

# Cours 4 : Multiprotocol label switching MPLS

R302 : Réseaux opérateurs  
IUT R&T 2<sup>e</sup> année

Fatma Essaghraier

# HISTOIRE ET INTÉRÊT DE MPLS

## Début d'Internet

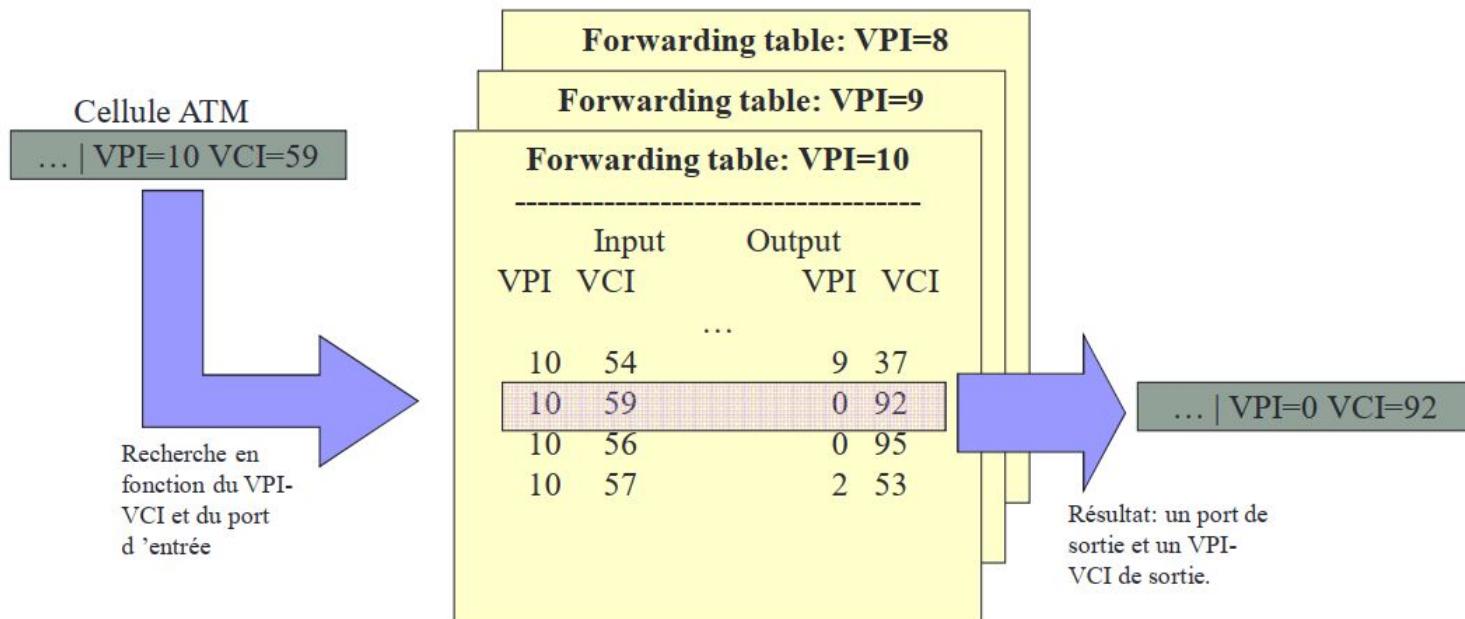
- But : amener les paquets à destination
  - Topologie des réseaux relativement simple
  - Trafic peu important

## Milieu des années 90

- Augmentation de la taille des réseaux et du trafic
  - Apparition de goulots d'étranglements : routeurs trop lents
- Diversification des services offerts
- Nouvelles applications nécessitant CoS et QoS
  - Nécessité de tenir compte des délais et des congestions de réseaux.
- Deux solutions possibles:
  - Faire fonctionner IP sur ATM
  - Faire de la commutation de IP

# Asynchronous Transfer Mode (ATM)

- Approche de réseaux orientés connexion
- Un protocole de la couche « liaison de donnée» à **commutation** de cellules, qui a pour objectif de multiplexer différents flots de données sur un même lien physique

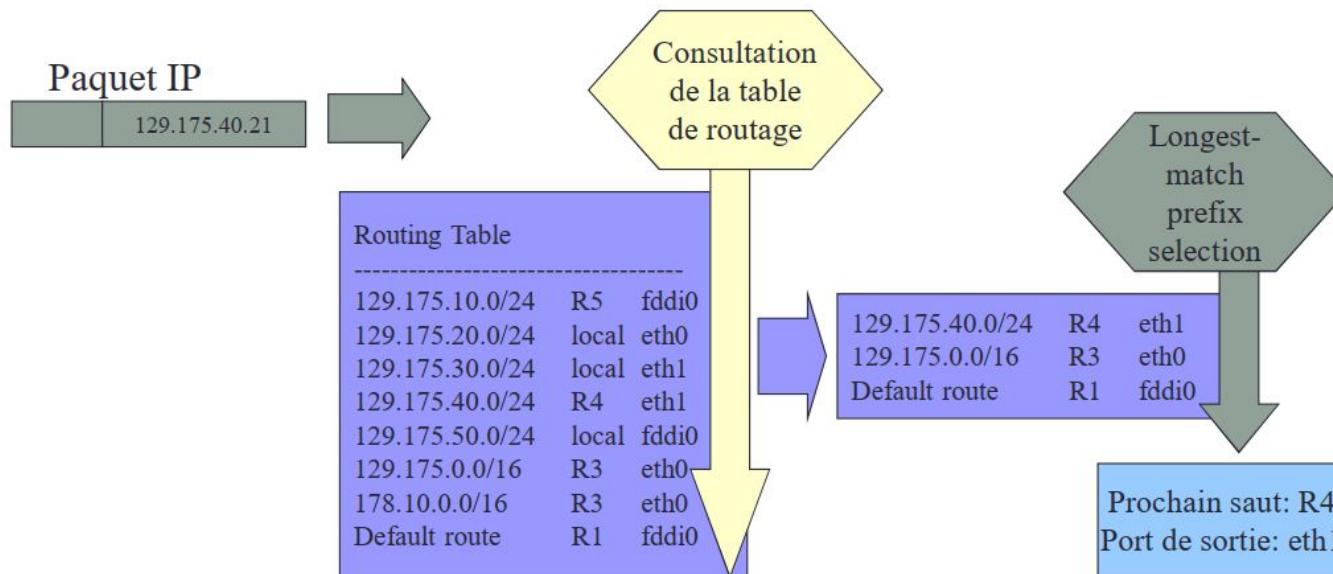


VPI: Virtual Path Identifier

VCI: Virtual Channel Identifier

# Acheminement des paquets IP

- Un protocole de la couche «réseaux»
  - Les données circulent sur le réseau Internet sous forme de datagrammes (commutation des paquets)
- Réseau en mode datagramme (connectionless network)
    - Lecture de la table de routage
    - Longest prefix match

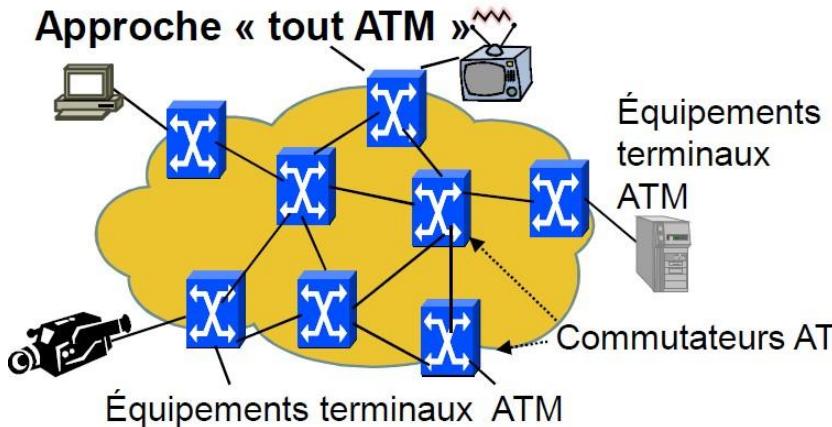


# Routage vs Commutation

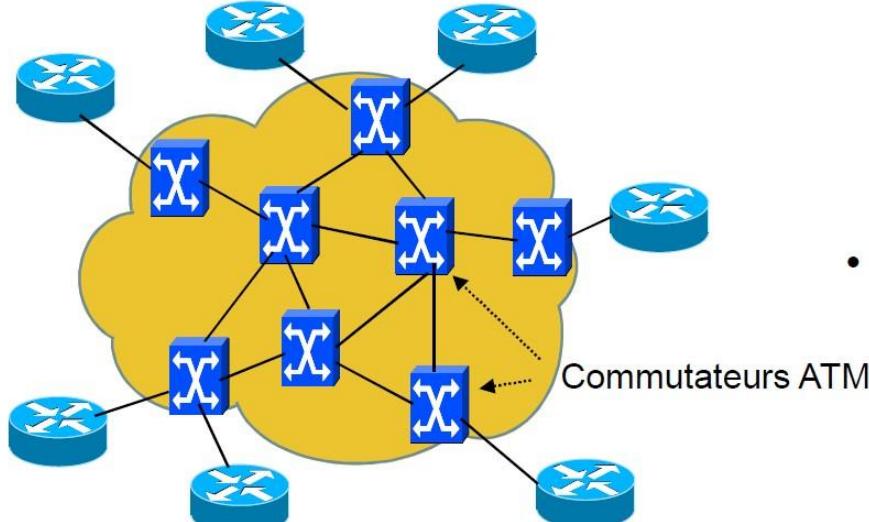
<b>Routage IP (Niveau 3)</b>	<b>Commutation de paquet (Niveau 2)</b>
<ul style="list-style-type: none"><li>• <b>Avantages</b><ul style="list-style-type: none"><li>• Mode non connecté</li><li>• Routage adaptatif (flexibilité)</li><li>• Simplicité (pas de signalisation)</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <b>Avantages</b><ul style="list-style-type: none"><li>• N'utilise pas les informations de niveau 3</li><li>• Performances élevées</li><li>• Mode connecté (négociation de la qualité de services)</li><li>• Table de commutation réduite, chemin dédié</li></ul></li></ul>
<ul style="list-style-type: none"><li>• <b>Inconvénients</b><ul style="list-style-type: none"><li>• Utilise les informations de niveau 3 (consommation CPU)</li><li>• Faibles performances (routage à chaque saut)</li><li>• Pas de gestion de la Qos</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <b>Inconvénients</b><ul style="list-style-type: none"><li>• Délai de latence supplémentaire (établissement de la liaison)</li><li>• Complexité</li><li>• Routage non adaptatif</li><li>• Signalisation requise (exemple : RSVP)</li></ul></li></ul>

# Approches possibles des opérateurs

Approche « tout ATM »



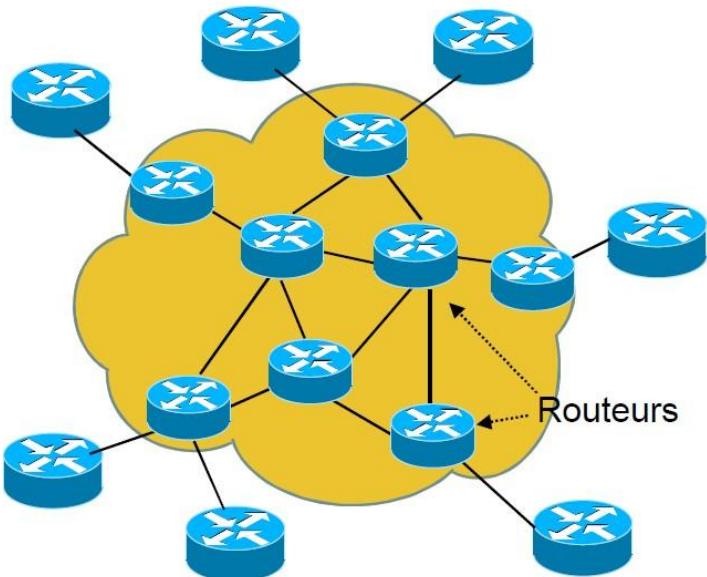
Approche de superposition : IP sur ATM



- Les opérateurs avaient choisi une approche « tout ATM » sans IP
  - ATM « sans couture »
  - Le succès d'Ethernet et d'IP a éliminé cette approche
- Les opérateurs ont alors utilisé leur infrastructure ATM pour transporter les paquets IP
  - Le mode circuit virtuel d'ATM permet aux opérateurs de faire de l'ingénierie de trafic
    - Choisir sur quel circuit virtuel transporter tel type de trafic
- Cohabitation de deux technologies
  - Non conçues pour interopérer
  - Besoin de doubles compétences

# Approches possibles des opérateurs

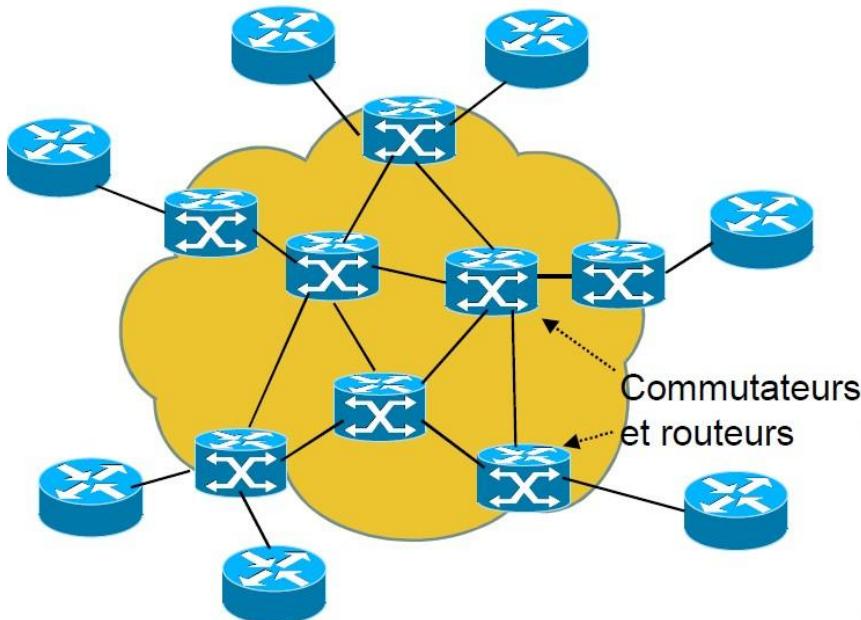
## Approche IP pur sans ATM



- **Les opérateurs ont alors envisagé une approche « tout IP »**
  - Une seule compétence
- **Le routage dans le réseau de l'opérateur est celui du mode datagramme IP**
  - Basé sur l'adresse destinataire du paquet IP
  - Tous les paquets sont envoyés sur la meilleure route IP
- **Les routeurs au départ étaient plus lents que les commutateurs ATM**
  - Mais les routeurs rapides ont corrigé ce problème
- **Pas de possibilité d'ingénierie de trafic et d'équilibrage de trafic**

# Approches possibles des opérateurs

## Approche d'intégration : MPLS



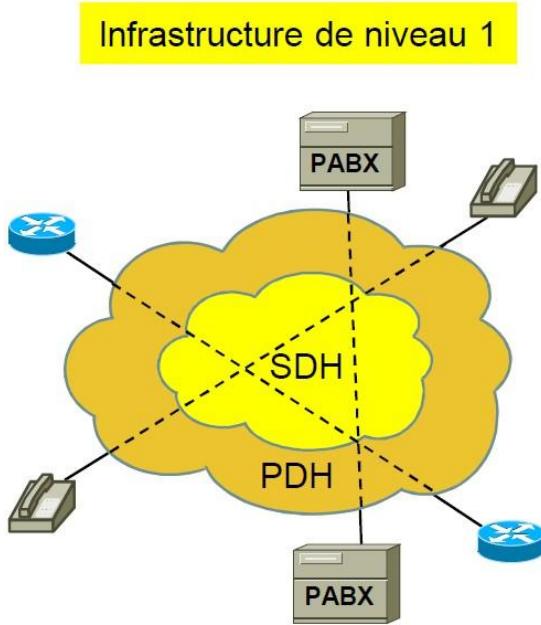
- **Une approche intermédiaire d'intégration a été proposée**
  - Un seul plan d'adressage IP
  - Les équipements internes de l'opérateur sont des équipements hybrides
    - Ils peuvent fonctionner comme des routeurs IP
    - Ils peuvent aussi fonctionner dans un mode proche du circuit virtuel en commutant selon un numéro de label
- **Le routage n'est plus forcément corrélé à l'adresse destinataire IP**
  - L'ingénierie de trafic est possible
- **IP et MPLS sont des technologies proches conçues pour interopérer**

- **Quelle technologie va servir de base pour l'infrastructure unique de convergence pour les réseaux d'opérateurs?**
- **ATM était le choix naturel**
  - Solution éprouvée
  - Investissements souvent déjà engagés
  - Possibilité de haut débit grâce à son fonctionnement hardware
  - Fonctions riches pour assurer différents niveaux de qualité de service
    - Selon le type de trafic ou le type de service offert au client de l'opérateur
  - Possibilités d'ingénierie de trafic
    - Agrégation de trafics sur des PVC respectant des contraintes
- **Mais l'environnement technique a changé depuis la conception d'ATM**
  - IP est devenu le protocole de niveau 3 incontournable
  - Le hardware est monté en puissance
  - La bande passante est plus abondante et moins chère
  - Les stations d'extrémité sont plus intelligentes

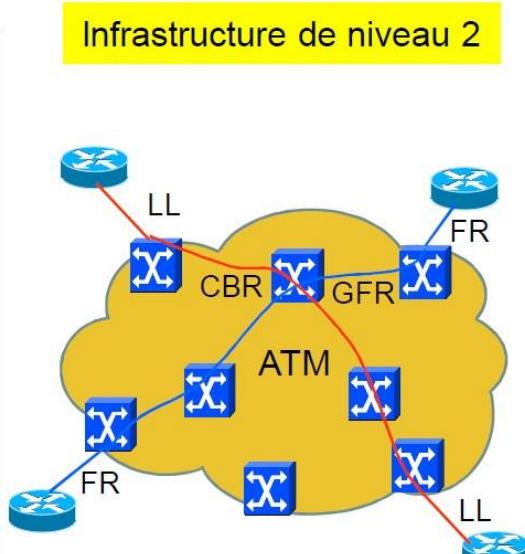
- **Dans le contexte actuel, ATM présente des inconvénients**
  - Il cohabite mal avec IP
    - Conversion d'adresses, mode multicast différent
    - Duplication des protocoles de routage
  - Le hardware permet maintenant le traitement de paquets de longueur variable
  - Les petites cellules ont moins d'intérêt à très haut débit
    - Et pénalisent même le traitement (plus de cellules à traiter)
  - ATM va trop loin dans les possibilités de qualité de service
    - Les stations d'extrémité peuvent s'adapter à une qualité de service un peu moins bonne
    - La qualité de service native est meilleure à très haut débit
- **De nombreux constructeurs ont proposé des solutions de commutation IP faisant la synthèse de la commutation ATM et du routage IP**
  - IP switching (Nokia), ARIS (IBM), Tag Switching (Cisco), etc...
- **MPLS (MultiProtocol Label Switching) est la synthèse IETF de ces propositions**

# Evolution des infrastructures réseau des opérateurs

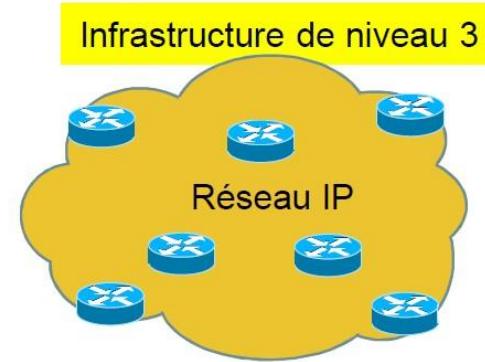
- L'infrastructure des opérateurs a subi des profondes migrations**



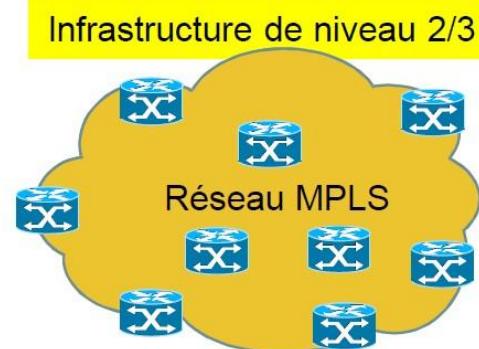
- Services de niveau 1**
  - Liaisons louées
  - Téléphonie classique
  - Interconnexion de PABX



- Services de niveau 1 et 2**
  - Liaisons louées (CBR)
  - Frame Relay (GFR)
  - Vidéo (VBR-rt)
  - RNIS-Large Bande



- Services de niveau 3**
  - Accès Internet
  - VPN IPsec



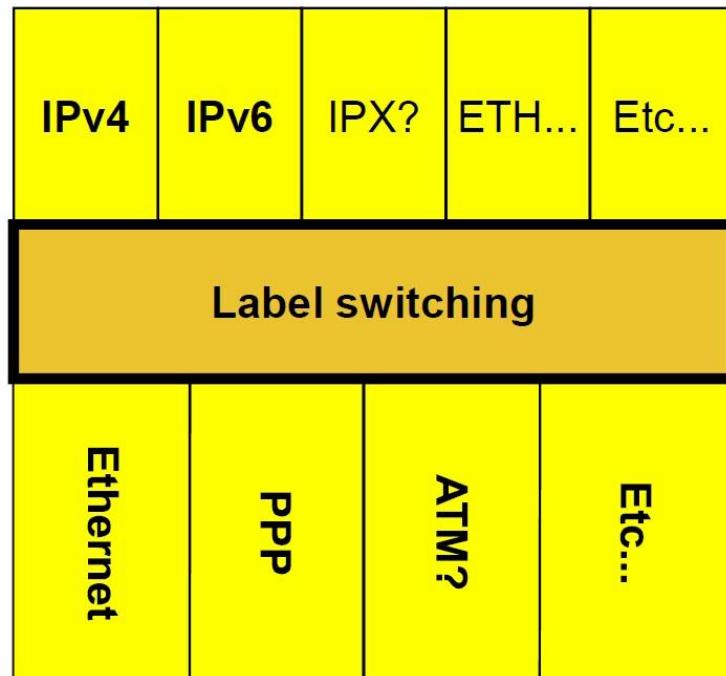
- Services de niveau 1, 2 et 3**
  - Différents types de VPN

# FONCTIONNEMENT DE MPLS

- MPLS est une technologie réseau qui utilise des **étiquettes** pour router efficacement les données à travers un réseau.
- Envoie les paquets le long de **chemins réseau prédéterminés**.
- Crée par un groupe de travail à l'IETF en Avril 1997.
- Fortement inspiré du tag switching de Cisco
- Fonctionne sur **la couche OSI " 2.5"**, sous la couche 3 (réseau) et au-dessus de la couche 2 (liaison de données)
  - Souplesse du niveau 3 + puissance du niveau 2
- **Application** : L'intérêt du MPLS réside dans les services qu'il permet:
  - a. Gestion de QoS,
  - b. L'ingénierie du trafic,
  - c. les réseaux VPN,
  - d. et les services de télécommunication...

- **Protocole supérieur quelconque**
  - IPv4 ou IPv6 (niveau 3)
  - Ethernet (pour service VPLS)
- **Protocole de niveau 2 quelconque**
  - ATM (pour migration)
  - PPP (sur liaisons Sonet/SDH)
  - Ethernet 1 ou 10 Gbps
  - Combinaison des approches précédentes
- **MPLS est donc flexible**
  - Peut utiliser l'infrastructure ATM existante, puis migrer vers Ethernet ou autre
  - Peut évoluer facilement vers IPv6
  - Peut transporter n'importe quel trafic
    - Par ex. des trames Ethernet (VPN de niveau 2 (VPLS))

**Multiprotocole au dessus**



**Label switching**

**Multiprotocole au-dessous**

- Quand MPLS est utilisé sur une infrastructure de commutation traditionnelle, il s'appuie sur les techniques existantes
  - Facilité d'adaptation (pas de nouveaux investissements)
- La valeur du premier label MPLS affecté est utilisée comme étiquette de commutation : DLCI ou VPI/VCI.
- MPLS s'appuie sur un protocole de routage IP pour définir les chemins optimaux. Ensuite, il utilise un protocole de distribution de labels (LDP ou RSVP-TE).
- Les paquets sont acheminés via des labels plutôt que des adresses IP.

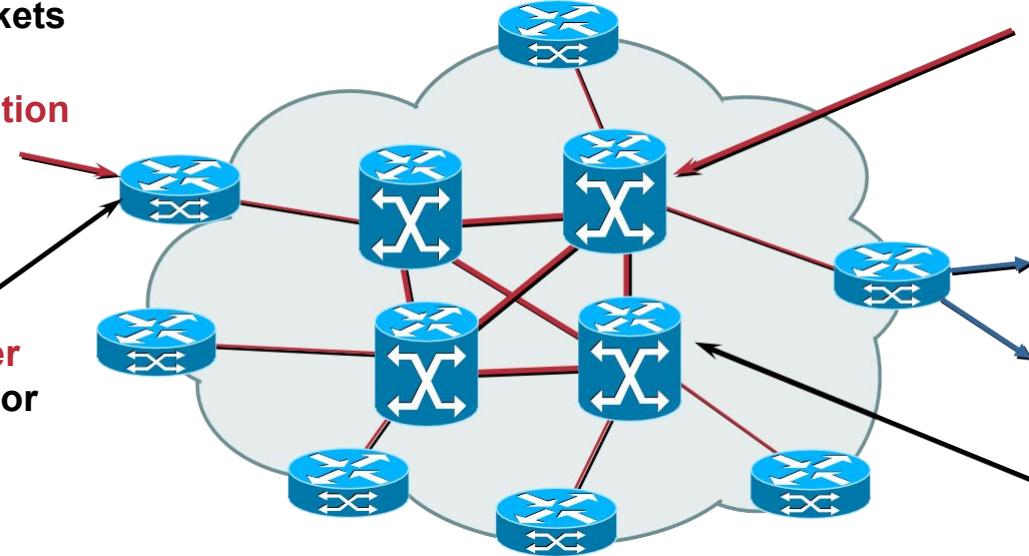
# Principe de MPLS

## At Edge:

- Classify packets
- Label them

### Label Imposition

Edge Label  
 Switch Router  
 (ATM Switch or  
 Router)



## In Core:

- Forward using labels (as opposed to IP addr)
- Label indicates service class and destination

### Label Swapping or Switching

## At Edge:

Remove Labels and  
 forward packets

### Label Disposition

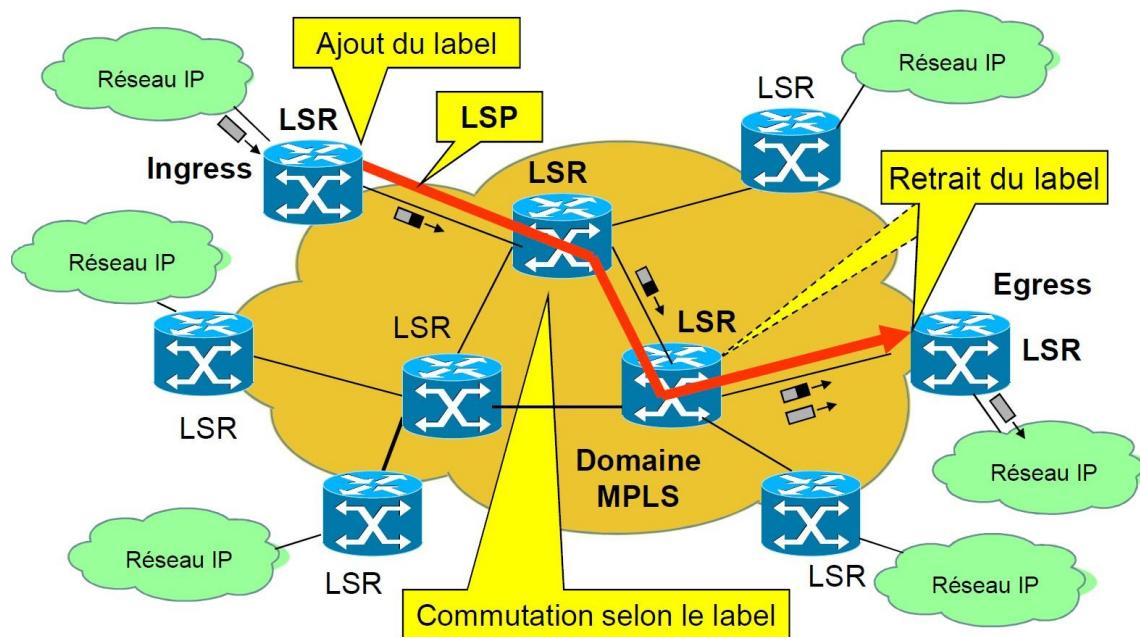
### Label Switch Router (LSR)

- Router
- ATM switch + Label Switch Controller

- Chaque paquet traversant le réseau reçoit une étiquette unique (**label**). Ce label contient toutes les informations nécessaires pour l'acheminement.
- Les équipements MPLS s'appellent des LSR (**Label Switching Routers**)
- **Label Edge Router (LER)** sont situés à la périphérie du réseau MPLS.
- Les **LSP (Label Switched Path)** définissent des chemins prédéfinis reliant les extrémités des réseaux.

# Principe de MPLS

- A l'entrée du réseau, le 1er LSR (« Ingress LSR ») analyse le paquet IP
  - Il choisit alors le LSP et insère un label devant le paquet IP
- Les équipements suivants ( les LSR du cœur de réseau) relaient le paquet en se basant seulement sur le label
- Le LSR de sortie (« Egress LSR) retire le label
  - Dans certaines implémentations, c'est l'avant dernier LSR qui retire le label
- A la sortie le paquet est routé selon le fonctionnement IP traditionnel



Le **forwarding** désigne le processus par lequel les paquets de données sont transférés d'un point à un autre dans un réseau en utilisant des **étiquettes (labels)** au lieu des adresses IP traditionnelles : Acheminement des paquets.

- 1. Assignation des labels**
- 2. Commutation basée sur les labels**
- 3. Chemin préétabli (LSP)**
- 4. Démultiplexage (Sortie du réseau MPLS)**

## Au niveau du routeur d'entrée (ingress LSR) :

- Lorsqu'un paquet de données entre dans un réseau MPLS, un **Label Edge Router (LER)** l'analyse et lui attribue une **étiquette (label)**.
- Ce label identifie le **Forwarding Equivalence Class (FEC)** du paquet
  - Les paquets appartenant à la même FEC sont acheminés de la même manière.
  - Du point de vue de l'acheminement les paquets d'une même FEC sont indistinguables.
- Le routeur **ingress LSR** encapsule un paquet IP dans un paquet MPLS

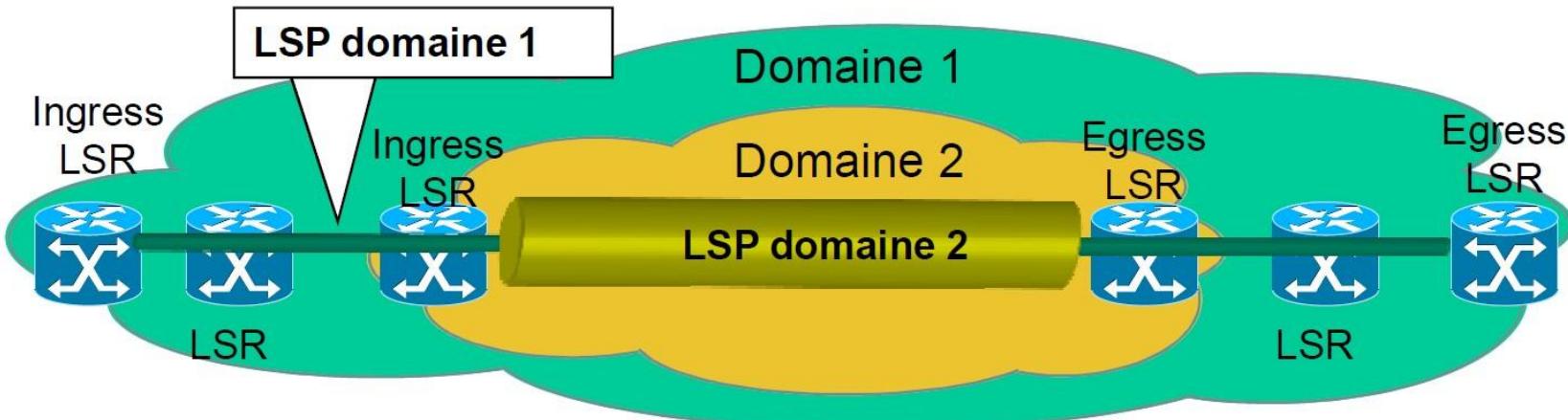
## Au niveau des routeurs intermédiaires (in the core) :

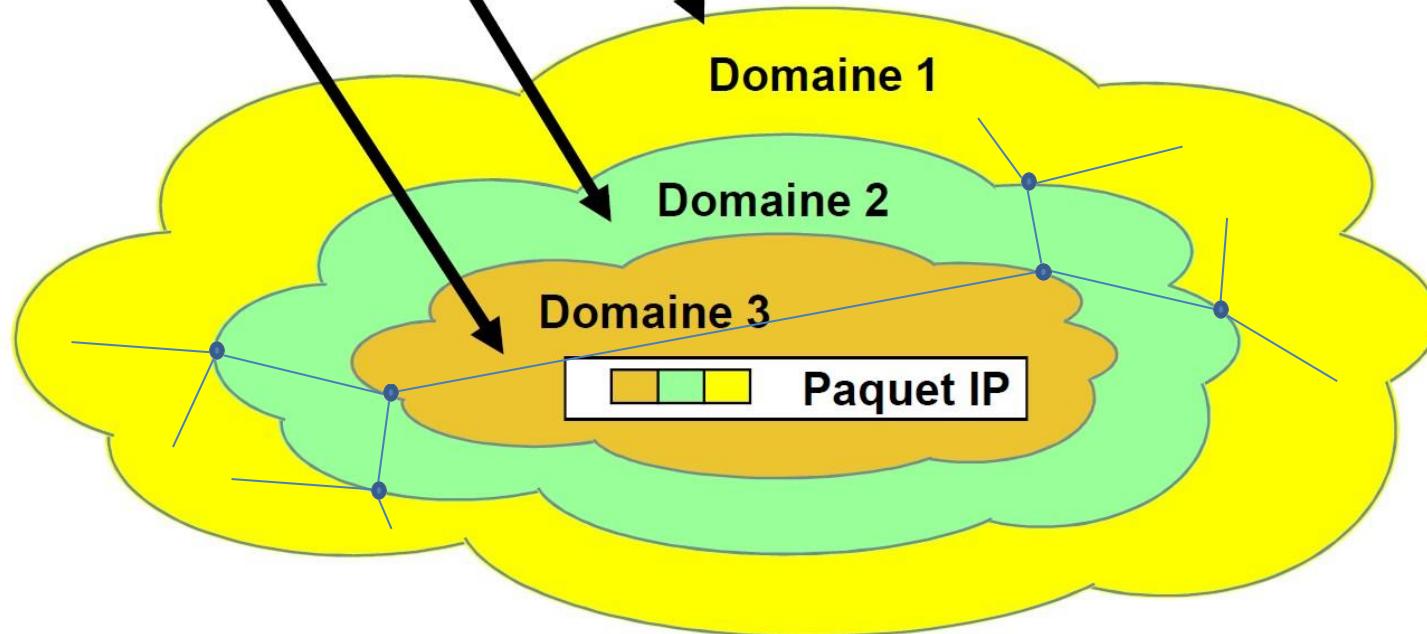
- Lorsqu'un **LSR** reçoit un paquet MPLS, il examine l'étiquette attachée au paquet. Cette étiquette contient des informations sur la classe d'équivalence de routage (**Forwarding Equivalence Class** ou **FEC**), ce qui indique comment le paquet doit être acheminé.
- Le LSR consulte sa table de routage spécifique à MPLS, appelée **LFIB (Label Forwarding Information Base)**, pour déterminer l'action à effectuer. Cette table contient des règles de correspondance qui indiquent quel label doit être remplacé par quel nouveau label et où le paquet doit être envoyé (prochain saut).
- Le LSR remplace l'étiquette existante du paquet par une nouvelle étiquette, en fonction de l'information trouvée dans la LFIB. Ce processus d'échange de label est appelé **label swapping**.
- Après avoir effectué le label swapping, le LSR transmet le paquet au prochain routeur MPLS dans le chemin prédéfini appelé **Label Switched Path (LSP)**.

## Au niveau des routeurs sortants (degress LSR) :

- **Démultiplexage** : Lorsqu'il atteint le **Label Edge Router (LER)** à la sortie du réseau MPLS, l'étiquette MPLS est supprimée et le paquet retourne à son format d'origine, c'est-à-dire un paquet IP classique. L'opération **Pop tag** permet de supprimer le label de haut de pile, alors que **Untag** supprime le dernier label.
- On retire l'en-tête MPLS pour extraire le paquet IP original qui sera ensuite routé de manière traditionnelle.
- Une fois que le paquet IP a été désencapsulé, le routeur (le LER ou un routeur classique après la sortie MPLS) consulte la FIB pour déterminer quel est le **prochain saut** (le routeur suivant ou la prochaine étape) où le paquet doit être envoyé pour atteindre sa destination finale.
- **Le saut suivant** est la prochaine étape dans le chemin réseau pour acheminer le paquet vers sa destination finale.

- **Le réseau peut être découpé en domaines administratifs**
  - Ces domaines peuvent être hiérarchisés
- **Relais entre les domaines**
  - Entre ses LSR d'extrémité, le LSP du domaine 2 sert de tunnel au LSP du domaine 1
    - Le paquet est alors précédé d'une pile de 2 labels
      - La pile peut contenir un nombre quelconque de labels
      - Similaire aux conduits ATM, mais plus de 2 niveaux de hiérarchie
    - Permet de réaliser des niveaux d'agrégation dans le cœur de réseau

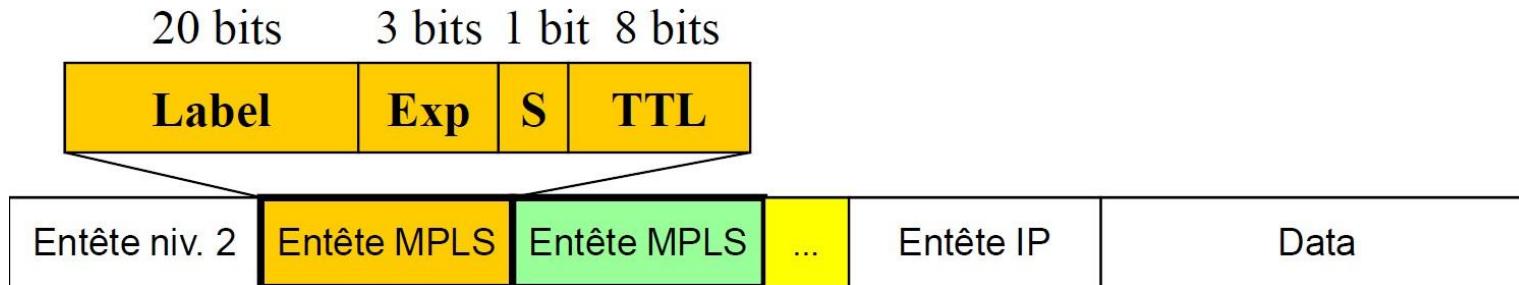




- Les domaines MPLS peuvent être hiérarchisés grâce aux piles de labels
  - Pour augmenter les performances au cœur du réseau
  - Pour permettre les interactions entre opérateurs
- Les piles de labels sont aussi utilisées pour garantir l'étanchéité des VPN

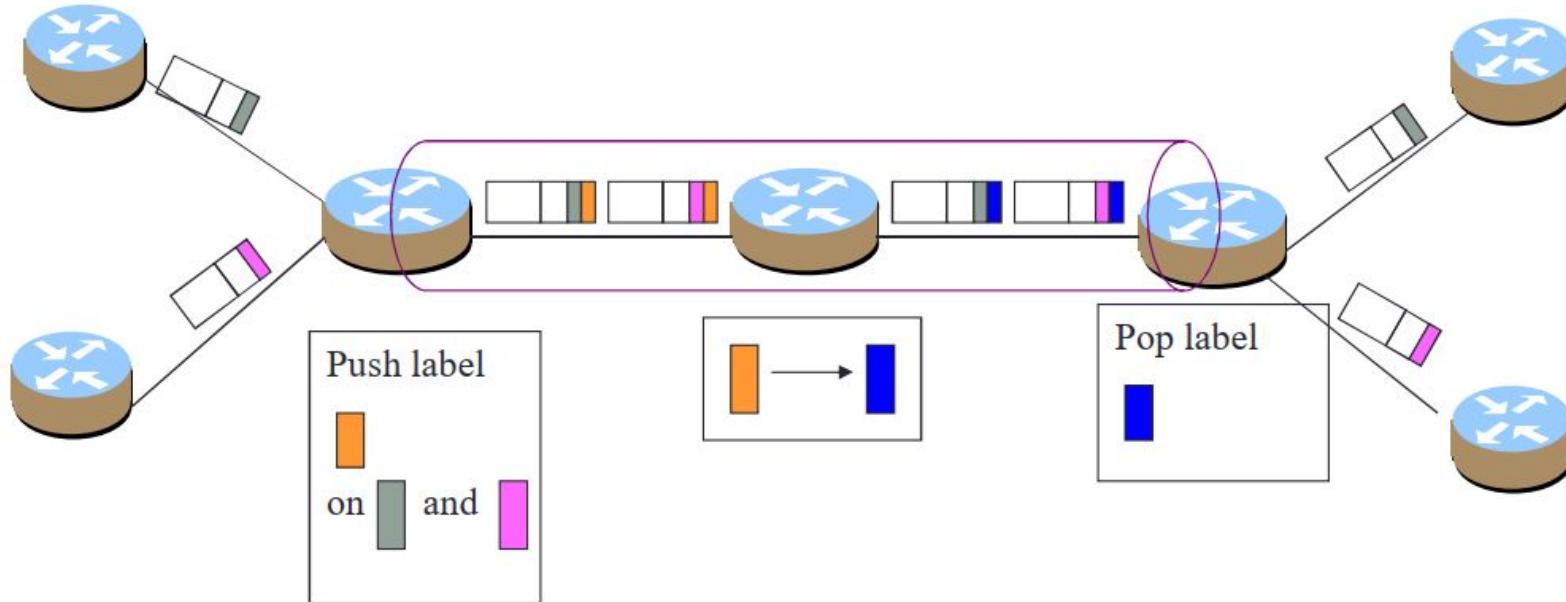
- **L'en-tête MPLS est inséré entre le niveau 2 et l'en-tête IP**
  - Label : numéro sur 20 bits (Valeurs 0 à 16 réservées)
  - S sert à gérer des labels hiérarchisés (Stack)
    - Marque le dernier label avant l'entête IP
  - Exp peut être utilisé pour traiter la QoS : files d'attente et rejet
    - Fonctionnement conforme à DiffServ
  - TTL a le même rôle que dans IP (détection de boucles)
- **Opérations sur les labels**
  - Swap (dans les LSRs), push (dans ingress LSR), pop (dans egress LSR)
- **Le label peut éventuellement être implicite**
  - Par exemple une longueur d'onde

# Structure d'une étiquette MPLS



- **Label** (20 bits) : Identifiant unique du chemin à suivre (un mot par label).
- **EXP**, Classe de service (3 bits) : Pour gérer la qualité de service (QoS).
- **S**, Bottom of Stack (1 bit) : Indique si le paquet est au bas de la pile d'étiquettes.
- **TTL**, Time To Live (8 bits) : Temps de vie du paquet pour éviter des boucles infinies.  
Le TTL est similaire à celui d'un paquet IP, utilisé pour limiter le nombre de sauts.

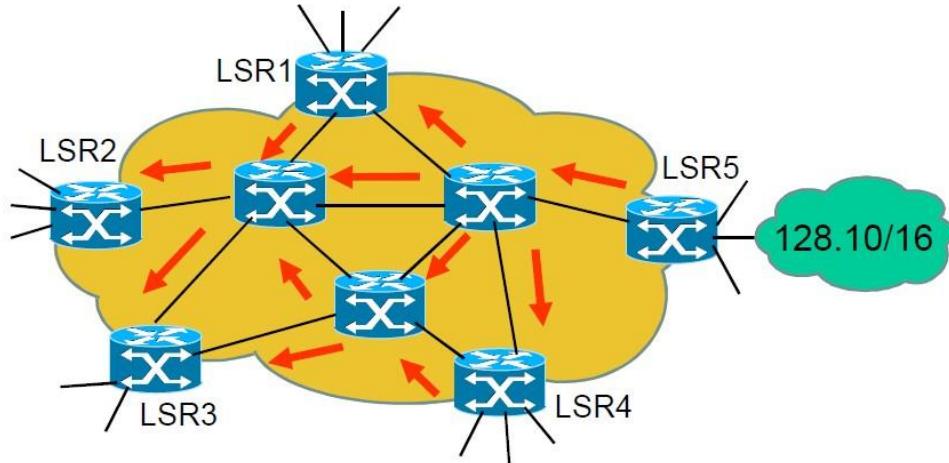
# Hiérarchie MPLS



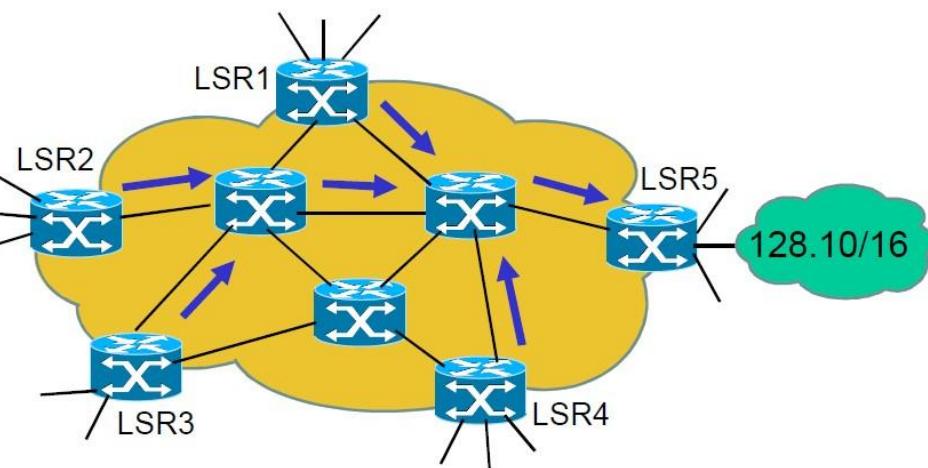
- Possibilité d'avoir une concaténation de plusieurs étiquettes
- Seule la première étiquette est prise en compte par le routeur

# Exemple de signalisation par LDP

- Le préfixe **128.10/16** est annoncé par le protocole de routage
  - Par les messages OSPF →
  - Les LSR d'entrée (LSR1, LSR2, LSR3, LSR4) apprennent l'existence du préfixe 128.10/16

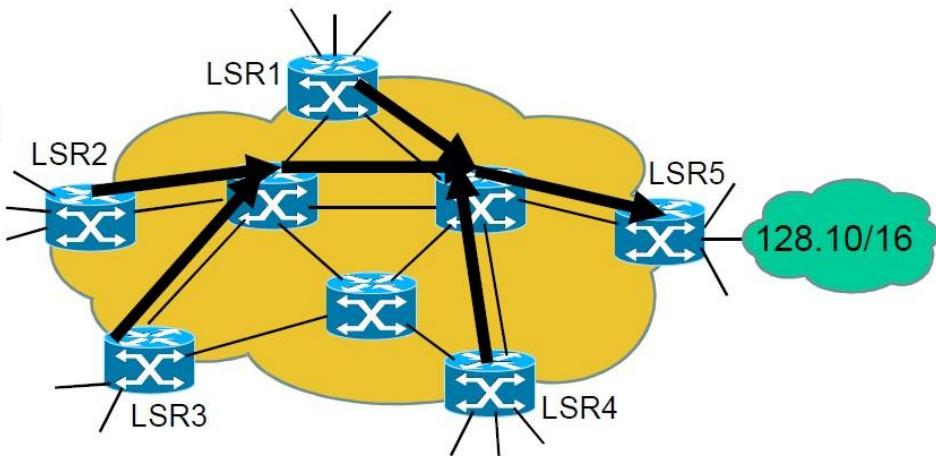
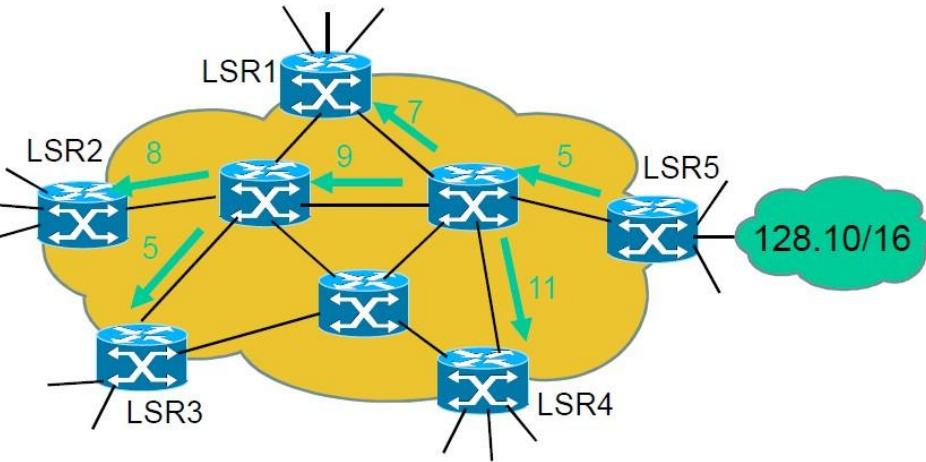


- Les LSR d'entrée (LSR1, LSR2, LSR3 et LSR4) demandent l'établissement d'un LSP vers 128.10/16
  - Par des messages *Label Request* de LDP
  - Ces messages suivent la meilleure route IP vers 128.10/16



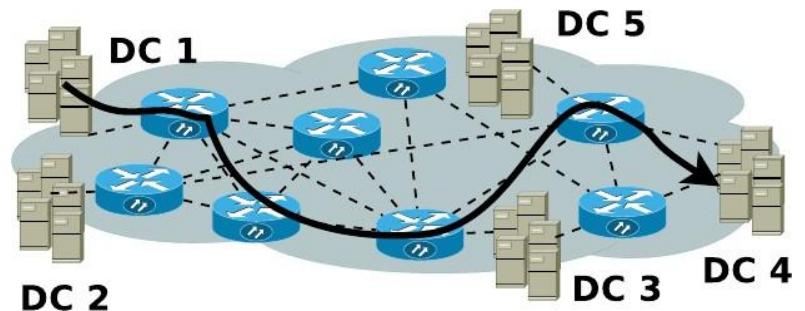
# Exemple de signalisation par LDP

- **Les labels sont attribués en commençant par l'aval**
  - En partant de l'egress LSR (LSR5), chaque LSR répond au message *Label Request* par un message *label mapping* → contenant un n° de label
  - Les Ingress LSR reçoivent leur label
- **Le LSP (multipoint à point) est établi, depuis chaque ingress LSR vers 128.10/16**



# MPLS Traffic Engineering (MPLS-TE)

- Ingénierie de trafic (TE) : processus de décision pour router/répartir le trafic à travers le réseau du SP
- Les mécanismes de TE permettent d'utiliser efficacement les ressources du réseau tout en maintenant de bonnes performances pour le trafic.
- MPLS permet de choisir entièrement le chemin suivi par le trafic, alors que TE basé sur le routage (OSPF) ne permet que d'employer le plus court chemin -> pas souvent optimal
- Le TE basé sur MPLS est le plus répandu aujourd'hui, et supporté par les fabricants majeurs tels que Cisco et Juniper.
- Tous les SP de Tier 1, et la plupart de Tier 2, 3 et 4 utilisent MPLS pour TE et pour les VPN de niveau 3 et 2.



# Algorithme MPLS-TE

- Après qu'un chemin est sélectionné, le LSP décompte la bande passante (BP) requise sur l'interface de sortie de chaque routeur du chemin. Chaque interface de sortie de routeur maintient un compteur pour sa BP courante réservable.
- **L'information de BP réservable et la base Traffic Engineering Database (TED )** est périodiquement disséminée sur le réseau (=graphe de connexions avec BP réservable sur chaque branche).
- **Priorité et préemption** : Chaque LSP est configuré avec 2 valeurs de priorité
  - La **priorité d'établissement** détermine si un nouvel LSP peut être établi en préemptant un LSP existant.
  - La **priorité de maintien** détermine dans quelle mesure un LSP existant peut garder sa réservation.

Un nouvel LSP avec une haute priorité d'établissement peut préempter un LSP existant avec une basse priorité de maintien si : (a) il n'y a pas assez de BP réservable dans le réseau; ou (b) le nouvel LSP ne peut pas être établi à moins qu'un LSP existant ne soit effacé.

# Algorithme MPLS-TE

---

- **CSPF (Constrained Shortest Path First)** : algorithme qui trie les LSP selon leurs priorités et sélectionne le plus court chemin pour chaque LSP.
  - Commence avec le LSP de plus haute priorité, élague le TED en enlevant les liens qui n'ont pas une BP réservable suffisante,
  - Assigne ensuite le chemin le plus court dans ce TED élagué au LSP et met à jour la BP réservable sur les liens affectés.
  - Ce processus se poursuit jusqu'à ce qu'il ne reste plus de LSP.
- **Ré-optimisation** : CSPF est lancé périodiquement pour ré-assigner à chaque LSP un meilleur chemin si possible

# Algorithme MPLS-TE

---

- **AutoBP** : MPLS ne contrôle pas le débit (BP) utilisé par le trafic sur un LSP : un LSP peut porter tout débit de trafic indépendamment de sa BP réservée.
  - Un mécanisme d'autoBP permet à un LSP d'ajuster sa BP réservée au débit courant.
  - Pour utiliser autoBP, un LSP a besoin de plusieurs paramètres en plus : seuil d'ajustement, intervalle d'ajustement et intervalle d'échantillonnage.
  - A chaque intervalle d'échantillonnage (ex : 5 min), un LSP mesure le débit moyen qu'il supporte. A chaque intervalle d'ajustement (ex : 15 min), il calcule le max du débit moyen mesuré sur chaque intervalle d'éch.
  - Si le max du débit utilisé diffère de la BP réservée courante de plus que le seuil d'ajustement, alors le LSP invoque CSPF avec le max du débit comme nouvelle BP à réserver.

## Avantages de MPLS TE

### 1. Meilleure utilisation de la bande passante :

- En redirigeant intelligemment le trafic vers des chemins sous-utilisés, **MPLS TE** permet de maximiser l'utilisation de la capacité réseau, évitant ainsi que certains liens soient surchargés tandis que d'autres restent inutilisés.

### 2. Optimisation des performances réseau :

- **MPLS TE** garantit que les applications critiques, comme la voix et la vidéo, disposent de la bande passante et de la qualité de service requises, tout en réduisant la latence et la congestion.

### 3. Routage flexible :

- MPLS TE permet de contourner les chemins de routage traditionnels, offrant ainsi une grande **flexibilité** dans la gestion du trafic réseau. Cela aide à éviter les zones congestionnées du réseau ou à réagir rapidement en cas de défaillance ou de panne.

### 4. Routage basé sur les contraintes :

- **MPLS TE** permet de configurer des **chemins constraints**, c'est-à-dire des chemins qui répondent à certaines exigences en matière de bande passante, de latence, ou d'autres critères, pour s'assurer que le trafic est toujours dirigé de manière optimale

## Cas d'usage de MPLS TE

### 1. Réseaux d'entreprises multisites :

- Pour les entreprises avec des bureaux répartis géographiquement, **MPLS TE** permet de garantir une **connectivité fluide** avec une bande passante suffisante pour les applications critiques, comme les systèmes VoIP ou la vidéoconférence.

### 2. Réseaux de fournisseurs de services (ISP) :

- Les fournisseurs de services peuvent utiliser **MPLS TE** pour offrir à leurs clients des **niveaux de service différenciés (SLA)** en fonction des besoins spécifiques de bande passante, de priorité et de qualité de service.

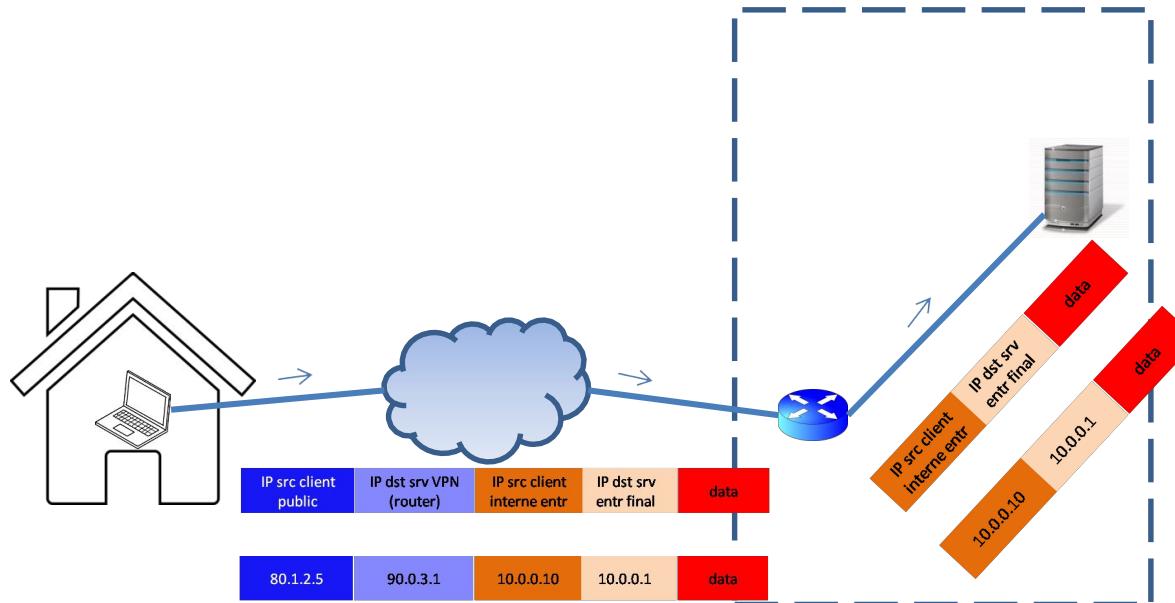
### 3. Optimisation du trafic réseau :

- Dans les environnements où la **congestion réseau** est un problème courant, **MPLS TE** peut redirige intelligemment le trafic pour **équilibrer la charge** et éviter les surcharges.

# MPLS VPN

# Principe des VPNs

Le **tunneling** est un concept clé dans la création de réseaux privés virtuels (**VPN**, Virtual Private Network). Il permet de **transporter des données privées** de manière sécurisée à travers un réseau public, tel que l'Internet, en **encapsulant des paquets de données** dans un autre protocole, formant ainsi un "tunnel". Ce tunnel protège les données lors de leur transit, garantissant confidentialité et sécurité.



- > Le client peut faire les mêmes opérations que s'il était dans les locaux de l'entreprise.
- > Les ISPs n'ont pas (et ne peuvent pas si IPSec) à lire le paquet destiné au réseau d'entreprise (@IP privées utilisables).
- > Les ISPs traitent le paquet entreprise comme un payload de couche 4 normal.

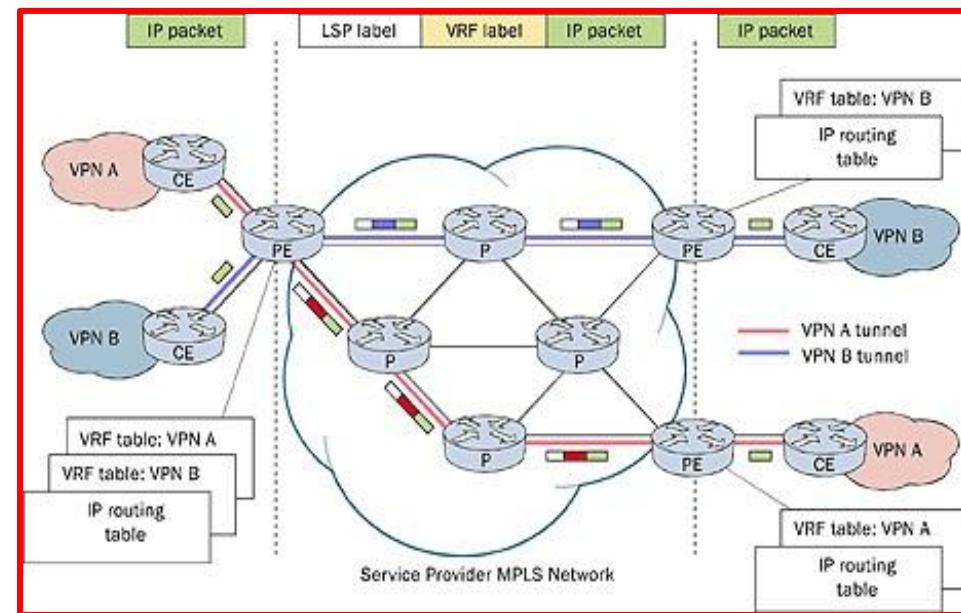
# Types de VPN basés MPLS

---

- MPLS permet le support des **VPNs multipoints**: service fournis par les ISPs aux entreprises pour interconnecter plusieurs LANs distants comme si elles possédaient un routeur ou switch dédié:  
  
**L3VPN (Layer 3 VPN)** : le fournisseur de services gère non seulement l'infrastructure MPLS, mais également le routage IP entre les sites de l'entreprise. Les **routeurs MPLS** du fournisseur distribuent des routes à chaque site client, ce qui simplifie la gestion pour l'entreprise.  
L'entreprise voit le réseau de l'opérateur comme un routeur qui lui appartient
- **L2VPN (Layer 2 VPN)** : MPLS est utilisé pour fournir un lien entre les réseaux locaux (LAN) des différents sites, mais l'entreprise gère elle-même le routage IP. Cela permet une plus grande flexibilité, mais nécessite une plus grande gestion réseau côté client. L'entreprise voit le réseau de l'opérateur comme un switch qui lui appartient

# Principe de fonctionnement : la séparation des tables de routage ou d'adressage

- Pour la confidentialité entre VPNs: les sites clients (leurs tables) interconnectés par des LSP MPLS différents
- La table dépend du type de VPN:
  - L3 VPN : les tables contiennent les préfixes IP et s'appellent Virtual Routing and Forwarding Tables (VRF). Les VRFs sont simplement des tables de routage dédiées.
  - L2 VPN : Virtual Forwarding Tables (VFT), contiennent les adresses de couches 2, ou les DLCI de FR, etc...
  - VPLS : contiennent les adresses MAC Ethernet, et les VLAN IDs si VLAN, mappées aux LSPs menant aux autres sites. Même rôle que les MAC tables dans les switches Ethernet.



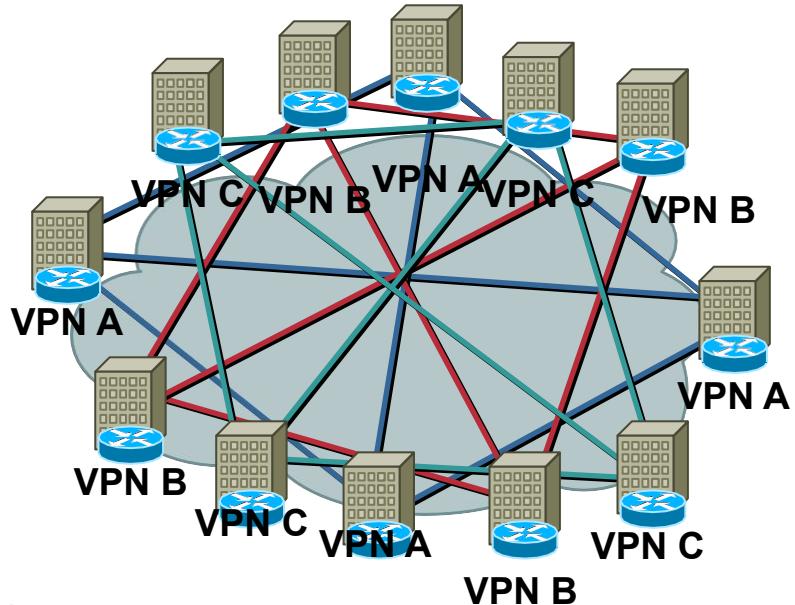
- **Service sans connection** : Internet doit son succès à la techno TCP/IP basique: pas d'action nécessaire avant la communication entre 2 hôtes. Un VPN basé MPLS supprime le besoin du d'encryption pour assurer la confidentialité, donc beaucoup moins de complexité.
- **Passage à l'échelle** : seuls les routeurs PE mémorisent les routes des VPN qu'ils gèrent. Les routeurs P non. Donc pas d'augmentation de complexité dans le coeur du réseau avec l'augmentation de clients.
- **Sécurité** : Les paquets d'un VPN ne peuvent pas par erreur aller dans un autre VPN:
  - Sur le bord, assure que les paquets d'un client sont placés dans le bon VPN.
  - Dans le coeur, le trafic des VPN reste séparé. Le spoofing (essai d'avoir accès à un routeur PE) est quasi- impossible car les paquets reçus des clients sont IP. Ces paquets IP doivent être reçus sur une interface ou sous-interface particulière attachée à un seul label VPN.

# Les avantages des VPN basés MPLS

---

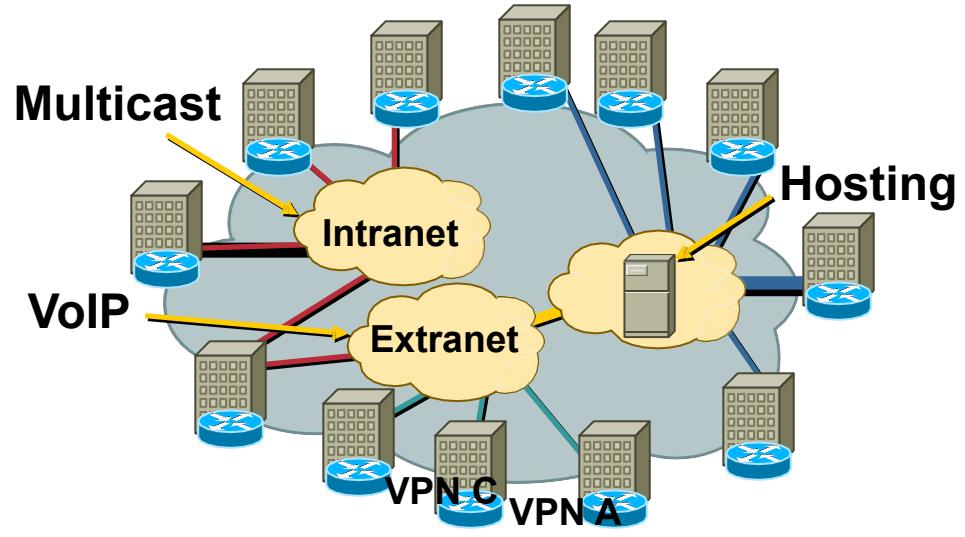
- **Adressage flexible** : beaucoup de clients utilisent des plages d'adresses privées, et ne veulent pas les convertir en public (temps et argent). Les VPN MPLS permettent à ces clients de continuer à utiliser ces adresses privées sans besoin de NAT.
- **Qualité de service** : MPLS permet d'assurer la qualité de service pour des applications critiques comme la voix (VoIP) ou la vidéo, avec une faible latence et une faible perte de paquets. Permet de satisfaire 2 contraintes importantes pour les VPN:
  - Performance prédictible et implémentation de politiques pour SLA
  - Supporte plusieurs niveaux de service dans un VPN MPLSLe trafic est classifié et labellisé au bord pour être traité de façon différenciée selon les classes (avec différents délais ou proba d'abandon par exemple).
- **Optimisation des performances** : Les paquets sont acheminés rapidement et efficacement grâce aux labels MPLS.

# Fonctionnement du VPN



**Overlay VPN**

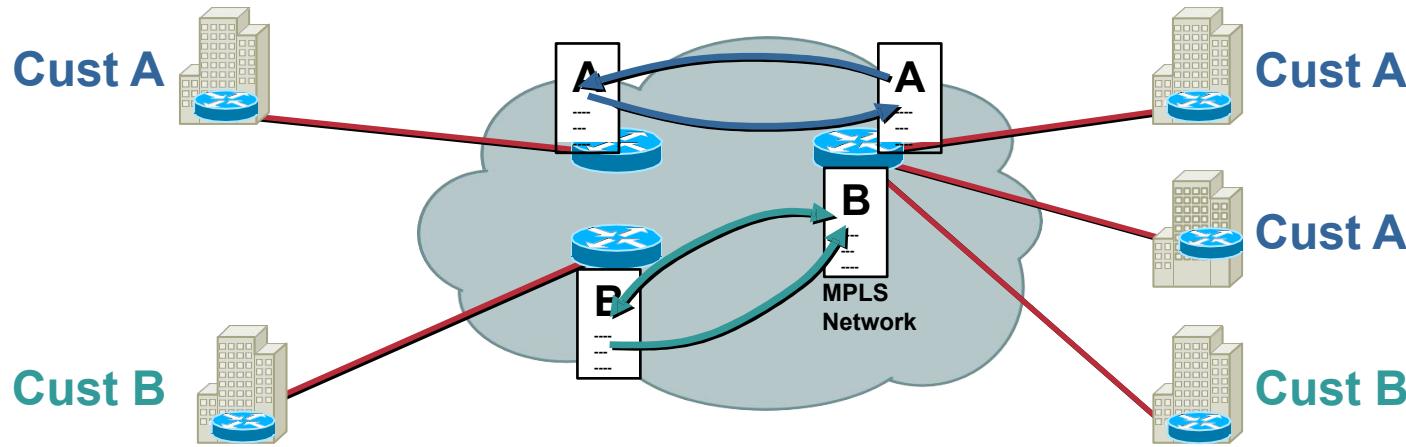
- Les coûts augmentent de façon exponentielle.
- Dépendant du transport
- Regroupe les points de terminaison, pas les groupes
- Overlay complexe avec QoS, tunnels, et IP



**MPLS based VPN**

- Permet l'hébergement de contenu à l'intérieur du réseau.
- Courbe des coûts stable
- Indépendant du transport
- Regroupement facile des utilisateurs et des services
- Permet la QoS à l'intérieur des VPN

# Utilisation des labels pour IP VPN



Un **VPN MPLS** combine la capacité de routage optimisé de MPLS avec la sécurisation des connexions qu'offre un VPN. Cette solution est principalement utilisée par les entreprises pour **connecter plusieurs sites distants** ou des **filiales** à leur siège principal sur un réseau privé, tout en profitant des performances élevées et de la qualité de service offerte par MPLS.

Les **paquets de données** circulent à travers un réseau MPLS, où chaque paquet se voit attribuer un **label**. Ce label détermine comment le paquet sera acheminé à travers le réseau.

MPLS fournit une connectivité de type VPN sans utiliser de **tunnels chiffrés** comme dans les VPN traditionnels (par exemple, ceux basés sur IPSec). Cependant, le réseau reste **isolé** du reste du trafic Internet, créant ainsi un environnement sécurisé.