

# CoS et QoS

Intserv – Diffserv, MPLS, RSVP,  
LDP, CR-LDP, VPN

# Cause: (r)évolution de l'internet

- Traditionnellement, les applications ne tournaient pas en temps réel (ftp, mail, telnet ...)
- De plus en plus, les applications requièrent temps réel: voix, vidéo
- Les entreprises ne peuvent plus se passer d'un service essentiel et assurant une certaine qualité et confidentialité.

# Définitions – Flux – Délai – Jitter

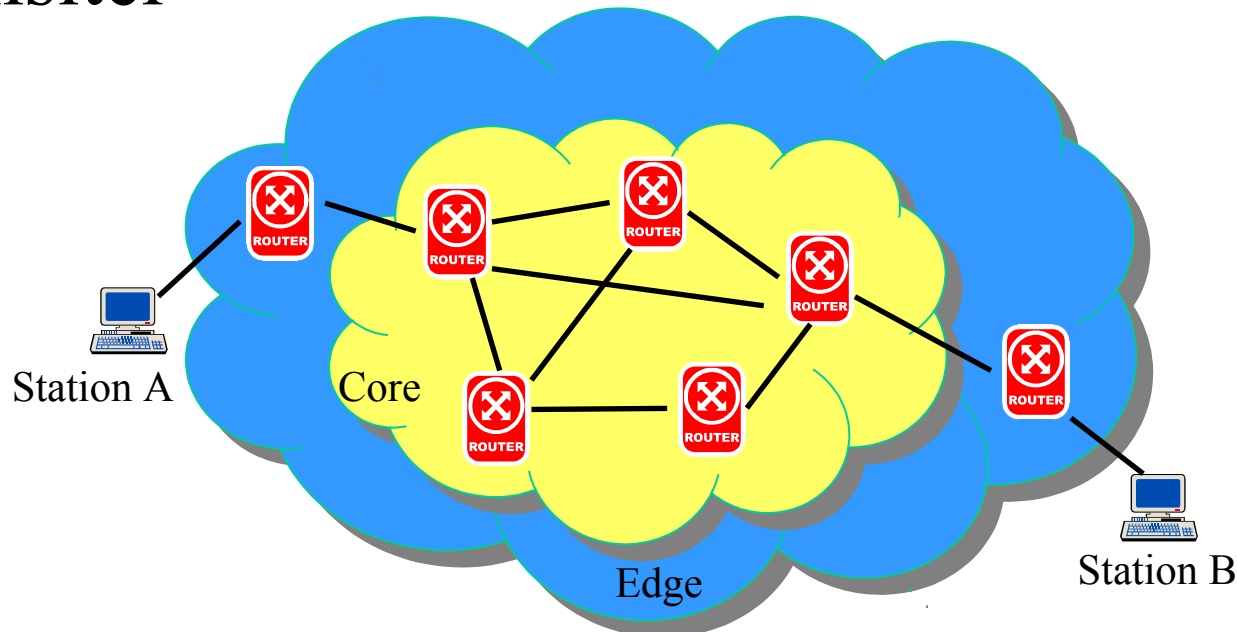
- Flux: Ensemble de paquets définis par:
  - Adresse IP destination
  - Adresse IP source
  - Port TCP / UDP destination
  - Port TCP / UDP source
  - Protocole de transport (UDP / TCP)
- Délai (delay) introduit par un device: temps mis par un paquet entre le moment où le premier bit entre dans le device et le moment où le dernier bit sort du device
- Jitter introduit par un device: différence de temps entre l'intervalle séparant deux paquets avant et après leur passage dans le device

# Définitions – PHB

- PHB: Per Hop Behavior. Définition du traitement que vont subir les paquets qui transittent par un device. Un PHB peut inclure:
  - Policing / Shaping
  - (Re-)Marking
  - Queue Drop criteria
  - Queue Scheduling
  - Dropping
  - (Re-)Directing

# Définitions – Core – Edge

- Edge: endroit où l'utilisateur arrive dans le réseau
- Core: endroit du réseau où les utilisateurs n'arrivent pas, leurs paquets ne font qu'y transiter



# QoS et CoS – Introduction

- IP est par nature ‘Best Effort’
- Initialement, l’Internet est prévu pour interconnecter des scientifiques
- Aujourd’hui, et de plus en plus, des sociétés commerciales
- « IP Telephony is the killer application »
- Stream (vidéo (sensible au délai), téléphonie (sensible au jitter)) vs Burst (data)
- QoS peut être au niveau 2 ou au niveau 3

# QoS – Détails

- Quality of Service: capacité d'un élément du réseau à assurer un certain niveau de qualité en terme de délai, de débit, de bande passante...
- Limité par
  - Le point le moins performant du chemin emprunté par le flux
  - L'état du réseau à ce moment-là
- Deux possibilités, éventuellement combinées:
  - Réservation de ressources (Intserv, RSVP)
  - Prioritisation (Diffserv)

# QoS – Implications

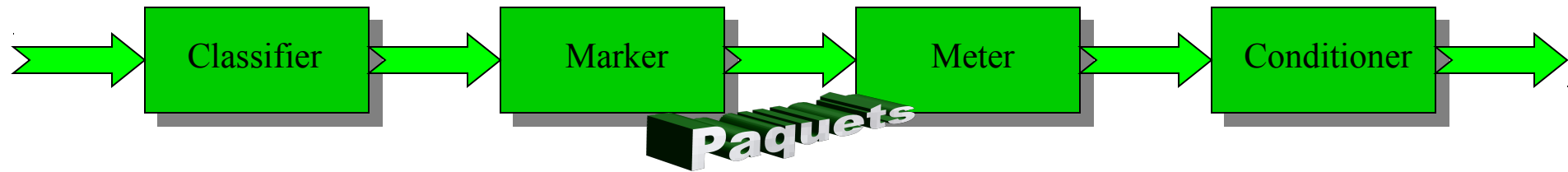
- Configuration manuelle
- Policy management: COPS (Common Open Policy Service) est un protocole de gestion de police distribuée. Il s'agit de traiter certains paquets différemment en fonction de certaines de leurs caractéristiques, et de centraliser cette gestion sur une machine qui joue le rôle de centre de décision
- Authentication: basé sur des certificats gérés par une autorité centralisée conférant des droits (cf carte de crédit)
- Accounting / Billing: indispensable pour la facturation



# CoS – Détails

- Class of Service
- Le trafic est réparti en classes afin de le traiter en fonction de différentes priorités, décidées par
  - Le router manager (config. Manuelle, Diffserv)
  - Le COPS server (COPS)

# Flux: conditionnement



- Classifier: décision de la classe à laquelle le trafic appartient et donc un PHB
- Marker: marquage des paquets
- Meter: mesure, à intervalles réguliers, de la quantité de trafic
- Conditioner: mise en forme du trafic

# IntServ

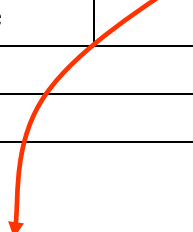
- Integrated Services
- Idée: établir des flux de bout en bout et leur réserver, le long du chemin sélectionné, des ressources (bande passante, priorité...)
- Problème: nombre de flux traversant un routeur peut être très (trop) important
- Deux type de services:
  - Contrôlé
  - Garanti

# DiffServ

- Differentiated Services
- Marquage en classes (fait à l'edge):
  - Expedited Forwarding (EF)
  - Assured Forwarding (AF)
  - Default behavior; best Effort (DE)

# DiffServ – Fonctionnement

|                     |     |                 |                 |  |
|---------------------|-----|-----------------|-----------------|--|
| Version             | IHL | Type of Service | Total length    |  |
| Identification      |     | Flags           | Fragment Offset |  |
| Time To Live        |     | Protocol ID     | Header Checksum |  |
| Source Address      |     |                 |                 |  |
| Destination Address |     |                 |                 |  |



|      |   |   |   |   |   |    |   |
|------|---|---|---|---|---|----|---|
| 1    | 2 | 3 | 4 | 5 | 6 | 7  | 8 |
| DSCP |   |   |   |   |   | CU |   |

CU: Inutilisés (définis récemment dans la RFC 3168, sep 01, pour le contrôle de flux)

DSCP: DiffServ Code Point

Selon la RFC 2474 (sep 98), les bits 4, 5 et 6 doivent être à 0, les trois premiers indiquant le ‘class selector’ (pour correspondre à la RFC 1349, voir le champ ToS).

# DiffServ – Les classes

- Pour la classe AF, il y a 4 classes prédéfinies, chacune ayant 3 niveaux de ‘drop precedence’

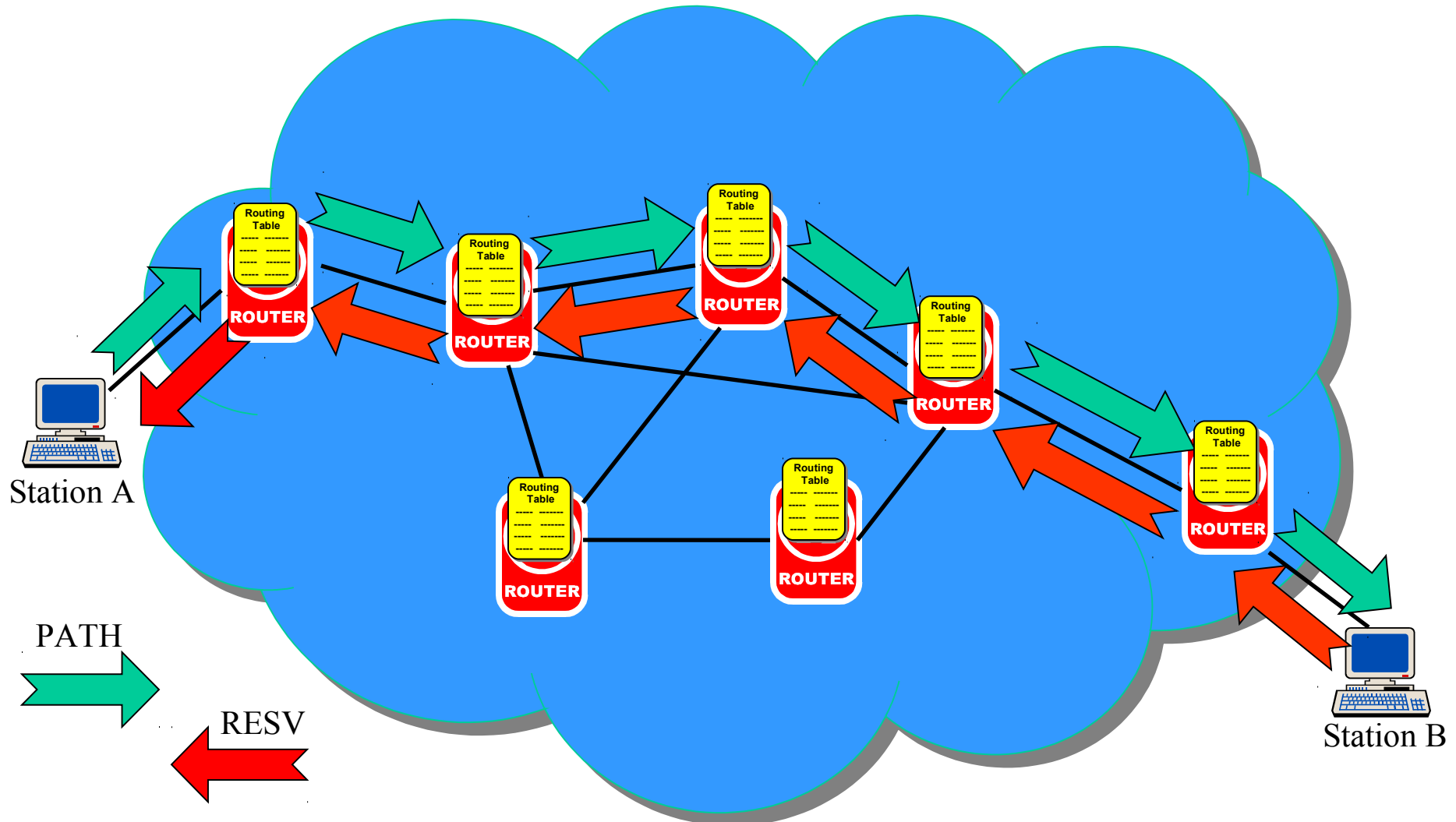
| Précédence  | Class 1 | Class 2 | Class 3 | Class 4 |
|-------------|---------|---------|---------|---------|
| Low drop    | 001 010 | 010 010 | 011 010 | 100 010 |
| Medium drop | 001 100 | 010 100 | 011 100 | 100 100 |
| High drop   | 001 110 | 010 110 | 011 110 | 100 110 |

- La classe EF garantit une latence faible, un jitter faible, une bande passante et des pertes faibles. Elle apparaît comme une ligne louée et utilise le DSCP « 101 110 ». C’est le service ‘premium’, le plus cher !

# RSVP

- Resource reSerVation Protocol
- Protocol à état (nécessite un keepalive régulier)
- Peut définir une QoS
- Sert à réserver des ressources au sein du réseau
- Reprend l'idée de IntServ

# RSVP – Réserve d'un chemin

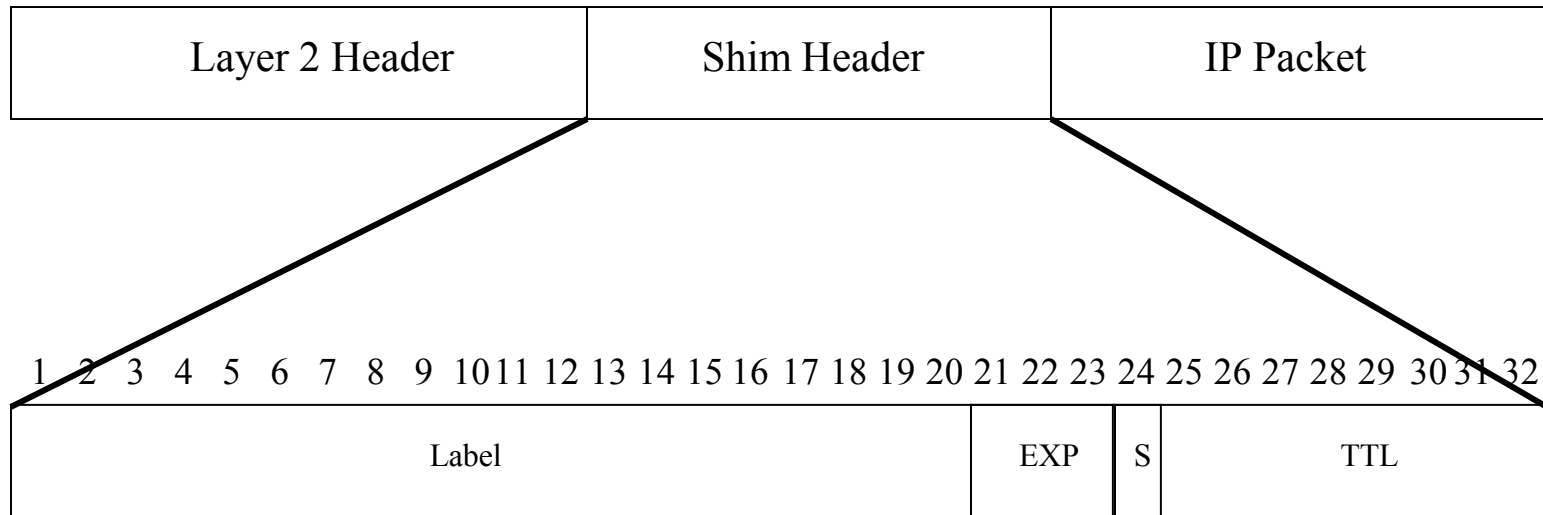




# MPLS

- Multi Protocol Label Switching
- Idée de base: switcher plutôt que router (vitesse)
- Shim header, MPLS label de 20 bits
- Création de LSP (donc, il y a un état dans le réseau, pas comme en IP...). Création – utilisation – fin d'utilisation...
- LSR (Label Switch Router) vs LER (Label Edge Router)
- Pas lié à IP (Multi Protocol)
- Possibilités de TE
- Marquage à l'Ingress et démarquage à l'Egress par paquet !

# MPLS – Shim header

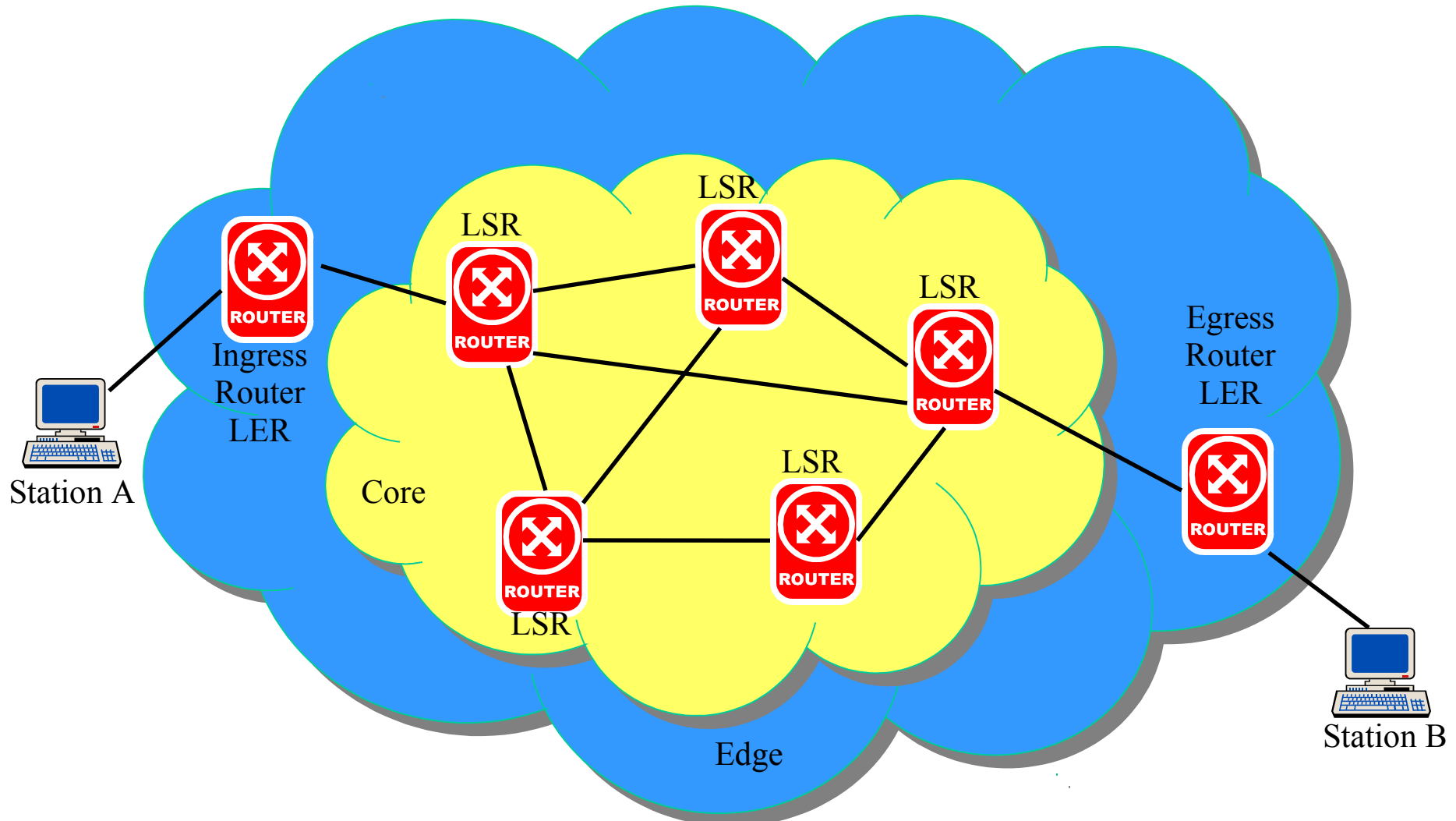


- Label: 20 bits: identifiant pour le switching
- Exp: 3 bits: experimental bits, utilisé pour QoS
- S: 1 bit: Stack (MPLS dans MPLS, ou VPN)
- TTL: 8 bits: Time to live

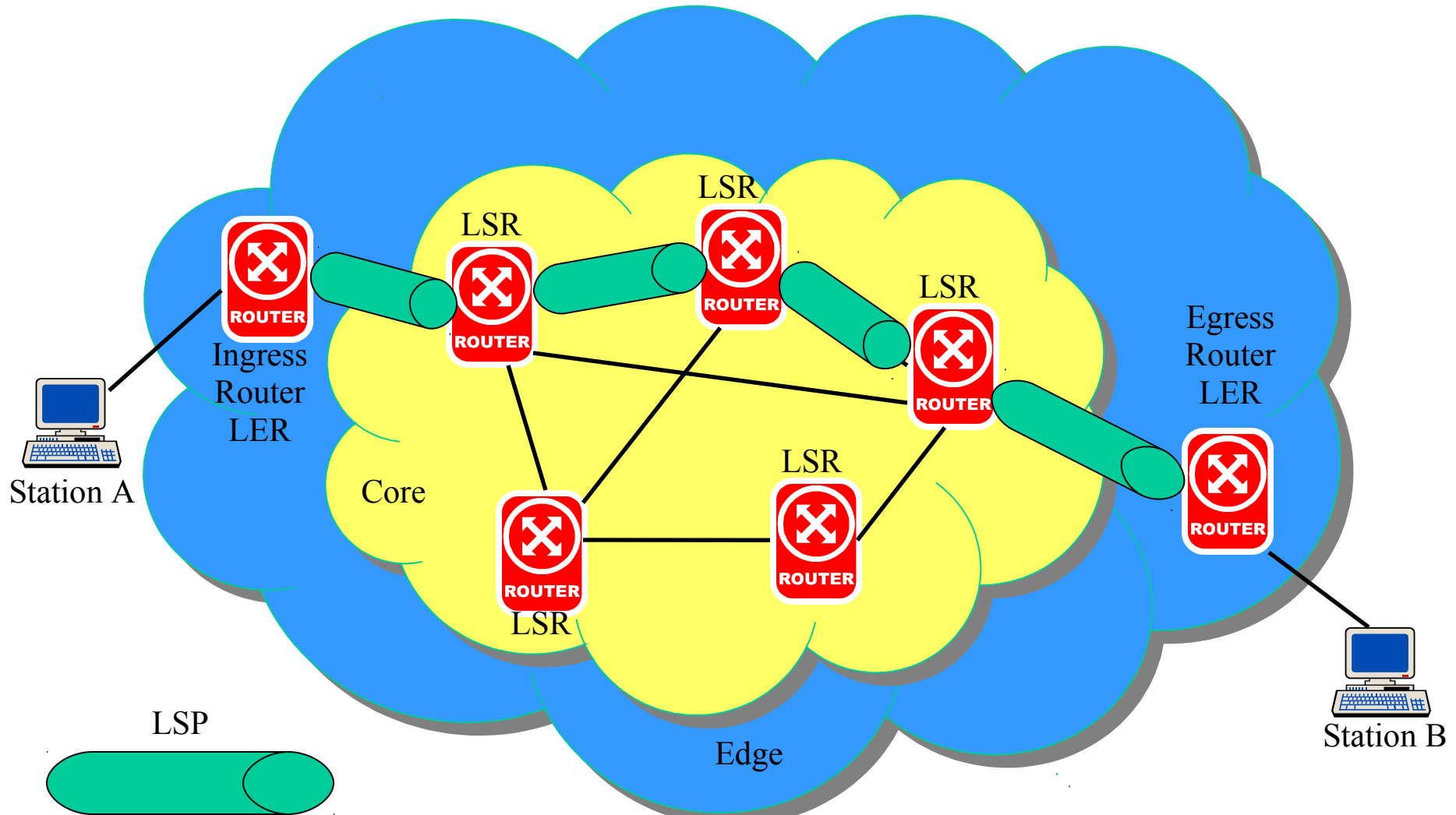
# MPLS – Opérations

- Trois opérations possibles:
  - PUSH: ajoute un label
  - SWAP: échange un label
  - POP: retire un label
- LSP établis soit manuellement soit par signaling
- LSP unidirectionnels !
- LSP peut être vu comme un tunnel
- LSP peut être point à point ou faire du ‘merging’ (gain de labels)

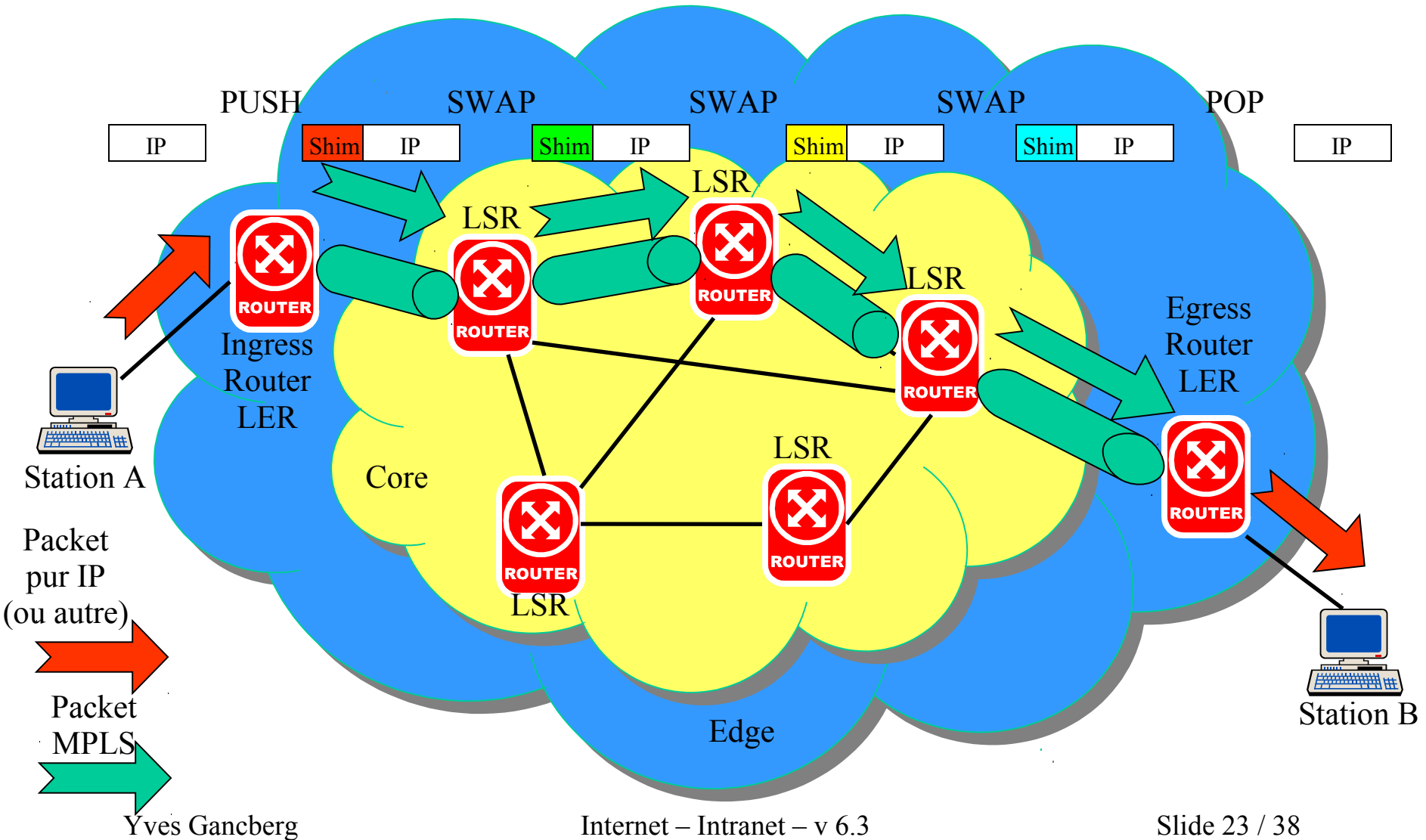
# MPLS – Exemple



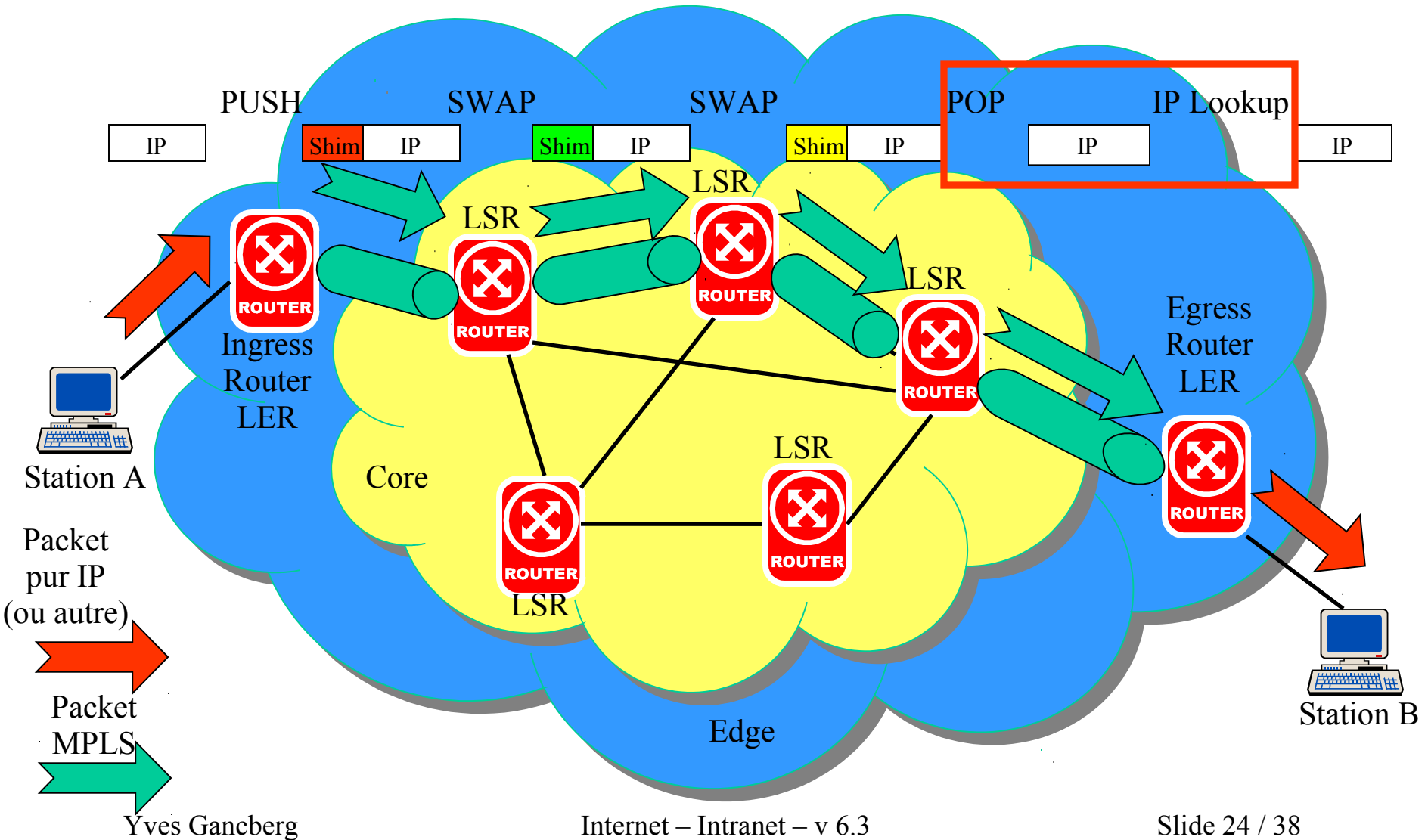
# MPLS – Fonctionnement



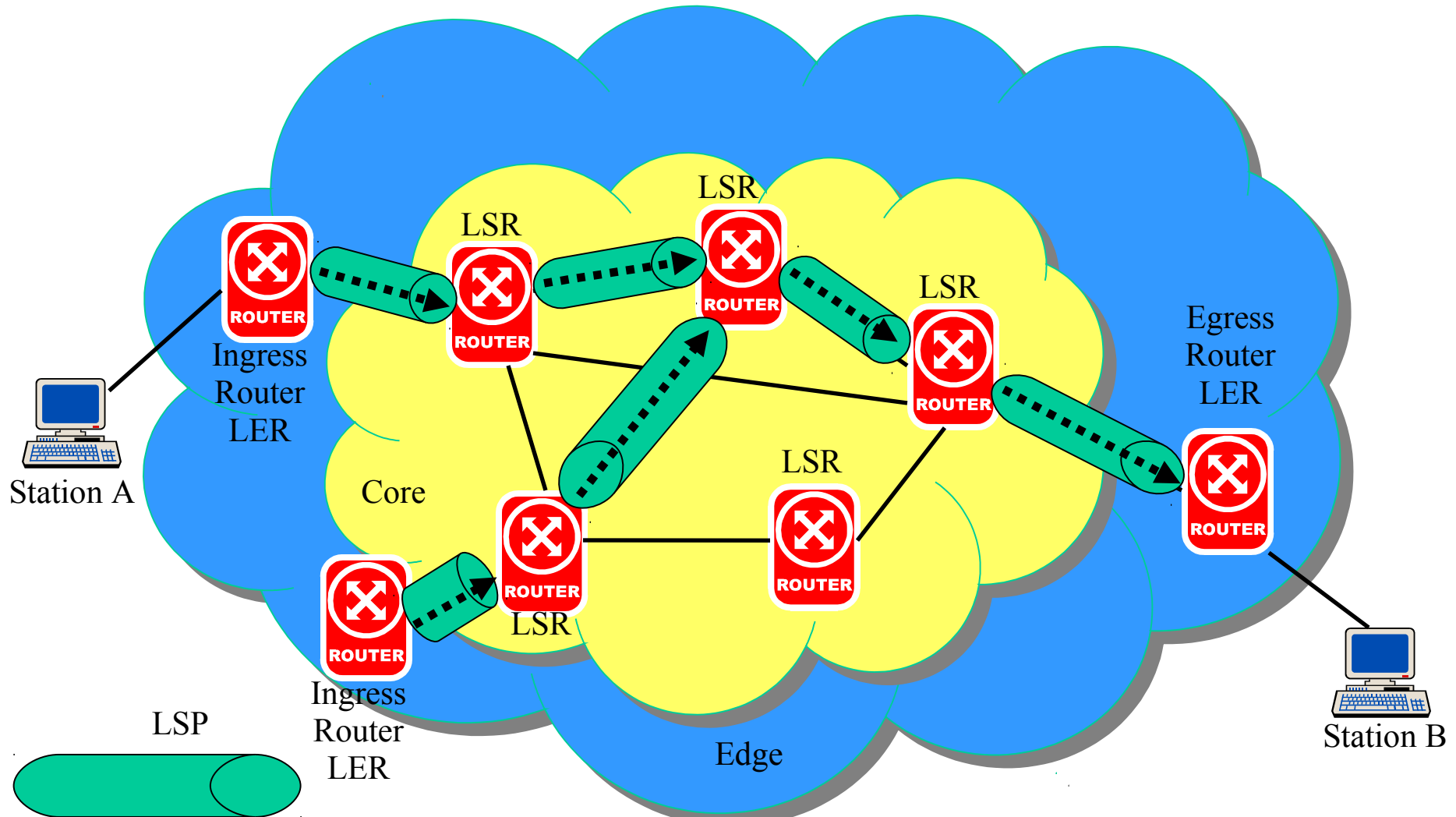
# MPLS – Parcours d'un paquet



# MPLS – PHP



# MPLS –Merging





# MPLS - Applications

- TE !
- Contraintes sur un circuit en IP (ATM vs IP): QoS
- VPN
- (Performances)
- Peut servir à remplacer iBGP dans le core (mais pas forcément)
- (Possibilité de transporter n'importe quel protocole dans l'Internet)

# LDP

- Label Distribution Protocol (générique ou protocole particulier) (RFC 3036)
- Sert à distribuer automatiquement les labels dans le réseau (et donc créer des LSP)
- Permet de simplifier considérablement la configuration
- Permet de faire du Merging de LSP
- Pas de spécifications de bande passante ou d'autres paramètres de trafic
- Utile dans le cas de:
  - Réduction de la taille des tables de routage
  - VPN tunnels !
- TCP port 646

# LDP – Fonctionnement

- Le mode de distribution des labels:
  - Downstream on demand
  - Downstream unsolicited
- Le mode de gestion des labels:
  - Libéral (permet de conserver des informations dont on n'a pas directement besoin, mais plus rapide en cas de ré-établissement de LSP)
  - Conservatif (plus économe en mémoire et en processing, mais nécessite plus de temps en cas de problème sur le LSP)
- Le mode de contrôle:
  - Ordonné
  - Indépendant

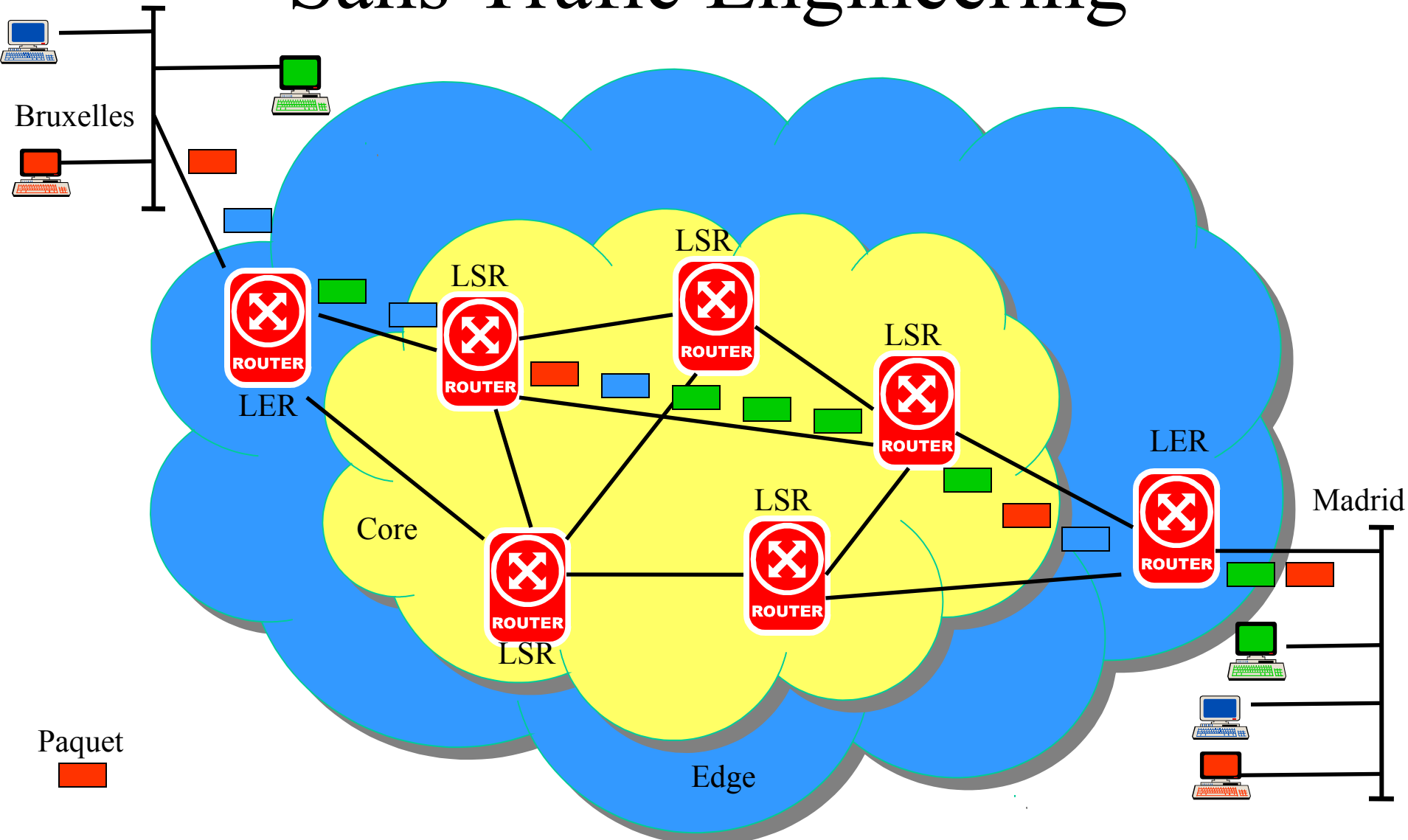
# Notion de FEC

- Forwarding Equivalent Class
- Une FEC est un ensemble de paquets qui seront forwardés de la même manière par le routeur
- Cela peut être vu comme l'ensemble des paquets ayant la même adresse de destination (point de vue routage). C'est l'adresse du routeur où le LSP s'arrête !

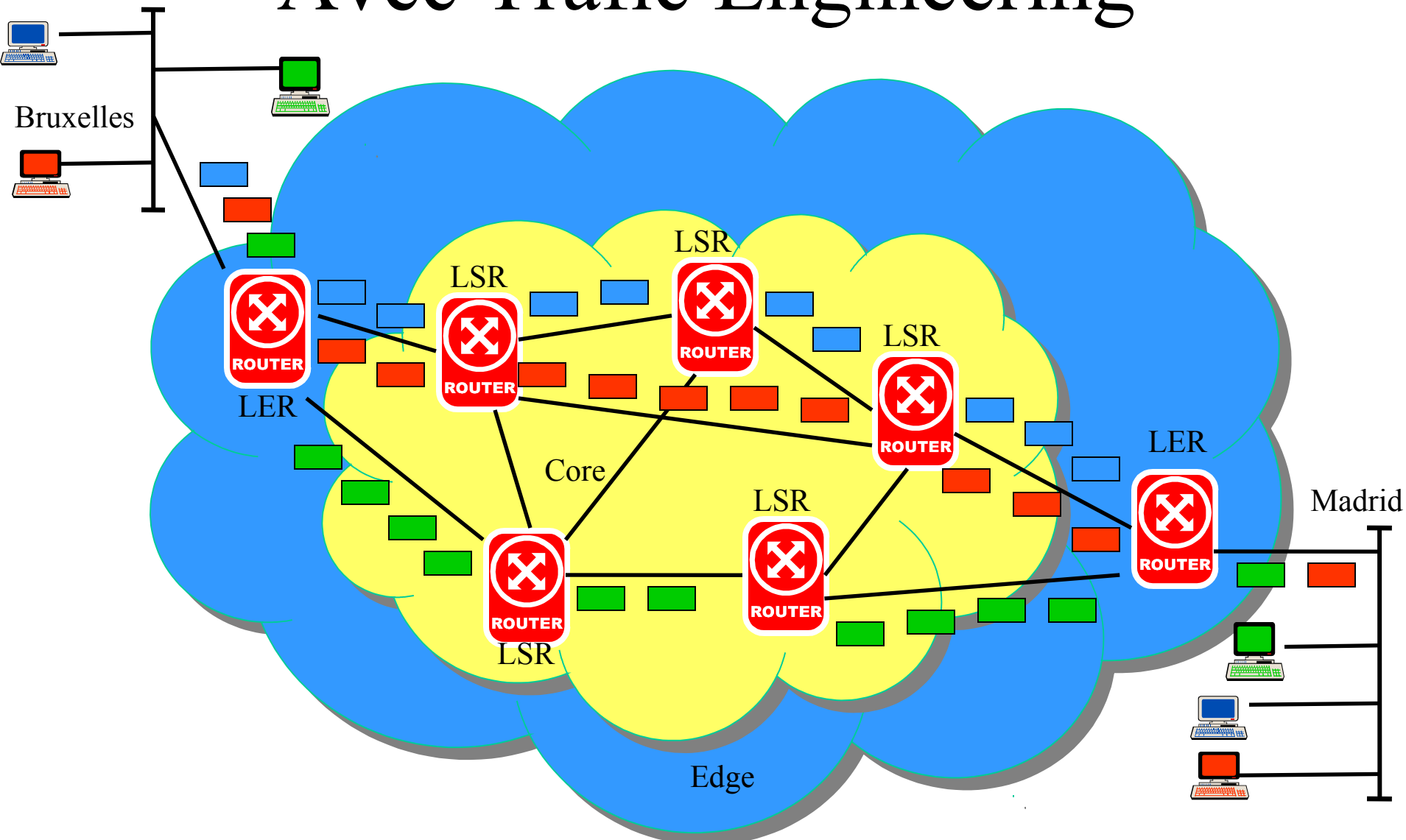
# Traffic Engineering – Protocoles

- Extensions des IGP (OSPF, IS-IS) et de l'EGP (BGP) pour supporter des fonctionnalités de TE
- But: mieux contrôler le trafic (moins se baser sur les protocoles de routage classiques)
- CR – LDP : Constraint-based Routing – LDP
- RSVP – TE : RSVP – Traffic Engineering

# Sans Traffic Engineering



# Avec Traffic Engineering



# VPN

- Virtual Private Network
- Offre une sécurité et une privacité, bien que basé sur des réseaux publics ! C'est le concept même des VLANs !
- Mode et finance (amorti en 2 mois...)
- Protocoles de tunneling peuvent être impliqués (PPTP, L2TP (L2F !), IPSec...)
- Il existe des VPN de niveau 2 et de niveau 3



# VPN – Points essentiels

- Sécurité
  - se passe généralement dans un réseau public... Internet.
  - encryption
- Performance
  - L'edge peut faire du trafic shaping ou du policing
- Gestion et administration
  - Indispensable et compliqué par les demandes de plus en plus strictes en termes de souplesse et de sécurité

# VPN – Différentes vues

- X25: CUG
- FR: DLCI
- ATM: PVC
- Firewall: Extension du domaine protégé par le FW
- Routeur: MPLS LSP

# VPN: 2 types

- Level 2 VPN
  - Fournis par l'ISP
  - Le routage est fait par l'ISP
  - Identique à un ensemble de lignes louées (donc niveau 2)
  - Peut être basé sur des ATM ou des FR PVCs
- Level 3 VPN
  - ISP pas concerné
  - Basés sur des tunnels
  - L'encryptage et le routage sont faits par le client (!) (donc niveau 3)
  - Protocoles de tunneling (PPTP, L2TP, IPSec, GRE...), encapsulation d'IP dans IP, récemment BGP / MPLS LSP

# RFC 2547 bis

- Implémente un VPN sur base d'un full mesh (bidirectionnel) de LSP entre les différents PoPs (donc basé sur MPLS)
- L2 VPN
- Obligation de supporter LDP
- Aussi appelé BGP/MPLS VPN
- Notion de VRF (Virtual Routing and Forwarding instance)

# RFC 2547 bis

Full mesh bidirectionnel de LSP !

