AUFFRAY Guillaume
SERRE Samuel
THEVENON Julien

Multi Protocol Label Switching [NE520]

Introduction

Au début de l'Internet, la préoccupation majeure était de transmettre les paquets de données à leur destination. La topologie du réseau était relativement simple et le trafic peu important. Ensuite, des mécanismes inhérents à TCP ont été développés pour faire face aux conséquences induites par les pertes de paquets ou la congestion du réseau. Mais, depuis le milieu des années 1990, la taille des réseaux et le trafic ont tellement augmenté que la communauté des fournisseurs de services (ISPs) qui administrent l'Internet est confrontée non seulement au problème de croissance explosive mais aussi à des aspects de politique, globalisation et stabilité du réseau. Cela fait apparaître des goulots d'étranglement et aussi la lenteur des routeurs.

Par ailleurs, il apparaît une très forte diversification des services offerts. Ainsi, de nouvelles applications se développent sur le réseau : téléphonie, vidéoconférence, diffusion audio et vidéo, jeux en réseau, radio en direct… La croissance exponentielle du nombre d'utilisateurs et le volume du trafic ajoutaient une nouvelle dimension au problème. Les classes de services (CoS) et la qualité de services (QoS) devaient être prises en compte pour répondre aux différents besoins de chaque utilisateur du réseau. Or, la majorité des protocoles de routage déployés se basait sur des algorithmes permettant d'obtenir le passage le plus rapide sur le réseau, mais ne prenait pas en compte d'autres mesures, comme les délais ou les congestions qui pouvaient sérieusement diminuer les performances du réseau: la propagation de l'information n'était pas maîtrisée.

Pour cela deux solutions étaient possibles :

- Faire fonctionner IP sur ATM
- Faire de la commutation IP

Routage et commutation de paquet

Le routage de niveau 3 et la commutation de niveau 2 possèdent autant d'avantages que d'inconvénients et aucun ne répond de manière satisfaisante aux besoins exprimés précédemment.

- **Routage IP** :
  - Avantages :
    - Mode non connecté
    - Routage adaptatif - flexibilité
    - Simplicité – pas de signalisation
  - Inconvénients :
    - Utilise information de niveau 3
    - Faible performance
    - Pas de gestion de la qualité de service
- **Commutation** :
  - Avantages :
    - Utilise information protocolaire de niveau 2 (Liaison)
    - Performance élevée
    - Mode connecté – négociation de la qualité de service
    - Table de commutation réduite, chemin dédié
  - Inconvénients :
    - Délai de latence supplémentaire (RTT)
    - Complexe
    - Routage non adaptatif
    - Signalisation requise (RSVP, GSMP, …)

Principes de MPLS

MPLS ou *MultiProtocol Label Switching*.

Historique du MPLS

Les constructeurs ont développé leurs propres protocoles basés sur le même principe en attendant une normalisation de l'IETF:

- IP Navigator (CASCADE / ASCEND / LUCENT)
- Tag Switching (CISCO)
- ARIS (IBM)
- IP Switching (IPSILON / NOKIA)

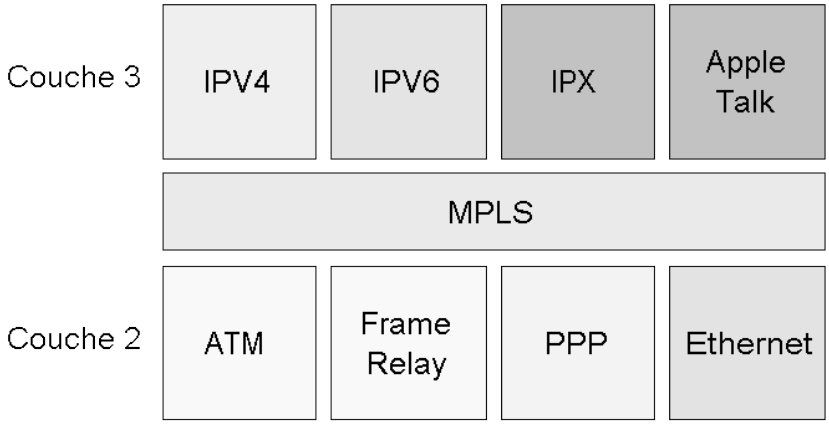
Création d'un groupe de travail à l'IETF (*Internet Engineering Task Force*) en Avril 1997. MPLS s'est fortement inspiré du TAG Switching de Cisco.

Le mécanisme de recherche dans la table de routage est consommateur de temps CPU et avec la croissance de la taille des réseaux ces dernières années, les tables de routage des routeurs ont constamment augmenté. Il était donc nécessaire de trouver une méthode plus efficace pour le routage des paquets. Le but de MPLS était, à l'origine, de donner aux routeurs IP une plus grande puissance de commutation, en basant la décision de routage sur une information de *label* (ou *tag*) inséré entre le niveau 2 (*Data-Link Layer*) et le niveau 3 (*Network Layer*). La transmission des paquets était ainsi réalisée en commutant les paquets en fonction du label, sans avoir à consulter l'entête de niveau 3 et la table de routage. Ainsi, MPLS combinait la souplesse du niveau 3 et la rapidité du niveau 2.

Toutefois, avec le développement de techniques de commutation et la mise au point de nouveaux ASIC (*Application Specific Interface Circuits*), les routeurs IP ont vu leurs performances améliorées sans le recours à MPLS. L'intérêt de MPLS n'est actuellement plus la rapidité mais l'offre de services qu'il permet, avec notamment les réseaux privés virtuels (VPN) et le Traffic Engineering (TE), qui ne sont pas réalisables sur des infrastructures IP traditionnelles.

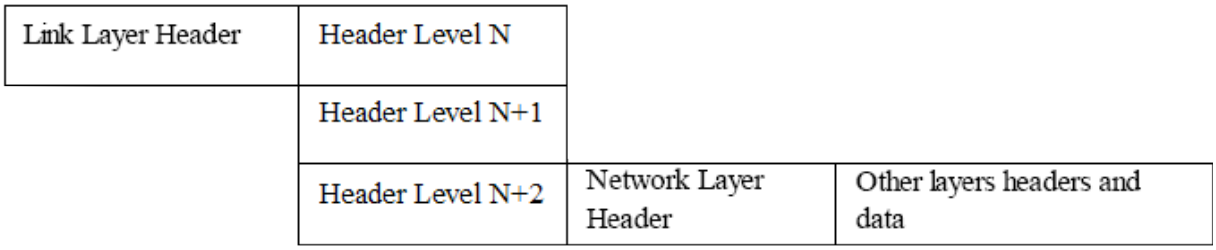
Place dans le modèle OSI

Dans le modèle OSI, MPLS est un protocole situé entre la couche 2 et la couche 3. Il est indépendant des protocoles de ces deux couches. Cependant, il interagit avec des protocoles de routage existants.



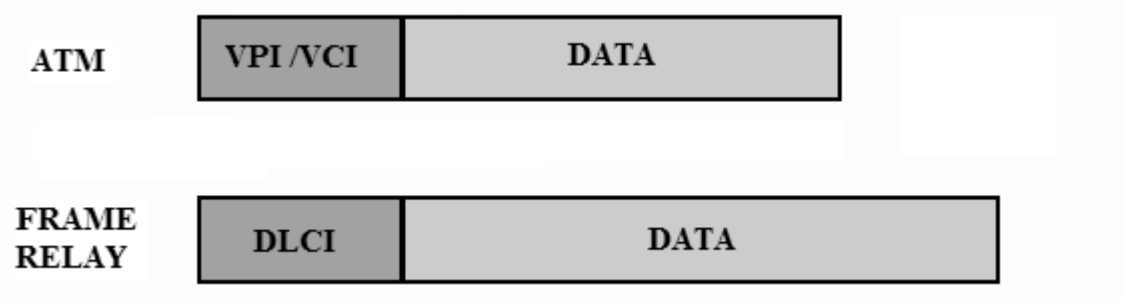
Caractéristiques

La commutation MPLS est **hiérarchique**, c'est-à-dire qu'en plus de commuter des étiquettes, il est possible d'en ajouter ou d'en enlever. Le header MPLS attaché à un même paquet IP représente une **pile d'étiquettes** appelée ***label stack***. Dans la pratique, le protocole MPLS se traduit par l'ajout d'une pile d'entêtes dans la trame :



Encapsulation avec une pile composée d'une seule entête.

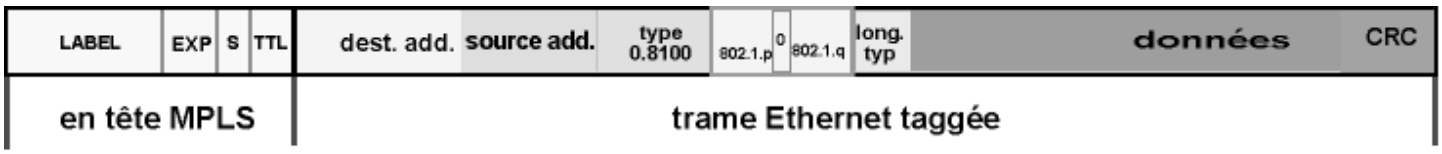
Bien qu'il soit indépendant du protocole du niveau 2, le placement de l'entête est différent suivant le protocole utilisé. En effet, dans le cas d'un protocole de niveau 2 utilisant la commutation de cellule, le champ correspondant au label sera utilisé comme label MPLS.



Dans le cas du protocole Ethernet, le « préambule » et le « start » de la trame Ethernet sont remplacés par l'entête MPLS.

Trame Ethernet sans MPLS :

Trame Ethernet avec MPLS :



Entête MPLS

L'entête MPLS possède 32 bits soit 4 octets et comporte 4 champs :

Label sur 20 bits : codage de la valeur du label
COS ou **EXP** sur 3 bits : classe de service du paquet
S sur 1 bit : stack Indicator indique le bas de la pile de label (1 pour le dernier label, 0 pour les autres).
TTL sur 8 bits : durée de vie du paquet pour gérer les boucles. Champ géré par MPLS car la gestion des boucles n'est pas assurée par tous les protocoles de niveau 2.

Les composants

- **Label :** Un label est un entier qui est associé à un paquet lorsqu'il circule dans un réseau MPLS et sur lequel ce dernier s'appuie pour prendre des décisions de routage.

- **LSP (Label Switch Path)** : Séquence de labels à chaque nœud du chemin allant de la source à la destination. Elle est établie en fonction du type de transmission de données ou après détection d'un certain type de données. Un LSP est unidirectionnel et le trafic de retour doit donc prendre un autre LSP.

- **MPLS Ingress node ou routeur d'entrée MPLS** : C'est un routeur gérant le trafic qui entre dans un réseau MPLS. Il possède à la fois des interfaces IP traditionnelles et des interfaces connectées au réseau MPLS. C'est lui qui impose

le label aux paquets entrants. Il est aussi appelé LER (Label Edge Routeur) car il connecte le réseau MPLS au monde extérieur.

- **MPLS Egress node ou routeur de sortie MPLS** : C'est un routeur gérant le trafic qui sort d'un réseau MPLS. Il possède à la fois des interfaces IP traditionnelles et des interfaces connectées au réseau MPLS. C'est lui qui retire le label aux paquets sortants sauf si le mode **PHP** (***Penultimate Hop Popping***) est activé.

- **LSR (Label Switch Router)** : C'est un routeur d'un réseau MPLS qui est capable de retransmettre les paquets au niveau de la couche 3 en s'appuyant seulement sur le mécanisme des labels. Toutes ses interfaces supportent le protocole IP.

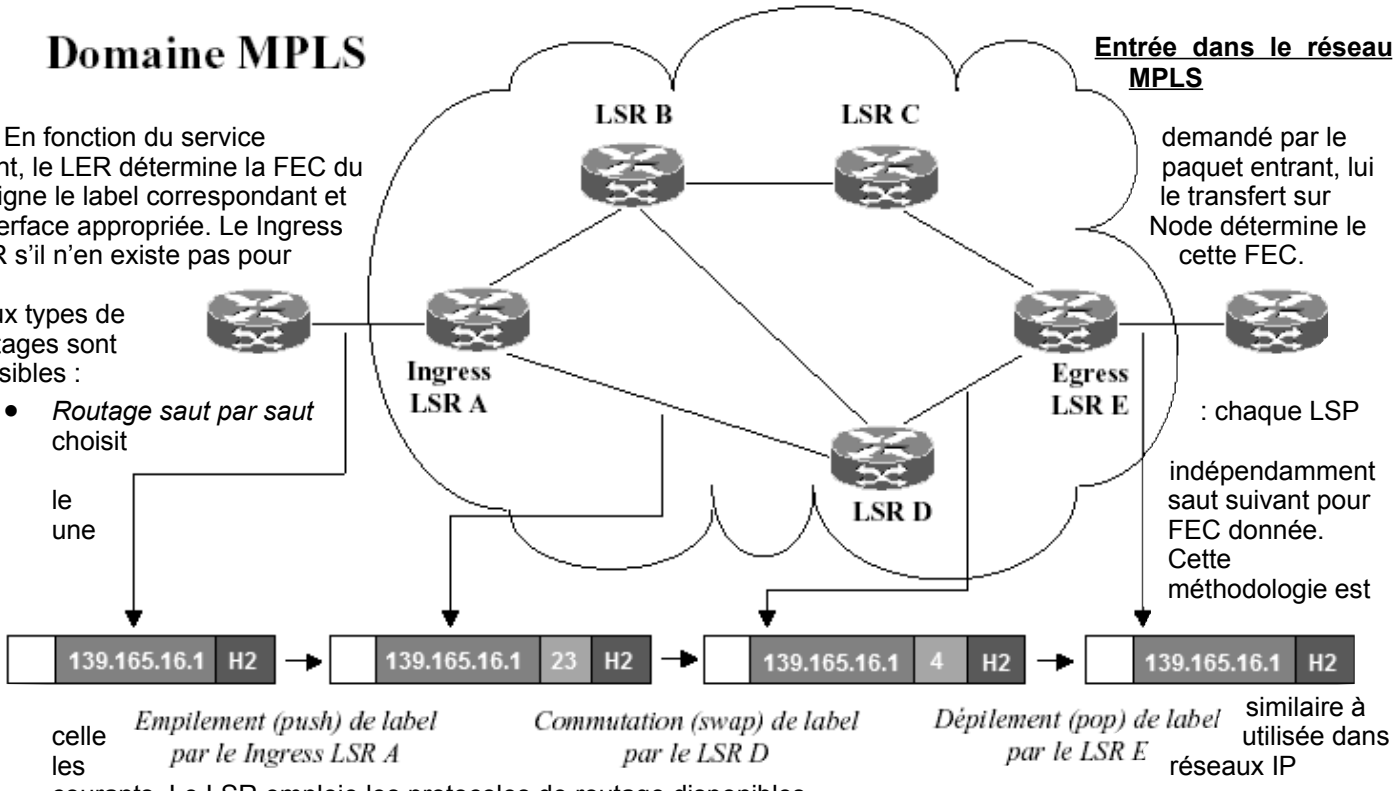
- **LER (Label Edge Routeur)** : Un LER est un LSR qui fait l'interface entre le réseau MPLS et le monde extérieur. C'est lui qui est chargé par exemple de " labelliser " les paquets à leur entrée dans le réseau MPLS. Il est équivalent à un *ingress node* ou *egress node*. En général, une partie de ses interfaces supportent le protocole MPLS et l'autre un protocole style IP.

- **FEC (Forward Equivalence Class) :** Représentation d'un groupe de paquets qui a en commun les mêmes besoins quant à leur transport. Tous les paquets d'un tel groupe reçoivent le même traitement au cours de leur acheminement. Contrairement aux transmissions IP classiques, dans MPLS, un paquet est assigné à une FEC une seule fois, lors de son entrée sur le réseau. Les FEC sont basées sur les besoins en terme de service pour certains groupes de paquets ou même un certain préfixe d'adresses. Chaque LSR se construit une table pour savoir comment un paquet doit être transmis. Cette table est appelée **Label Information Base** (**LIB**).

- **LDP (Label Distribution Protocol) :** LDP est un protocole permettant d'apporter aux LSR les informations d'association des labels dans un réseau MPLS. Il est utilisé pour associer les labels aux FEC, ce qui crée des LSP. Les sessions LDP sont établies entre deux éléments du réseau MPLS qui ne sont pas nécessairement adjacents. Il construit la table de commutation des labels sur chaque routeur et se base sur le protocole **IGP** (**Internal Gateway Protocol**) pour le routage.

Fonctionnement

Dans un réseau mettant en oeuvre MPLS, tout paquet entrant se voit attribuer un "label" par un **Label Edge Router (LER)**. Les paquets sont routés le long d'un **Label Switch Path (LSP)** où chaque **Label Switch Router (LSR)** prend les décisions de routage en s'appuyant seulement sur la valeur des " label ". A chaque " saut ", le LSR remplace l'ancien " label " par un nouveau qui indique comment router le paquet au prochain saut.



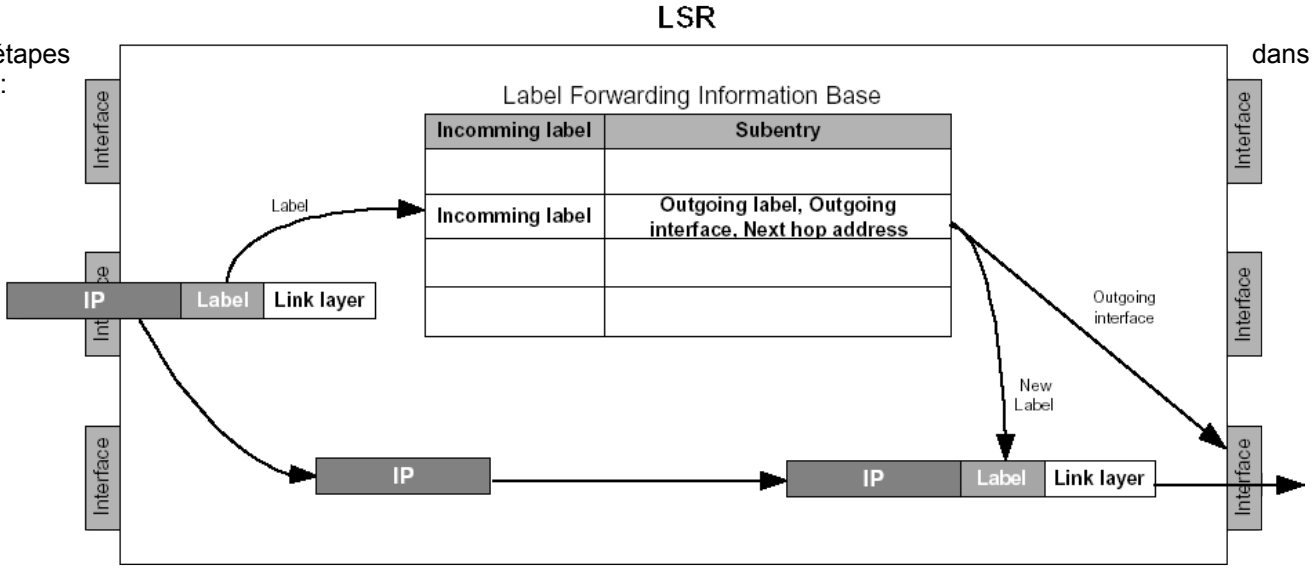
En fonction du service demandé par le client, le LER détermine la FEC du paquet entrant, lui assigne le label correspondant et le transfert sur l'interface appropriée. Le Ingress Node détermine le LSR s'il n'en existe pas pour cette FEC.

Deux types de routages sont possibles :

- *Routage saut par saut* : chaque LSP choisit indépendamment le saut suivant pour une FEC donnée. Cette méthodologie est celle utilisée dans les réseaux IP courants. Le LSR emploie les protocoles de routage disponibles.
- *Routage explicite* : le premier LSR détermine la liste des nœuds à suivre. Le chemin spécifié peut être non optimal

Routage saut par saut sans commutation hiérarchique dans le réseau MPLS

Schéma de principe de la commutation au niveau d'un LSR :



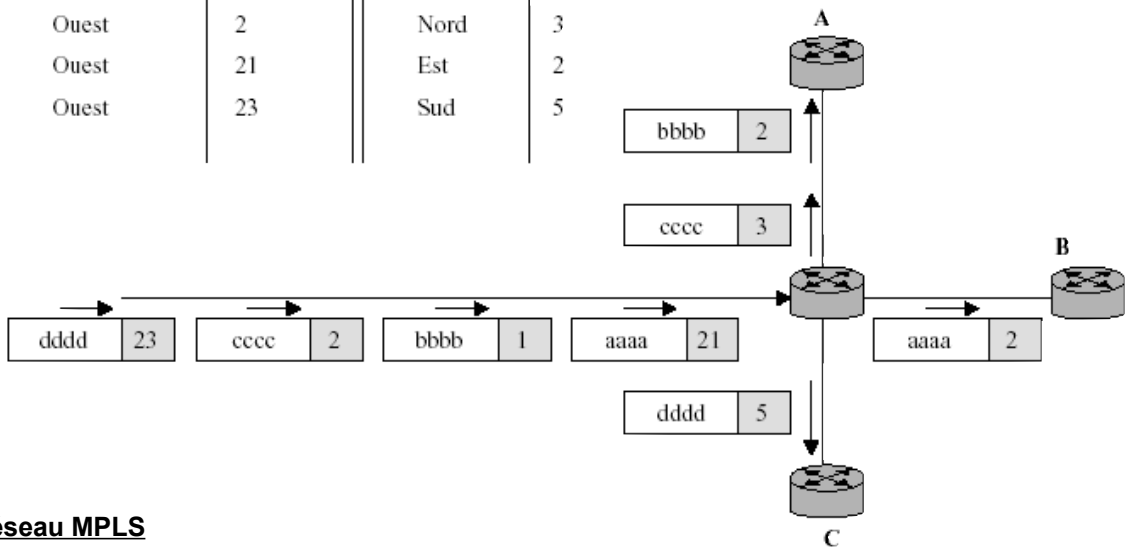
Les étapes dans un LSR :

- Récupération du label du paquet.
- Recherche de la ligne de la LIB correspondant à l'interface d'entrée et au label du paquet.
- Détermination du nouveau label ainsi que de l'interface sur laquelle le paquet sera renvoyé.
- Transfert du paquet avec le nouveau label.

Exemple de routage

Label Forwarding Table

InPort	InLabel	OutPort	OutLabel
Ouest	1	Nord	2
Ouest	2	Nord	3
Ouest	21	Est	2
Ouest	23	Sud	5



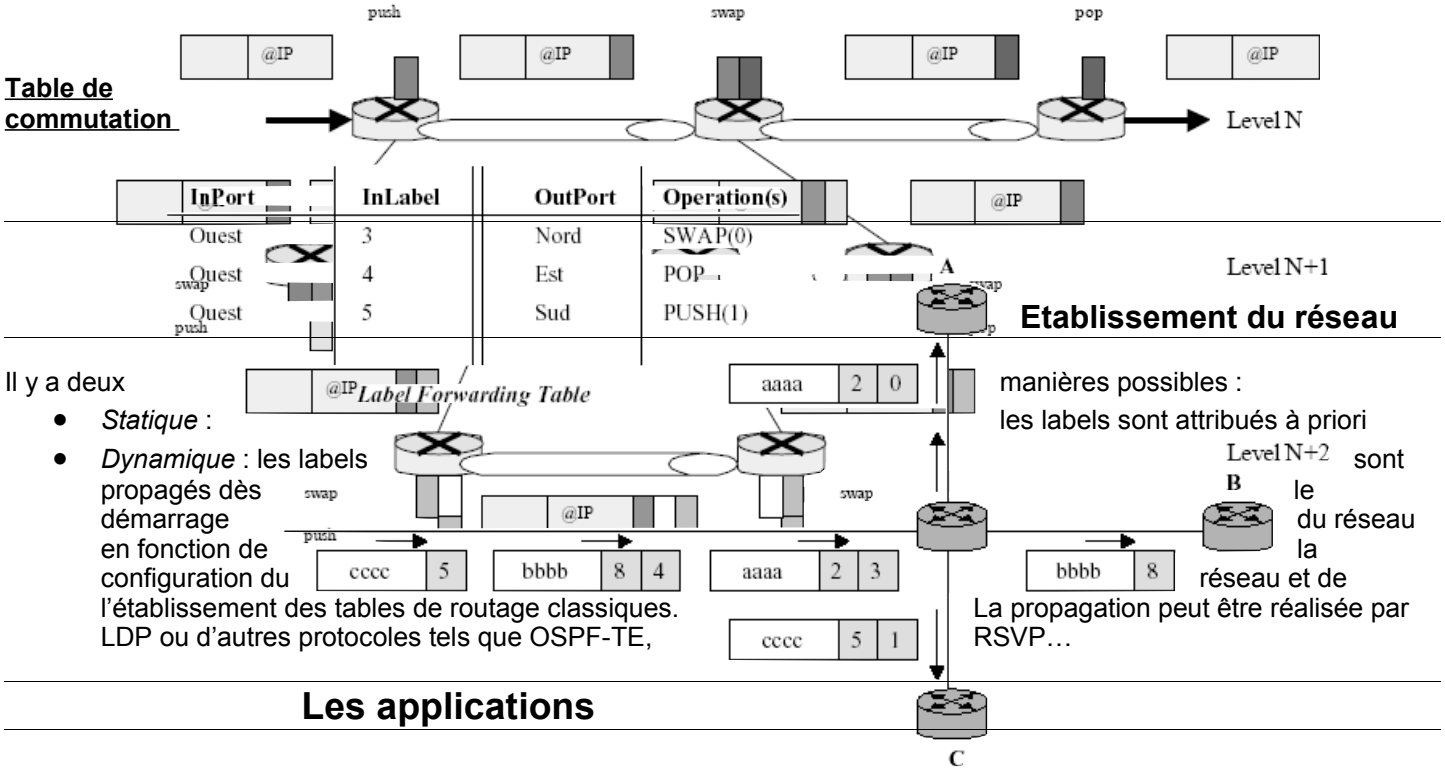
Sortie du réseau MPLS

Le Egress Node retire les labels des paquets qui proviennent du réseau MPLS pour redonner au flux entrant sa nature initiale mais effectue automatiquement une recherche dans sa LIB, puis détermine l'interface de sortie à l'aide d'un protocole de routage de niveau 3.

L'opération de recherche dans la LIB est inutile, le mode PHP permet d'éviter cela en faisant supprimer le label par l'avant dernier nœud. Ainsi lorsque le paquet arrive sur le Egress Node, il est routé directement suivant le protocole de niveau 3.

Commutation hiérarchique

Dans le cas d'une commutation hiérarchique seul le label situé au sommet de la pile est pris en compte. Les LSR n'effectuent plus seulement des échanges de labels, ils font aussi de l'empilement et du dépilement. La commutation hiérarchique permet l'agrégation de LSP afin de réduire les tables de routage.



Il y a deux manières possibles :

- *Statique* : les labels sont attribués à priori
- *Dynamique* : les labels sont propagés dès le démarrage du réseau en fonction de la configuration du réseau et de l'établissement des tables de routage classiques. La propagation peut être réalisée par LDP ou d'autres protocoles tels que OSPF-TE, RSVP…

QoS : Qualité de Service

En terme de qualité de services, MPLS n'apporte rien de plus par rapport à IP : il permet de dérouler les mêmes algorithmes, basés sur les mêmes informations. Cependant, il peut le faire plus rapidement car le marquage n'est fait qu'une fois à l'entrée du réseau MPLS et non à chaque routeur comme dans IP et il achemine en se basant sur la seule étiquette MPLS.

On trouve deux approches de la QoS avec MPLS :

- L-LSP : le choix du chemin est fait en fonction de la QdS du flux passant sur ce chemin.
- E-LSP : le mode associé au champ expérimental (EXP) de trois bits.

Les LER prennent en compte les demandes des clients en terme de type de service souhaité (TOS), identifient une FEC et créent ou simplement utilisent un LSP préexistant et correspondant à cette FEC.
Dans la pratique, le nombre de FEC est restreint, les opérateurs se limitant fréquemment à quelques FEC, appelées classes de services (CoS : champ EXP).

Exemple de classes de services :

- *Standard* : données traditionnelles.
- *Premium* : besoins précis en terme de bande passante.
- *Multimédia* : priorité absolue sur les autres flux. Débit constant (données non compressées) ou variables (données compressées), peu de gigue.

Traffic Engineering

Le but est d'optimiser l'utilisation des ressources du réseau (répartition de la charge, exploitation des liens les plus rapides).

Les protocoles classiques permettent de router des paquets au sein d'un réseau MPLS, mais ne peuvent éviter les congestions s'ils redirigent les paquets vers un LSP de priorité haute.
Le Traffic Engineering (TE) permet d'optimiser l'emploi des liaisons en établissant des tunnels LSP dans un réseau MPLS, indépendamment de l'IGP. Ceci peut être combiné avec la réservation de bande passante.
Les tunnels peuvent être déterminés statiquement ou automatiquement par les LSR. Plusieurs tunnels peuvent être utilisés pour répartir le trafic si celui-ci est trop important pour être véhiculé par un seul chemin.

Un certain nombre de protocoles existants permet de prendre en compte des notions de QoS tels CR-LDP (*Constraint-based Routed Label Distribution Protocol*), RSVP-TE ou OSPF-TE. Ce sont des extensions pour respectivement les protocoles LDP, RSVP et OSPF.

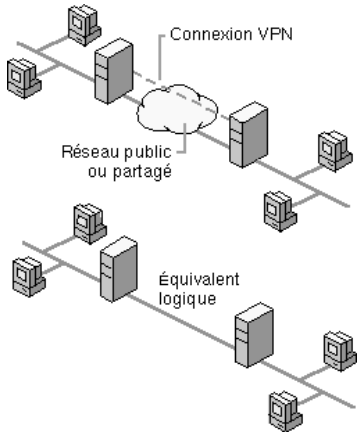
Les VPN

Les VPN permettent de faire communiquer à distance deux réseaux d'entreprises ou un ordinateur et un réseau d'entreprise, de façon confidentielle et ceci en utilisant Internet.

Avantages : Faible coût de l'accès à Internet (contrairement aux lignes louées, inaccessibles aux petites entreprises).

Un VPN présente l'apparence, les fonctions et les avantages d'un réseau étendu privé, mais il utilise (en partie) l'infrastructure partagée d'un réseau public. Un VPN est privé dans la mesure où les communications sont limitées aux seuls membres du VPN, sans ouverture vers les autres utilisateurs du réseau public. Il est également privé dans le sens où le trafic n'a pas à se conformer aux règles d'un réseau public tel que l'adressage.

Pour émuler une liaison point à point, les données sont encapsulées ou enveloppées, avec un en-tête qui fournit les données de routage leur permettant de traverser l'inter réseau partagé ou public afin d'atteindre la destination finale. Pour émuler une liaison privée, les données envoyées sont cryptées afin de préserver leur caractère confidentiel. Les paquets qui sont interceptés sur le réseau partagé ou public sont indéchiffrables sans les clés de cryptage. La liaison dans laquelle les données privées sont encapsulées et cryptées s'appelle Connexion VPN.



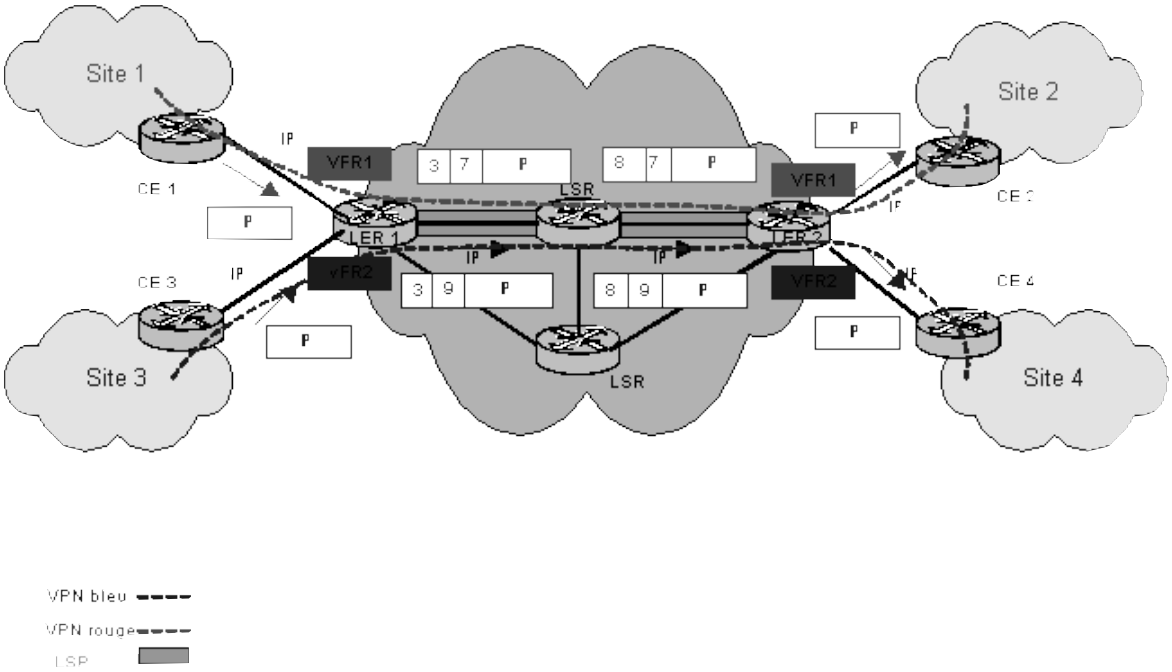
Face à cette demande, les opérateurs télécoms proposent généralement aux sociétés deux types de solutions : la première reposant sur le protocole IPSec (*IP Security*) qui privilégie la sécurisation des flux d'informations par encryptage des données, la seconde s'adossant à la norme plus récente MPLS (*Muti Protocol Label Switching*) qui gère les problèmes de qualité de service et de prioritarisation des flux.

IPSec :
- Intégrité et authenticité
- Chiffrement des paquets IP
- Négociation des paramètres de sécurité

MPLS :
- Gestion de la qualité de service
- Prioritarisation des flux
- VPN de niveau 2 ou 3, Routeurs Virtuels

IPSec, de part la possibilité de rendre les données confidentielles, s'adresse plutôt au réseau public tandis que MPLS est destiné à être utilisé dans les réseaux privés (pas d'aspects de sécurité).

*


Site 1
Site 2
Site 3
Site 4
CE 1
CE 2
CE 3
CE 4
IP
VFR1
VFR2
LER 1
LER 2
LSR
LSR
P
3 7 P
8 7 P
3 9 P
8 9 P
VPN bleu
VPN rouge
LSP

MPLS dans la pratique

Le choix de MPLS par les opérateurs est motivé par différents aspects :

- L'accélération du temps de transit des paquets (moins vrai actuellement),
- La mise en oeuvre de la Qualité de Service,
- Les possibilités de gestion du trafic ou Ingénierie de Trafic (TE) pour éviter les congestions de réseaux ou encore amener de la redondance,
- L'établissement de tunnels IP permettant la mise en oeuvre des Virtual Private Networks ou VPN,
- L'utilisation de MPLS sur un ensemble de réseaux hétérogènes permet de remonter certains contrôles de la couche 2 à la couche 3 et amène ainsi une simplification de la gestion des réseaux pour les opérateurs et par la même une simplification de gestion de services sur des réseaux tels ATM ou Frame Relay.
- La possibilité de cohabitation de MPLS orienté connexion avec IP orienté non-connexion,
- Mise en place de "circuit-switched paths" au travers de LSP en étant indépendant de la technologie employée à la couche de niveau 2 (FR, ATM, etc...)
- Téléphonie et plus généralement tous services avec des contraintes au niveau temporel,
- Sécurité : création de VPN au niveau 2 ou 3 (tunnels IP),
- Possibilité d'utiliser des solutions de cryptage style IPSec par-dessus des MPLS-VPN.
- Mise en place de réseaux partiellement maillés au niveau de la couche 2 avec une indépendance de la solution utilisée (Frame Relay ou ATM),
- Mise en place de réseaux complètement maillés au niveau de la couche 3,
- Problématique de migration vers un coeur de réseau basée sur une technologie autre qu'ATM,
- Routage explicite ou via un protocole de routage,
- Diminution des coûts.

MPLS permet à la fois une grande souplesse de connectivité au sein des réseaux avec une plus grande efficacité de l'utilisation des débits disponibles tout en assurant en permanence l'affectation des priorités. Cependant, la mise en œuvre et la configuration des routeurs de réseaux à grande distance sont des opérations lourdes, et ceci à plus forte raison, lorsqu'il s'agit de configurations mettant en jeu plusieurs exploitants. Une nuance sérieuse doit encore être ajoutée, en effet, sur le plan de l'homogénéité des équipements MPLS réalisés par les industriels. Des incompatibilités de fonctionnement sont encore notées lors de la mise en regard d'équipements d'origine différente. Ce qui veut dire qu'en VPN géré par le même exploitant d'un bout à l'autre du monde (AT&T, Equant, BT, etc.), l'entreprise cliente est assurée de disposer d'une bonne qualité de services.

Dans un réseau cogéré par plusieurs exploitants, et justement là où le trafic peut subir de grandes variations d'intensité, il n'est pas certain que la dernière version de MPLS proposée par les industriels permette un haut niveau de qualité de services. Peut-on imaginer des routeurs d'accès disposant de 30 000 à 60 000 accès de circuits virtuels alors que les équipements MPLS actuels n'en présentent pas plus de quelques centaines ? Aussi, des exploitants comme *Sprint* n'utilisent pas encore MPLS.

MPLS se heurte aux traditions établies dans les réseaux qui préfèrent continuer à soutenir les protocoles déjà en place, comme le relais de trame (FR), IPSec, etc., qui jusqu'ici ont donné satisfaction aux entreprises utilisatrices de réseaux privés virtuels (VPN).

Perspectives

Conçu pour rendre plus efficaces les coeurs de réseaux en mode paquets, le MPLS, technologie de commutation intelligente de niveau 2, pourrait servir à commuter des liaisons physiques matérialisées par des longueurs d'ondes sur fibre optique. Une telle perspective est à l'étude dans le cadre de la commutation multi protocole avec étiquetage des flux, dite généralisée (Generalized MPLS). Cette infrastructure possède des fonctionnalités supplémentaires par rapport à MPLS et autoriserait une connectivité naturelle entre la partie transport et la partie IP, modifiant ainsi radicalement la façon dont les réseaux ont été pensés et bâtis par les opérateurs au cours des deux dernières décennies tout en faisant circuler les paquets par le réseau à la vitesse de la lumière.