Les VPN MPLS

B. DAVENEL

Ingénieurs 2000, Université Paris-Est Marne la Vallée

Sommaire

Bibliographie

- PUJOLLE, Guy. *Les réseaux, Quatrième édition*, Eyrolles
- HARDY, Daniel. MALLEUS, Guy. MEREUR Jean-Noël. *Réseaux : Internet, téléphonie, multimédia*, De Boeck
- `http://www.frameip.com/mpls`
- `http://www.frameip.com/vpn`
- `http://www.cisco.com`

Sommaire

Les réseaux d'entreprise

ATM

- Commutation de cellules
- Etablissement de circuits virtuels (manuel / automatique)
- Chemins qui ne varient pas au cours du temps
- Multiplexage des flux de données pour atteindre des débits importants
- Haut débit jusqu'à 2,4 GBits/s

Avantages et inconvénients

+	-
Commutation rapide Haut Débit Gestion de la Qualité de Service	Cher Complexe à mettre en oeuvre Complexe à gérer Inadapté à l'explosion du trafic sur Internet

Frame Relay

- Niveaux 1 et 2 du modèle OSI
- Remplaçant du X.25 (liaisons louées, chères)
- Accès à un réseau fournisseur, partagé entre plusieurs clients
- "Fourchette de débit"
- Circuits virtuels $=>$ simulation de VPN
- Performances privilégiées, au dépend de la fiabilité

Avantages et inconvénients

+	-
Contrôle de flux allégé	Inadapté au transport de la voix ou de la vidéo
Adapté aux débits variables	Débits peu élevés
Gestion de la Qualité de Service	Complexe à gérer
	Inadapté à l'explosion du trafic sur Internet

Besoins

- S'adapter au "Tout IP"
- Améliorer les performances
- Qualité de service
- Sécurité
- Souplesse
- Simplification des SI
- Réduction des coûts

Sommaire

Définition

- **Virtual** : pas de liaison physique dédiée
- **Private** : authentification, cryptage, sécurisation des échanges
- **Network** : accès à un site ou un hôte distant

En bref : il s'agit d'un LAN étendu

Connexion VPN

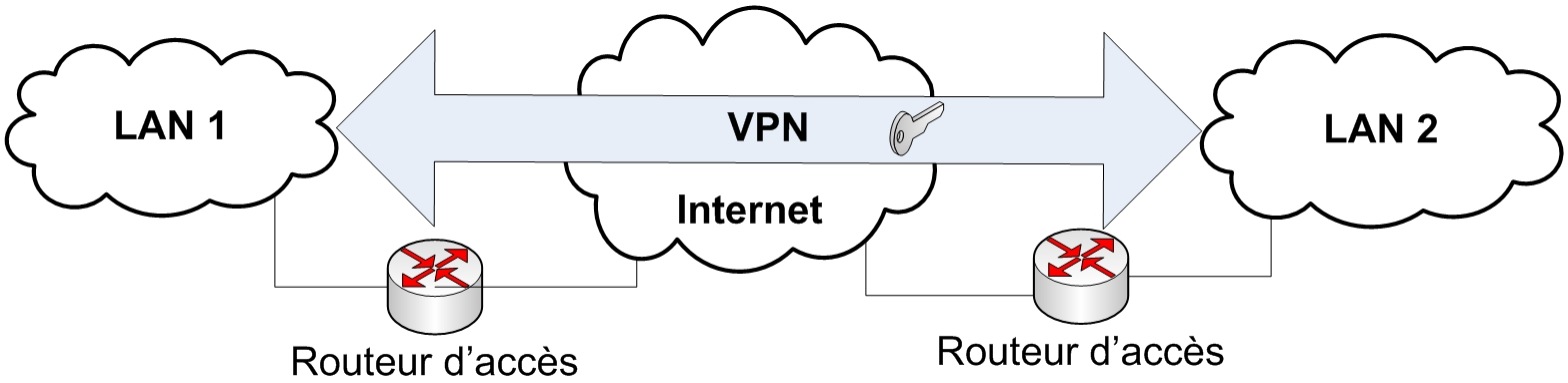
Un VPN est "seulement" un PRINCIPE :

- Isolation de trafic
- Sécurité

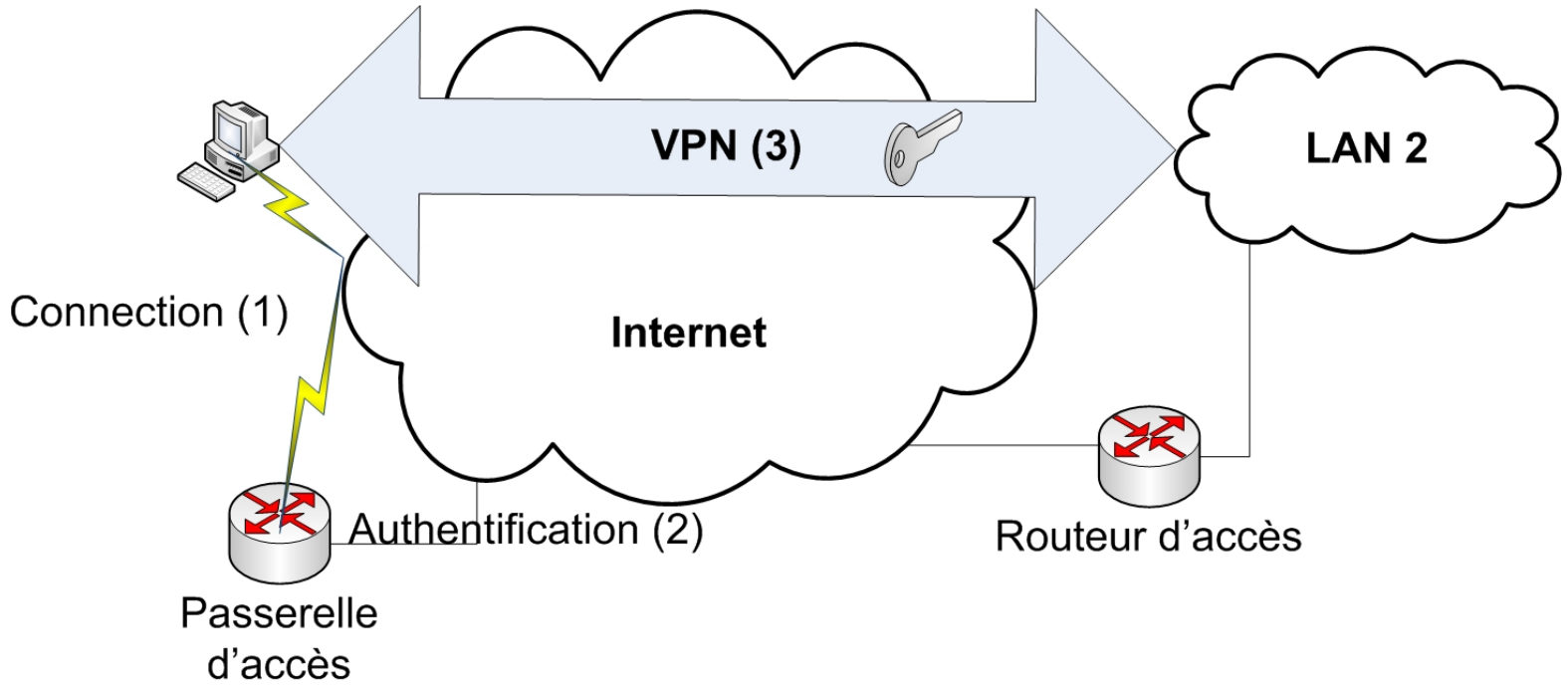
Protocoles d'établissement d'une connexion VPN :

- Niveau 2
  - PPTP
  - L2TP
- Niveau 3
  - IPSEC
  - MPLS

LAN to LAN



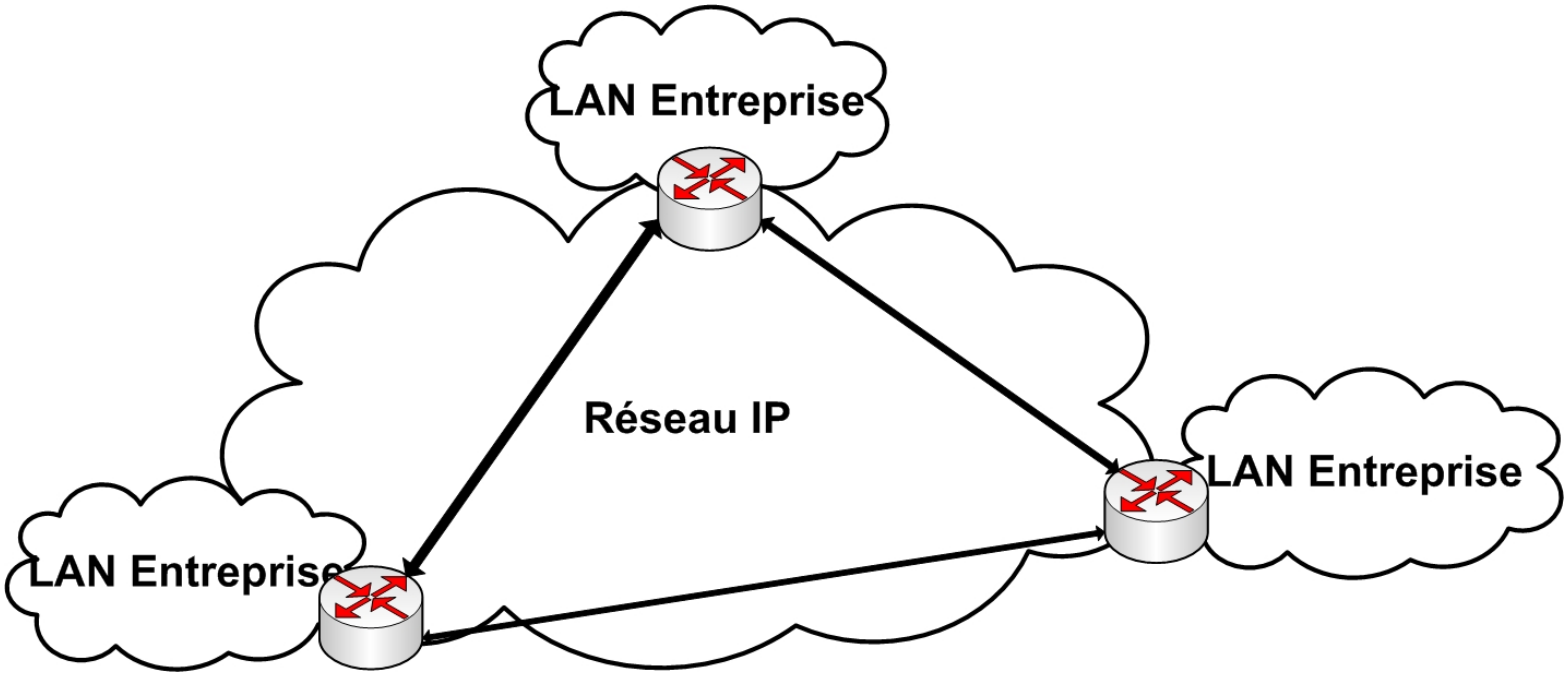
Host to LAN


VPN (3)
LAN 2
Connection (1)
Internet
Authentification (2)
Routeur d'accès
Passerelle
d'accès

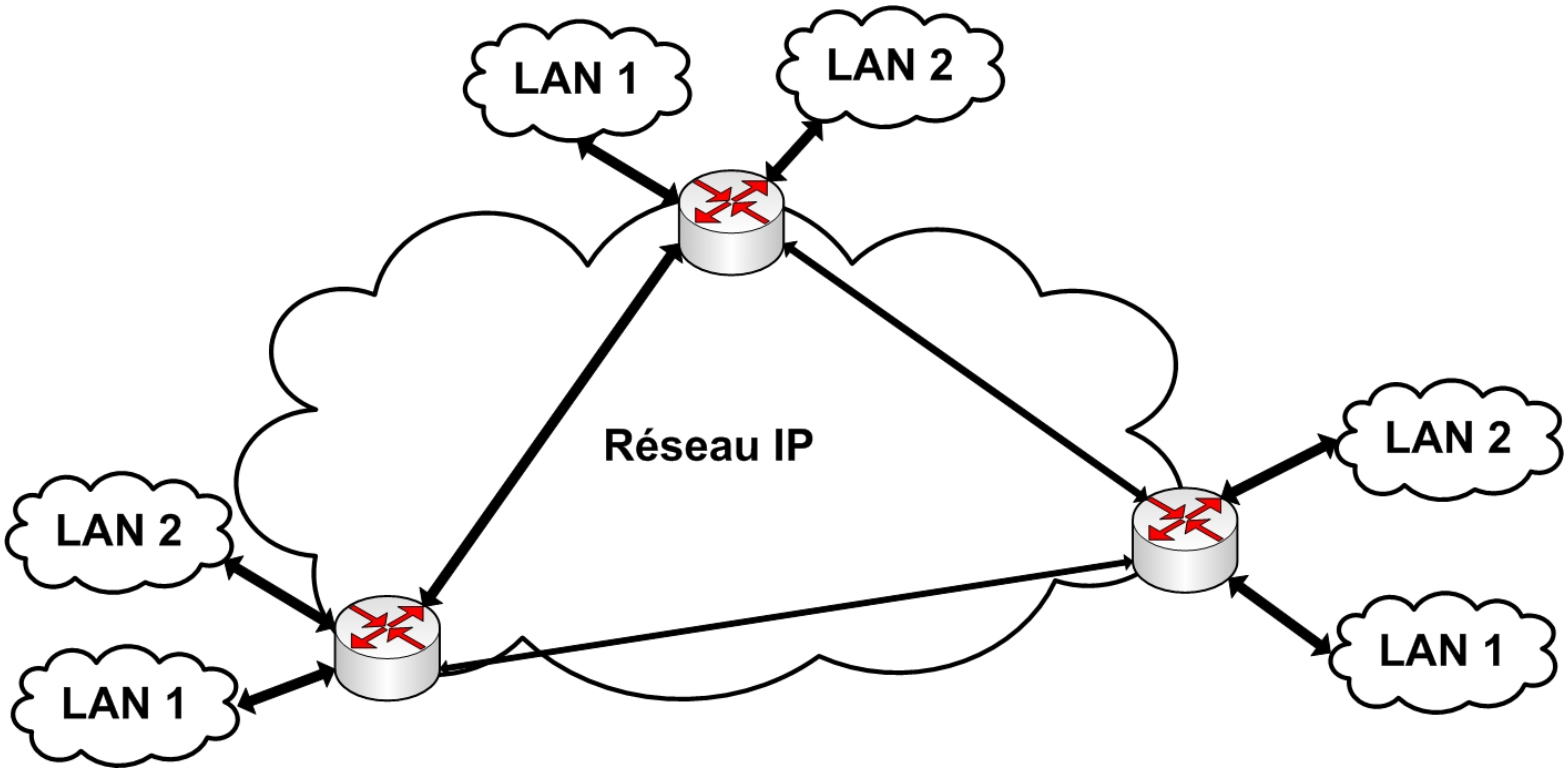
Intérêts

- Confidentialité et intégrité des échanges
- Authentification des équipements
- Authentification des utilisateurs
- Protection du client
- Qualité de service
- Protection contre les pannes

VPN de niveau 2



VPN de niveau 3

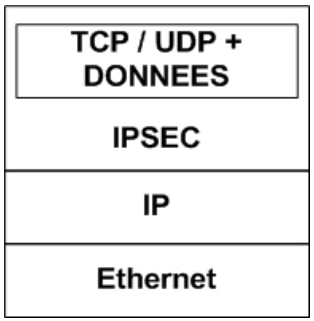


IPSEC

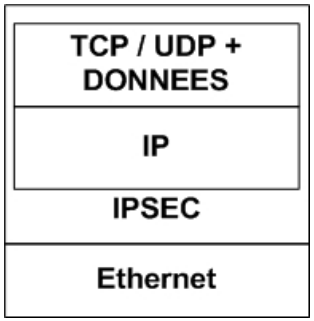
Fournit des services de sécurité au niveau de la couche réseau du modèle OSI

2 modes de fonctionnement :

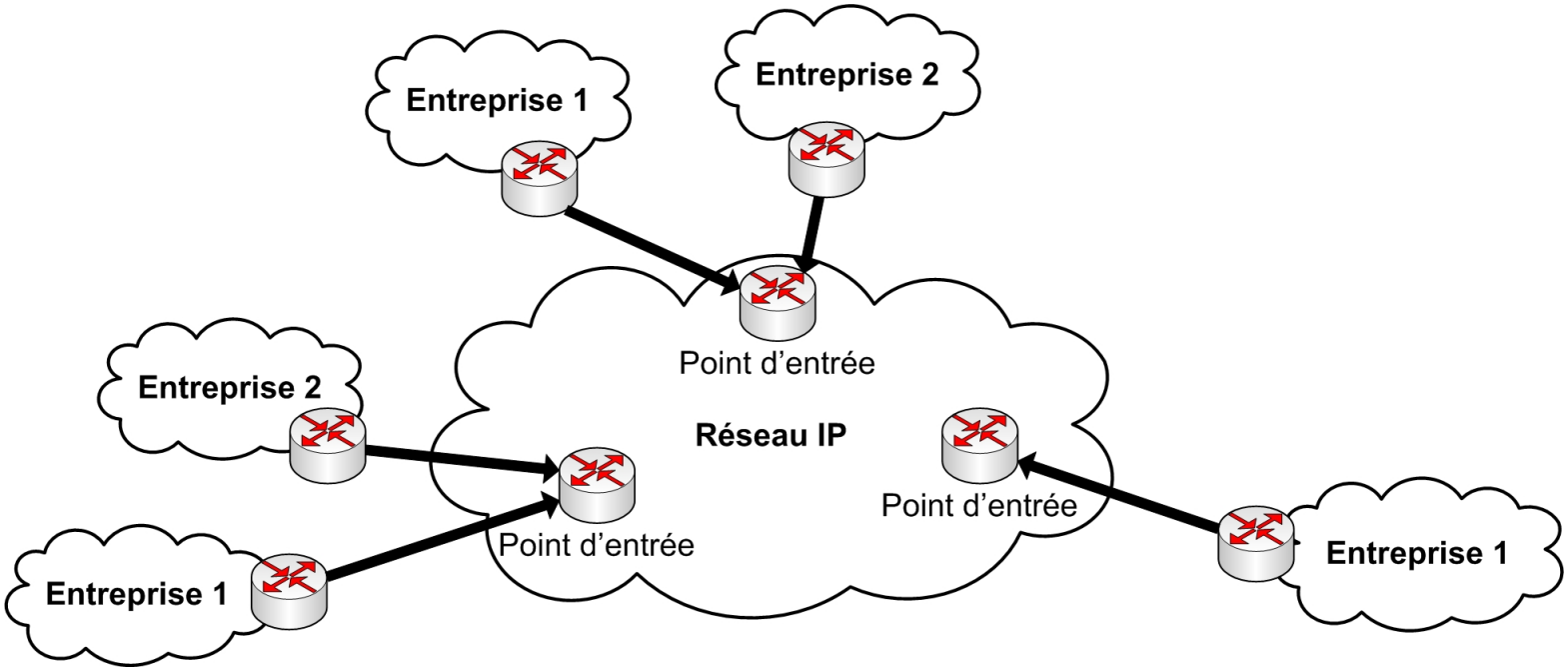
- Mode transport



- Mode tunnel



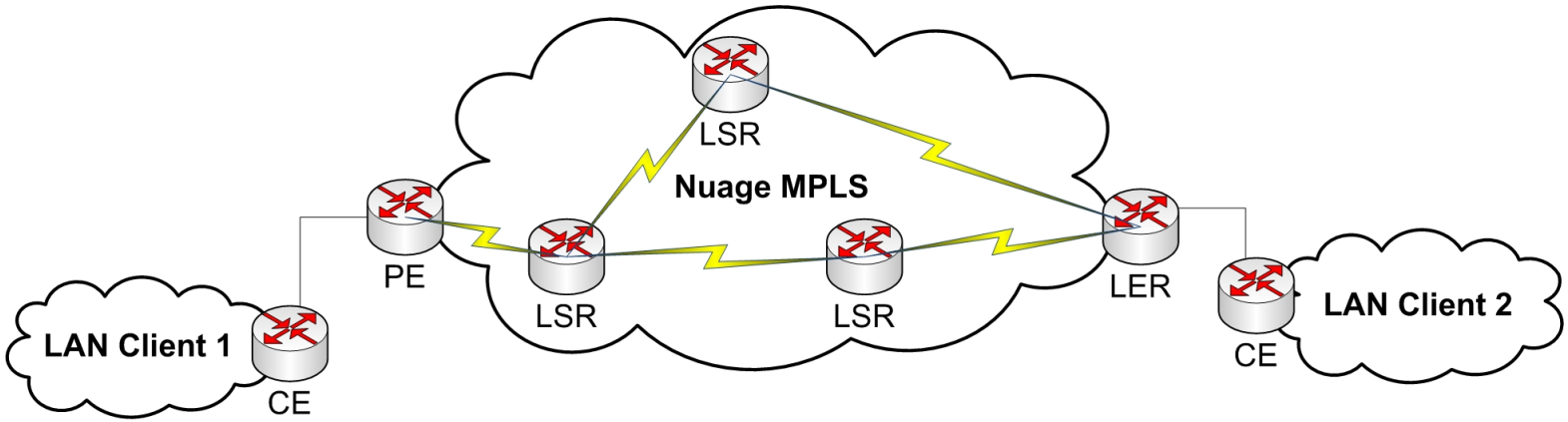
MPLS


Entreprise 1
Entreprise 2
Point d'entrée
Réseau IP
Entreprise 2
Point d'entrée
Point d'entrée
Entreprise 1
Entreprise 1

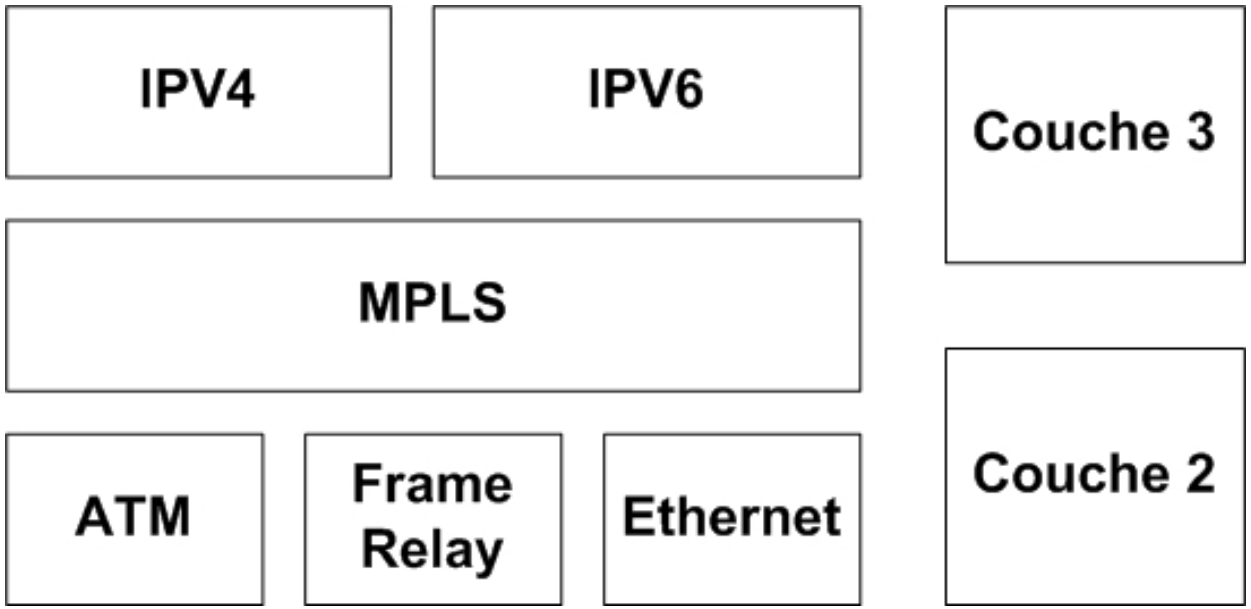
Sommaire

Un peu de vocabulaire

- **CE** : Customer Edge => routeur client
- **PE / LER** : Provider Edge / Label Edge Router => point d'entrée sur le réseau MPLS
- **LSR** : Label Switching Router => routeur de coeur de réseau
- **ELSR** : terme CISCO pour désigner un PE
- **Nuage** : réseau MPLS



MPLS dans le modèle OSI



Définition et principes

Multi Protocol Label Switching
Combine les principes du routage (IP) avec les principes de la commutation (ATM, Frame Relay)

- **Multi Protocol** : indépendant du protocole utilisé pour la couche inférieure
- **Label Switching** : commutation en fonction d'une étiquette attachée à un paquet

- Routage à l'entrée du nuage
- Commutation à l'intérieur du nuage

Objectifs

- Améliorer les performances
- Proposer de la Qualité de Service
- Réduire la taille des tables de routage
- Fonctionner avec n'importe quel protocole de couche 2

Pour les opérateurs :

- Nouveaux services
- Tout en s'appuyant sur l'infrastructure en place

Labels

Etiquette de 20 bits insérée dans un paquet
Calcul : port d'entrée => @IP destination => **label** => port de sortie

InPort	IpDest	**label**	OutPort
Eth1	82.10.234.0/16	L1	Eth4

LIB : Label Information Base

Comportement d'un LSR :

- Arrivée du paquet labellisé
- Identification du prochain saut (LSR suivant)
- Mise à jour du label + décrémentation du TTL
- Envoi au noeud suivant

InPort	InLabel	OutPort	OutLabel
Eth2	L1	L6	Eth8

Le protocole de routage de niveau 3 n'est jamais activé

Affectation des labels

Plusieurs méthodes de création :

- Selon la topologie (adresses IP)
- Selon le flux
- Selon le trafic
- Envoi au noeud suivant

Distribution des labels sur un VPN : protocole BGP

Les raisons du succès

- Production de profit
- Suivi de l'évolution d'IP
- Souplesse
- Neutralité vis à vis des couches adjacentes
- Utilisation de l'existant
- Evolutivité
- Possibilité de mesures précises

Combien ça coûte

Liaison à 2Mb/s, symétrique, entre 2 sites, chez Orange : environ 1000 euros TTC par mois

- Accès au réseau
- Qualité de service minimale
- Accès secouru
- Services supplémentaires en option
- Augmentation de débit à la demande

Sommaire

Nouveaux besoins

- Gestion simplifiée
- Optimisation du trafic
- Optimisation des décisions de routage

Travaux en cours par l'IETF

G-MPLS

Globalized MPLS
"Nouveaux" LSR :

- Routeurs
- Commutateurs de niveau 2
- Commutateurs optiques

Adaptation aux couches physiques
Un Generalized Label peut-être un intervalle de temps, une longueur d'onde, un port physique, un label "classique"

Conclusion

- Implémentation de services non proposés par IP : VPN, classes de services, ingéniérie de trafic
- Nouvelles possibilités de routage : on n'utilise plus exclusivement l'adresse IP de destination
- Contrôle et données séparés

Questions