# Module M3102 – TP4

# MPLS : L2-VPN par Ethernet over MPLS (EoMPLS)

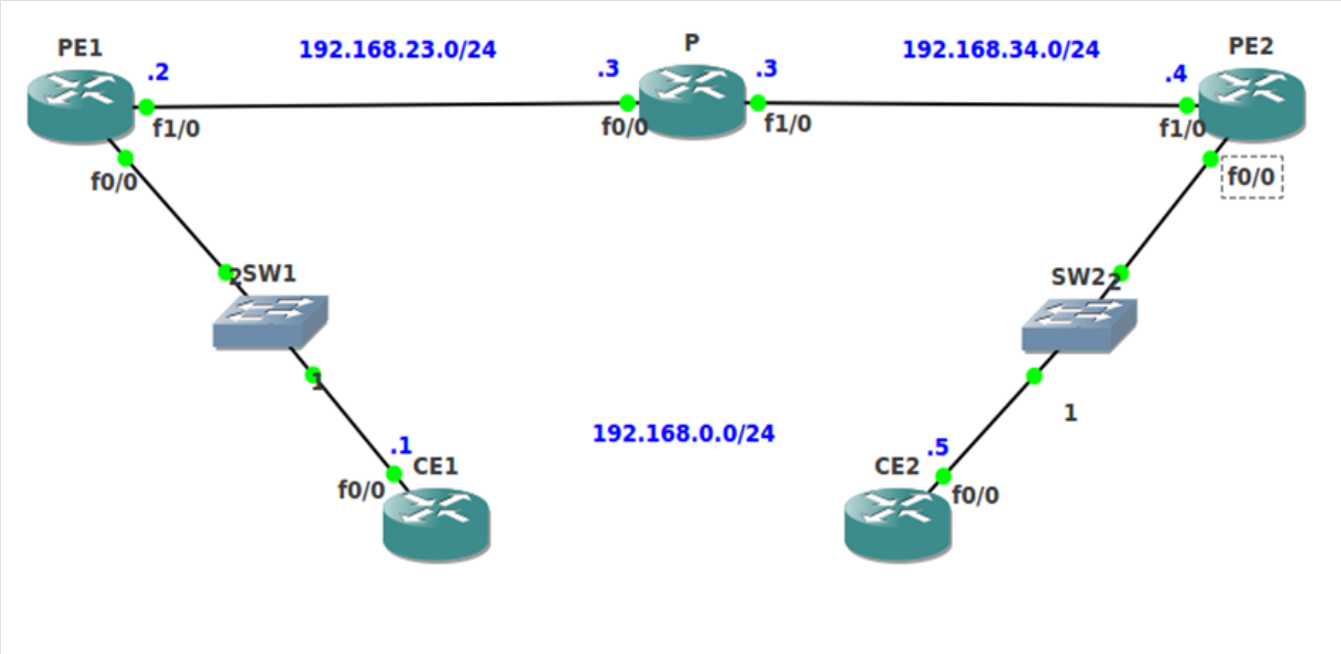
***Ce qu'on veut faire dans ce TP*** : Permettre à l'ISP d'établir un VPN de couche 2 entre les sites distants de chaque client (1 client ici, donc 1 VPN). Le client veut voir l'ISP comme un switch qu'il possède entre ses 2 sites. Les CE de chaque site appartiennent donc au même LAN.

***Pourquoi*** : Car chaque client veut être parfaitement isolé des autres possibles clients de l'ISP : ne voir aucun trafic, ni de données ni de contrôle d'autres clients (comme updates de spanning tree, broadcasts ARP, etc.), ainsi qu'avoir la possibilité d'utiliser n'importe quelles adresses MAC, indépendamment des autres clients.

***Comment*** : Par une configuration de VPN de niveau 2, à travers le réseau de l'ISP. Utilisation de tunnels MPLS bi-directionnels nommés pseudowires.

**Consignes générales** :

- Vous vous loggez sous votre compte perso, machine physique en Ubuntu.
- 1 compte-rendu par étudiant·e. Vous récupérez le pdf et l'odt du sujet depuis http://www.i3s.unice.fr/~sassatelli/M3102/
- Récupérez aussi le répertoire de topologie GNS3 *TP4_MPLS_l2VPN_initial.zip*.
- Joindre au rapport le fichier de config final du routeur (copié-collé de la config finale).




Les adresses IP de toutes les interfaces ont été configurées pour vous, comme indiqué sur le schéma. Tous les routeurs ont une interface de loopback L0 :

- CE1 : 1.1.1.1

- PE1 : 2.2.2.2
- P : 3.3.3.3
- PE2 : 4.4.4.4
- CE2 : 5.5.5.5

1. Configurer OSPF Area 0 entre les routeurs de l'ISP (PE1, P et PE2), en empêchant que les updates soient envoyées vers le client grâce à la commande `passive-interface`. Exemple sur PE 1 :

   ```
   router ospf 1
   network 0.0.0.0 255.255.255.255
   passive-interface fastethernet 0/0
   ```

2. Vérifier que les loopbacks de PE1, PE et PE2 peuvent se pinger.
3. Activer mpls sur les bonnes interfaces de ces routeurs par la commande

   ```
   mpls ip
   ```

4. Vérifier la table mpls des 3 routeurs, et la commenter (commande `sh mpls forwarding-table`).

5. Corroborez votre commentaire en réalisant et expliquant une capture wireshark sur Fa0/0 de P d'un ping depuis PE1 vers PE2 (ping 4.4.4.4 source loopback 0).

6. Nous allons maintenant créer un « pseudowire » entre fastethernet 0/0 de PE1 et fastethernet 0/0 de PE2, c'est-à-dire 2 LSPs, un dans chaque sens, pour établir la connectivité au niveau Ethernet entre CE1 et CE2. Pour cela, rentrer sur PE1 et PE2 les commandes adéquates sur les interfaces reliées au client (donc fastethernet 0/0) :

   ```
   xconnect <IP address of peer> <Vcid> encapulation mpls
   ```

   où :

   IP address of peer : adresse IP du routeur PE avec qui le pseudowire est établi. Toute trame entrant par l'interface sera envoyée vers ce PE distant avec l'encapsulation MPLS adéquate.

   VCid : numéro du pseudowire. Le couple (peerIP@,VCid) détermine le traitement subi par la trame au PE destination.

   Indiquer dans le rapport les commandes entrées, dans quel équipement et dans quel mode.

7. Vérifiez avec la commande

   ```
   sh mpls l2transport vc
   ```

   sur les 2 PE que le pseudowire est effectivement établi (état « up »).

   Faîtes un ping entre CE1 et CE2. Si le ping est un succès, c'est bon. Sinon, debuggez.

   Les 2 questions suivantes peuvent être faîtes en parallèle si c'est plus facile pour vous.

8. Examinez le résultat des 2 commandes suivantes et expliquer le traitement exact que va subir une trame ethernet arrivant de CE1 à destination de CE2, à chaque saut :

   ```
   sh mpls l2transport vc detail
   ```

```
sh mpls forwarding-table
```

9. Lancez 4 captures : sur Fa0/0 de PE1, sur Fa0/0 de P, sur Fa1/0 de PE2 et sur Fa0/0 de PE2. Faîtes un ping de CE1 vers CE2 (qui doit être un succès), puis arrêtez les captures. Ouvrez ces 4 captures et détaillez en expliquant le traitement subi à chaque saut par la trame Ethernet encapsulant le ICMP echo request émise par CE1.

**Epilogue**

Dans ce TP, vous avez configuré un VPN de niveau 2, point à point. Point à point signifie que seul un pseudowire est établi, pour joindre donc uniquement 2 sites client. Si on désire un VPN multi-point au niveau Ethernet entre plus de 2 sites, alors il s'agit de la technologie VPLS qui permet de gérer les tables MAC par client à chaque PE. Ceci ne peut cependant pas être implémenté en TP à l'IUT car les équipements Cisco implémentant VPLS sont la série ASR 1000, correspondant à de lourds équipements fournis aux ISP en tant que PE, ou le CSR 1000V, image virtuelle qu'on peut insérer dans GNS3. Cependant cette image nécessite beaucoup de RAM, mais surtout une architecture de processeur post-Nehalem, soit au moins un Intel Core i7.

## *Source*

R. Molenaar, *GNS3vault - Free Cisco labs for CCNA, CCNP and CCIE students*, online