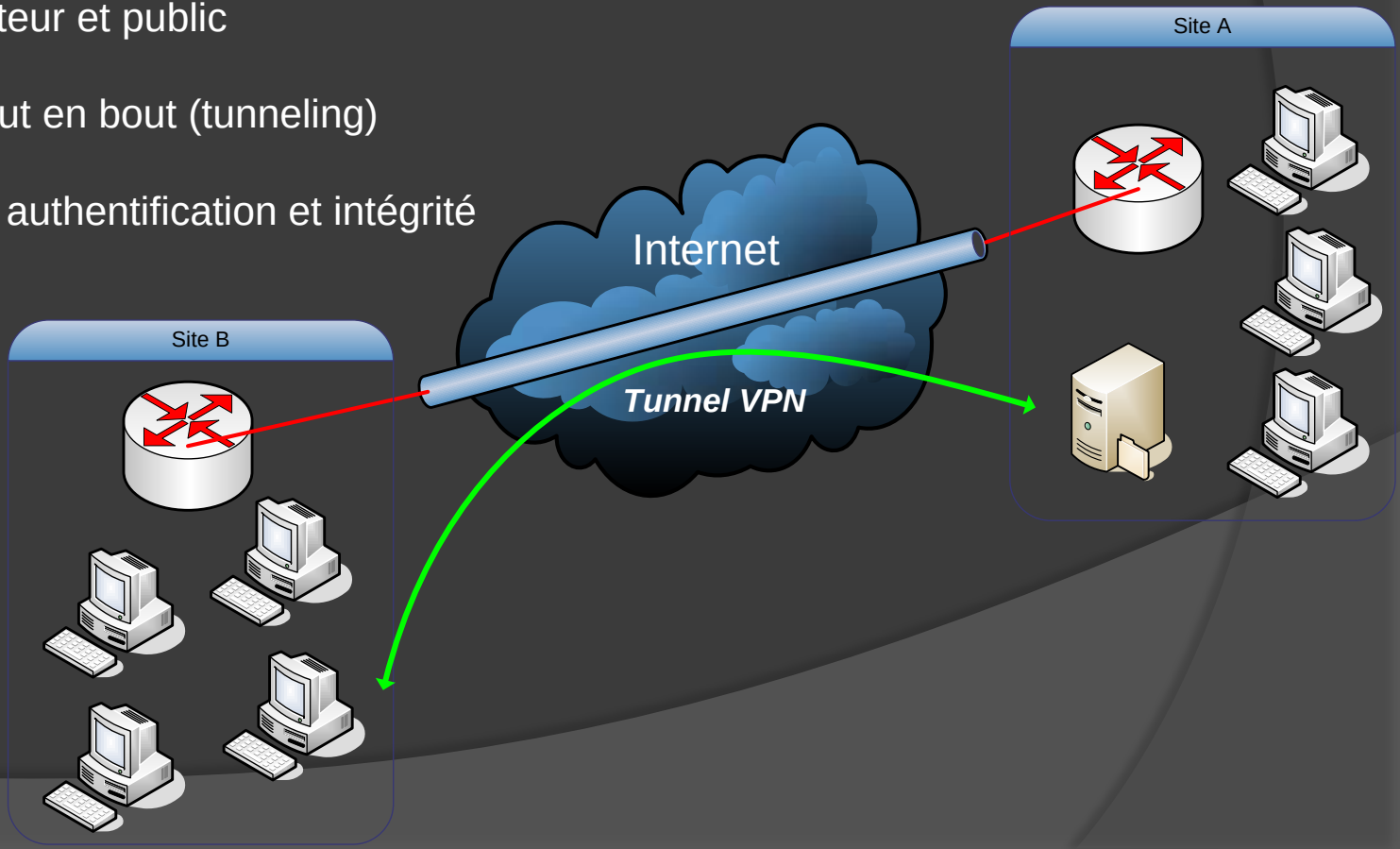
VPN BGP MPLS

- Technologies : VPN, BGP & MPLS
- État de l'art
- Avantages / Inconvénients
- Avenir

VPN – Virtual Private Networks

- Extension des réseaux locaux
- 2 types : opérateur et public
- Sécurisé de bout en bout (tunneling)
- Confidentialité, authentification et intégrité



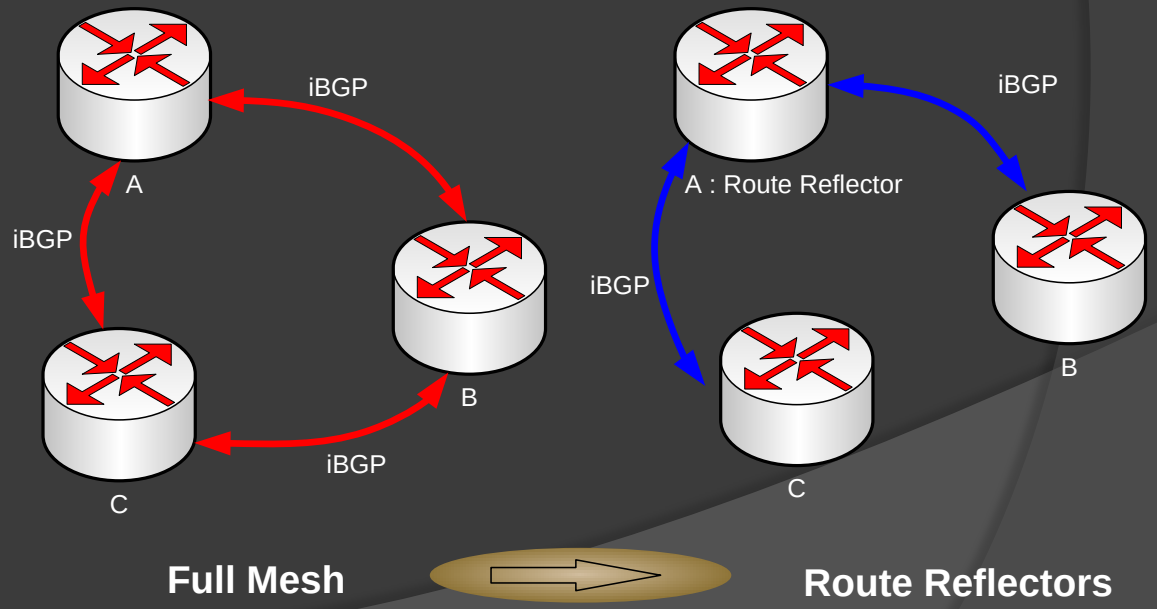
BGP – Border Gateway Protocol

- Protocole EGP (Exterior Gateway Protocol)

- Routage sur Internet

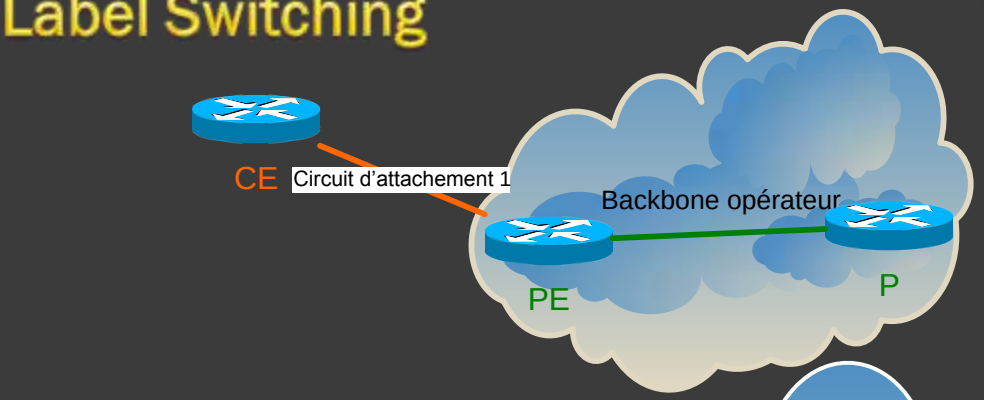
- Protocole en deux parties :
  - eBGP
  - iBGP

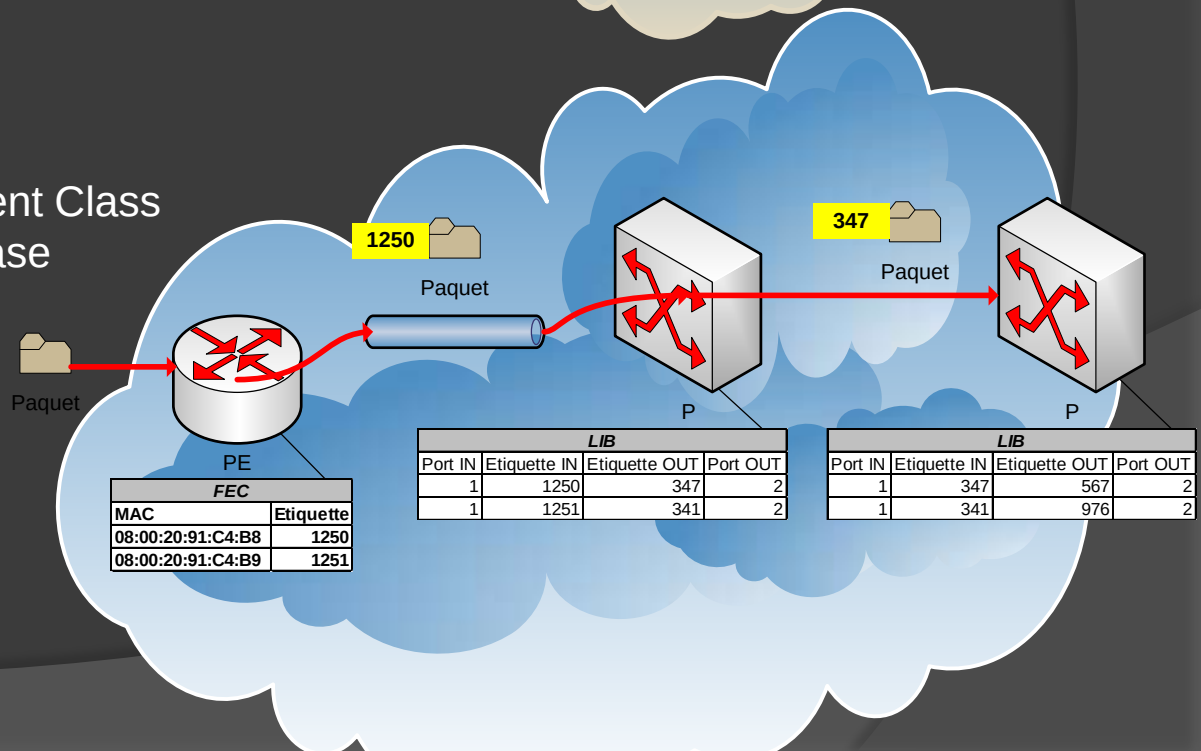
- Optimisation :
  - Routes summarization
  - Routes reflectors



MPLS – Multi Protocol Label Switching

- Elément MPLS : CE, PE & P
- Multi Protocoles
- Commutation de paquets
- 2 tables :
  - FEC : Forwading Equivalent Class
  - LIB : Label Information Base
- Echange de labels avec LDP
- Gestion du trafic & QoS



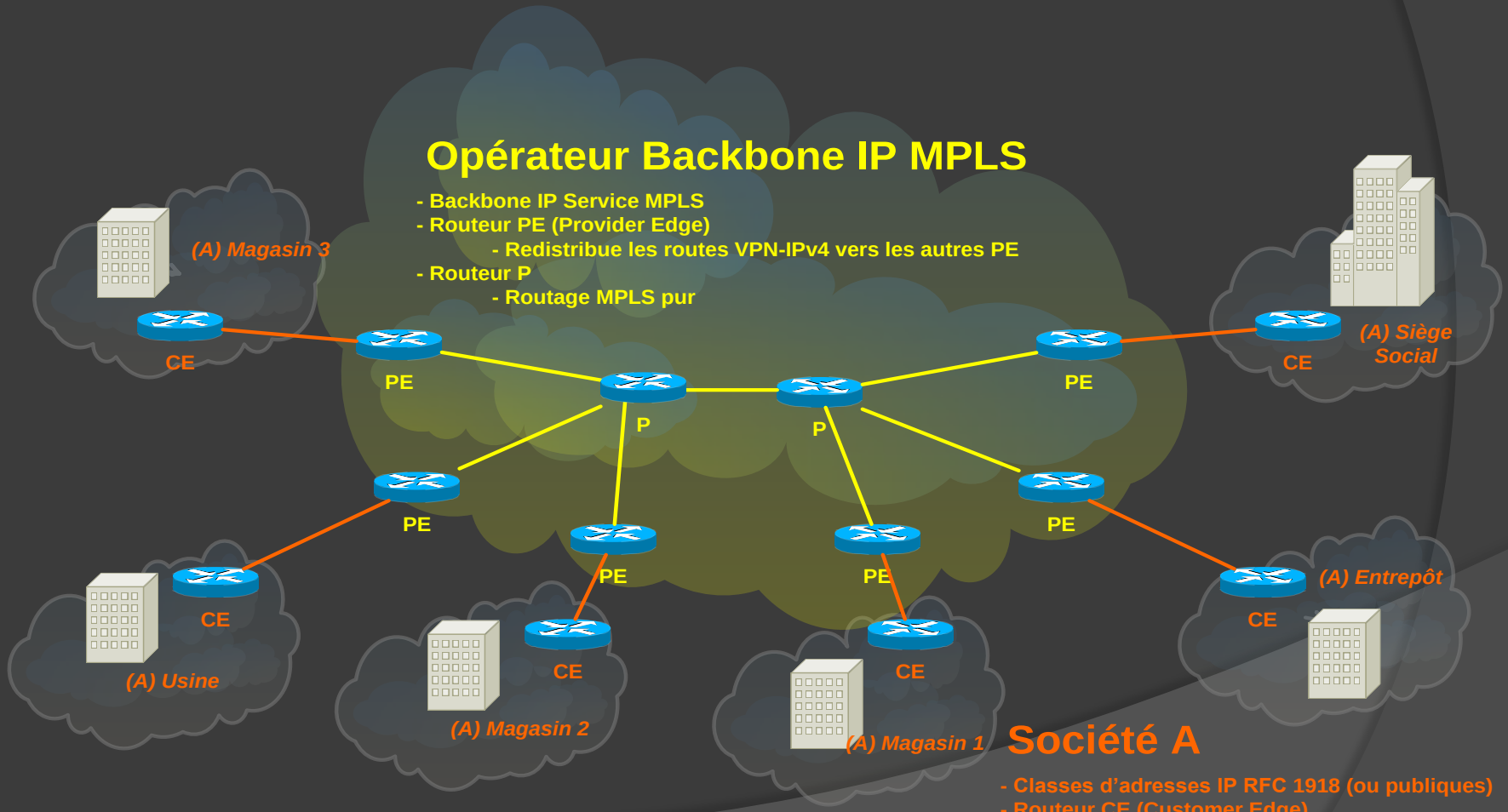


FEC	
MAC	Etiquette
08:00:20:91:C4:B8	1250
08:00:20:91:C4:B9	1251

LIB			
Port IN	Etiquette IN	Etiquette OUT	Port OUT
1	1250	347	2
1	1251	341	2

LIB			
Port IN	Etiquette IN	Etiquette OUT	Port OUT
1	347	567	2
1	341	976	2

VPN BGP MPLS : Structure et Entités



VRFs – VPN Routing & Forwarding Tables

- Chaque PE maintient des tables de transfère séparées :
    - La table par défaut
    - Les VRFs
- Circuit d'attachement associé avec une VRF
- L'ingress-PE utilise la VRF pour router le paquet vers le PE de destination
- Si aucune VRF, on utilise la table par défaut
- Lorsqu'un paquet arrive sur un PE :
    - Circuit d'attachement + caractéristiques du paquet déterminent la VRF de pénétration
    - Lookup dans la VRF pour connaître la route à utiliser
    - Permet d'avoir des politiques de routage différentes en fonction du paquet

-Peuplage des VRFs de 2 façons :

- Apprentissage des routes des CE
- Routes fournies par Les autres PE

Famille d'adresses VPN-IPv4

- Rendre unique l'adresse IPv4 sur Internet
- Utilisation d'un Route Distinguisher (RD – 8 octets)
- RD administré par l'opérateur

Adresse VPN-IPv4 (12octets)	
Route Distinguisher (8octets)	Adresse IPv4 (4octets)

Réseaux Privés Virtuels
VPN BGP / MPLS

Etat de l'art

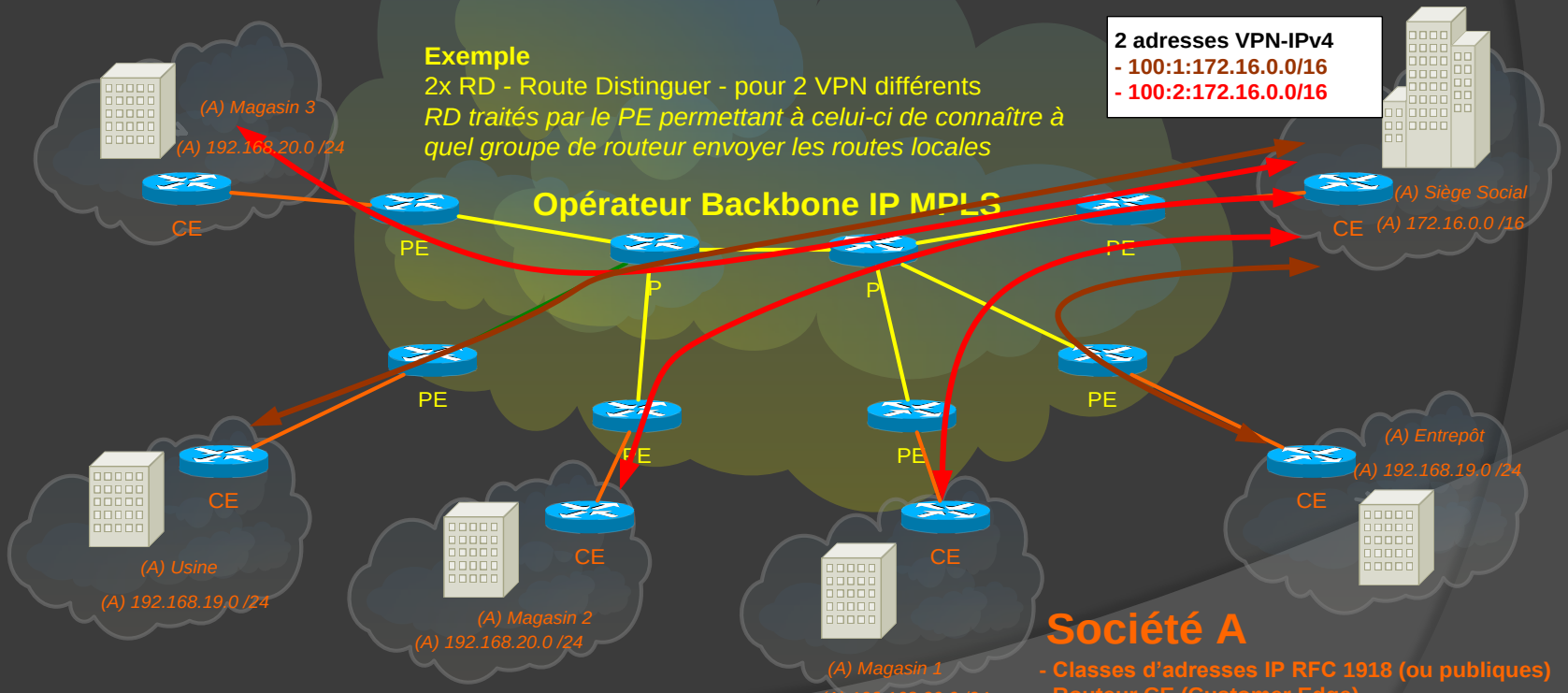
Famille d'adresses VPN-IPv4

RD Type 1 *8 octets* ⟷ **RD 100:1** / **RD 100:2**

Le RD permet de garantir l'unicité des routes VPN-IPv4 échangées entre PE

Exemple
2x RD - Route Distinguer - pour 2 VPN différents
RD traités par le PE permettant à celui-ci de connaître à quel groupe de routeur envoyer les routes locales

2 adresses VPN-IPv4
- **100:1:172.16.0.0/16**
- **100:2:172.16.0.0/16**



Société A

- **Classes d'adresses IP RFC 1918 (ou publiques)**
- **Routeur CE (Customer Edge)**
- **Routes locales statiques ou dynamiques**
- **Autonomous System (AS 129)**

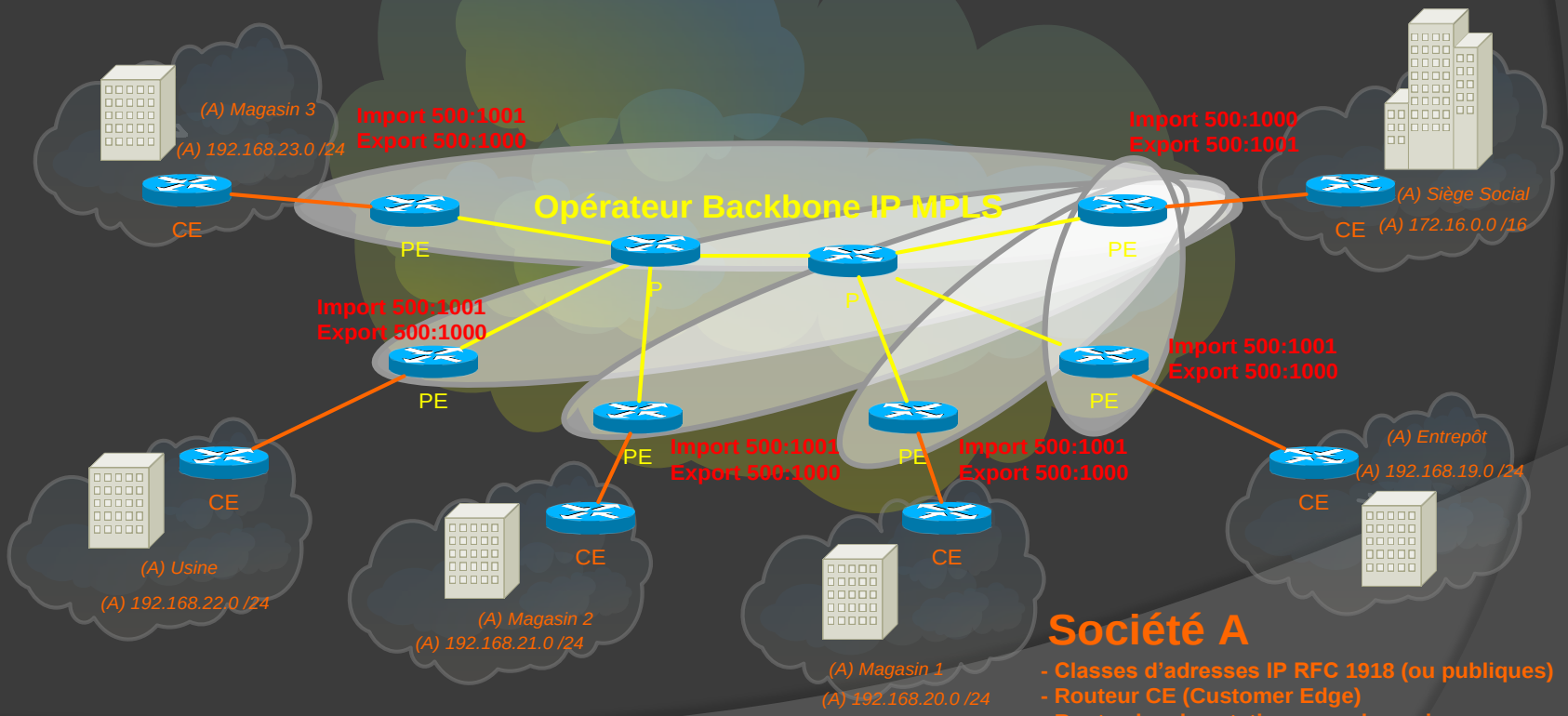
Contrôle de la redistribution des routes

- Notion de Route Cible (« Route Target – RT »)
- Un ou plusieurs RT par adresse VPN-IPv4
- Vu comme identifiant d'un ensemble de sites
- Routes distantes : Import RT
- Routes locales : Export RT

Contrôle de la redistribution des routes

Route Target
Hub'n'Spoke

Chaque VRF définie sur un PE est configurée pour exporter ses routes suivant un certain nombre de RT
- Les routes du siège sont distribuées aux autres PE
- Les autres PE distribuent leurs routes au siège
- Routes uniques en Hub'n'spoke (pas de recouvrement au niveau adressage IP)



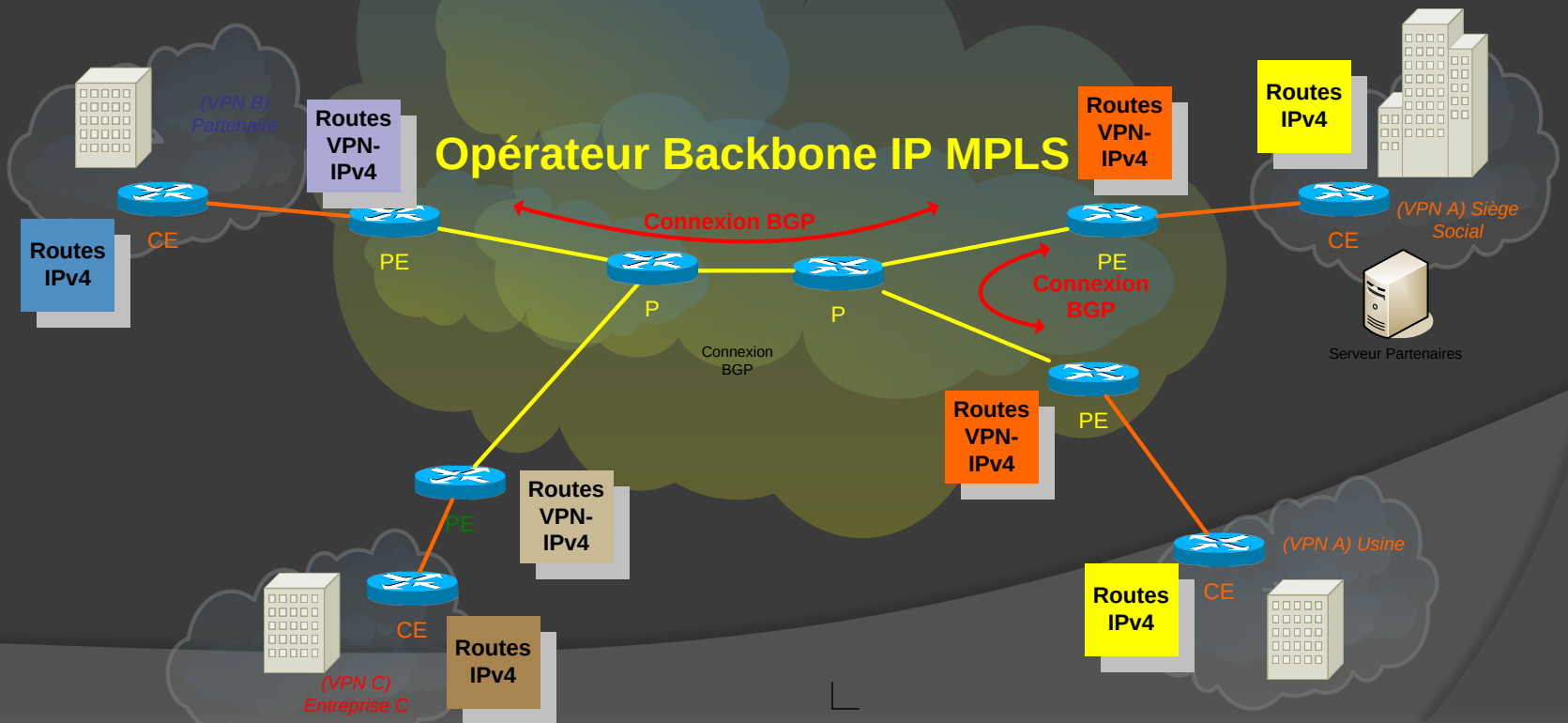
Société A

- **Classes d'adresses IP RFC 1918 (ou publiques)**
- **Routeur CE (Customer Edge)**
- **Routes locales statiques ou dynamiques**
- **Autonomous System (AS 129)**

Réseaux Privés Virtuels
VPN BGP / MPLS

Redistribution des routes par BGP

- Les CE connaissent les routes de leurs réseaux,
- Les CE annoncent les routes aux PE,
- Les PE peuplent leurs VRFs,
- PE avertissent leurs "peers" des routes du VPN,
- Les PE d'extrêmité peuplent leurs VRFs



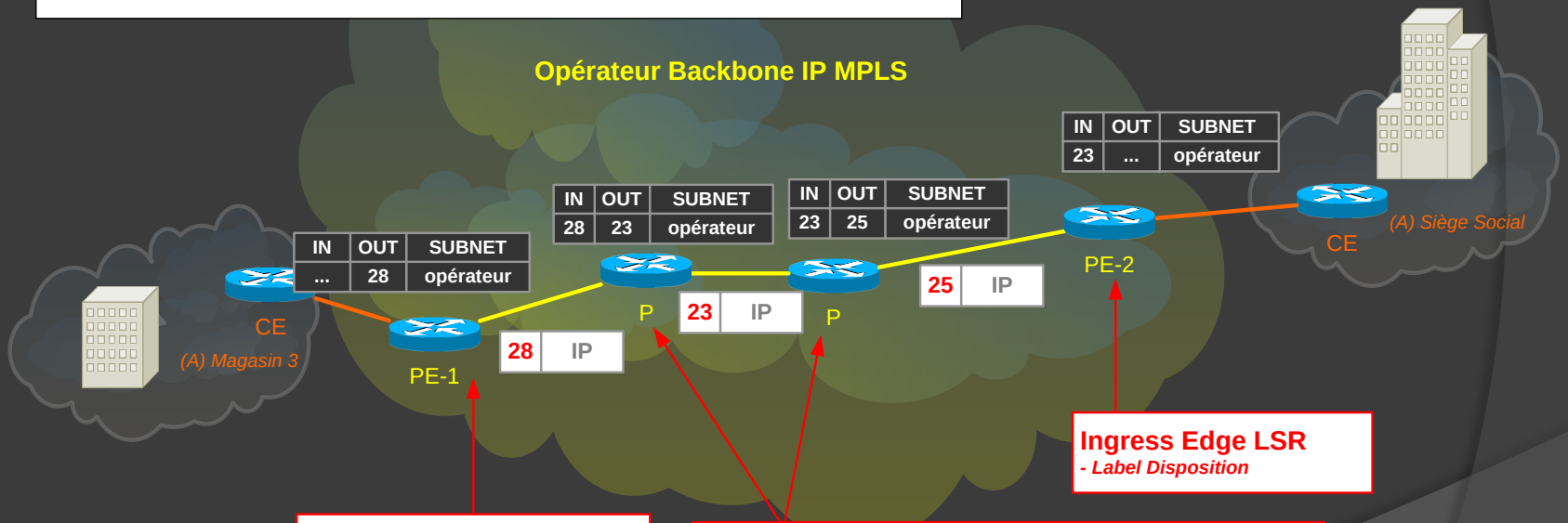
Transport des paquets

MPLS Label Swapping

- Le magasin envoie un paquet qui est taggué par le PE-1
- Le routeur PE-2 supprime le tag MPLS

Société A

- Classes d'adresses IP RFC 1918 (ou publiques)
- Routeur CE (Customer Edge)
- Routes locales statiques ou dynamiques



Ingress Edge LSR
- Label Disposition

Egress Edge LSR
- Label Imposition
- Fonction QoS ou Routes internes

MPLS Label Swapping
- Label Swap
- Pas de reclassification du paquet
- Connaissent les P voisins par LDP (Label Distribution Protocol – IETF) ou TDP (Tag Distribution Protocol – Cisco)

TFIB		
IN	OUT	SUBNET
X	Y	opérateur

TFIB - Tag Forwading Information Base
- Combinaison de le FIB et de la table de routage IP
- Permet de savoir vers quelle interface router le paquet

Avantages - Inconvénients

- Recouvrement possible de classes d’adresses
- Monte très bien en charge
- Très flexible : connexions internet, multi-opérateurs, etc.
- Pas une technologie d'overlay : backbone entièrement BGP-MPLS
- Commutation rapide par paquet, complexité à l’extrémité
- Extensibilité
- Beaucoup de marketing autours de MPLS :
  - Gestion de trafic utilisée par personne pour le moment,
  - QoS était possible avec d'autres protocoles anciens (ATM...).

- Inconvénient : technologie uniquement opérateur

Avenir des VPN BGP MPLS

- Prêt pour IPv6 (RFC 4659) : nouvelle famille d'adresses VPN-IPv6

- Développé par les principaux équipementiers : Juniper, Cisco, Alcatel, Nortel, etc.

- Sécurité : tunnels IPsec entre PE/PE (Draft IETF)

- QoS : extensions MPLS (RFC 3032), backbone ATM, RSVP (RFC 3209)