Les tunnels & les VPN

ORGANISATION INTERNATIONALE DE la francophonie

cedric.foll@(education.gouv.fr|laposte.net)
Ministère de l'éducation nationale

Atelier sécurité
Rabat – RALL 2007

L'enjeu

« There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government. »

Bruce Schneier

Plan

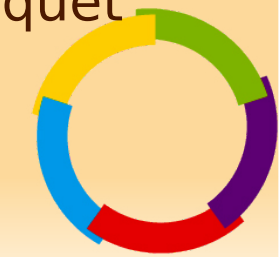
- Le principe des tunnels
- Les VPN

Les tunnels

- Objectif
  - Permet de contourner des problèmes de routage ou de filtrage
    - Interconnecter deux sites IPv6 en passant par un réseau IPv4.
    - Faire transiter un adressage privé (RFC1918) sur un réseau public.
    - Propager un réseau de couche 2 au dessus d'un réseau IP.
    - Contourner la politique de filtrage d'un firewall
    - ...

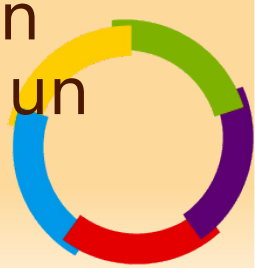
Quelques exemples

- En général on encapsule de la couche 2 ou 3 dans de la couche 3.
  - Tunnel GRE (generic router encapsulation)
    - Encaspulation de couche 3 au dessus de couche 3, supporté par la plupart des matériels.
    - Protocole IP numéro 47
  - IPSec, nativement sur IPv6, porté sur IPv4
    - Encapsulation d'un paquet de couche 3 chiffré et/ou signé dans un paquet de couche 3 (ESP) ou 4 (ESP over UDP ou TCP)
  - L2TP
    - Encapsulation d'un paquet de couche 2 dans un paquet de couche 4 (UDP port 1701)
  - IPv6 over IPv4 (et le contraire)



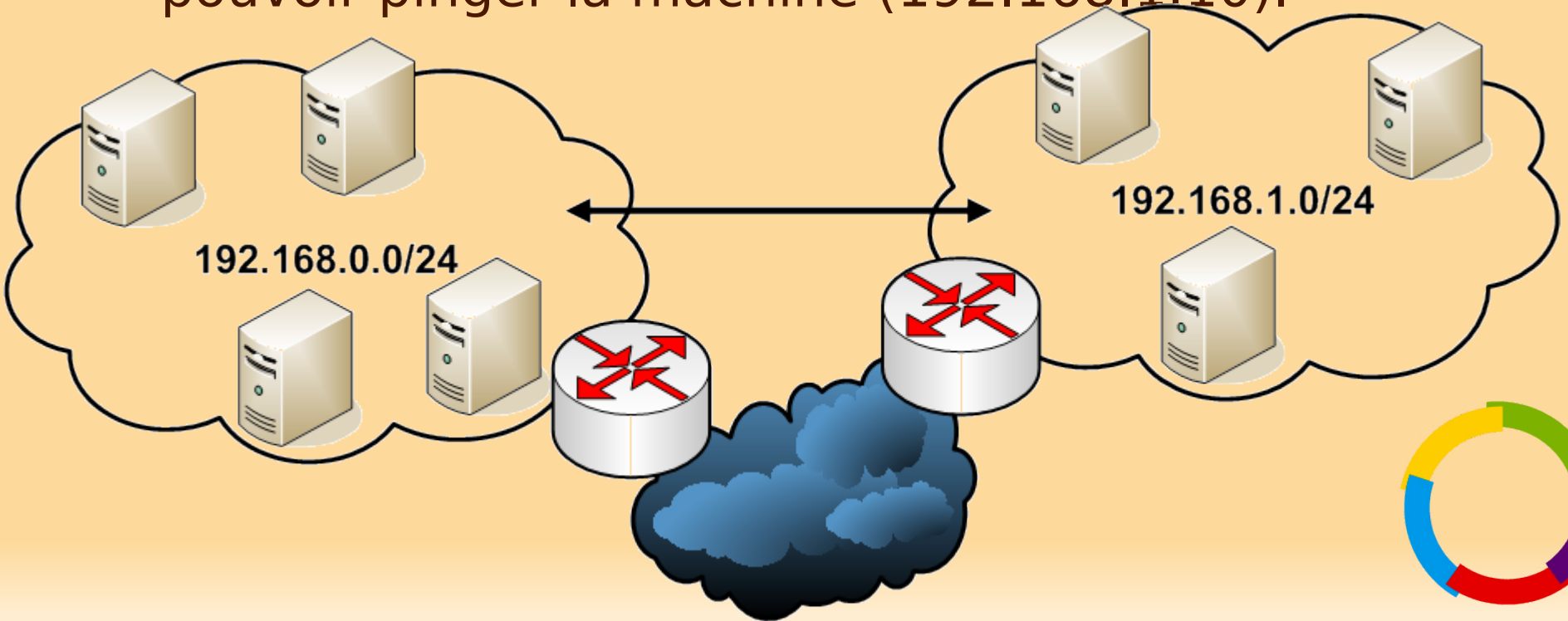
Quelques exemples

- On peut aussi monter des tunnels plus exotiques pour contourner une politique de filtrage sévère
  - IP sur ICMP, SMTP, HTTP, SSL, ...
  - IP sur DNS (« pratique » pour ne pas payer le wifi à l'hotel)
- Ou monter des tunnels dans des tunnels
  - L2TP over IPSec
    - On encapsule dans un paquet IP/ESP (IPSec) un paquet IP/UDP (L2TP) qui lui même encapsule un paquet de couche 2 (la charge utile).



L'exemple de GRE

- Problématique
  - Deux sites en adressage privé et connectés à Internet veulent communiquer.
    - Une machine d'un site (192.168.0.10) veut pouvoir pinger la machine (192.168.1.10).



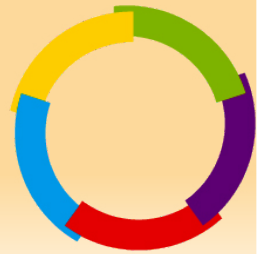
Création des tunnels GRE

- Sur le routeur de gauche d'IP 194.167.110.1 et 192.168.0.250

```
création du tunnel
#ip tunnel add netb mode gre remote
  194.167.110.128 local 194.167.110.1 ttl 255
montée de l'interface à laquelle on assigne une ip
#ip link set netb up
#ip addr add 192.168.0.251 dev netb
on peut router par cette interface
#ip route add 192.168.1.0/24 dev netb
```

- Sur le routeur de droite d'IP 194.167.110.128 et 192.168.1.250

```
#ip tunnel add netb mode gre remote 194.167.110.1
  local 194.167.110.128 ttl 255
#ip link set netb up
#ip addr add 192.168.1.251 dev netb
#ip route add 192.168.0.0/24 dev netb
```



Pour aller plus loin

- Si l'on veut pouvoir propager ses VLANs d'un site à l'autre?
  - Il faut un tunnel de couche 2 tel que L2TPv3

Les VPN

- La problématique
  - Je dispose de sites interconnectés par un réseau public et je voudrais faire « comme si » je disposais d'un réseau privatif
    - On crée donc un « réseau privé virtuel » (PVC) ou en anglais un « virtual private network ».

Les VPN

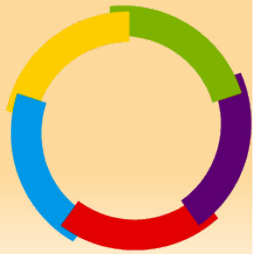
- Un réseau privatif ?
  - Propagation de ma couche 3 (je tire des cables entre mes routeurs d'entrée de site).
  - Propagation de ma couche 2 (je tire des cables entre mes switchs).
  - J'ai de la sécurité (personne ne peut écouter mon trafic ni le modifier).
  - J'ai un excellent niveau de service car, étant le seul utilisateur des liens, mon trafic n'est pas gêné par le trafic d'autres clients.
- Le problème
  - ...c'est cher

Les VPN

- Beaucoup de technologies existent répondant à tout ou partie de ces problèmes
  - L'exemple du GRE
    - Ne répond qu'à une propagation de couche 3...
    - Peut mieux faire...

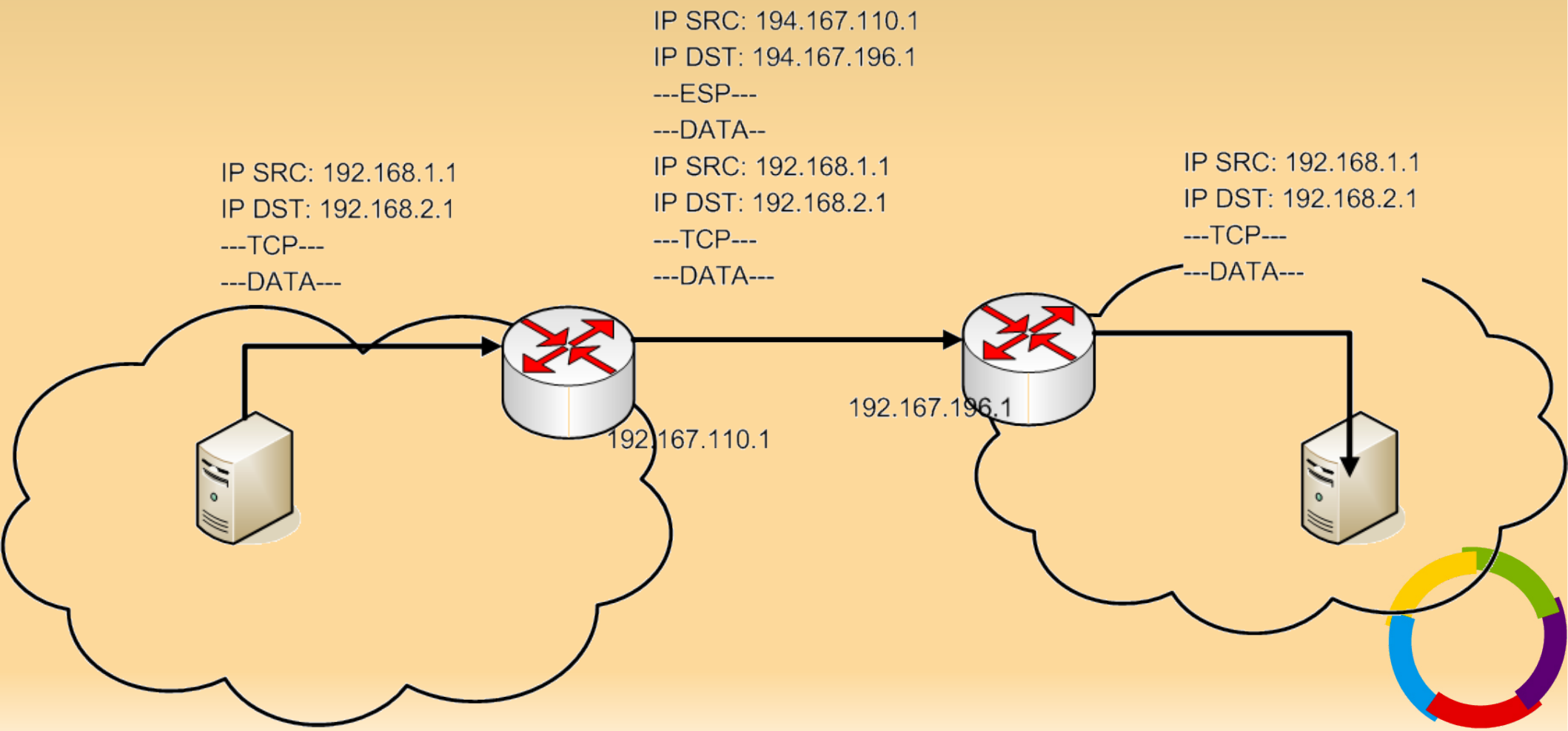
Les VPN

- Plan
  - GRE (déjà vu)
  - IPSec
  - MPLS
  - L2TPv3, un MPLS light
  - Group Encrypted Transport (GET) VPN
    - Le MPLS « IPsecisé » par cisco



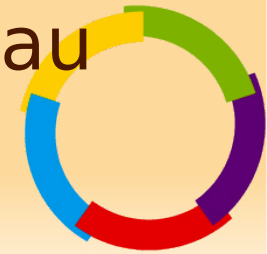
Solution IPSec

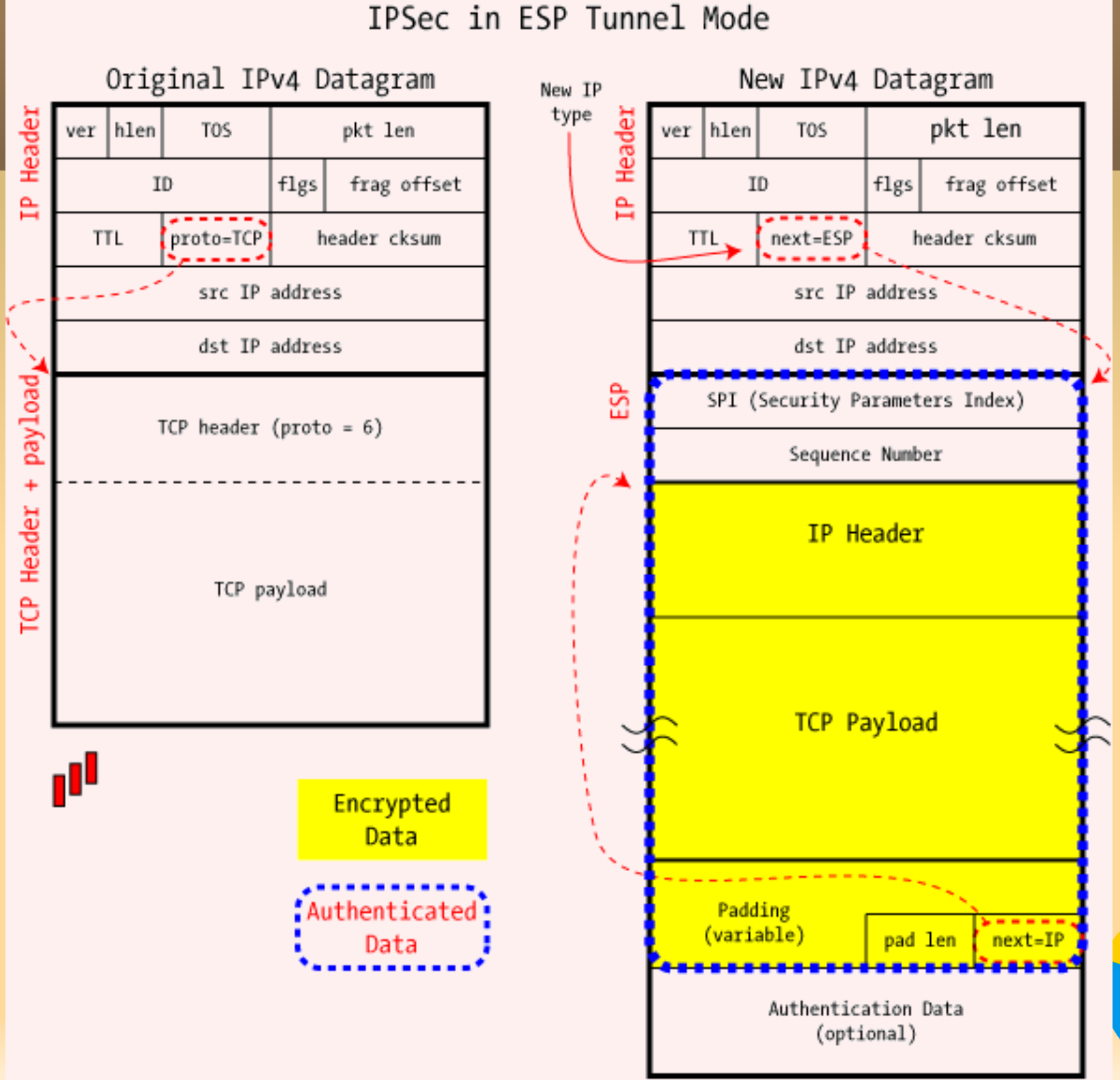
- Le paquet IP est encapsulé dans un autre paquet.



IPSec

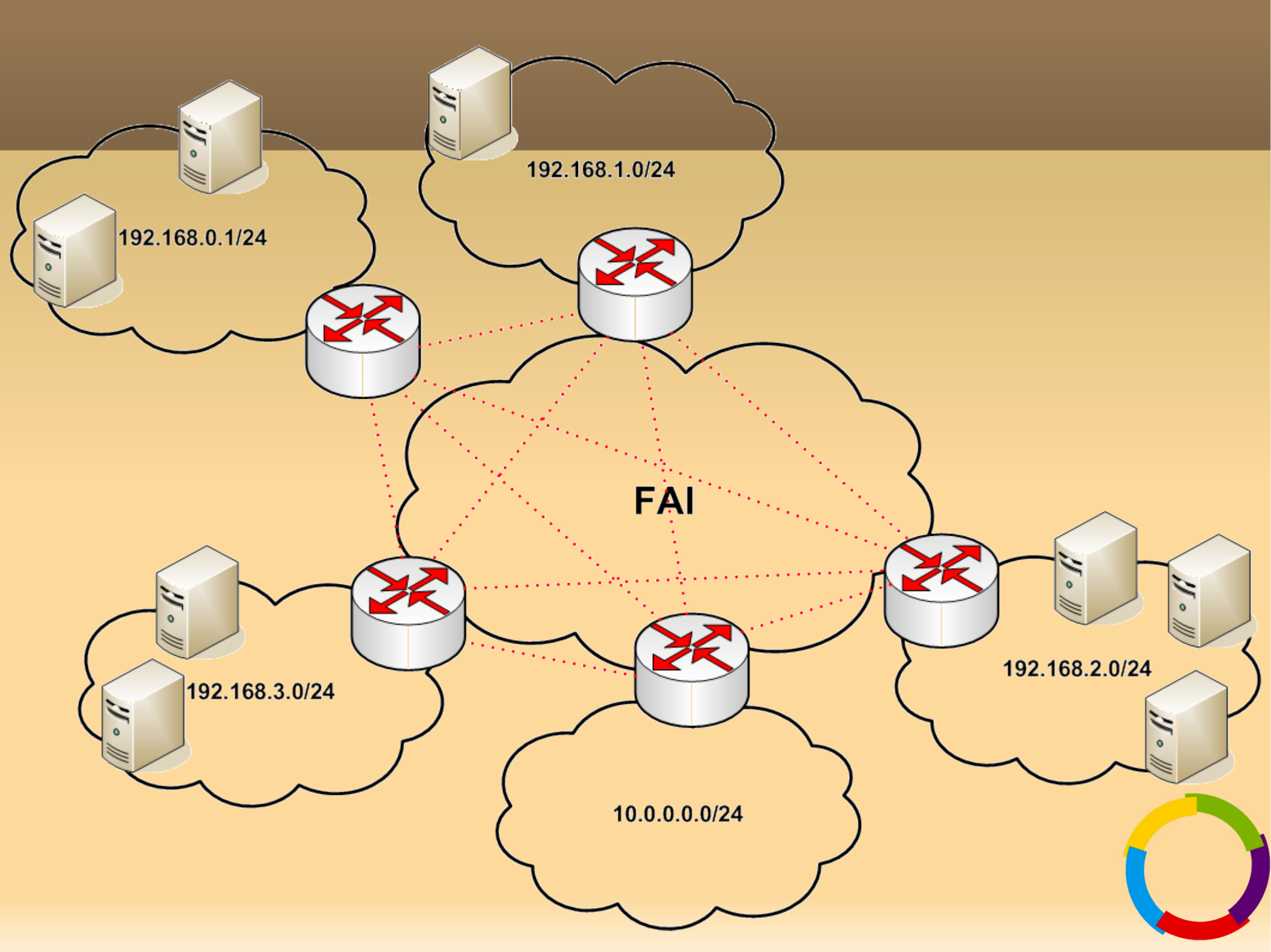
- Les paquets IP sont encapsulés par les routeurs IPSec.
  - Le protocole de couche 4 est AH (Authentication Header) ou ESP (Encapsulating Security Payload)
    - AH: les paquets sont stockés en couche data et signés numériquement.
    - ESP: les paquets sont stockés de manière chiffrée en couche data.
  - Remarque: il est possible d'utiliser IPSec autrement qu'en mode tunnel. Dans ce cas IPSec sert seulement à augmenter le niveau de sécurité, utilisé par exemple pour les postes nomades.




IPSec in ESP Tunnel Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
Encrypted Data
Authenticated Data
New IP type
New IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
next=ESP
header cksum
src IP address
dst IP address
ESP
SPI (Security Parameters Index)
Sequence Number
IP Header
TCP Payload
Padding (variable)
pad len
next=IP
Authentication Data (optional)

IPSec

- Initialisation de la connexion:
  - Via Pre-shared Key
    - Comme un Diffie-Hellman mais les tiers possèdent un secret en commun évitant une attaque MITM.
  - En mode PKI.


192.168.1.0/24
192.168.0.1/24
FAI
192.168.3.0/24
192.168.2.0/24
10.0.0.0/24

Remarques

- Sur chaque routeur il faut définir une route pour chacun des réseaux.
- Pour N routeurs il faut définir N*(N-1) routes.
- L'ajout ou la suppression d'un routeur implique une intervention sur tous les autres.

IPSec

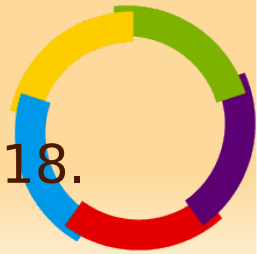
- Les plus:
  - Permet de réaliser un VPN assez simplement et à bas coût (un pc sous linux fait l'affaire).
  - Système robuste et offrant un niveau de sécurité élevé.
  - S'appuie sur une PKI avec les avantages en terme de sécurité tel qu'isoler un site en révoquant son certificat (en cas de compromission).

IPSec

- Les moins:
  - Performances moyennes. Peu adapté aux flux multimédias, en particulier la VoIP.
    - Procédure de chiffrement/déchiffrement « limite » les débits et ajoute de la latence.
    - Impossible de faire de la QoS
      - Les techniques de QoS se basent généralement sur des champs de la couche IP et là ils sont cryptés...
  - Lourd en terme de configuration:
    - Dès que l'on ajoute un réseau il faut construire une route sur chacun des routeurs.
  - Il faut un routeur IPSec dans chaque local à relier au VPN.

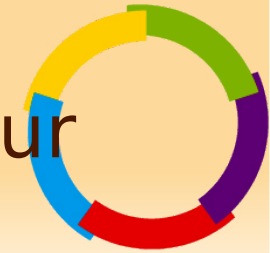
IPSec

- Réseau RACINE (Réseaux d'Accès et de Consolidation des INtranets de l'Education nationale)
  - Réseau interconnectant tous les collèges, lycées et sites administratifs (Rectorat, Administration Centrale) de l'éducation nationale française.
    - 10 000 sites interconnectés en IPSec (métropole et DOM/TOM)
    - Un backbone full mesh de 30 sites (Rectorats) composé de PIX 515E
    - Un réseau étoilé interconnectant les collèges et lycées (10 000 sites) au Rectorat dont ils dépendent composé d'une distribution linux maison (http://eole.orion.education.fr/)
    - Un plan d'adressage IP normalisé basé sur la RFC1918.



VPN IP par MPLS
Multiprotocol Label Switching

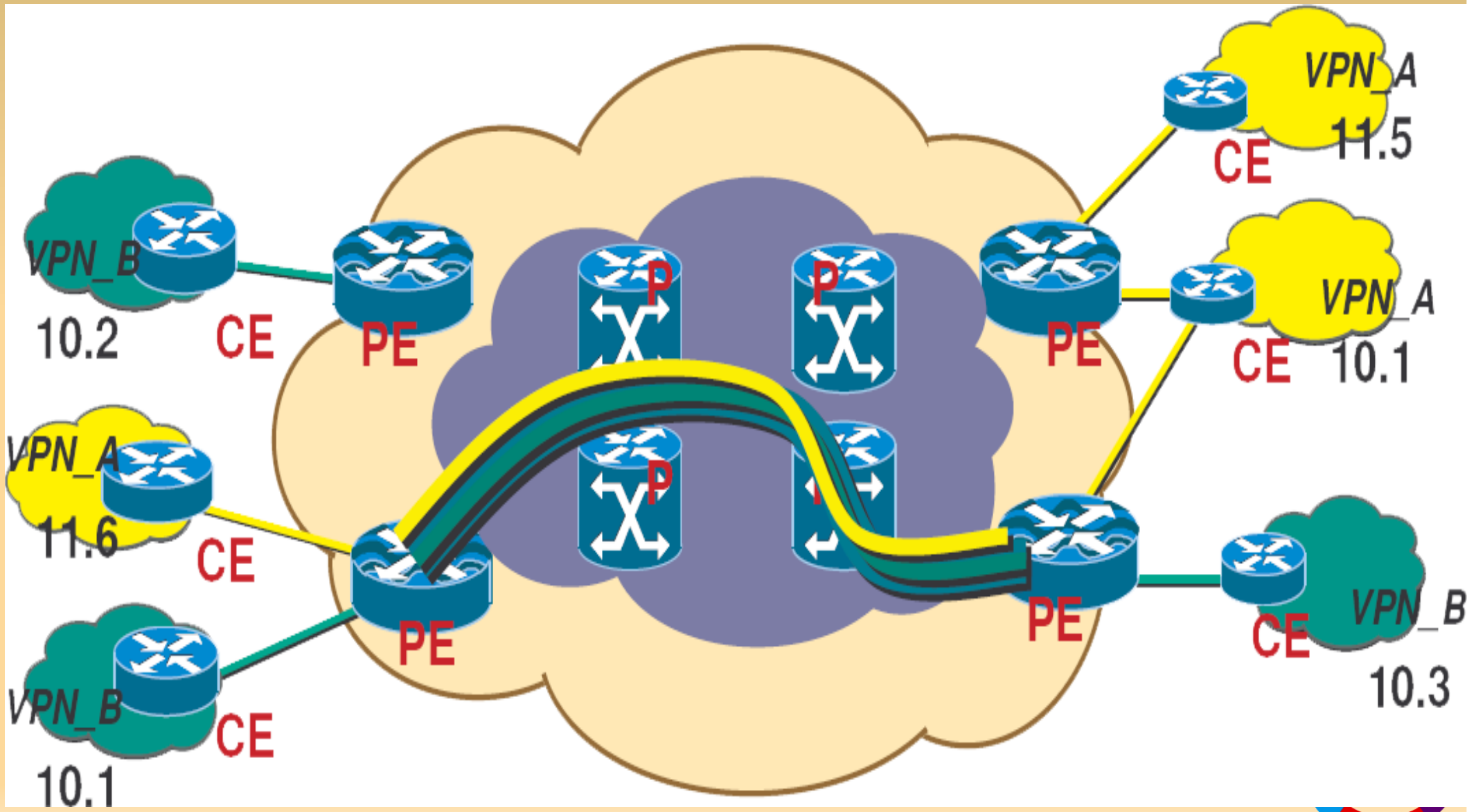
- Technologie de couche 2,5 (ie 2 et 3).
- L'opérateur « tag » les flux de chacun de ses clients.
- Sur chacun des routeurs de l'opérateur, une VRF (Virtual Routing and Forwarding) est créée pour chacun des tags.
- Complètement transparent du coté du routeur du client (Custumer Edge):
  - Du point de vue du client, il est le seul utilisateur du FAI et peut donc propager sur son FAI son adressage privé.



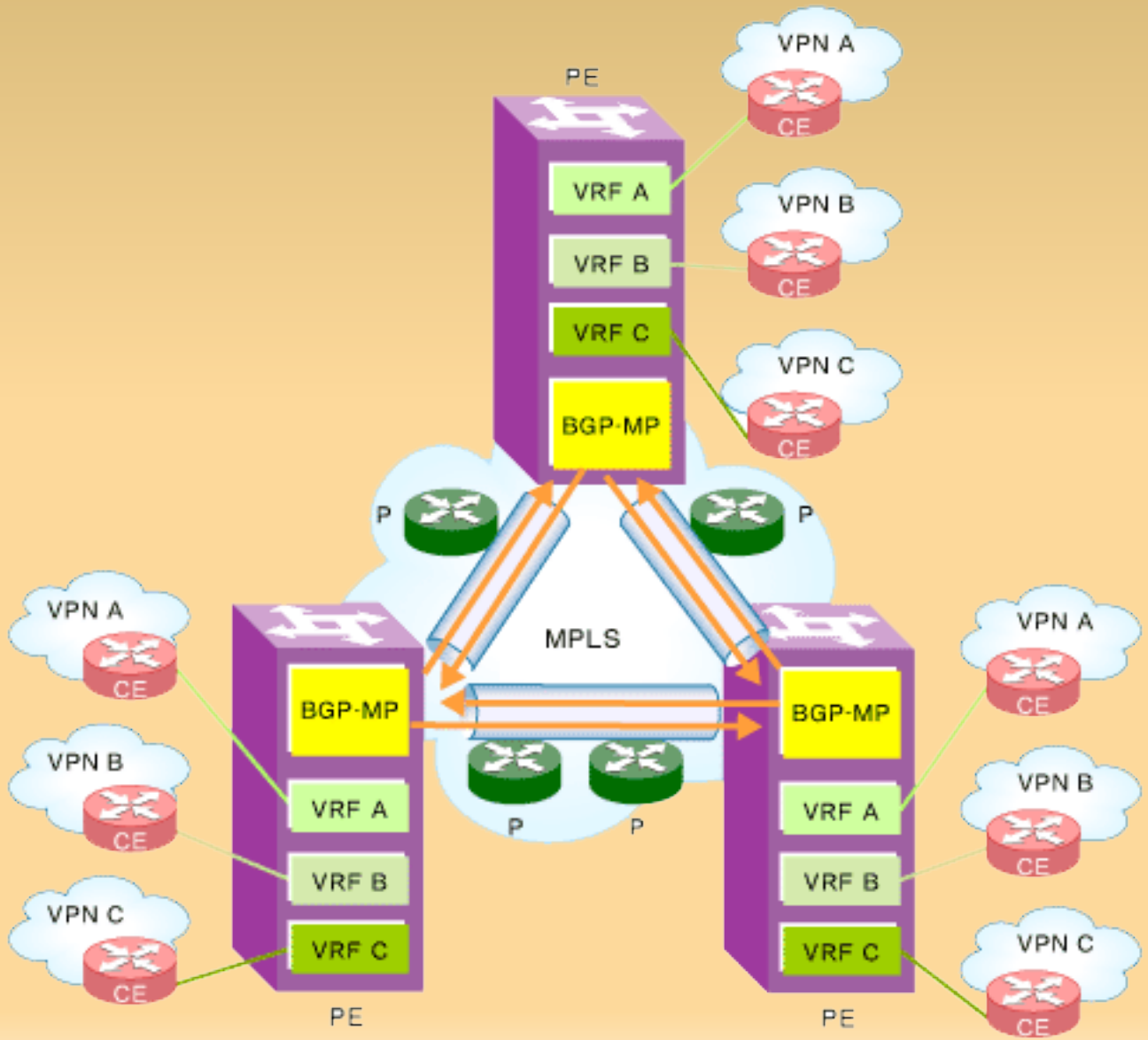
VPN IP par MPLS

- Configuration coté client (customer edge):
  - Aucune configuration nécessaire.
- Configuration coté ISP (provider edge):
  - Un tag est ajouté sur les paquets de chaque client.
  - Chacun des routeurs possède une table de routage spécifique pour chacun des clients (VRF).
  - Le routeur décide quelle VRF utiliser en analysant le tag MPLS sur le paquet reçu.
  - Les routes de chaque VRF sont échangées entre les routeurs de l'ISP via BGP.

VPN IP par MPLS



VPN IP par MPLS



VPN IP par MPLS<->IPSec

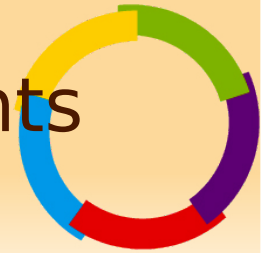
- Avec IPSec:
  - Tout le routage est géré par le client ... et c'est du routage statique.
    - Une opération (ie ajout/suppression) sur un réseau doit être répercutée manuellement sur tous les réseaux.
- Avec MPLS:
  - Le routage est géré par l'ISP via BGP.

VPN IP par MPLS

- Inconvénients par rapport à IPsec
  - Plus de chiffrement, un pirate réussissant à compromettre l'ISP va pouvoir lire tous les échanges et altérer des données.
  - C'est l'opérateur qui gère le VPN
    - L'opérateur doit le supporter (donc ce n'est pas un opérateur grand public ADSL...)
    - Cela a un coût!
    - Il faut être dans la pratique mono-opérateur pour chacun des sites.

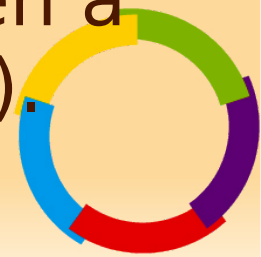
VPN IP par MPLS

- Avantages par rapport à IPSec:
  - Sécurité de niveau 2. A moins de compromettre l'ISP, un pirate ne pourra jamais atteindre un LAN privé à moins d'être branché au bon endroit (et donc d'être correctement taggé).
  - Il est possible de faire de la QoS de bout en bout (la couche IP n'est pas altérée, ce qui permet de classer les flux coté opérateur).
  - Plus de problèmes de routage à gérer.
  - Plus besoins d'équipements de chiffrements sur les sites.



MPLS, utilisation typique

- Pour les données VoIP
  - Ne peuvent pas être NATées
  - Les performances d'IPSec rendent l'utilisation de la VoIP quasi impossible.
- Pour les petits sites reliés via internet à la maison mère.
  - Sur chaque site quelques PC en adressage privé et un routeur d'entrée de gamme.
  - Reliés à la maison mère via VPN MPLS (rien à faire sur le site en terme de configuration).



Ethernet over MPLS (EoMPLS)

- MPLS permet également de propager son niveau 2
  - L'opérateur encapsule dans les paquets MPLS les paquets Ethernet des clients
    - Ceci est en fait de l'Ethernet encapsulé dans un paquet Ethernet avec un tag MPLS entre les deux.
  - Possibilité de propager ses VLANs sur Internet (le graal de l'architecte réseau)

L2TPv3

- Similaire à du GRE transportant du niveau 2
- Cisco remet le L2TP sur le devant de la scène (rfc 3931, mars 2005)
  - Possibilité d'encapsuler n'importe quel protocole de couche 2 (et plus seulement ppp) et donc possibilité de propager ses VLANs.
- Une alternative séduisante à EoMPLS
  - On perd certaines fonctionnalités de QoS offertes par MPLS et le routage géré par l'ISP.
  - On gagne une indépendance vis à vis de l'opérateur, la technologie ne repose plus sur lui.

Et si l'on en veut encore plus???

- On sait propager de la couche 2
  - EoMPLS ou L2TPv3
- On a de la QoS
  - EoMPLS et dans une moindre mesure L2TPv3
- Quid de la confidentialité/intégrité ?
  - Gestion en extrémité (ie remplacement de telnet par ssh, http par https, ...)
    - Insatisfaisant coté architecte réseau (car dépend des ingénieurs système)
  - Technologie Group Encrypted Transport (GET) VPN par cisco

Group Encrypted Transport (GET) VPN

- Comme son nom l'indique, on ne chiffre que la couche transport...
  - C'est de l'IPSec où la couche 3 n'est pas altérée
    - Le client doit s'appuyer sur un mécanisme, typiquement MPLS, pour propager son adressage privé sur le réseau opérateur.
      - On garde toute la souplesse de MPLS et les possibilités de QoS (la priorité des paquets est définie via un tag sur la couche IP)
      - On retrouve les mécanismes de chiffrements d'IPSec