
Faciliter l'usage de services réseau avancés : le cas de SIRES 2 sur RAP

**Catherine Grenet et Ludovic Ishiomin
(CNRS/UREC et CORAP)
JRES, Nantes, 2 décembre 2009**

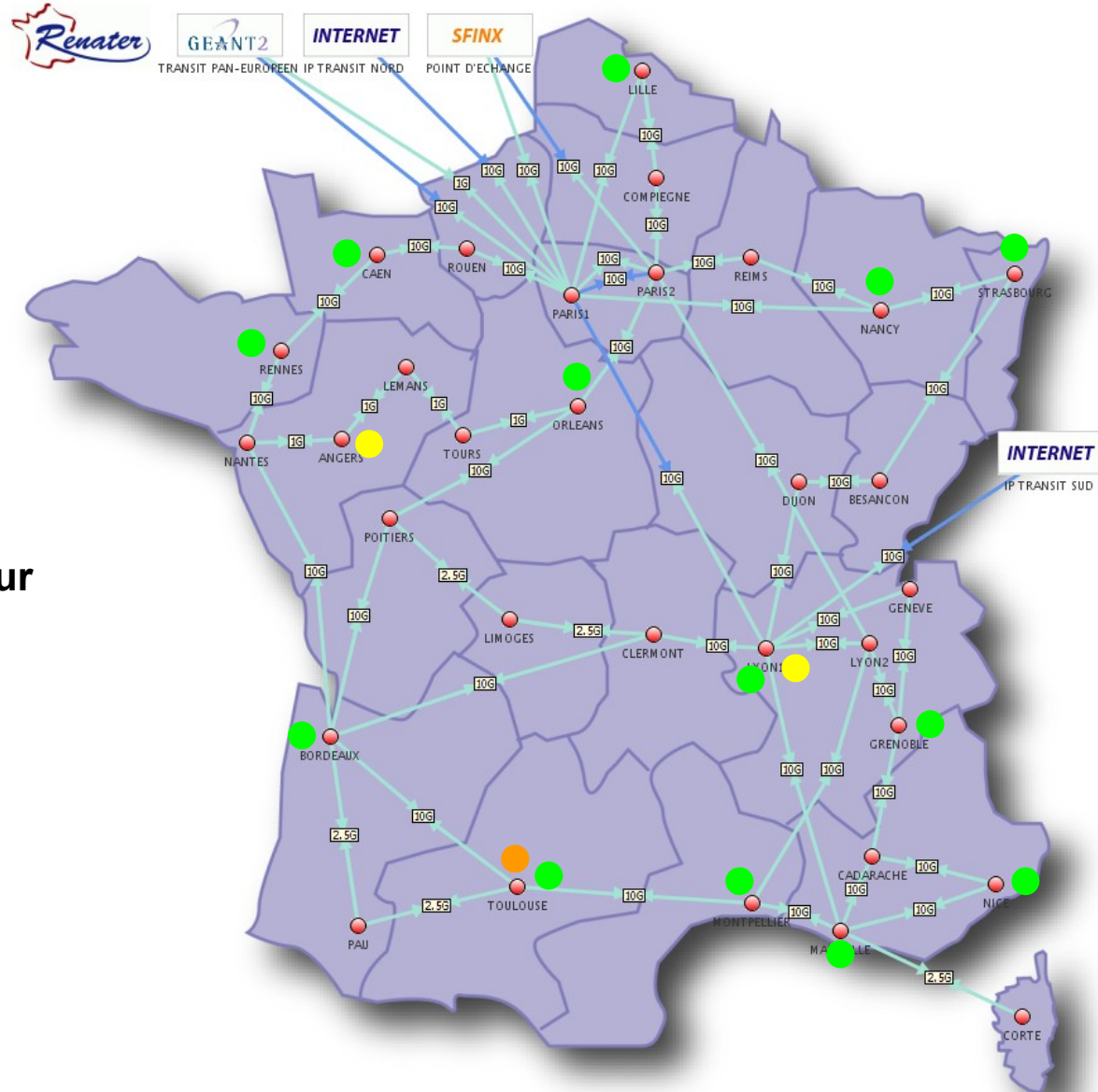
- Le réseau SIRES
 - historique
 - architecture de SIRES 2
 - mise en œuvre et premier déploiement sur RAP
- Les L3VPN sur RAP
 - architecture de routage
 - détails de la mise en œuvre
- SIRES 2 sur RAP : architecture cible

- Le réseau SIRES
 - historique
 - architecture de SIRES 2
 - mise en œuvre et premier déploiement sur RAP
- Les L3VPN sur RAP
 - architecture de routage
 - détails de la mise en œuvre
- SIRES 2 sur RAP : architecture cible

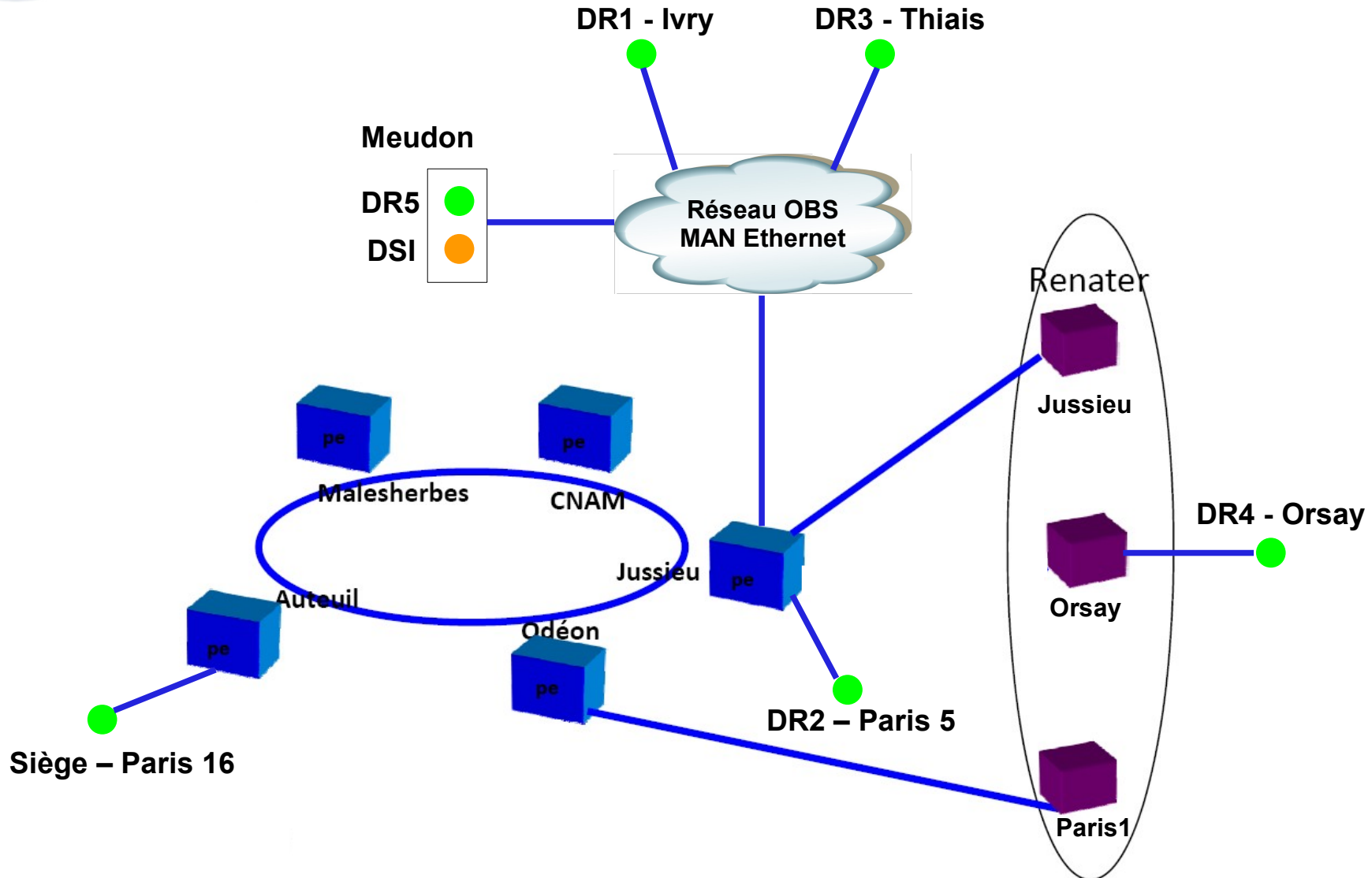
SIRES : historique

- réseau privé virtuel dédié au système d'information de gestion du CNRS
- principales applications :
 - gestion financière et comptable (BFC)
 - gestion des ressources humaines (Sirhus)
- 23 sites en France :
 - 2 centres serveur : Trélazé et Villeurbanne
 - 2 sites de la DSI : Toulouse et Meudon
 - siège du CNRS et 18 délégations régionales

Les sites de SIRES en France



- Centre serveur
- Site client
- Site DSI
- NR



SIRES : historique

- objectifs :
 - confidentialité
 - disponibilité
 - qualité de service
- 1999 : première version de SIRES
 - circuits virtuels ATM sur RENATER 2
 - architecture en étoile
 - connexion du site au NR par LS, FO, VC
 - liens de secours RNIS
 - seul le trafic SIRES emprunte le VPN

SIRES : historique

- 2002 : seconde version
 - RENATER 3 abandonne ATM
 - SIRES migre vers des tunnels IP dans IP (GRE ou IPsec)
- Evolutions jusqu'en 2007 :
 - migration des LS vers réseaux métro ou régionaux
 - migration des liens de secours vers ADSL
- 2007 : mise en service de nouvelles applications
 - augmentation des débits vers centre serveur
 - besoin accru de disponibilité

- GRE : impact fort sur les performances des équipements
- tunnels IP dans IP : problèmes solubles mais pénibles (MTU)
- architecture en étoile :
 - difficultés de passage à l'échelle
 - pas adaptée à un VPN « any to any »

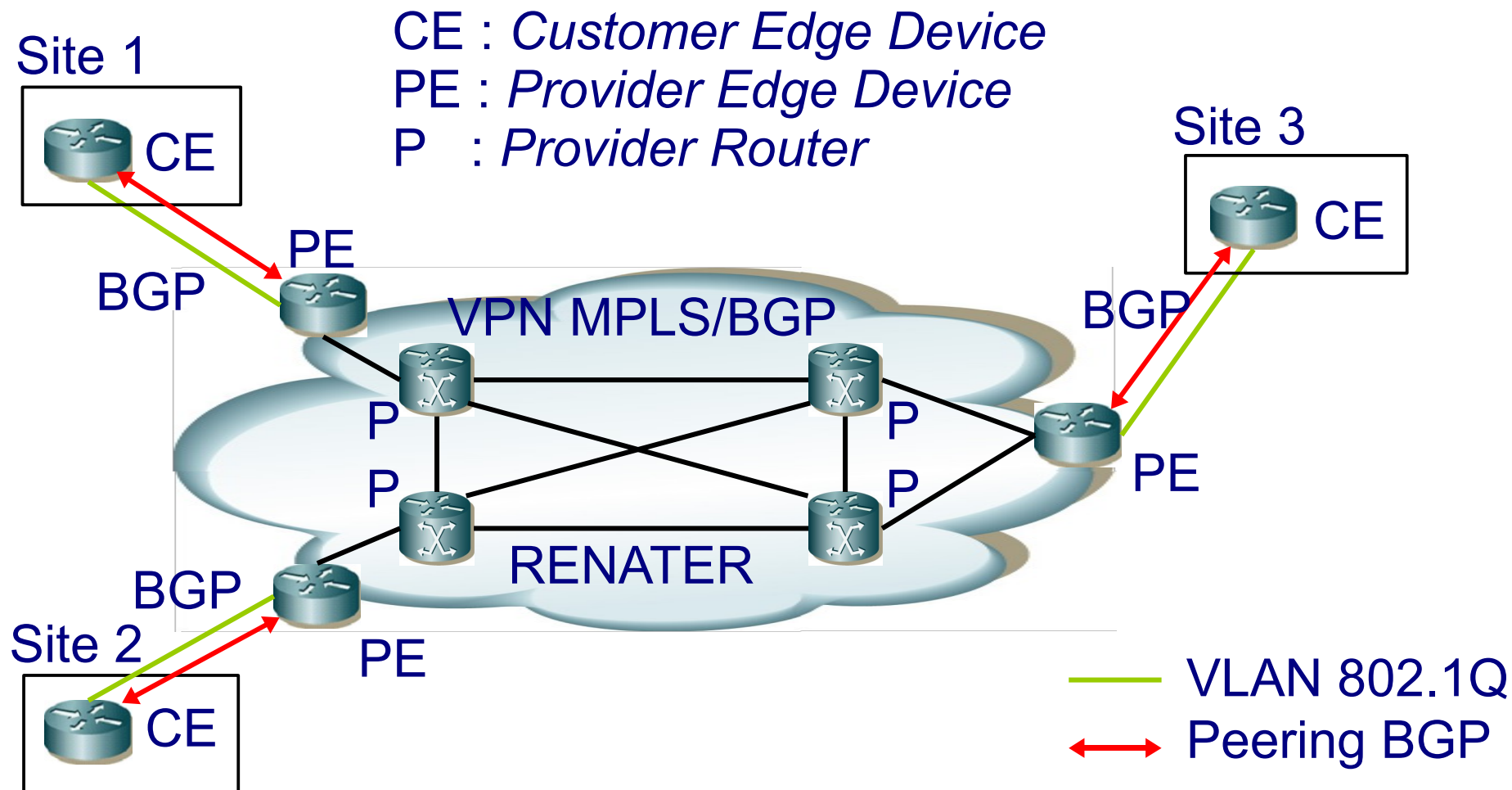
- Le réseau SIRES
 - historique
 - **architecture de SIRES 2**
 - mise en œuvre et premier déploiement sur RAP
- Les L3VPN sur RAP
 - architecture de routage
 - détails de la mise en œuvre
- SIRES 2 sur RAP : architecture cible

SIRES 2 : architecture

- L'architecture proposée s'appuie sur le service de VPN MPLS/BGP de RENATER
- RFC 4364 *BGP/MPLS IP Virtual Private Networks (VPNs)* (2006)
- Service de VPN de niveau 3
- Simule un réseau IP privé entièrement maillé
- Chaque site peut dialoguer directement avec chacun des autres sites

- L'ajout d'un nouveau site est aisé
- Gain de performance grâce à la suppression des tunnels GRE
~ réseau local (au RTT près)
- La complexité est gérée par l'opérateur
- Dans l'avenir :
 - IPv6
 - multicast IPv4
 - classes de service

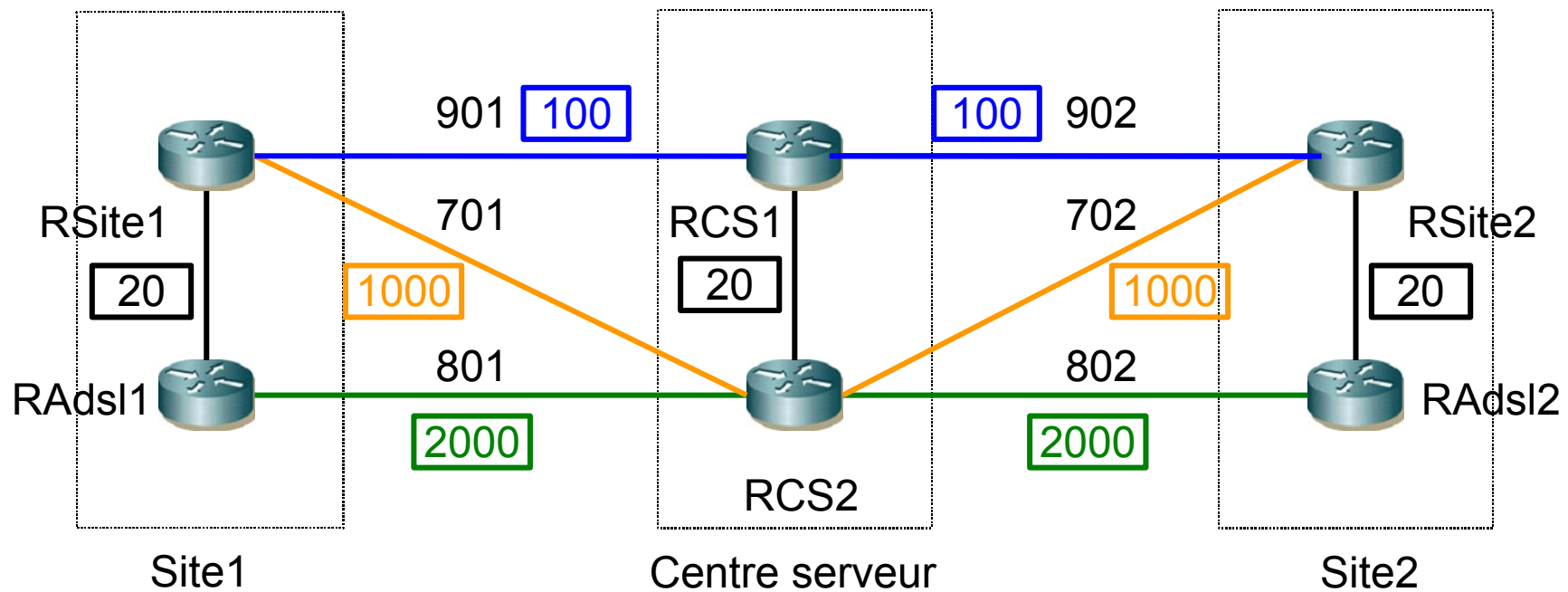
Interface de raccordement



L'équipement du site n'a pas à connaître le protocole MPLS

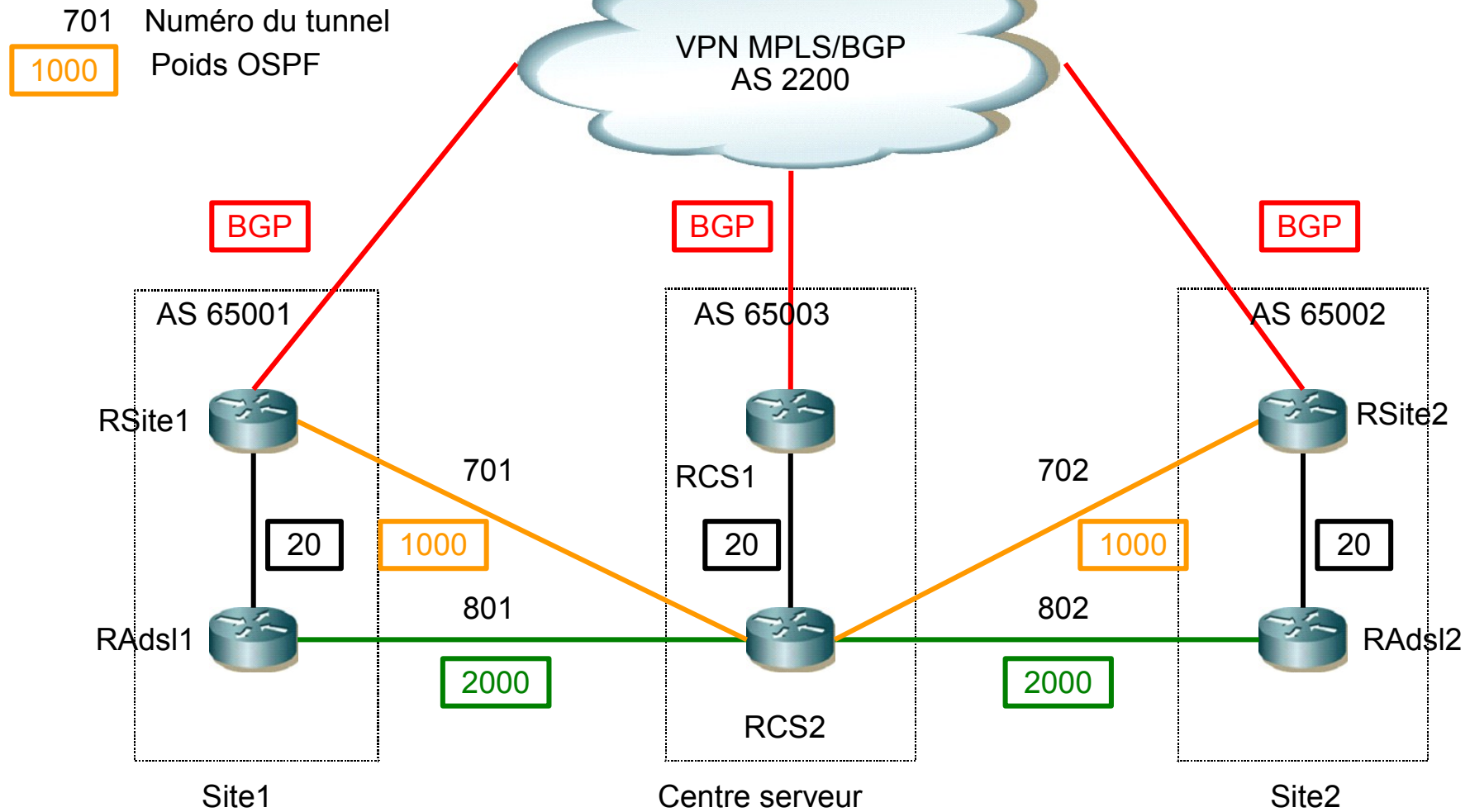
Architecture de routage

La version précédente de SIRES était fondée sur OSPF

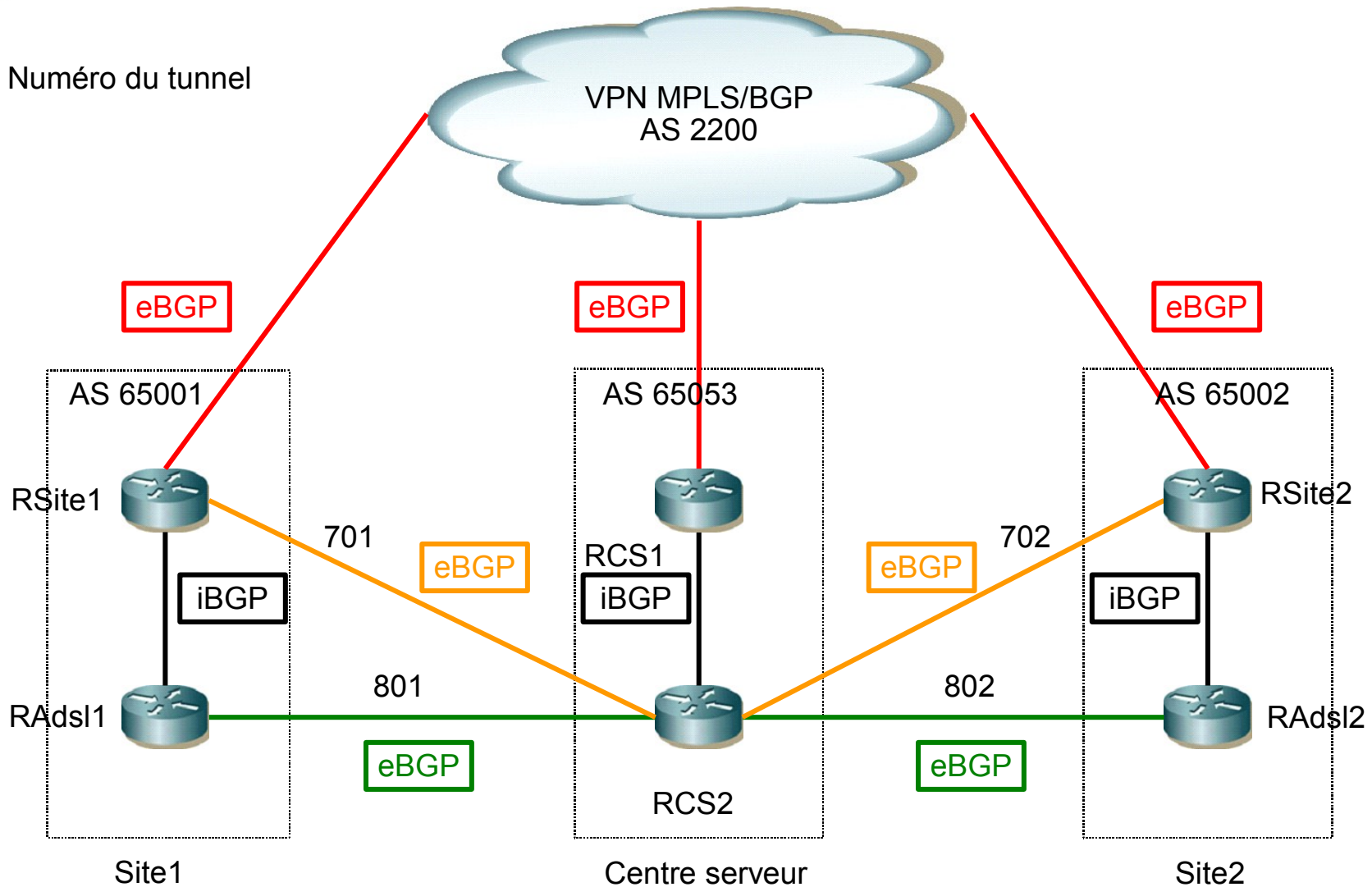


901 Numéro du tunnel

100 Poids OSPF



701 Numéro du tunnel

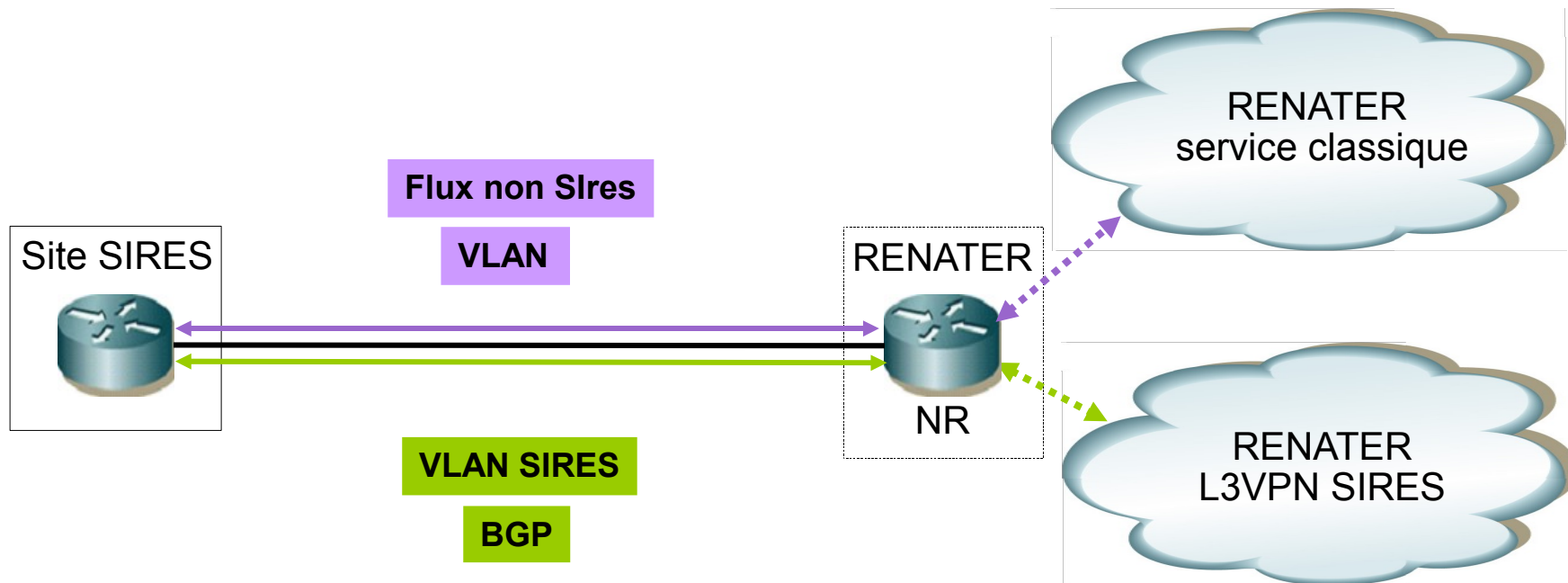


Temps de convergence

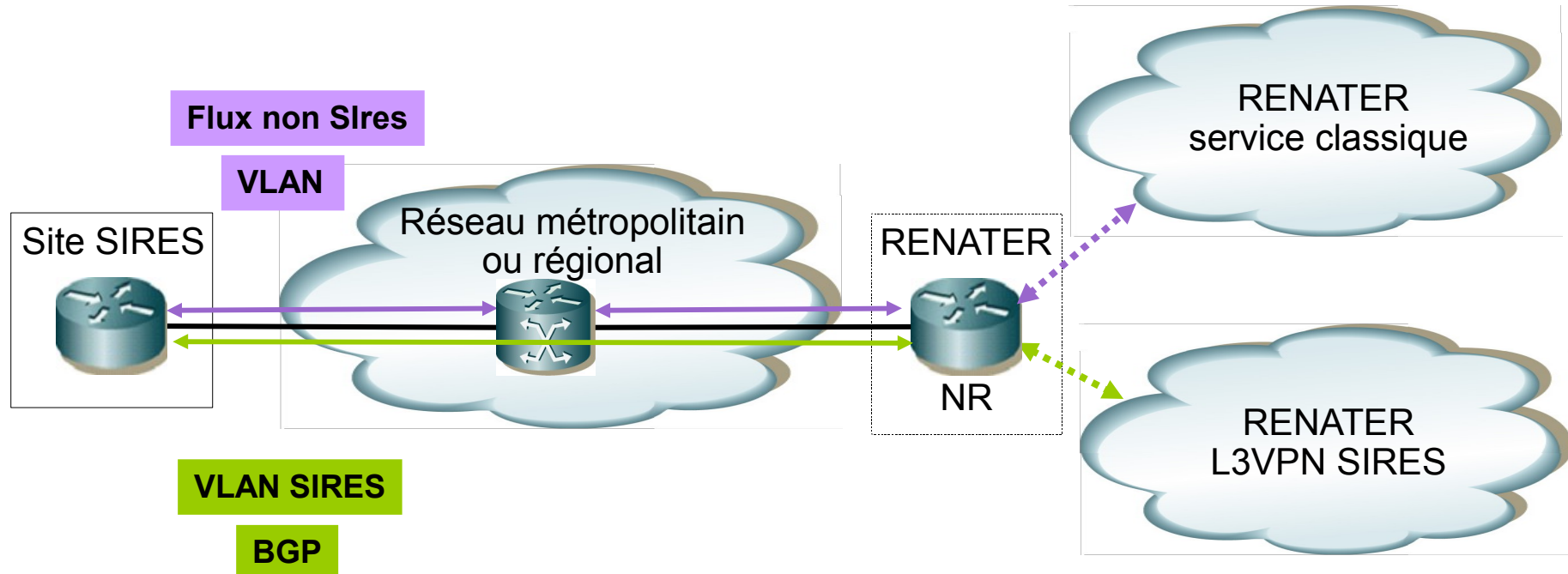
- Première mesure du temps de bascule sur liaison de secours : ~ 140 s
 - à cause des temporisations BGP par défaut
- Utilisation de BFD : diminution du temps de bascule ~ 6 s

- Le réseau SIRES
 - historique
 - architecture de SIRES 2
 - mise en œuvre et premier déploiement sur RAP
- Les L3VPN sur RAP
 - architecture de routage
 - détails de la mise en œuvre
- SIRES 2 sur RAP : architecture cible

7 sites sur 23 sont directement connectés à un NR

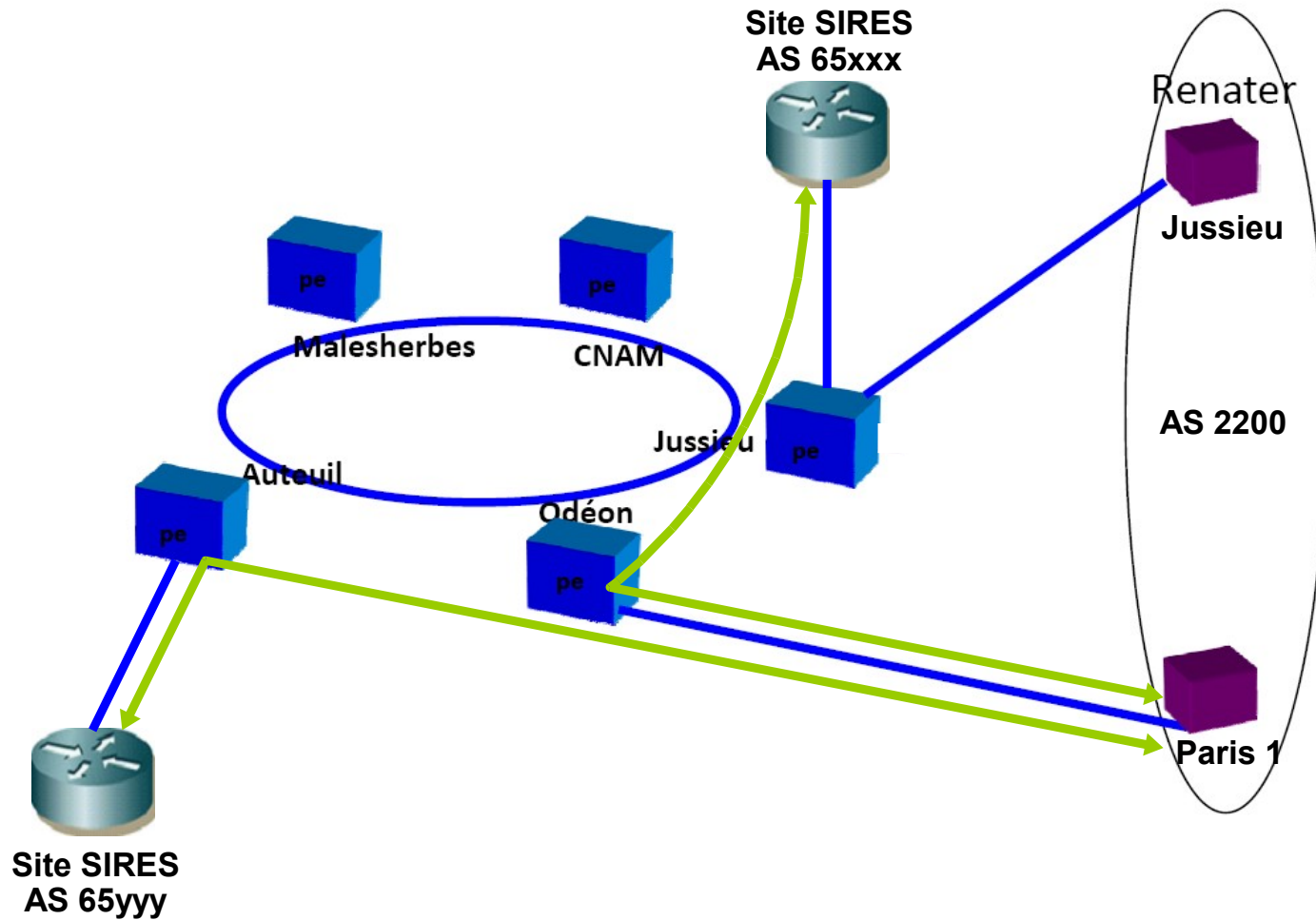


Les 16 autres sont raccordés à travers un MAN / RR



Inconvénients :

- autant d'interlocuteurs que de domaines traversés
- pas de bénéfice des services avancés rendus par le réseau (redondance)



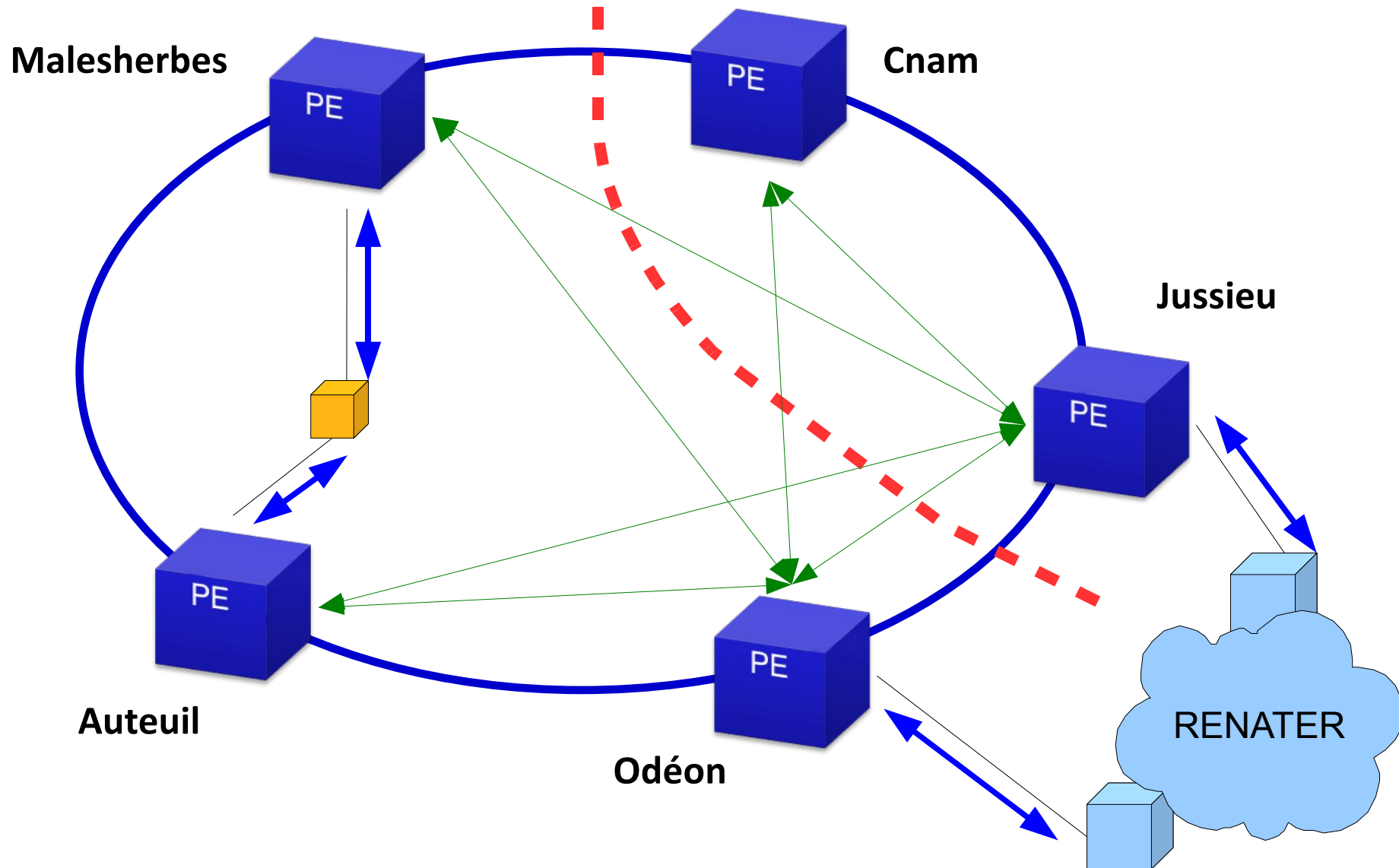
↔ L2VPN entre les sites SIREs et le NR de Paris 1

- Le réseau SIRES
 - historique
 - architecture de SIRES 2
 - mise en œuvre et premier déploiement sur RAP
- **Les L3VPN sur RAP**
 - architecture de routage
 - détails de la mise en œuvre
- SIRES 2 sur RAP : architecture cible

Les L3VPN sur RAP

- Échange des routes basé sur :
 - OSPF pour la topologie
 - BGP pour toutes les autres routes
- Raccordement fiabilisé vers RENATER :
 - local-preference iBGP => communauté BGP RENATER
 - next-hop des routes RENATER résolu par l'IGP
- Raccordement fiabilisé des sites :
 - communauté BGP pour l'annonce des routes
 - => local-preference dans l'iBGP RAP

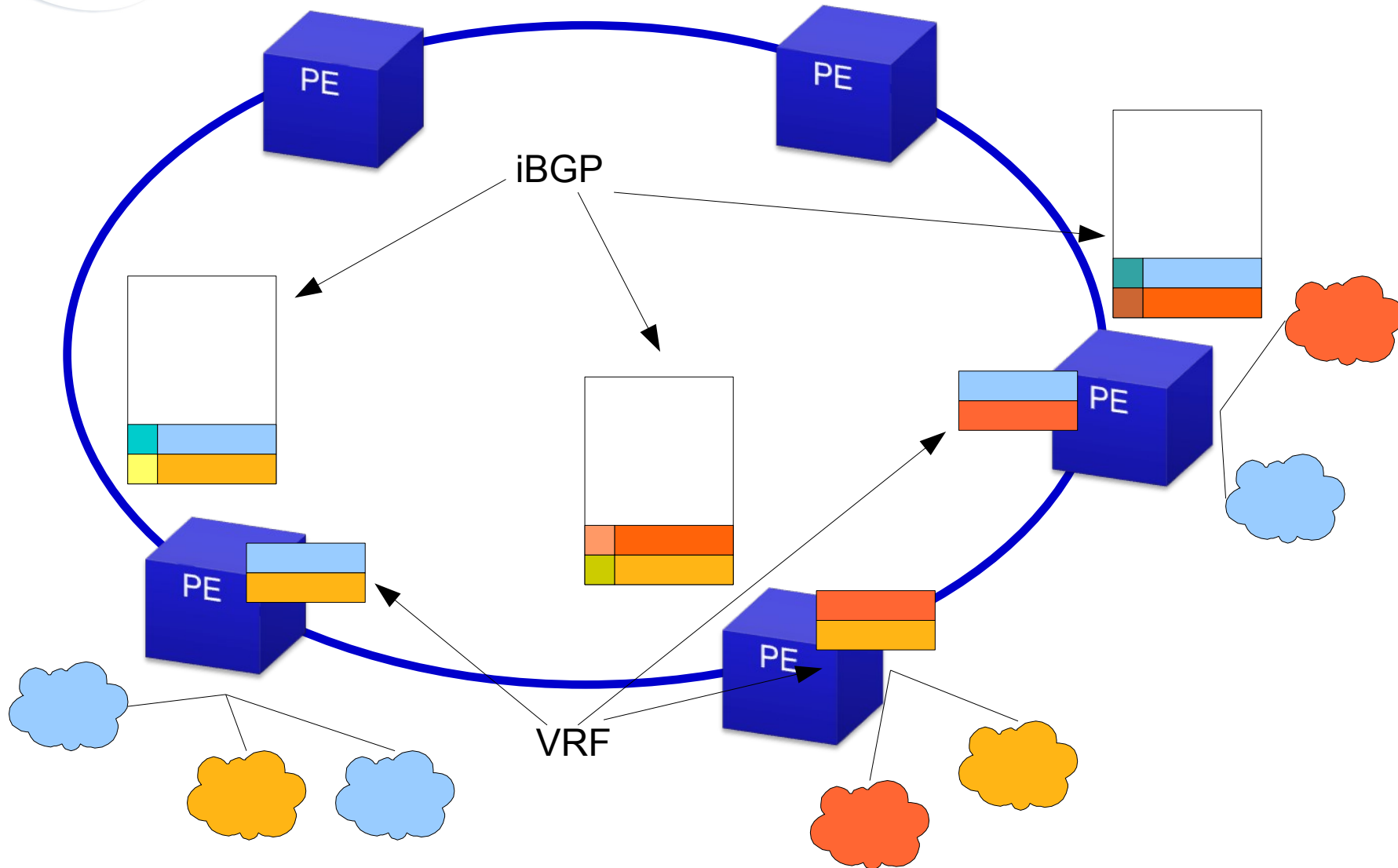
Les L3VPN sur RAP



Les L3VPN sur RAP

- Architecture MPLS basée sur RSVP
 - chemin uni-directionnel entre 2 PE
 - chemin redondant pré-calculé
- Échange des routes des VPN (VRF) entre PE
 - iBGP (AFI = 1, SAFI=128)
 - individualisation des routes (route-distinguisher)
 - ajout d'une communauté étendue (route-target)
- Règles d'import-export des routes entre VRF et iBGP

Les L3VPN sur RAP

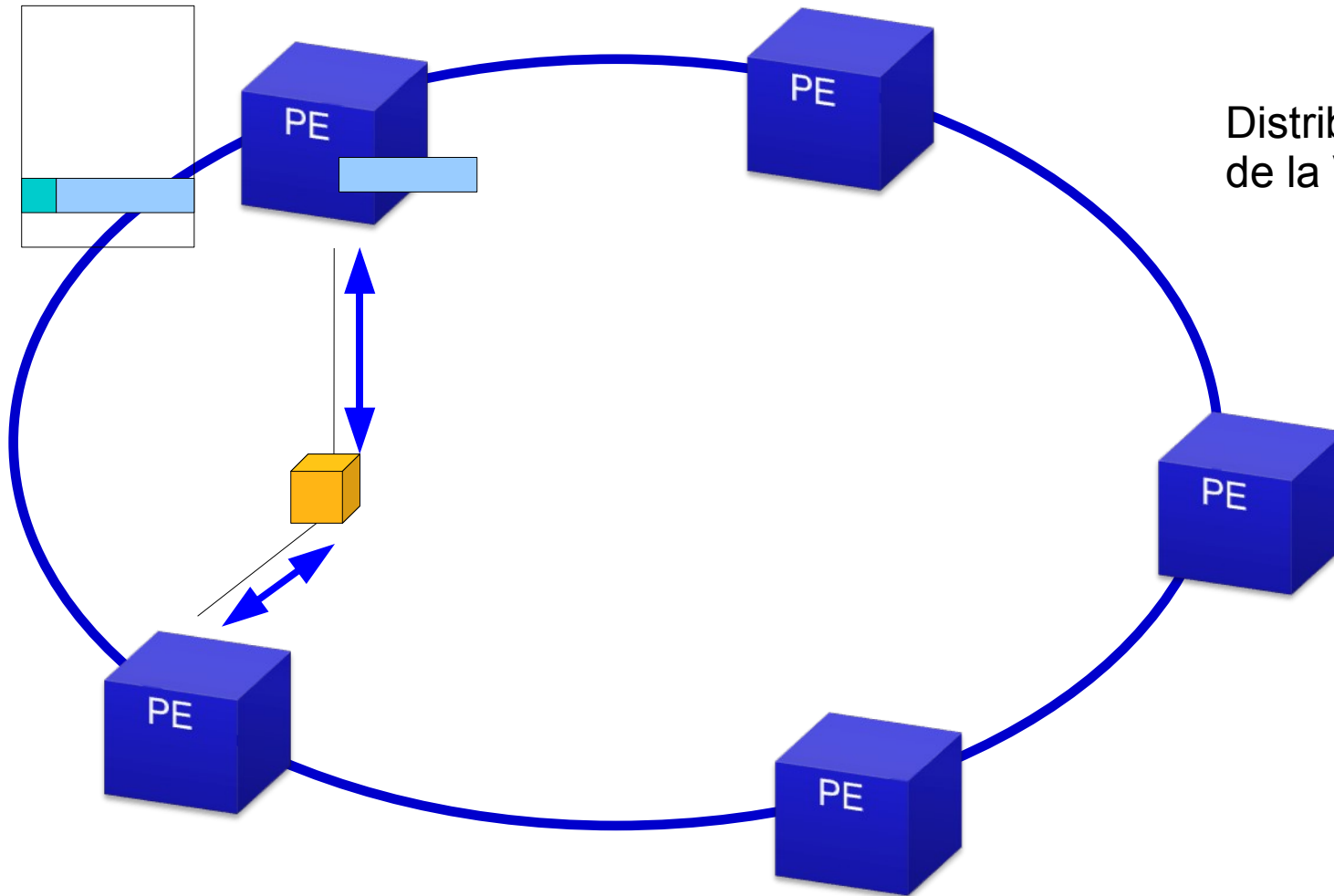


Les L3VPN sur RAP

- Raccordement fiabilisé d'un site au L3VPN
- => local-preference dans l'iBGP

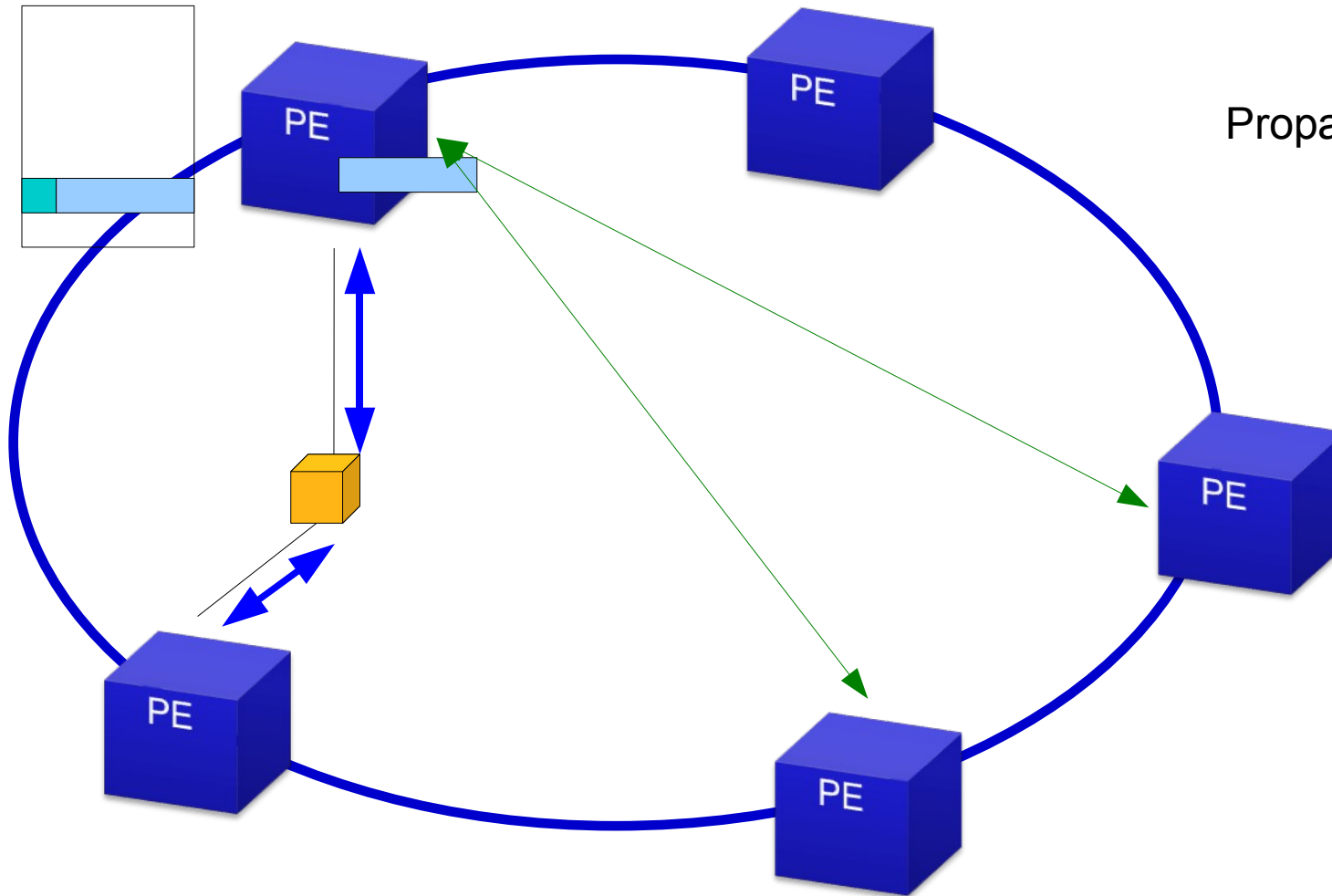
Les L3VPN sur RAP

Distribution de la route de la VRF vers l'iBGP

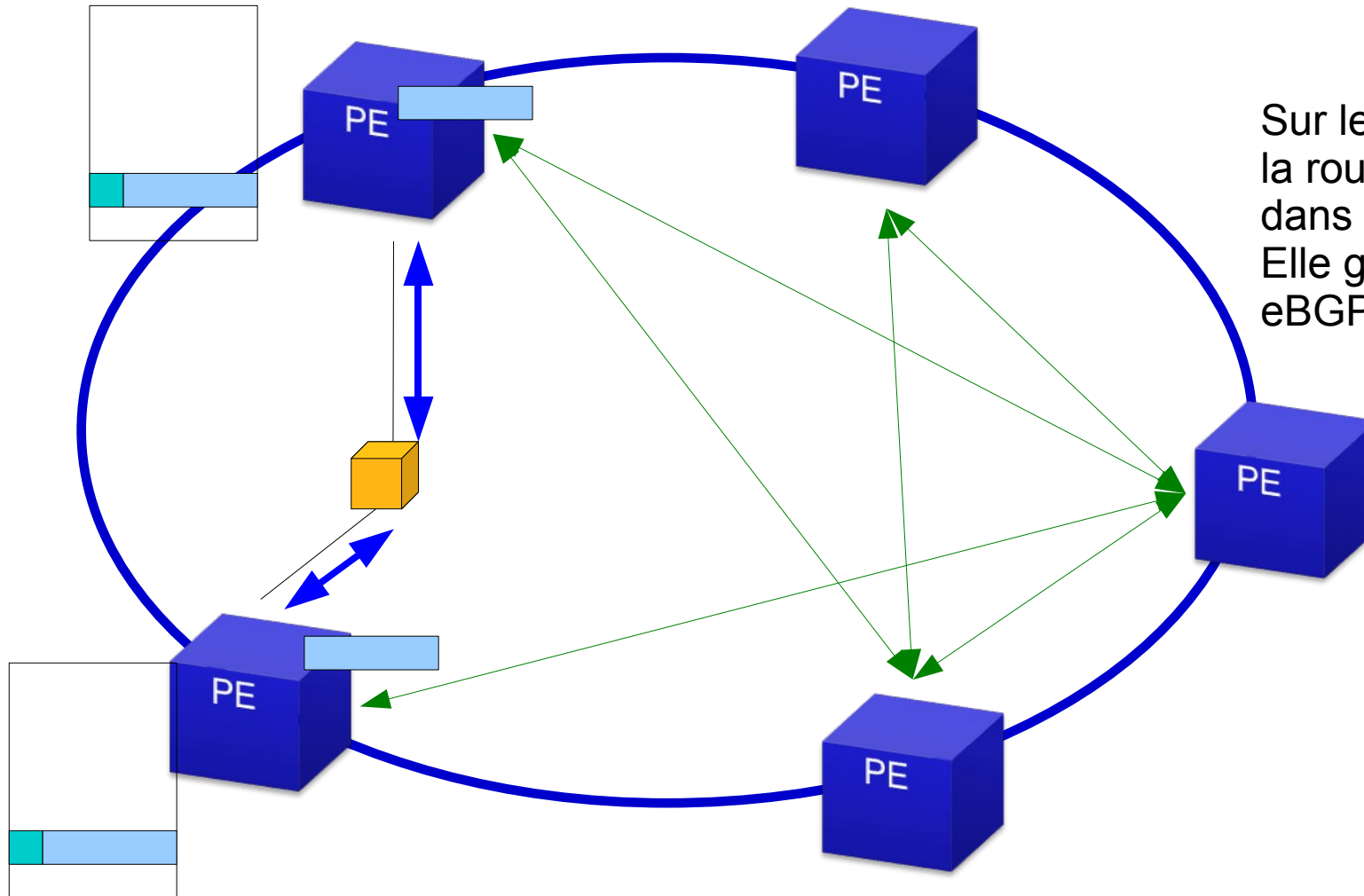


Les L3VPN sur RAP

Propagation dans l'iBGP

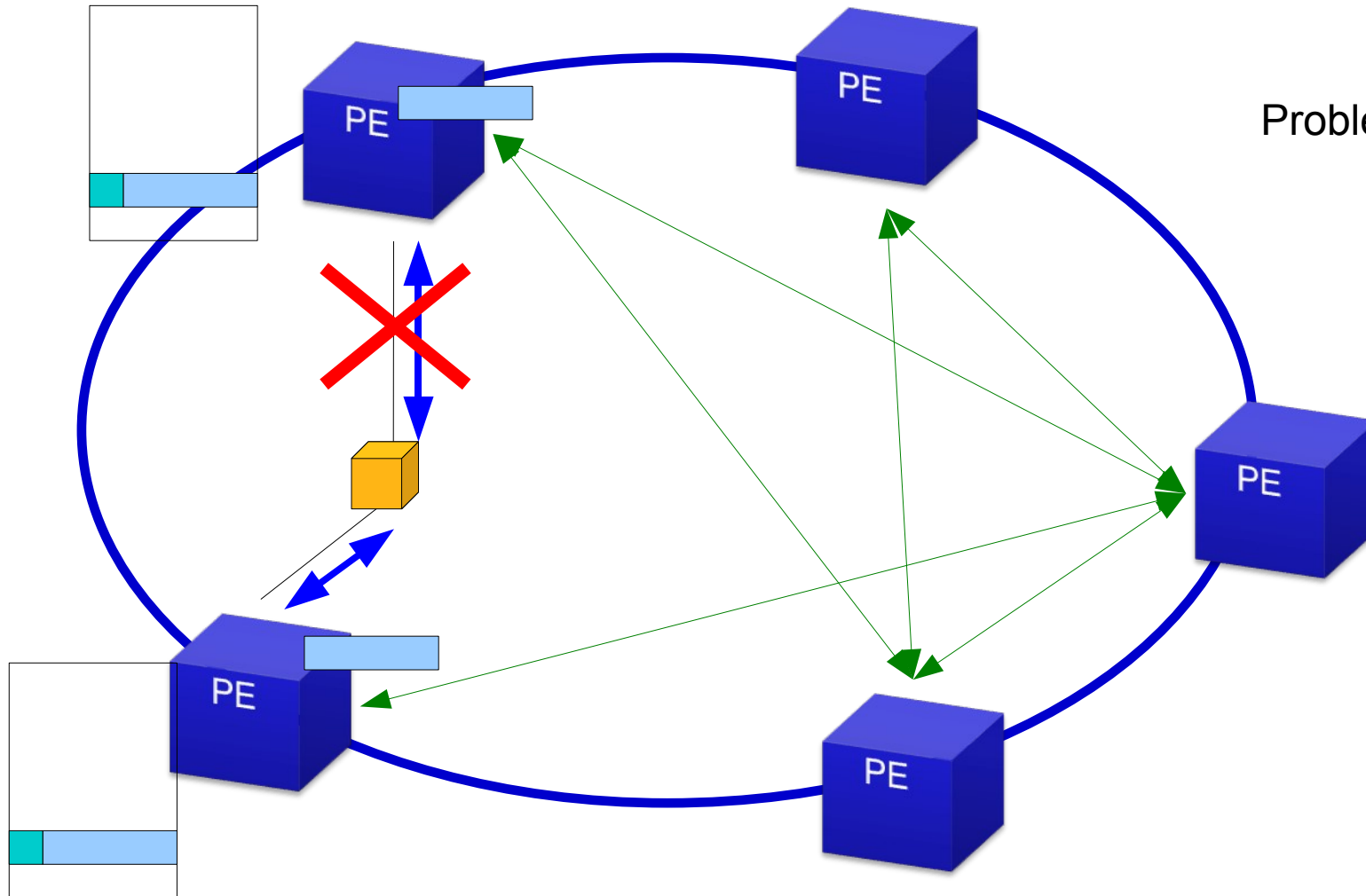


Les L3VPN sur RAP



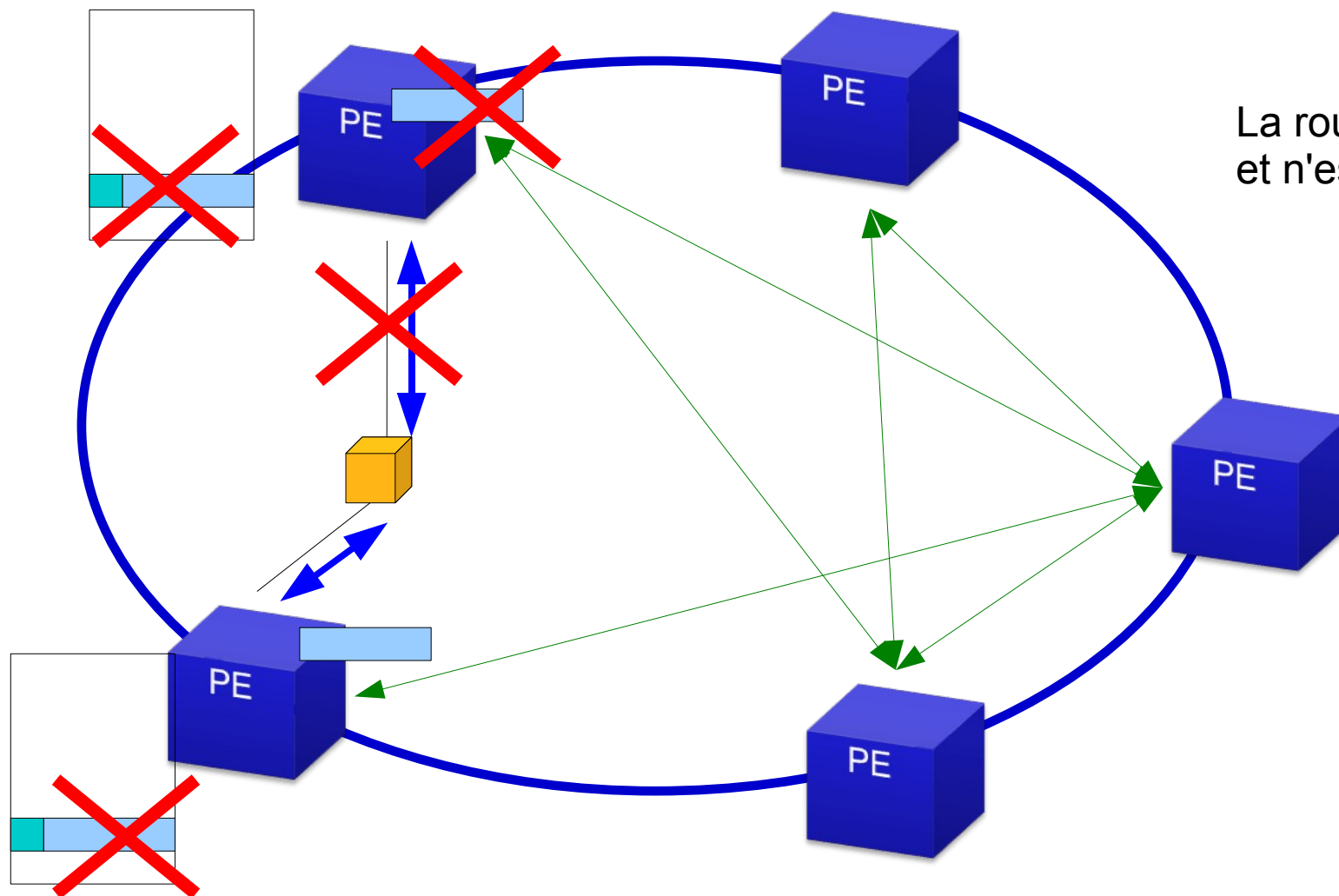
Sur le deuxième PE,
la route iBGP est reprise
dans la VRF
Elle gagne contre la route
eBGP car local-preference

Les L3VPN sur RAP



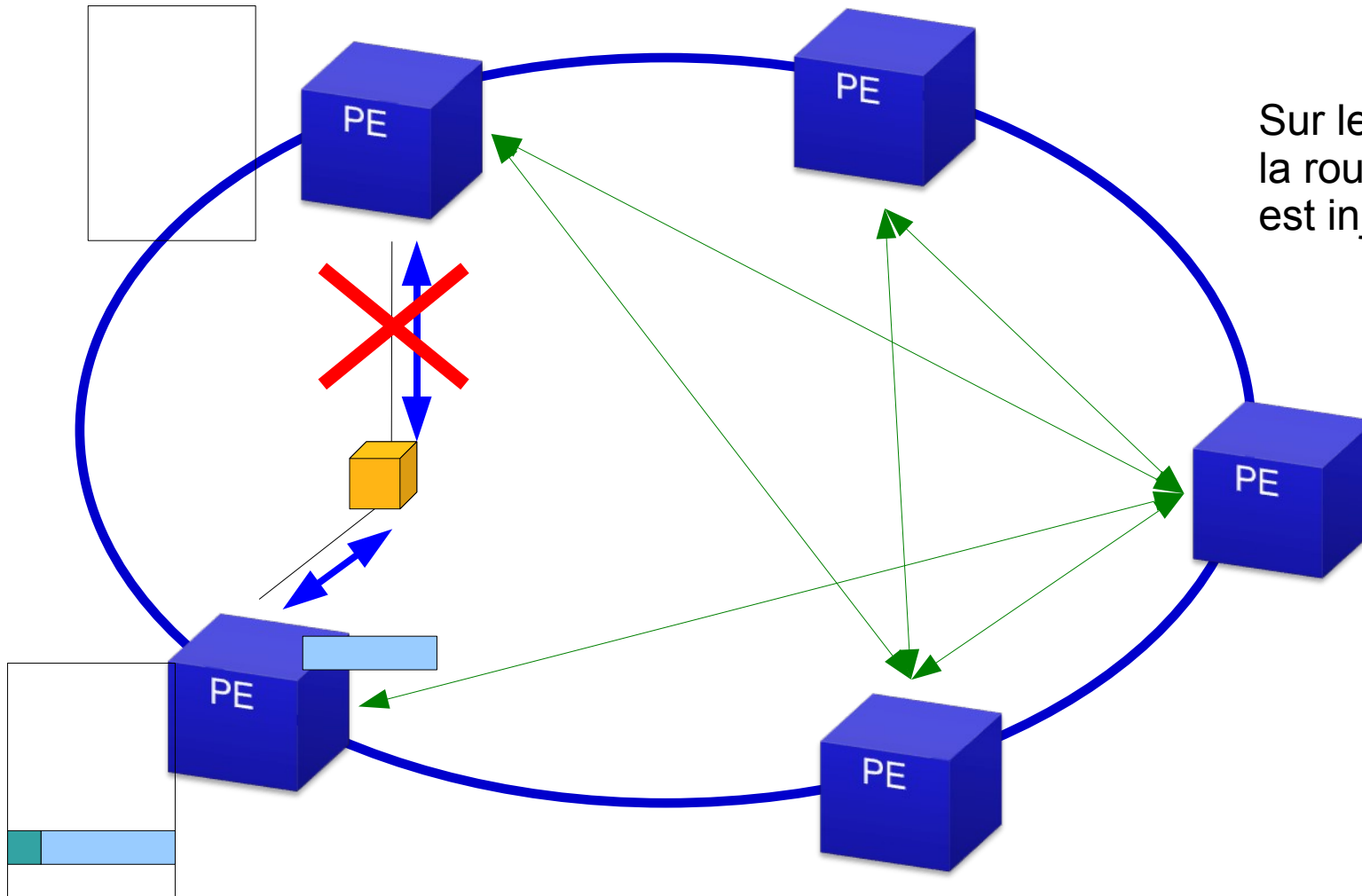
Problème sur le lien nominal

Les L3VPN sur RAP



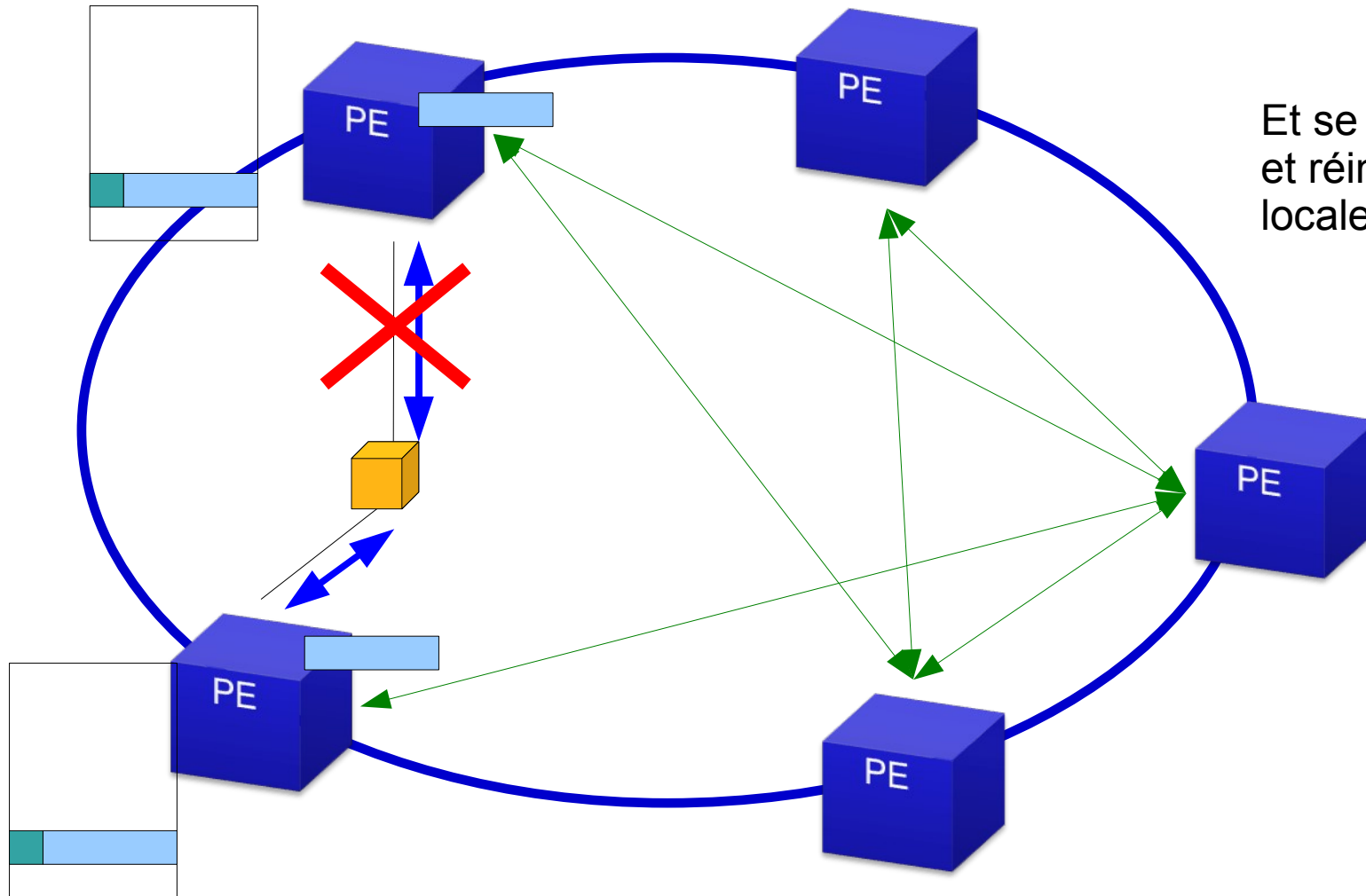
La route disparaît de la VRF et n'est plus propagée

Les L3VPN sur RAP



Sur le PE de secours,
la route eBGP de la VRF
est injectée dans l'iBGP

Les L3VPN sur RAP



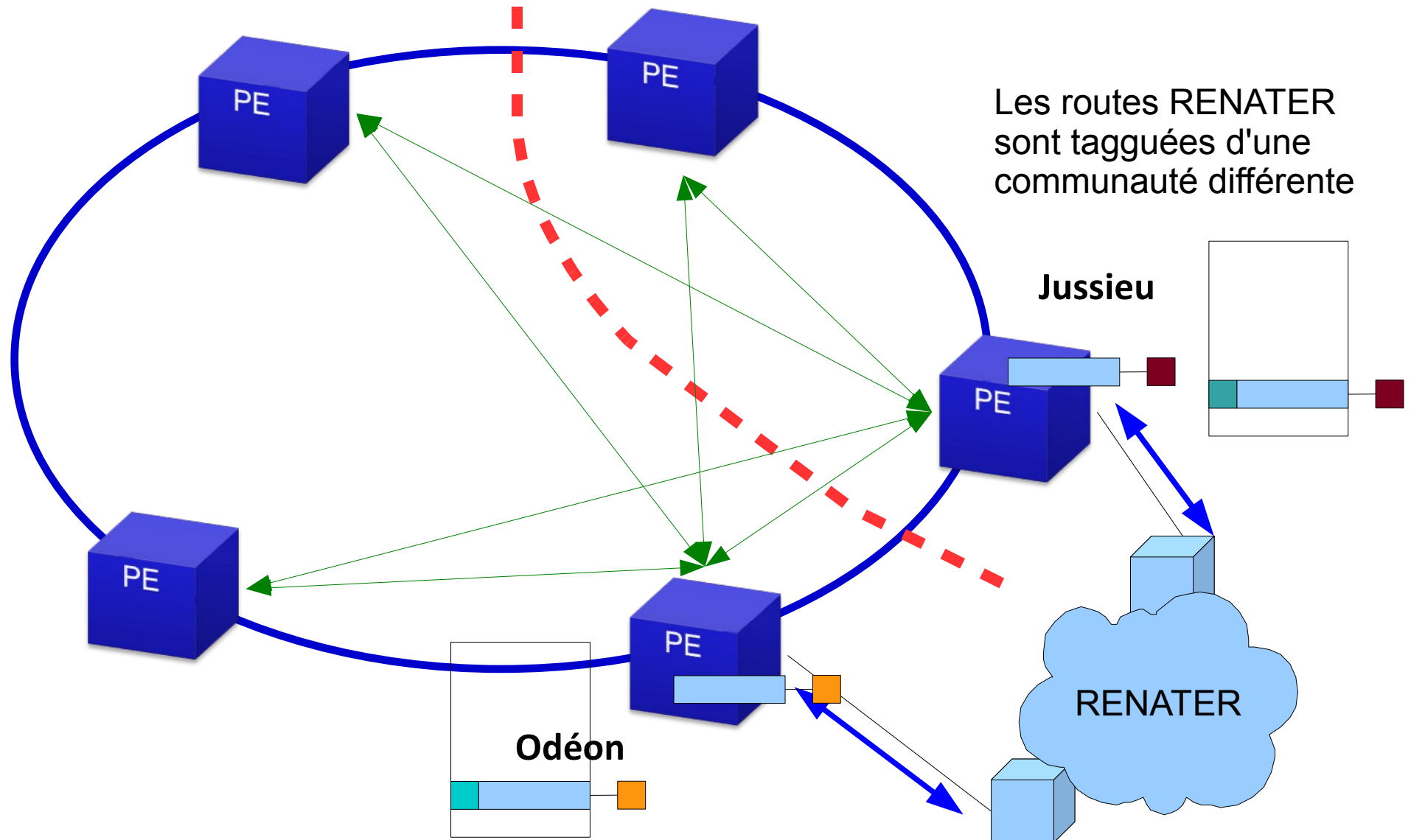
Et se retrouve propagée et réinjectée dans les VRF locales

Les L3VPN sur RAP

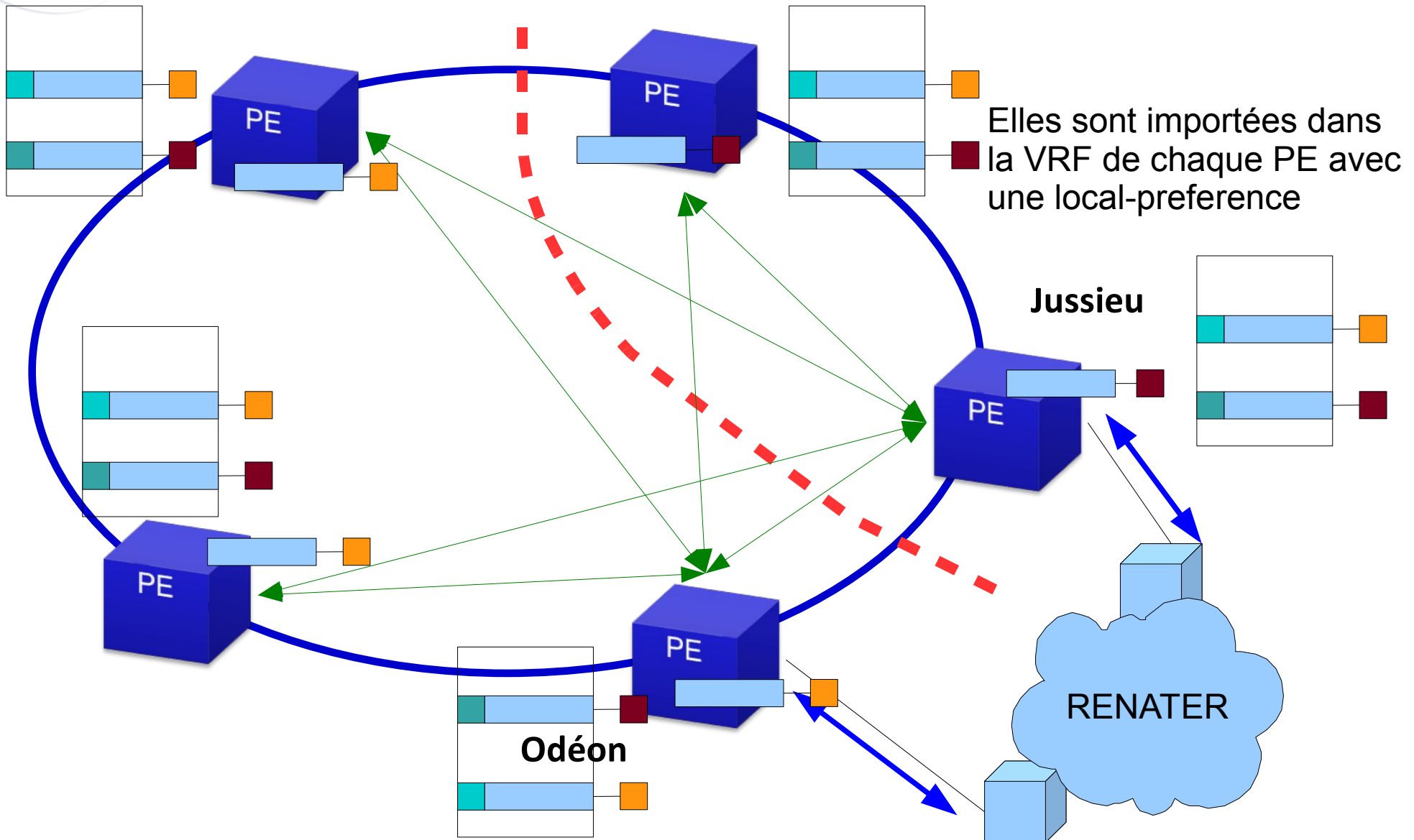


- Raccordement vers RENATER
- => communauté BGP pour réaliser la répartition des flux

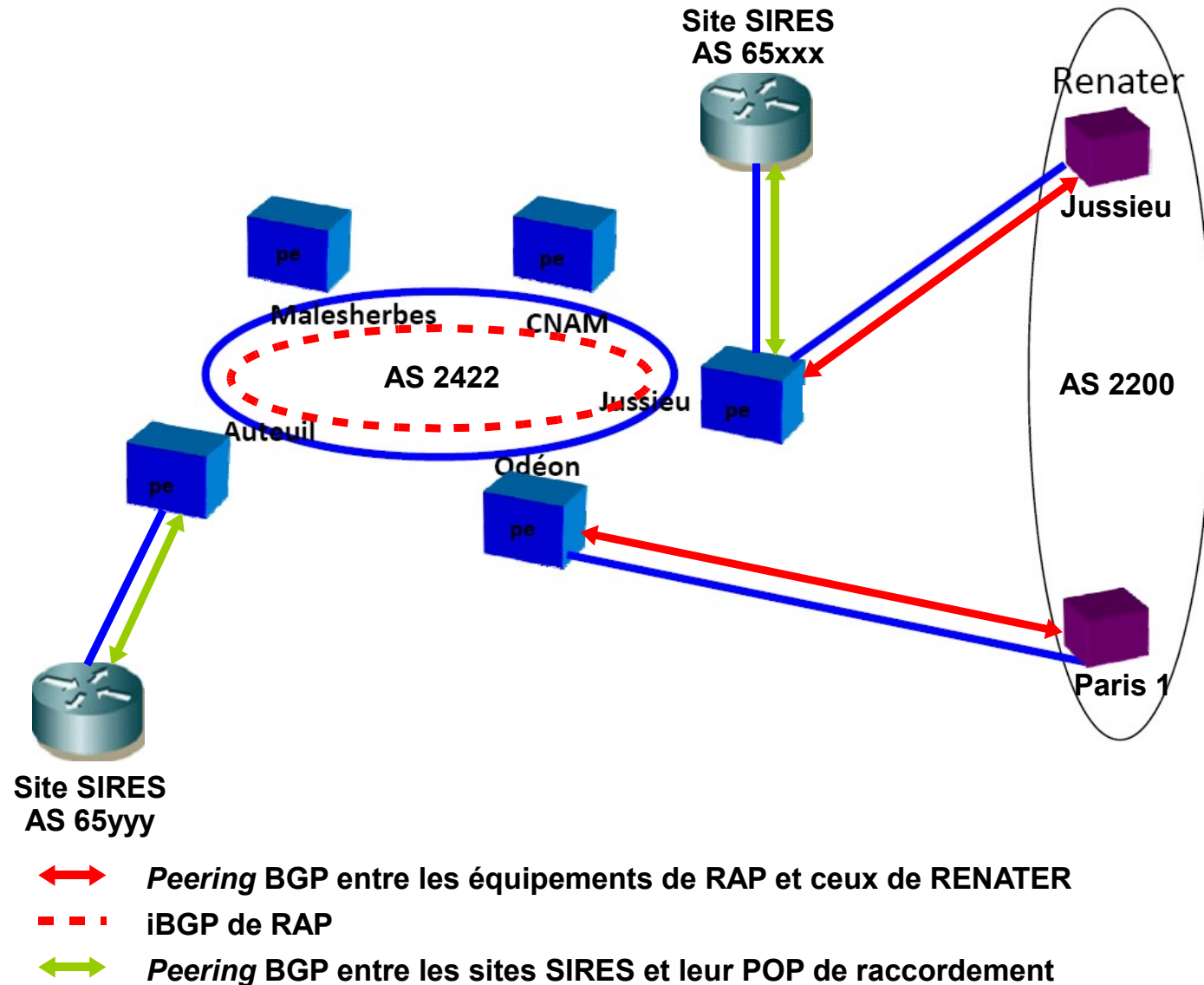
Les L3VPN sur RAP

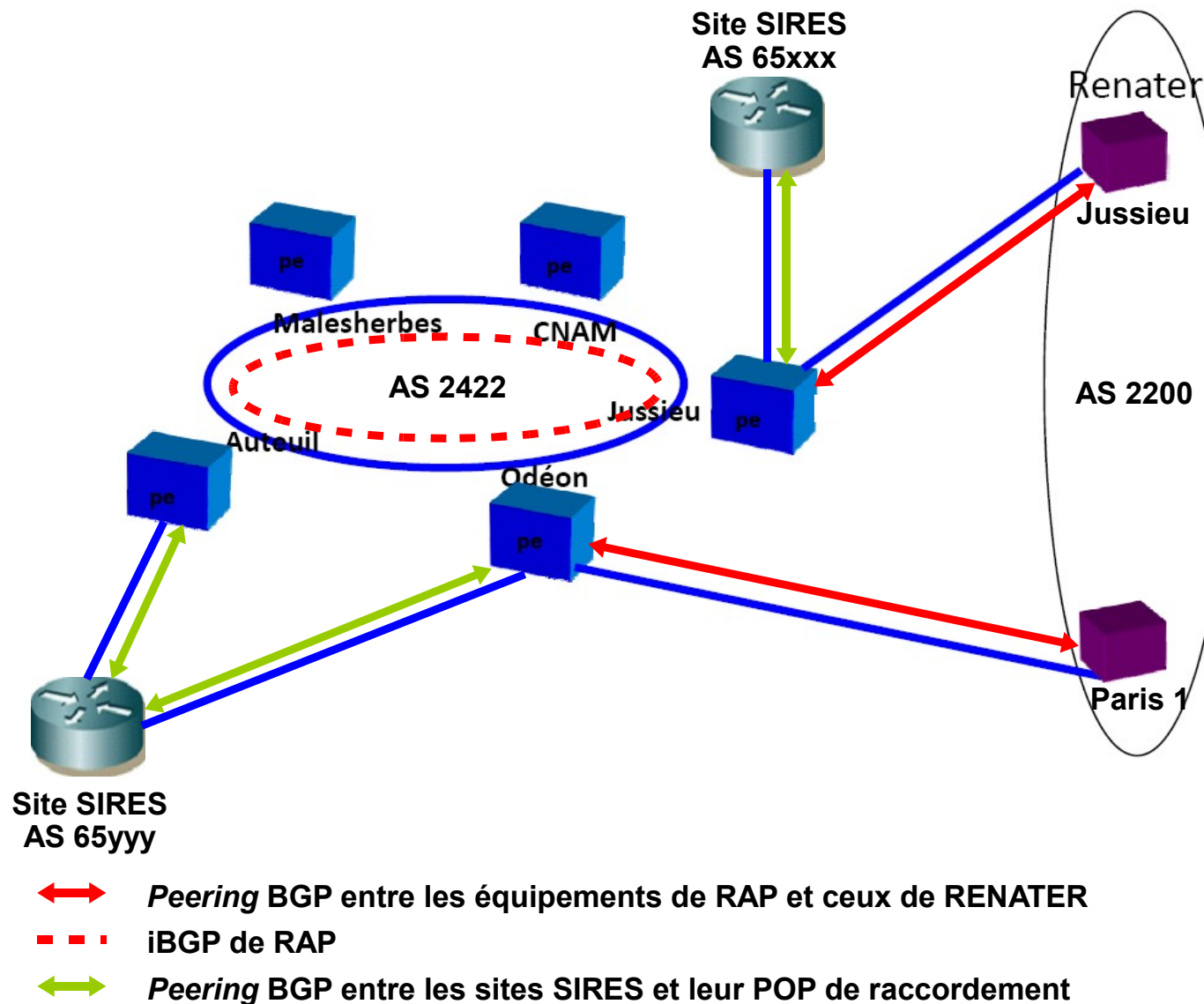


Les L3VPN sur RAP



- Le réseau SIRES
 - historique
 - architecture de SIRES 2
 - mise en œuvre et premier déploiement sur RAP
- Les L3VPN sur RAP
 - architecture de routage
 - détails de la mise en œuvre
- **SIRES 2 sur RAP : architecture cible**





Conclusion

- Les L3VPN permettent de disposer d'une infrastructure de routage dédiée à moindre coût
- La complexité du routage est prise en charge par l'opérateur

Remerciements

A tous ceux qui ont participé au projet :

- cellule réseau de la DSI du CNRS
- équipes RSI des DR du CNRS
 - et plus particulièrement ceux qui ont participé à la maquette
- RENATER
- Réseaux métropolitains et régionaux
 - et plus particulièrement RAP