que é ineficiente à medida que o tamanho da rede cresce, pois, para definir qual será o próximo salto do pacote, cada roteador tem que analisar mais informações do que realmente é necessário.

Entre 1995 e 1997 a Internet teve sua grande popularização e seus serviços e utilizações começaram a ser bastante diversificados. O ATM (*Asynchronous Transfer Mode*), que foi lançado para dominar o cenário mundial, começou a perder terreno em um âmbito geral, pois, além de ser caro, de difícil implementação e não ser facilmente escalonável, não era compatível com o protocolo IP.

Em resposta a essas dificuldades, diversos fabricantes de equipamentos e centros de pesquisas viram a necessidade de criar uma tecnologia que não fosse simplesmente usada para conexão a sistemas finais, e sim uma rede de trânsito que transportasse pacotes entre pontos de entrada e saída e, principalmente, fosse compatível com IP.

A empresa Ipslon Networks iniciou um projeto chamado *IP Switching* onde o objetivo era conectar subredes IP através de nuvens ATM. O problema deste projeto era que, apesar de estar completamente ligado à tecnologia ATM, todo controle e sinalização eram revogados e os comutadores eram usados apenas para encaminhamento dos pacotes.

No mesmo período, o Instituto de Tecnologia de Tóquio desenvolveu uma tecnologia, que depois foi melhorada pela Toshiba, muito similar ao *IP Switching,* chamado CSR (*Cell Switching Routers*). A diferença era que o *IP Switching* só era capaz de rotear pacotes IP e o CSR podia rotear pacotes de protocolos que não fossem IP.

Diante dessa corrida pela criação de novas arquiteturas, a Cisco desenvolveu uma tecnologia que pretendia ser totalmente transparente em uma rede heterogênea e que já apresentava a maior parte das características da atual tecnologia MPLS, chamada *Tag Switching*. Seu funcionamento era similar ao do MPLS de forma que quando um pacote entrava em uma nuvem *Tag Switching*, ele era etiquetado (*Tag*). Essa etiqueta é conceitualmente igual ao rótulo do MPLS e muito similar aos campos VPI / VCI de um cabeçalho ATM. Sua diferença é meramente por questões de direitos autorais.

Tanto a Ipslon quanto a Cisco iniciaram esforços pela padronização de suas respectivas arquiteturas, porém sem sucesso. Em contrapartida a IETF (*Internet Engineering Task Force*) criou um grupo de trabalho o qual padronizou o MPLS através da combinação destas tecnologias, o que permitiu que roteadores de núcleo, distribuição e acesso comutassem pacotes de forma mais rápida e simples.

2.2 CARACTERÍSTICA

O MPLS é um protocolo de roteamento baseado em pacotes rotulados, onde cada rótulo representa um índice na tabela de roteamento do próximo roteador e os pacotes são encaminhados com base nesses rótulos para o caminho mais adequado. Pacotes com o mesmo rótulo e mesma classe de serviço são indistinguíveis entre si e por isso recebem o mesmo tipo de tratamento. Esse

processo traz o benefício de simplificar o encaminhamento dos pacotes e permitir escalabilidade para taxas de comunicação elevadas sem o roteamento e o encaminhamento nó-a-nó. Encaminhar pacotes com base em rótulos em vez de roteá-los com base nos cabeçalhos traz inúmeras e significativas vantagens, pois os pacotes são processados mais rapidamente fazendo o tempo gasto ser muito menor, pode-se atribuir prioridade aos rótulos e o principal de todos: traz a sofisticação do protocolo orientado à conexão para o mundo IP sem conexão.

Ele é chamado de multiprotocolo, pois pode ser usado com qualquer protocolo da camada 3 (camada de rede).

Os principais pontos fortes do MPLS que faz com que seja bastante utilizado são a engenharia de tráfego, serviço de QoS e criação de VPN's. Com a implementação de QoS, os diversos tipos de tráfegos podem ser diferenciados de forma distinta, dando prioridade às aplicações mais sensíveis, como é o caso das aplicações de tempo real, tornando a rede escalonável.

Resumindo: o MPLS proporciona melhor desempenho e capacidade de criação de serviços para a rede.

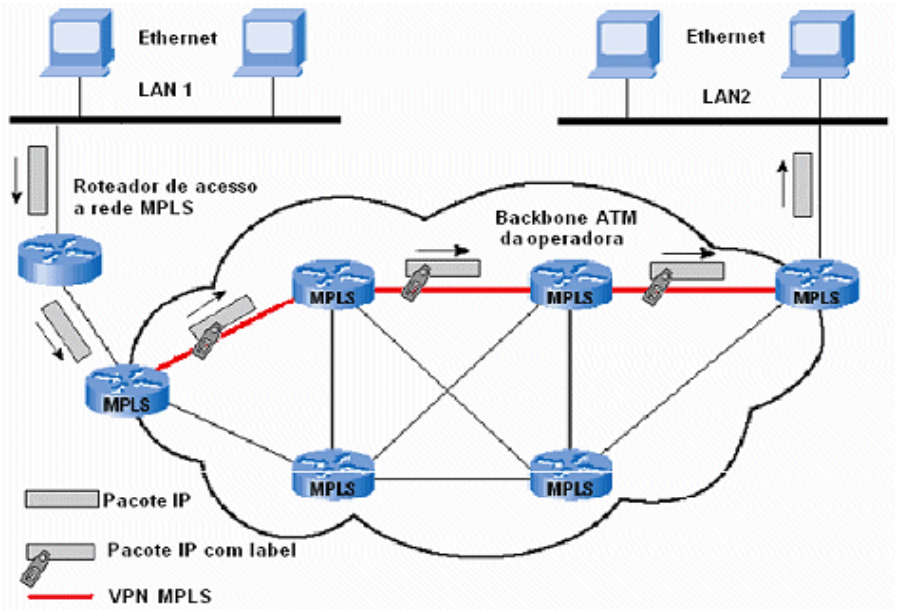


Figura 1 – Rede MPLS

2.3 FUNCIONAMENTO

O MPLS propõe um método para gerar uma estrutura de comutação sob qualquer rede de datagrama criando circuitos virtuais a partir das rotas organizadas pelos protocolos de roteamento da camada de rede. A informação é processada e dividida em classes de serviço e os dados são encaminhados através de rotas estabelecidas por essas classes, sendo feita apenas a comutação e preservando o nível de enlace.

Quando um pacote é enviado e entra na nuvem MPLS, recebe um rótulo (*label*) do roteador de borda (LER – *Label Edge Router*) e é associado a uma classe de encaminhamento (FEC – *Forwarding Equivalency Class*). O rótulo serve como uma representação curta para o cabeçalho IP, reduzindo a complexidade do processamento em todos os nós. Os pacotes são encaminhados por um caminho comutado por rótulos, denominado LSP (*Label Switch Path*) formado por roteadores de comutação de rótulos, chamado LSR (*Label Switch Router*). Cada LSR toma decisões de encaminhamento baseado apenas no rótulo do pacote. Em cada salto, o LSR retira o rótulo existente, utiliza-o como índice na tabela de roteamento residente, também chamada de NHLFE (*Next Hop Label Forwarding Entry*), verifica o rótulo de saída e aplica um novo que informará ao próximo roteador como encaminhar o pacote. Essas tabelas de roteamento podem ser implementadas em nível de nó (uma única tabela por nó) ou em nível de interface (uma tabela por interface). O mais importante é que apenas um único algoritmo de encaminhamento é necessário para todos os tipos de comutação e por isso pode ser implementado em hardware para maior velocidade.

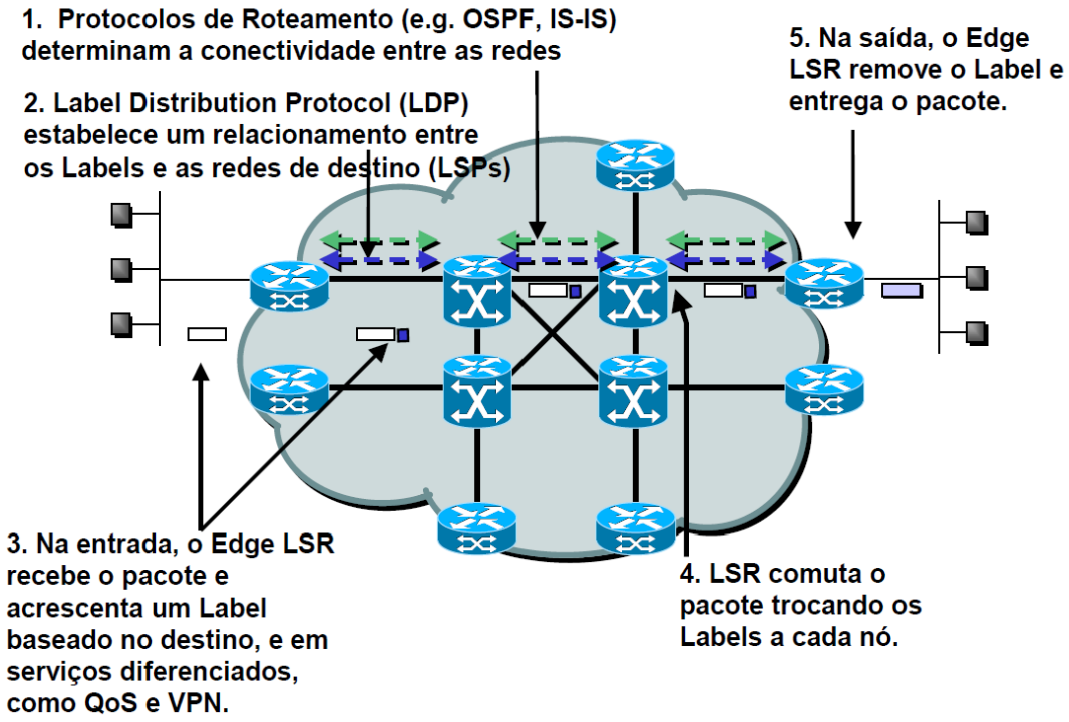


Figura 2 – Funcionamento da rede MPLS

2.4 CONCEITOS

Nesta seção serão apresentados alguns conceitos do MPLS.

2.4.1 Label (Rótulo)

O rótulo (*Label*) é um identificador relativamente curto e de comprimento fixo, definido em 32 bits, usado no processo de encaminhamento dos pacotes e associado a uma FEC para identificá-la, normalmente com significado local conforme figura 3.

Deve ser posicionado depois de qualquer cabeçalho de camada 2 e antes de um cabeçalho de camada 3 e é conhecido como *Shim Header* como pode ser visto na figura 4.

Os rótulos são análogos ao DLCI usado em redes Frame Relay ou o VPI/VCI usado em ambientes ATM. 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 o roteador faria.

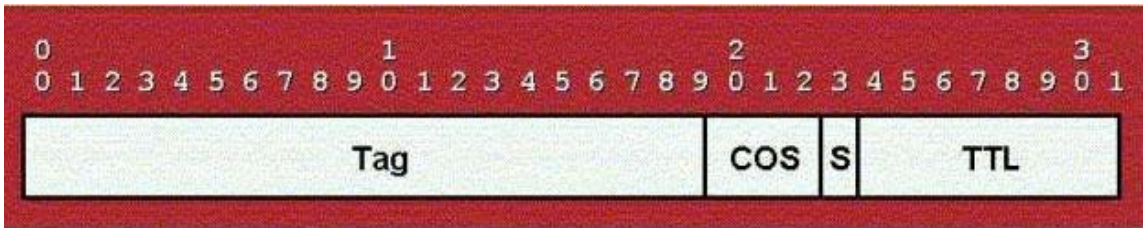


Figura 3 – Formato do rótulo MPLS

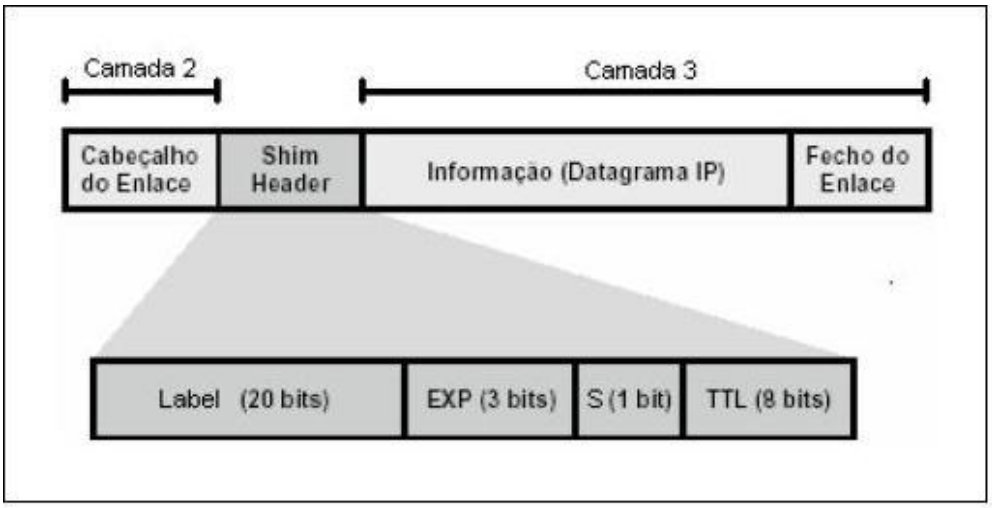


Figura 4 – Pacote em rede MPLS

Onde:

- Campo *Label*/***Tag*** (20 bits) carrega o valor atual do rótulo MPLS;
- Campo *EXP*/***COS*** (3 bits) define a classe de serviço a que um pacote pertence, indicando assim a prioridade. Pode afetar o enfileiramento e algoritmos de descarte aplicados ao pacote enquanto ele é transmitido;
- Campo *Stack*/**S** (1 bit) suporta o enfileiramento de rótulos. Será utilizado quando receber mais de um rótulo;
- Campo TTL (*Time To Live*)(8 bits) tem o mesmo papel que no IP convencional: especificar um limite de quantos roteadores o pacote pode

atravessar num total de 255. Quando chegar a esse limite, o pacote é descartado para evitar loops.

2.4.2 LER (*Label Edge Router*)

O LER é um roteador que fica na borda da rede que, além das funções de encaminhamento e controle, é responsável pela inserção do rótulo ao pacote e atribuí-lo a uma FEC. Este processo de ligação de pacotes a uma FEC pode ser tão complexo quanto necessário sem afetar o desempenho geral da arquitetura, pois é efetuado somente na admissão do pacote. Quando um LER está na saída do domínio MPLS é responsável pela retirada do rótulo, mantendo a semântica normal de um pacote IP a fim de ser entregue a uma rede não MPLS. Também deve poder se conectar com redes de diferentes tipos já que faz fronteira entre o domínio MPLS e as demais.

LER é uma definição à parte do padrão MPLS pois foi criado para facilitar a visão do domínio. É na verdade um LSR que tem a capacidade de fazer fronteira com outras redes como Ethernet, Frame Relay, ATM e etc.

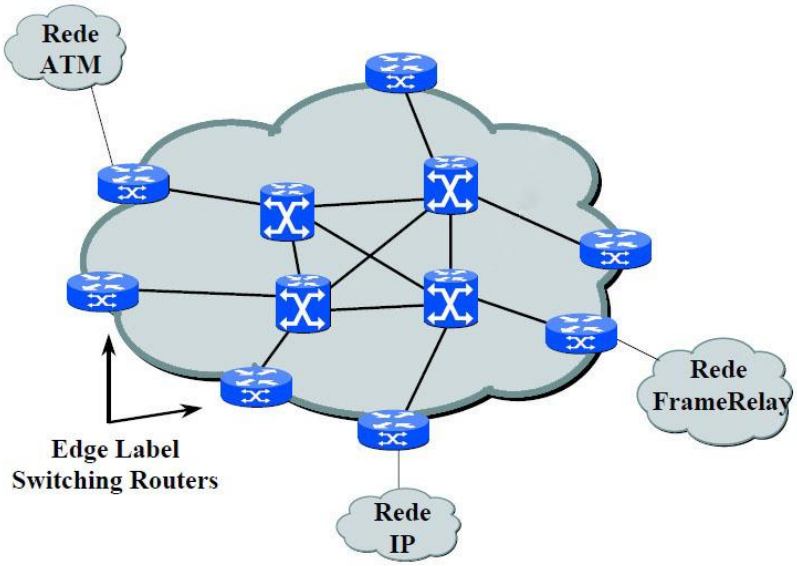


Figura 5 - Label Edge Router

2.4.3 FEC (*Forwarding Equivalency Class*)

Uma FEC consiste em um conjunto de parâmetros que irão determinar o mesmo caminho e mesmo modo de encaminhamento para os pacotes. É representada por um rótulo e cada LSP é associado a uma FEC. Pacotes de um mesmo fluxo de dados geralmente pertencem à mesma FEC. Requisitos de QoS também podem ser definidos com a designação de FEC. A associação do pacote a uma FEC acontece apenas uma vez: quando ele entra na rede MPLS. Isso proporciona grande flexibilidade e escalabilidade a este tipo de rede. A FEC pode ser determinada por um ou mais parâmetros, especificados pelo gerente de rede. Alguns desses parâmetros são:

- Endereço IP da fonte ou destino ou endereço IP da rede;
- Número da porta da fonte ou destino;
- ID do protocolo IP;
- QoS.

2.4.4 LSP (*Label Switched Path*)

O LSP consiste em um caminho através de uma sequência ordenada de LSR's, estabelecido entre uma origem e um destino no qual transitarão pacotes de mesma classe e que compartilham o mesmo destino. Ele é unidirecional, portanto é preciso ter dois LSP's para uma comunicação entre duas entidades: um para envio outro para retorno do tráfego. A rota deve ser estabelecida antes da transmissão dos dados por protocolos de roteamento convencionais ou com restrições. Após estabelecido o caminho fica definido e os pacotes pertencentes a ele não precisam mais ser roteados. Eles serão apenas comutados com base nos seus rótulos. Estes

rótulos são distribuídos entre LSR's no momento do estabelecimento de LSP's conforme mostrado na figura 6.

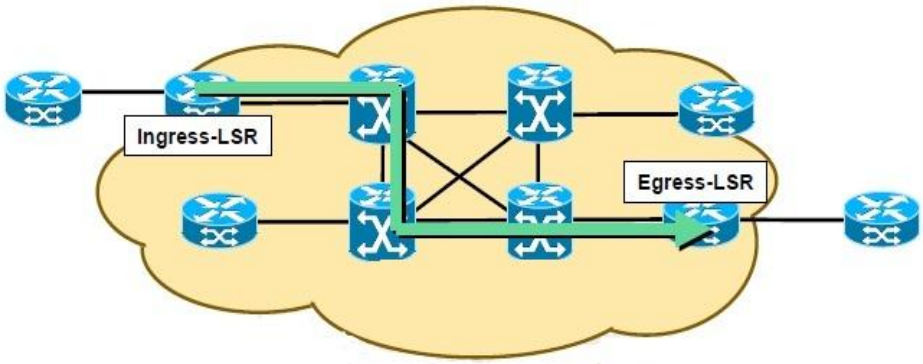


Figura 6 – Label Switched Path

2.4.5 LSR (*Label Switching Router*)

Os LSR's são os equipamentos de comutação com funcionalidades implementadas para MPLS que ficam no núcleo da rede e que executam os algoritmos de encaminhamento e mantêm as tabelas de encaminhamento atualizadas. Sua função é encaminhar os pacotes baseados apenas no rótulo de cada pacote. Ao receber um pacote cada LSR troca o rótulo existente por outro, passando-o para o próximo LSR até chegar no roteador de borda de saída.

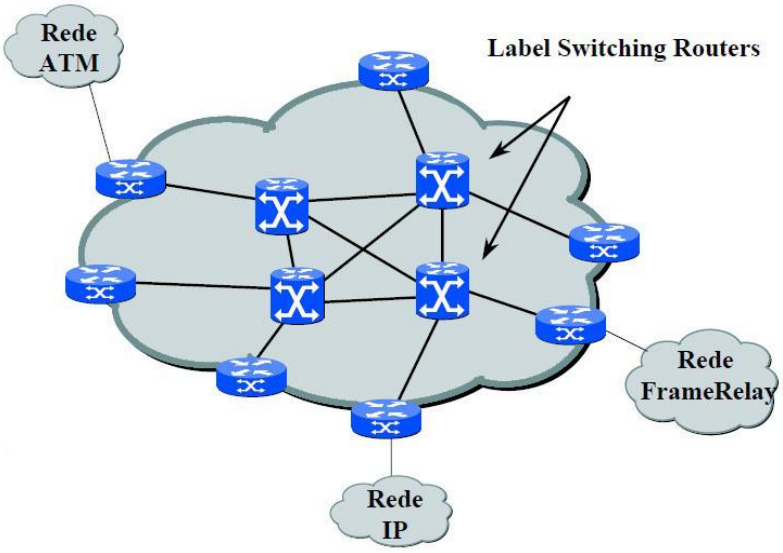


Figura 7 - Label Switching Router

2.4.6 NHLFE (*Next Hop Label Forwarding Entry*)

A NHLFE (registro de encaminhamento por rótulos para o próximo passo) é a tabela mais importante do MPLS e está presente em todos os roteadores. Ela consiste no conjunto de ações que os pacotes irão receber pelo roteador e segue, na grande maioria, o seguinte formato: [Ação sobre o Rótulo] x [Ação de Encaminhamento]. As ações sobre o rótulo podem ser: Remover, Inserir ou Trocar. A ação de encaminhamento indica qual o próximo salto.

Esta entrada, conforme exemplificada na Tabela 1, contém todas as informações que devem ser aplicadas à pilha de rótulos de um pacote e é usada juntamente com a ILM (*Incoming Label Mapping*) e FTN (FEC to NHLFE).

Tabela 1 – NHLFE

NHLFE	***Próxima interface***	***Ação***
1	1	Empilhar rótulo #5
2	2	Trocar rótulo do topo por #14
3	3	Trocar rótulo do topo da pilha por #16 + empilhar rótulo #62
4	8	Remover a pilha

O ILM é uma estrutura usada para interpretar rótulos de entrada e é implementada somente nos roteadores do núcleo, ou seja, é utilizado somente para os pacotes já rotulados. Ele faz o mapeamento de cada rótulo que entra no domínio em conjunto com o NHLFE conforme indicado na Tabela 2.

Tabela 2 - ILM

Rótulo de Entrada	***NHLFE***
123	1
130	3
320	4
402	2

Já o FTN é implementado somente nos roteadores de borda, ou seja, ele é utilizado apenas para pacotes não rotulados. Faz o mapeamento do FEC também em conjunto com o NHLFE como pode ser observado na Tabela 3.

Tabela 3 – FTN

FEC	***NHLFE***
64.13.10	1
64.13.20	4
64.12	2
64.10	3

2.4.7 Pilha de Rótulos (*Label Stack*)

O mecanismo de pilha de rótulos permite realizar uma operação hierárquica no domínio MPLS através da inclusão de mais de um rótulo em um pacote. Este empilhamento permite que os LSR's do núcleo da rede troquem informações entre si e ajam como nós de borda. Estes novos roteadores de "borda" definem um novo

domínio MPLS e os outros LSR's, que são nós internos ao domínio, não se preocupam com rotas inter-domínio nem com os rótulos associados a essas rotas.

Dentro de uma grande rede pode-se ter vários domínios. Para cada um tem-se um nível de rótulo associado. Esta técnica permite uma diminuição das tabelas de roteamento dos roteadores de entrada da rede MPLS.

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 os outros rótulos que podem haver abaixo deste.

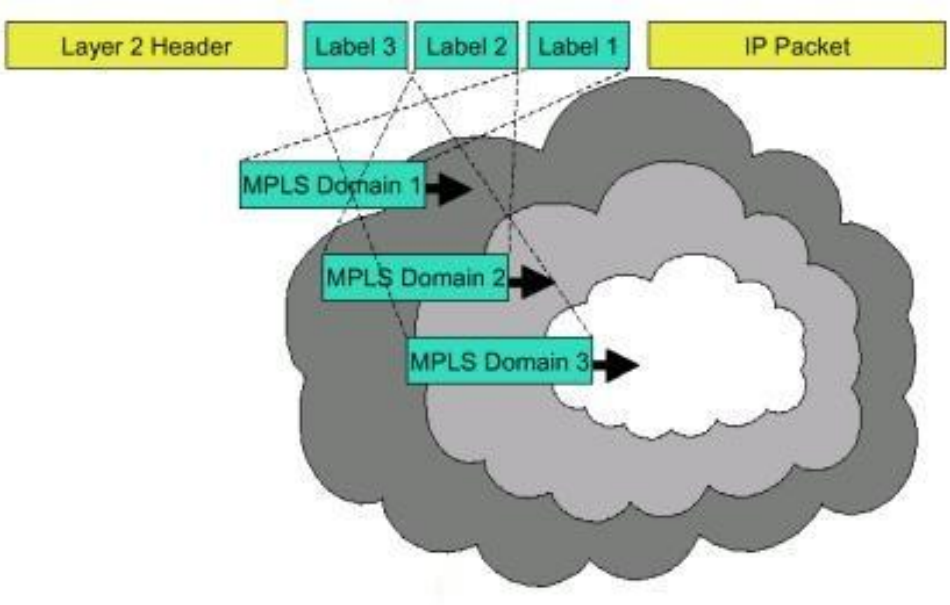


Figura 8 – Pilha de rótulos

2.4.8 LDP (*Label Distribuition Protocol*)

O LDP (Protocolo de Distribuição de Rótulo) é um protocolo cuja principal função é distribuir rótulos entre os LSR's permitindo assim a criação de LSP's. Para que isso ocorra o LDP oferece um mecanismo que permite que quando um LSR distribui rótulos, ele deixe que seus pares saibam desse rótulo, do seu significado,

concordem como o tráfego deve ser encaminhado e estabeleçam uma comunicação. O LDP possui as seguintes características básicas:

- Oferece mecanismo de descoberta de LSR para permitir os roteadores encontrem uns aos outros e estabeleçam comunicação;
- Define quatro classes de mensagens: *Discovery*, *Label Advertisement*, *Adjacency* e *Notification*;
- Roda sobre TCP para proporcionar fidelidade e garantia de entrega das mensagens.

2.4.9 LIB (*Label Information Base*)

É a tabela onde são armazenados os diversos vínculos de rótulos que um LSR recebe sobre o protocolo LDP.

3 QUALIDADE DE SERVIÇO (QoS)

Qualidade de serviço (QoS - *Quality of Service*), numa rede de comunicação de dados, é um conceito que exprime a capacidade de priorizar um determinado tipo de tráfego considerado mais importante sobre um tráfego considerado menos importante, além de garantir a entrega dos dados. Para que possa existir essa garantia, todos os pacotes de dados pertencentes a uma mesma sessão devem seguir o mesmo caminho (como em um tráfego orientado à conexão) e devem existir meios de garantir a reserva de recursos ao longo deste caminho.

O QoS tem como objetivo tratar o tráfego para otimizar o uso da rede de forma que aplicações mais sensíveis, como é o caso da voz e vídeo, tenham uma atenção especial.

Nas redes tradicionais IP não existe qualquer reserva de largura de banda porque a capacidade que estiver disponível será utilizada, o que pode ocasionar eventual insuficiência de banda para uma aplicação importante, como é o caso das aplicações em tempo real. Isso poderá causar a retenção dos pacotes por um tempo indeterminado nos buffers gerando atrasos elevados e até mesmo o descarte caso não haja mais espaço disponível no roteador.

Para tentar resolver este problema, o IETF desenvolveu dois mecanismos para implementação de QoS em redes IP: *Integrated Services (IntServ*) e *Differentiated Services (DiffServ*).

O *IntServ*, ou Serviços Integrados, é um modelo de implementação de QoS desenvolvido para garantir a qualidade do serviço para fluxos individuais de tráfego utilizando a sinalização fim-a-fim e a reserva de recursos de toda a rede, ou seja, dos roteadores intermediários até o roteador de destino.

O *DiffServ*, ou Serviços Diferenciados, é um modelo de implementação que trabalha com os fluxos de dados de forma completamente diferente do IntServ. Não é feita nenhuma reserva individual de recurso nos roteadores, mas uma negociação para os pacotes da rede simplificando o processamento dos roteadores de núcleo.

Algumas das situações onde deve ser implementado o QoS:

- Aplicações sensíveis à latência, atraso (*delay*) ou diferença entre atrasos (*jitter*) sendo trafegadas na rede;
- Redes com congestionamento nos horários de pico;
- Priorizar um tipo de tráfego sobre outros.

3.1 INTSERV (*INTEGRATED SERVICES*)

O modelo de serviços integrados (*IntServ*) é caracterizado pela reserva de recursos de toda a rede a fim de garantir a qualidade de serviço. Antes de iniciar uma comunicação, o emissor solicita ao receptor por meio de trocas de mensagens de controle, através do protocolo RSVP (Resource Reservation Protocol), a alocação dos recursos necessários para definir uma boa qualidade na transmissão dos dados. Alocação de recursos refere-se à largura de banda e ao tempo em que será mantida a conexão. Neste período o emissor tem uma faixa de largura de banda disponível para transmitir seus dados.

O *IntServ* é caracterizado pela alocação de recursos para dois novos tipos de serviços: os serviços garantidos para aplicações que necessitam de um atraso constante, e os serviços de carga controlada para aplicações que necessitam de segurança e destacam o serviço de melhor esforço.

Durante a transmissão dos pacotes são feitas classificações nos roteadores para cada fluxo, colocando-os em filas específicas para a aplicação. Como o

controle é feito basicamente nos roteadores, o grau de complexidade aumenta pois exige grande capacidade de processamento, armazenamento e bons algoritmos para tratamento de filas.

3.2 RSVP (*RESOURCE RESERVATION PROTOCOL*)

O RSVP (Protocolo de Reserva de Recursos) é um protocolo de sinalização usado por emissores, receptores e roteadores para reservar recursos na rede e para manter a informação de estado associada. Ele funciona no topo do protocolo IP e foi proposto em 1993 e adotado como protocolo padrão na arquitetura de Serviços Integrados (*IntServ*). Também é usado, com extensões, na tecnologia MPLS para distribuição de rótulos associados a LSP's e para estabelecer rotas explícitas.

O RSVP permite a reserva de recursos em cada nó da rede, mas não realiza funções de encaminhamento, controle de admissão ou escalonamento de pacotes implementados por outros componentes da arquitetura.

3.3 DIFFSERV (*DIFFERENTIATED SERVICES*)

O modelo de serviços diferenciados (DiffServ) implementa qualidade de serviço com base na definição de tipo de serviço. Ele parte do princípio que domínios adjacentes tenham um acordo sobre os serviços que serão disponibilizados entre os mesmos. Este acordo é chamado SLA (*Service Level Agreement* – Acordo de Nível de Serviço). Um SLA determina as classes de serviços suportadas e a quantidade de tráfego na banda entre os domínios. Os domínios podem definir um SLA estático ou dinâmico, sendo que, no dinâmico um protocolo de sinalização e controle será necessário para o gerenciamento da banda.

O *DiffServ* apresenta dois novos tipos de serviços especiais: serviços assegurados, que são utilizados por clientes que precisam de segurança em seus provedores no momento que ocorre congestionamentos, e serviços Premium, para aplicações que necessitam de baixo atraso e baixa variação de atraso (*jitter*).

Os serviços diferenciados têm sido o modelo mais utilizado para implementação de QoS pois exigem menos complexidade no processamento dos roteadores de núcleo, não necessitam de sinalização entre os roteadores da rede, necessitam pouca atualização de software para prover bons métodos de Classificação, Policiamento (*Policing*), Marcação de pacotes, Mecanismo de filas (*Queuing*), Descarte (*Dropping*) e Moldagem de tráfego (*Shaping*).

3.3.1 Classificação

O método de classificação separa os pacotes que entram na rede em diversas classes de serviços. Cada classe recebe posteriormente um tratamento diferenciado na rede e pode ser definida como o conjunto de regras que define o tráfego de cada classe. Por padrão, os pacotes são classificados de acordo com as portas TCP dos aplicativos.

3.3.2 Policiamento (*Policing*)

De acordo com o perfil contratado pelo cliente, o *backbone* da operadora pode realizar um policiamento de entrada. Assim o tráfego excedente de uma classe pode ser descartado ou transmitido em uma classe de menor prioridade.

3.3.3 Marcação de Pacotes

No modelo *DIffServ* cada nó realiza a classificação do tráfego para que ele receba o tratamento diferenciado. A classificação feita no cliente segue parâmetros internos como porta de acesso, IP de origem, porta TCP, dentre outros.

3.3.4 Mecanismo de Filas (*Queuing*)

O mecanismo de filas permite que cada classe de tráfego utilize filas diferentes no roteador. Com isso pode-se dividir a banda e os buffers de saída entre as classes.

Nos roteadores Cisco o mecanismo de fila padrão utilizado é o CBWFQ (*Class Based Weighted Fair Queuing*). Com o CBWFQ são formadas várias filas para diferentes classes de tráfego. A banda total da interface é dividida entre as diversas filas. Desta forma os pacotes de uma fila são encaminhados para a saída proporcional à cota de banda que possuem. A banda de uma classe pode ficar disponível para as outras classes quando não estiver sendo usada. A banda disponível para o CBWFQ corresponde a 75% da banda total da interface, sendo 25% reservados para a comutação de melhor esforço (classe de dados de baixa prioridade) e para tráfego de controle.

3.3.5 Descarte (*Dropping*)

Em casos de congestionamento, inevitavelmente ocorrem descartes de pacotes. Existem mecanismos de descarte que cumprem, basicamente, dois objetivos: evitar o congestionamento dos buffers e gerenciar estes buffers na situação de congestionamento.

3.3.6 Moldagem de Tráfego (*Shaping*)

Moldagem de tráfego é a ação do roteador de adequar o tráfego ao perfil contratado. Ele se caracteriza por buffers de saída que armazenam picos ou rajadas de tráfego e transmitem dentro dos limites configurados.

A ação de moldagem é diferente do policiamento, pois é aplicada na saída e é preventiva enquanto o policiamento é na entrada e restritiva.

4 VIRTUAL PRIVATE NETWORK (VPN)

Com o crescimento da economia, muitas empresas estão criando instalações secundárias, como filiais, espalhadas por todo o país ou até mesmo pelo mundo. Com essa situação elas precisam de uma maneira para manter uma comunicação rápida, segura e confiável onde quer que os seus escritórios estejam.

À medida que a Internet cresceu e se tornou mais popular, os escritórios se voltaram para ela como forma de ampliar suas próprias redes corporativas usando a estrutura já existente. O grande desafio estava em garantir a segurança dos dados transmitidos, uma vez que a Internet não prima pela segurança. A garantia deveria ser principalmente que os dados não fossem modificados durante a transmissão, que as partes envolvidas (origem e destino) fossem identificadas corretamente e mantivessem o sigilo, isto é, não permitir que pessoas não autorizadas visualizassem o conteúdo da mensagem.

A VPN surgiu com o propósito de possibilitar um acesso privado de comunicação utilizando redes públicas já existentes como a Internet, de forma que garantisse a integridade, autenticidade, confidencialidade e controle de acesso, reduzindo o risco de ataques externos. Basicamente, uma VPN é uma rede privada que usa a Internet para conectar sites remotos ou usuários ao invés de usar uma conexão física, como uma linha dedicada, criando conexões virtuais direcionadas via Internet ligando a rede privada corporativa a outro escritório ou a um funcionário que trabalha à distância.

A VPN possui seus próprios protocolos de comunicação, dentre eles PPTP, L2TP e IPSec que atuam em conjunto com o TCP/IP para criar o túnel virtual onde os dados trafegarão criptografados, garantindo a elegibilidade a pessoas não autorizadas. Os protocolos de autenticação são usados para garantir que as

mensagens tenham vindo de usuários válidos e que, se parte da mensagem for alterada, o pacote será descartado.

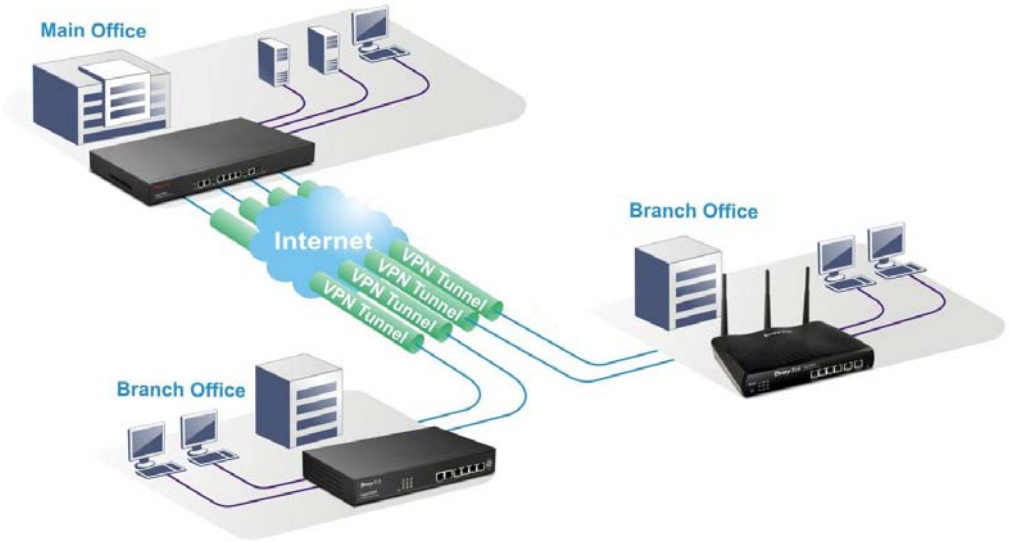


Figura 9 – Virtual Private Network

Algumas implementações de VPN utilizam software cliente nos computadores que se conectam à rede corporativa através da Internet. Essas implementações são chamadas VPDN (*Virtual Private Dial Network*). Essa opção é muito usada por clientes móveis. Outras implementações utilizam criptografia entre *gateways* VPN, não sendo necessária intervenção do usuário.

Independentemente da forma de VPN que é utilizada pelas empresas e clientes, os seguintes conceitos básicos de segurança devem ser cumpridos:

- Confidencialidade – Limita o acesso às informações para somente pessoas autorizadas;
- Integridade – Assegura que os dados não serão alterados;
- Disponibilidade – Garante que a informação estará sempre disponível para uso, de forma contínua e ininterrupta;

- Autenticidade – Verifica se a pessoa com quem está trocando informações é realmente quem diz ser;
- Irrevogabilidade – Evita o repúdio, a negativa de transações legítimas.

4.1 TUNELAMENTO

A VPN é uma rede privada virtual onde os links dedicados existentes em uma rede privada convencional são simulados por um túnel, através da técnica de tunelamento. Essa técnica é definida pelo processo do encapsulamento de um protocolo dentro de outro. O uso do tunelamento na VPN incorpora um novo componente importante: a criptografia.

Antes de o pacote ser encapsulado ele é criptografado de forma a ficar ilegível caso seja interceptado durante o transporte. O pacote criptografado é encapsulado e enviado até o destino onde será desencapsulado e decriptografado, retornando ao formato original.

O protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém informações de roteamento que permitem a chegada até o destino. Túnel é a denominação do caminho lógico percorrido pelo pacote ao longo da rede até o destino.

O tunelamento pode ser dividido de 2 formas: compulsório ou voluntário.

- Tunelamento Voluntário – utilizado quando uma estação de trabalho ou um servidor utiliza um software cliente de tunelamento para criar uma conexão até o servidor VPN. Esse método é utilizado por clientes *dial-up* que primeiro conectam-se à Internet para depois criar o túnel utilizando o software, com isso o fim do túnel passa a ser o cliente.

- Tunelamento Compulsório – utilizado quando existe um NAS (Servidor de Autenticação de Rede). Ele é responsável pela configuração e autenticação de forma que não é necessário que os clientes possuam nenhum software de tunelamento instalado. Nesse tipo o final do túnel é o servidor NAS.

Um ponto importante que deve ser observado é que na estrutura de redes privadas convencionais as conexões são mantidas por links permanentes entre dois pontos da rede. Já nas redes virtuais privadas as conexões são dinâmicas, pois elas são criadas no momento em que se tornam necessárias e são desativadas quando não são mais necessárias, fazendo com que a banda esteja disponível para outros usuários.

4.2 TIPOS DE VPN

Existem vários tipos de implementações de VPN. Cada uma tem suas especificações próprias, assim como características que devem ter uma atenção especial na hora de implementar.

Entre os tipos de VPN, destacam-se três principais: Intranet VPN, Extranet VPN e Acesso Remoto VPN.

4.2.1 Intranet VPN

Uma Intranet VPN é um tipo de VPN utilizada para conectar sites que geralmente possuem uma infraestrutura completa de rede local, podendo, ou não, ter seus próprios servidores e aplicativos locais, que necessitam compartilhar recursos. Esse tipo de VPN é facilmente utilizado entre departamentos de uma empresa onde alguns requisitos básicos, como necessidade de criptografia rápida

para não sobrecarregar a rede, confiabilidade e facilidade no gerenciamento, são necessários.

A Intranet pode ser entendida como um conjunto de redes locais de uma corporação geograficamente separadas e interconectadas através de uma rede pública de comunicação, como a Internet. Esse tipo de conexão também pode ser chamado de *Lan-to-Lan* ou *Site-to-Site*.

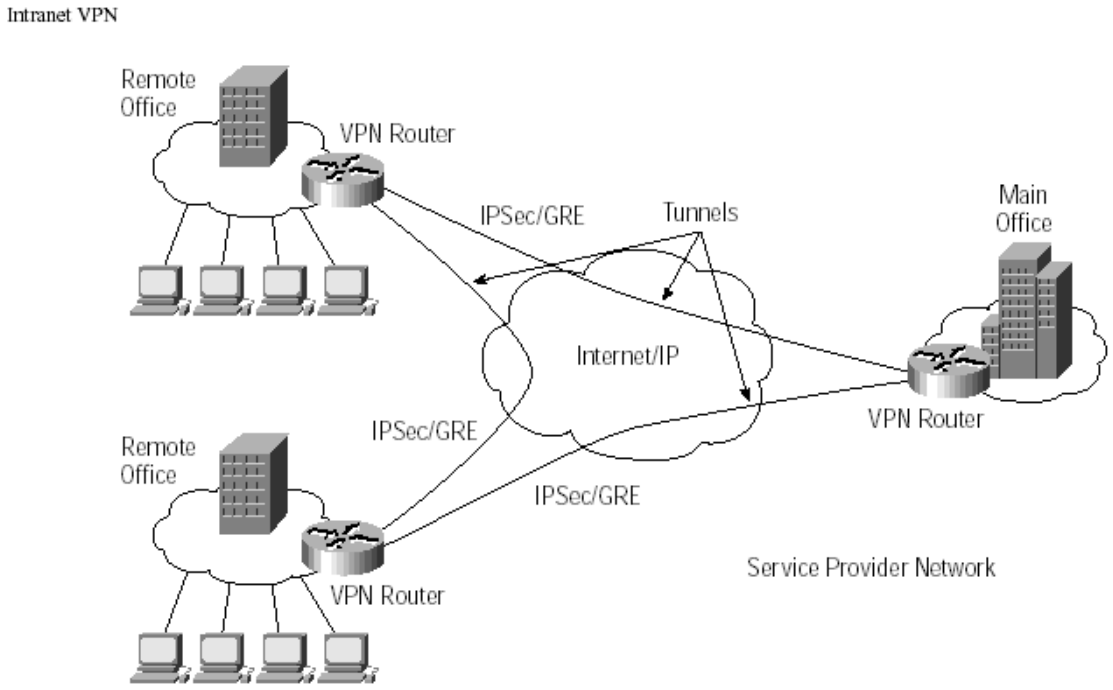


Figura 10 – Intranet VPN

4.2.2 Extranet VPN

Uma Extranet VPN é um tipo de VPN utilizada para disponibilizar acesso da empresa para seus parceiros, clientes e fornecedores. Nesse tipo de VPN é necessário que haja um controle de tráfego para minimizar os efeitos dos gargalos e uma solução grátis de VPN que garanta a interoperabilidade com as outras soluções das empresas envolvidas.

Esse tipo de conexão também pode ser chamado de *Lan-to-Lan* ou *Site-to-Site,* assim como na Intranet VPN.

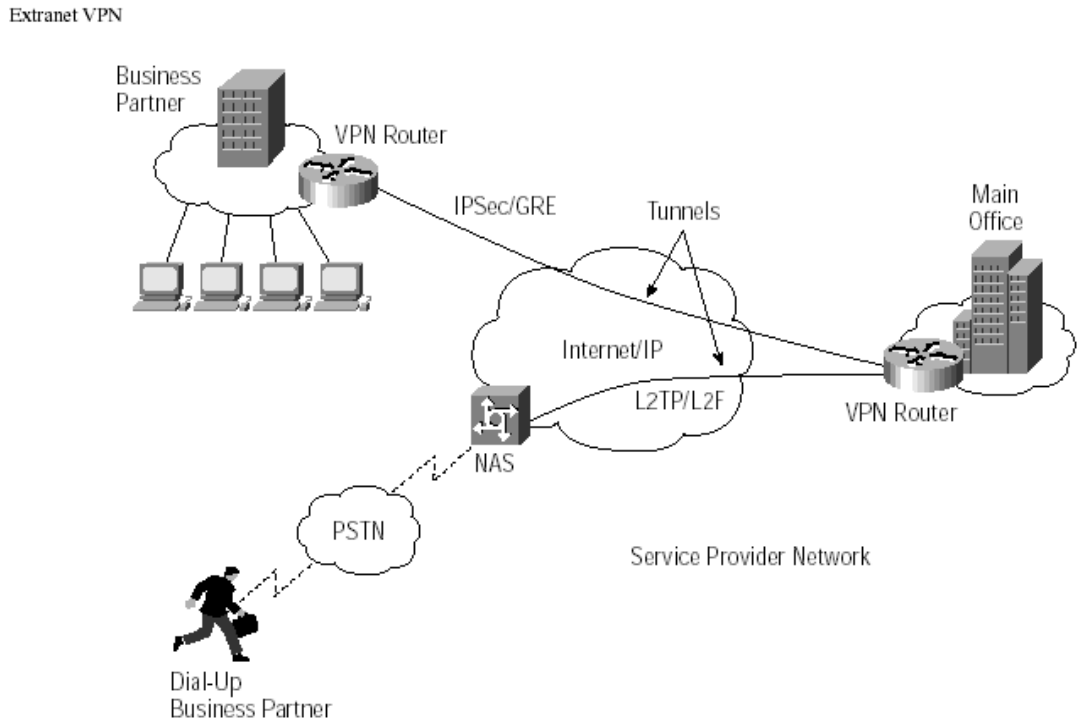


Figura 11 – Extranet VPN

4.2.3 Acesso Remoto VPN

Esse tipo de VPN é utilizado por usuários que estejam utilizando computadores móveis para conexão à rede corporativa. Neste caso é necessário um software cliente de acesso remoto.

Para utilizar o acesso remoto o mais importante que deve ser levado em consideração é o tratamento de QoS, pois o acesso é limitado à velocidade do modem. Também deve ser levado em consideração a autenticação que deve ser rápida e eficiente e o gerenciamento centralizado da rede, já que ao mesmo tempo pode-se ter vários usuários remotos logados.

Este tipo de conexão também pode ser chamado de *Point-to-Site* e está se tornando cada vez mais utilizada.

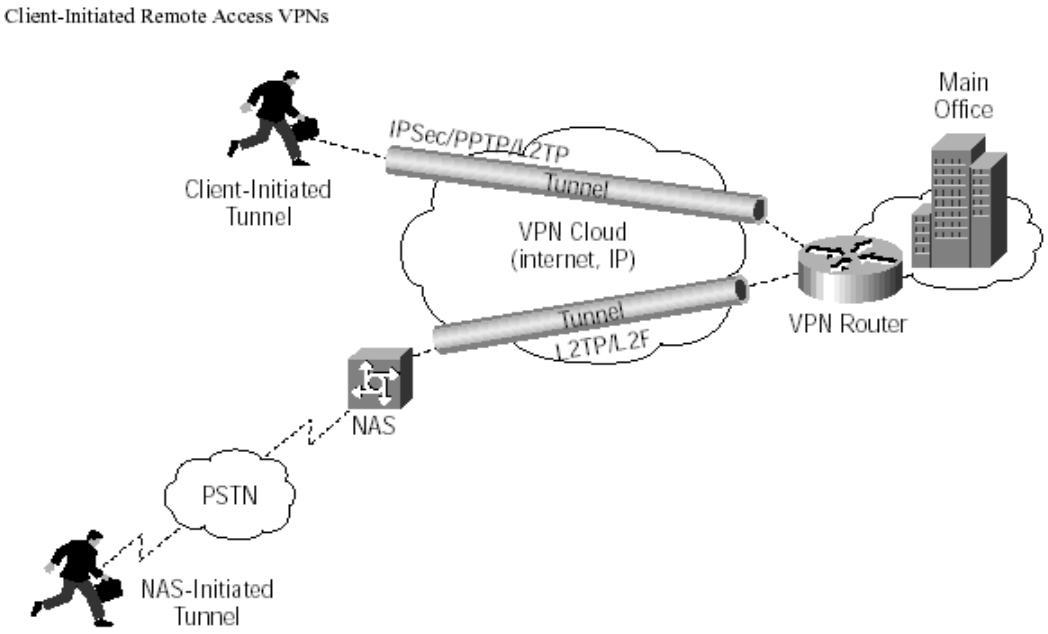


Figura 12 – Acesso Remoto VPN

4.3 TÉCNICAS DE IMPLEMENTAÇÃO

Dependendo da técnica utilizada na implementação da VPN, a privacidade das informações poderá ser garantida apenas para os dados ou para todo o pacote (cabeçalho e dados). Quatro técnicas podem ser usadas: Modo Transmissão, Modo Transporte, Modo Túnel Criptografado e Modo Túnel não Criptografado.

4.3.1 Modo Transmissão

Somente os dados são criptografados não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes.

4.3.2 Modo Transporte

Somente os dados são criptografados podendo haver mudança no tamanho dos pacotes. É uma solução de segurança adequada para implementações onde os dados trafegam somente entre dois nós da comunicação.

4.3.3 Modo Túnel Criptografado

Tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos com um novo endereçamento IP em um túnel estabelecido entre os pontos de origem e de destino.

4.3.4 Modo Túnel não Criptografado

Tanto os dados quanto o cabeçalho são empacotados e transmitidos com um novo endereçamento IP em um túnel estabelecido entre os pontos de origem e destino. No entanto, cabeçalho e dados são mantidos tal como gerados na origem não garantindo a privacidade.

5 CONFIGURAÇÕES MPLS EM ROTEADORES CISCO

Neste capítulo serão apresentados alguns comandos disponíveis em equipamentos Cisco para configuração de uma rede MPLS. Pelo fato desse tipo de configuração ser complexa, será apresentada apenas a programação do roteador MPLS de borda da rede MPLS (PE-Matriz). A configuração do roteador da filial é idêntica ao da matriz mudando apenas os IP's. Em anexo está disponível toda a configuração dos roteadores CE-Matriz e PE-Matriz, incluindo a configuração do protocolo de roteamento OSPF.

A topologia lógica apresentada, figura 13, mostra a rede interna de uma empresa dividida em Matriz e Filial. Em ambas as redes existe um roteador (CE – *Customer Edge Router*) que encaminha todos os pacotes e é ligado diretamente ao roteador que fica na borda da rede MPLS (PE – *Provider Core Router*).

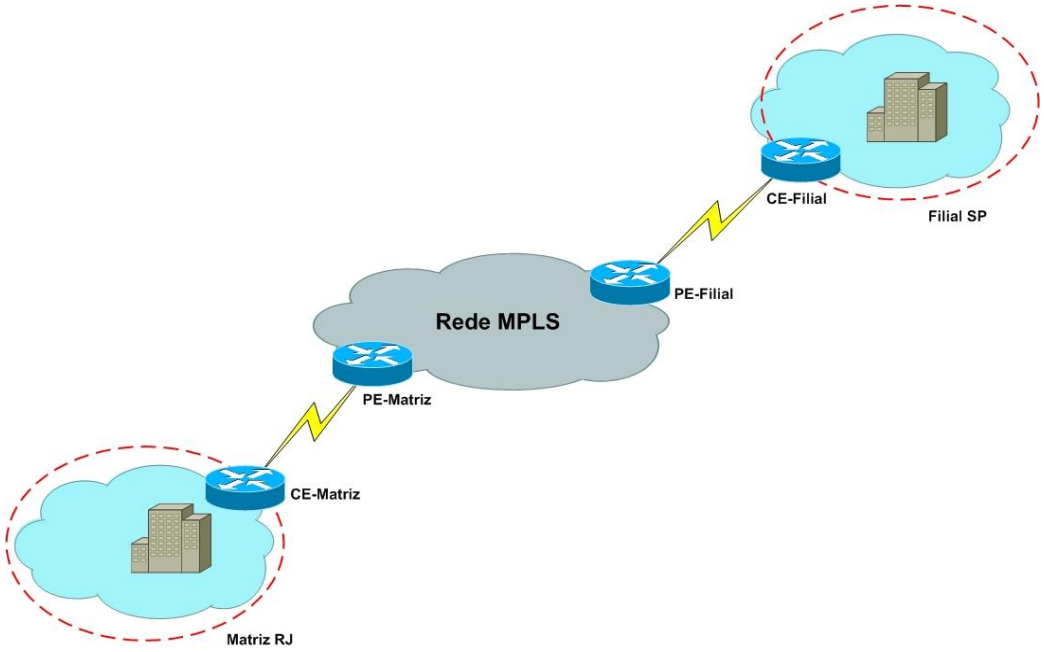


Figura 13 – Topologia Lógica

5.1 CONFIGURAÇÂO DO PE-MATRIZ

Esse roteador fica localizado na borda da rede MPLS e é conectado com o roteador da empresa através da porta Serial 1/0 por onde chegam todos os dados da rede interna. Em sua porta Gigabit Ethernet 2/0 tem-se a ligação com o próximo roteador MPLS, este já dentro da nuvem onde somente as operadoras de Internet têm acesso.

O primeiro passo é habilitar o *Cisco Express Forwarding,* que é uma avançada tecnologia de *swtiching* de IP que otimiza o desempenho e escalabilidade da rede, com o comando:

```
Router(config)# ip cef
```

Para habilitar o modo MPLS no modo LDP de forma global utiliza-se o seguinte comando:

```
Router(config)# mpls label protocol ldp
```

O Router-ID utilizado no MPLS, que geralmente é utilizado na interface de *loopback* pelo fato de outra interface não estar divulgada para o vizinho, pode ser configurado com o seguinte comando:

```
Router(config)# mpls ldp router-id loopback0
```

Para habilitar o MPLS em uma interface, utiliza-se o seguinte comando:

```
Router(config)# mpls ip
```

Para habilitar a VPN em MPLS em uma interface, utiliza-se o seguinte comando:

```
Router(config)# ip vrf forwarding CE-MATRIZ
```

5.2 CONFIGURAÇÂO DO CE-MATRIZ

Esse roteador fica localizado na borda da rede do cliente e é conectado com o roteador de MPLS através da porta Serial 1/0 por onde são enviados todos os dados da rede interna.

Nesse roteador não é feito nenhum tipo de configuração MPLS. O roteamento é estático para o roteador PE-Matriz.

6 CONCLUSÃO

A grande novidade atualmente nas grandes empresas é o uso de aplicações em tempo real, como videoconferência e VoIP. Dentre as várias vantagens em seu uso, redução de custo, economia de tempo e recursos multimídias, como por exemplo, gravação das reuniões, são os principais pontos.

Além destas vantagens, os softwares que realizam esses tipos de comunicação, em sua maioria, permitem visualização e alteração por parte dos integrantes do diálogo além do compartilhamento de informações e transferências de arquivos em tempo real.

O MPLS, que é uma novidade em relação ao Frame Relay e ATM, é muito utilizado, pois proporciona uma melhora significativa no processo de encaminhamento dos pacotes devido à sua simplicidade, adicionando rótulos de tamanho fixo e reduzido, além da escalabilidade e flexibilidade no endereçamento. Permite também a integração do IP com ATM e diversas outras tecnologias de camada 2 (Camada de Enlace) e camada 3 (Camada de Rede), convergência de voz, dados e vídeo, que é essencial para aplicações em tempo real, oportunidade de Engenharia de Tráfego e suporte a VPN.

Mas para que esse tipo de aplicação tenha um bom desempenho, mesmo em redes MPLS, é necessária a criação de um ambiente controlado por QoS para maior controle do tráfego na rede. Em resumo, QoS pode ser traduzido como a percepção do usuário quanto à eficiência de um serviço e característica do tempo de resposta, ou seja, se a fala de um participante vai atrasar ou ser cortada, se o vídeo estará sincronizado com a voz ou estará congelado, por exemplo.

Com o QoS é possível atribuir a largura de banda a um tráfego específico a fim de fornecer níveis previsíveis de taxa de transmissão de dados, priorizando o fluxo de dados e mantendo a qualidade nesse tipo de aplicação.

Por fim, o MPLS é uma excelente solução de rede que permite, com custos relativamente baixos, soluções importantes para esse tipo de aplicação, uma vez que possibilita inúmeras vantagens utilizando as redes IP já existentes nas empresas.

REFERÊNCIAS

[1] UNIVERSIDADE FEDERAL DO RIO DE JANEIRO. GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO. **GTA/UFRJ**. Disponível em http://www.gta.ufrj.br/grad/01_2/mpls/mpls.htm. Acesso em 5 out. 2012

[2] PINHEIRO, José Maria Santos. **O MPLS em Redes de Computadores**. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_mpls_em_redes.php. Acesso em 5 jul. 2012.

[3] GHEM, Maurício Bento. Proposta de uma Ferramenta de Monitoramento de Desempenho em Tempo Real para aplicações *Live Streaming baseadas no protocolo RTP* – Universidade do Vale do Rio dos Sinos, dezembro de 2009. Disponível em http://www.slideshare.net/impalador69/tcc-mauricio-bento-ghem-2009-verso-final. Acesso em 6 jul. 2013

[4] OSBORNE, Eirc. Engenharia de Tráfego com MPLS. 1 ed. Campus, 2002. 9 – 30 p.

[5] SOARES, L.F.G. ; LEMOS, G ; COLCHER, S. Redes de computadores das LANs MANs e WANs às Redes ATM. Rio de Janeiro. Campus, 1995. 576 p.

[6] TANENBAUM, Andrew S. Redes de Computadores.4 ed. Campus, 2003. 945p

[7] BATISTA, Thaís Vasconcelos. Segurança em Redes de Computadores. Natal, 2002. Disponível em: http://www.dimap.ufrn.br/~thais/Seguranca/home.html. Acesso em 10 out. 2012

[8] LEAL, Marco Aurélio de Araújo. QoS – Qualidade de Serviço em TCP/IP – Universidade Federal de Lavras, dezembro 2004. Disponível em: http://issuu.com/arlufla/docs/monomarcoaurelioleal?mode=windows&pageNumber=1. Acesso em: 15 out. 2012

[9] CHIN, Liou Kuo. Rede Privada Virtual – VPN. Disponível em http://www.rnp.br/newsgen/9811/vpn.html. Acesso em 07 nov. 2012

[10] TAPAJÓS, Mauro. Qualidade de Serviço em Redes. Disponível em http://slideshare.net/maurotapajos/redes-avancadas-6qos. Acesso em 20 out. 2012

[11] MIRANDA, Ivana Cardial. VPN – Virtual Private Network Rede Privada Virtual. Disponível em http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana/. Acesso em 08 nov. 2012

[12] FAGUNDES, Bruno. VPN Virtual Private Network. Disponível em: http://lncc.br/~borges/doc/VPN-Virtual%20Private%20Network.slides.pdf. Acesso em 10 nov. 2012

[13] CISCO. MPLS VPN Technology. Disponível em http://www.racf.bnl.gov/Facility/TechnologyMeeting/Archive/06-30-04-CISCO/MPLS-VPN-Technology.pdf. Acesso em 11 nov. 2012

[14] CISCO. Configuring Basic MPLS Using OSPF. Disponível em http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093f23.shtml. Acesso em 07 fev. 2013

[15] CISCO. MPLS Commands: A through L. Disponível em http://www.cisco.com/en/US/docs/ios/12_3t/mpls/command/reference/mp_a1gt.html. Acesso em 07 fev. 2013

ANEXO A – CONFIGURAÇÃO DO ROTEADOR PE-FILIAL

```
Building configuration...
Current configuration : 2496 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE-FILIAL
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ip domain lookup
!
ip vrf CE-MATRIZ
 rd 1:100
 route-target export 1:100
 route-target import 1:100
 route-target import 1:200
 route-target import 1:300
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
mpls label protocol ldp
!
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
!
interface Serial1/0
 ip vrf forwarding CE-MATRIZ
 ip address 172.16.1.1 255.255.255.252
 serial restart-delay 0
```

```
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface GigabitEthernet2/0
 ip address 203.115.18.2 255.255.255.252
 negotiation auto
 mpls ip
!
router ospf 1
 router-id 10.0.0.1
 log-adjacency-changes
 network 10.0.0.1 0.0.0.0 area 0
 network 203.115.18.0 0.0.0.3 area 0
!
address-family ipv4 vrf CE-MATRIZ
  redistribute connected
  redistribute static
  no synchronization
 exit-address-family
!
ip forward-protocol nd
ip route vrf CE-MATRIZ 192.168.10.0 255.255.255.0 172.16.1.2
!
mpls ldp router-id Loopback0
!
control-plane
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
!
!
end
```

ANEXO B – CONFIGURAÇÃO DO ROTEADOR CE-FILIAL

```
Building configuration...
Current configuration : 1271 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ip domain lookup
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 172.16.1.2 255.255.255.252
 serial restart-delay 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
no ip http server
no ip http secure-server
!
control-plane
!
gatekeeper
 shutdown
```

```
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
!
end
```