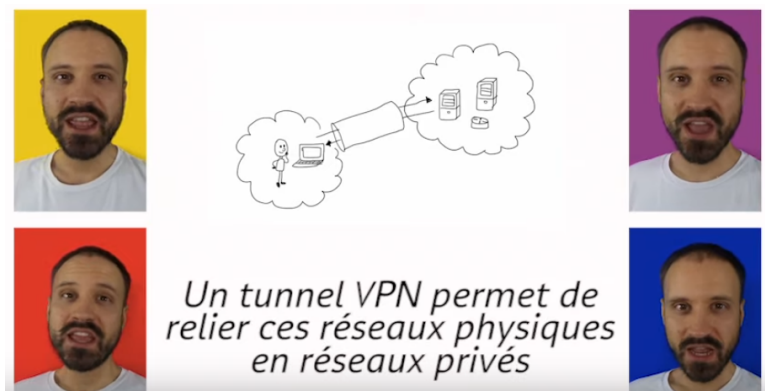




## ..... Les VPN ..... 06.03.2023

On voit le bout du Tunnel de ce module SMINFL6B... ouf... ☺

Auteur : Pascal Fougeray



source : <https://www.youtube.com/watch?v=2s-GZAoH67Y>

Allez voir cette vidéo ... ☺☺☺☺☺

## 1 Préambule

Après le pont et la passerelle, voici le tunnel et le fil virtuel ☺

Ce cours sur les VPN n'est qu'un début dans un domaine vaste qu'est la sécurité dans les réseaux. Au CT si vous savez expliquer comment on met en place un VPN et à quoi ça sert c'est bien...

Un VPN c'est

- Au niveau de la couche 5 la couche session : le chiffrement des données
- Au niveau de la couche 3 la couche réseau : une interface virtuelle pontée sur une interface physique sur laquelle on peut mettre une @IP virtuelle qui va générer une table de routage virtuelle dans éventuellement un routeur virtuel **VRF** et tout cela est bien réel...
- Au niveau de la couche 2 la couche liaison de données : une couche physique virtuelle, si si un fil virtuel que l'on nomme **pseudowire**

## 2 Introduction

Les VPN ne sont pas nouveaux, mais ces dernières années leur usage s'est intensifié.

Tout d'abord, suite à la présence sur le marché de nombreuses solutions VPN pour le grand public, mais aussi à cause de la pandémie de la Covid-19 qui a poussé les entreprises à recourir au télétravail. À l'origine, les VPN étaient utilisés majoritairement par les entreprises, mais aujourd'hui, tout le monde peut utiliser un VPN très facilement.

Je me demande à quoi peut bien servir un VPN...

Je me suis donc documenté sur le Web en n'utilisant pas de VPN... ☺

Pourquoi les gens utilisent-ils des VPN ?

Vous voulez la réponse ?

Et bien, pour le divertissement...



Les 4 avantages des VPN :

1. **Une protection contre les attaques de hackers**

Lorsqu'il "surfe" sur Internet, l'utilisateur laisse des "traces" derrière lui. La trace la plus évidente est son @IP. Elle permet aux hackers d'attaquer directement votre ordinateur avec pour éventuelle conséquence un vol de données ou une usurpation d'identité! Dans le pire des cas, cette attaque peut porter sur des données bancaires particulièrement sensibles et entraîner des dommages financiers considérables. Au contraire, toute personne qui surfe sur Internet par l'intermédiaire d'un VPN dissimule son adresse IP et se rend ainsi inattaquable!

**Mais que fait le NAT ?**

2. **Plus de films et de séries en streaming**

Toute personne qui désire regarder des films ou des séries peut tirer profit d'un accès VPN de bien des manières.

Aux Etats-Unis, Amazon met à disposition de nombreux contenus en avant-première, voire en exclusivité, pour ses spectateurs.

À l'aide d'un serveur VPN situé aux États-Unis, il est possible d'accéder à ces contenus de la France. Les Français en vacances à l'étranger peuvent regarder Amazon en passant par un serveur VPN situé en France et ainsi regarder leurs séries préférées en français, comme à leur habitude.

**Mais que fait le CSA ?**

3. **Un anonymat complet sur Internet**

L'@ IP permet de déterminer l'identité d'un utilisateur. Si vous souhaitez rester anonyme, il est conseillé de surfer sur Internet en passant par un serveur VPN afin d'effacer vos traces. De cette manière, vous dissimulez également votre identité.

**Mais qu'est-ce que les gens ont à cacher ☺ ?**

4. **Censure sur Internet et chiffrement**

Certains pays tels que la **Chine**, la **Russie**, **Cuba** ou la **Turquie** appliquent une censure d'état extrêmement restrictive, et de nombreux sites Internet sont donc bloqués!

Avec un VPN, ces blocages peuvent être contournés. La connexion chiffrée entre votre machine et le serveur VPN évite que les **pares-feux étatiques** puissent obtenir un aperçu de votre connexion Internet. Les VPN rendent visibles les contenus censurés ou bloqués et vous protègent également contre la connexion de tiers.

5. **Trouver des billets d'avion aux meilleurs tarifs** <- Ce n'est pas une blague ☺

Je vous laisse aller lire sur le site!

Source :<https://www.avast.com/fr-fr/c-benefits-of-a-vpn>

### 3 Qu'est-ce qu'un VPN ?

L'acronyme VPN signifie **Virtual Private Network**, qui donne en français : **réseau privé virtuel**.

L'**objectif** d'un VPN est de créer un lien virtuel entre 2 Machines un serveur et un client, 2 Sites, 2 réseaux d'entreprise.

**Ce lien est appelé tunnel**

Les données qui transitent dans ce tunnel sont **chiffrées** et **isolées** du reste du trafic.

Ce n'est pas obligatoirement chiffré!

Par exemple les VPN dans MPLS ne le sont pas.

Voilà tout l'intérêt du VPN et la notion de privé.

Le VPN permet donc de **créer une extension virtuelle de votre réseau local jusqu'à**

— **un autre réseau, un site ;**

— **un poste de travail distant.**

S'il y a chiffrement, le VPN va chiffrer les données de **bout en bout**. L'équipement qui ouvre le tunnel jusqu'à son point de terminaison.

Grâce à cela, il renforce la confidentialité des échanges au travers **de réseaux non sécurisés** par exemple les **hotspot Wifi** public.

Un **hotspot Wifi** est un emplacement physique fourni à l'utilisateur qui lui donne la possibilité d'utiliser son dispositif hors de chez lui.

Ils sont placés dans des établissements publics, tels les cafés, les centres commerciaux, les aéroports, les hôtels, etc et permettent de travailler à partir de cet emplacement.



## 4 Les types de VPN

### 4.1 Les VPN client-to-site

Un VPN *client-to-site*, ou en français client à site, est un tunnel VPN qui permet d'établir une connexion entre un ordinateur, smartphone, tablette, etc... et un réseau d'entreprise.

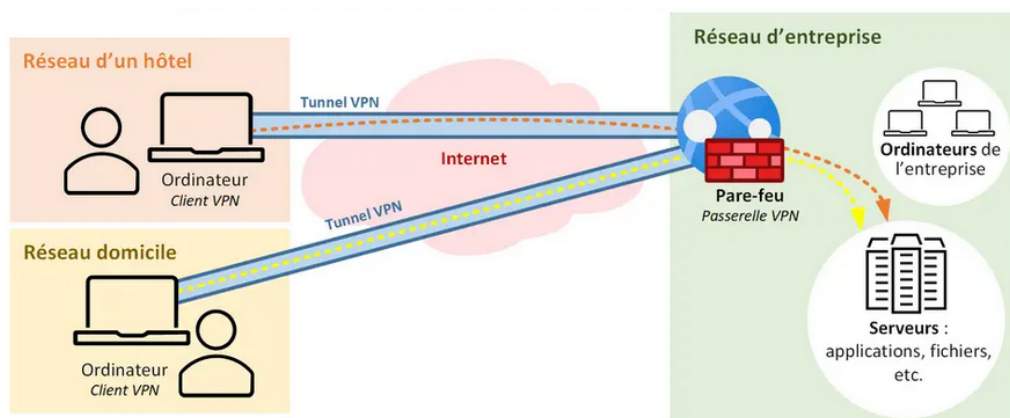
Ce type de VPN est utilisé lorsque l'on souhaite travailler de son domicile (télétravail grande mode depuis le Covid...) et que l'on a besoin d'accéder à un ensemble de ressources de son entreprise. C'est également utile pour les personnes nomades, afin de pouvoir se connecter depuis un hôtel, une gare, un restaurant, un bar... Ah non on ne travaille jamais au bar ☹etc...

Ainsi, on peut imaginer que plusieurs employés de l'entreprise se connectent au réseau d'entreprise, à distance, de façon sécurisée via un VPN. Grâce à cette connexion, ils peuvent accéder à leurs données sur les différents serveurs de l'entreprise.

Il n'est pas question de publier sur Internet les différents serveurs : ce serait un risque important en termes de sécurité.

Le VPN est également préférable à l'utilisation d'outils de connexion à distance comme *Team Viewer*, *AnyDesk*, etc.

Dans le cas où une entreprise s'appuie sur un Cloud tel qu'Office 365 pour héberger ses données, sa messagerie, etc...

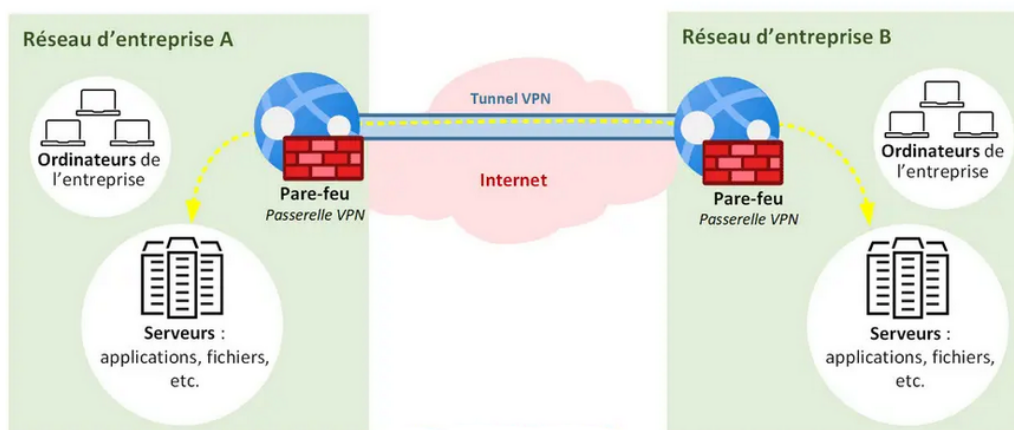


### 4.2 Les VPN site-to-site

Un VPN site-to-site, ou en français site à site, est un tunnel VPN qui permet d'interconnecter 2 réseaux d'entreprise entre eux.

Cette interconnexion est intéressante afin de permettre le partage de ressources entre les deux réseaux, par exemple une application hébergée sur le **site 1** qui doit être accessible par les utilisateurs connectés sur le **site 2**.

C'est ce que je vous propose en TP... On ne peut pas tout faire ☹



### 4.3 Les VPN grand public

Un VPN grand public est un tunnel VPN qui permet d'interconnecter un internaute à internet en étant "protégé" des méchants pirates qui sévissent sur Internet ☹



Très populaires et surtout lucratif, il existe une quantité importante de fournisseurs de ce type de VPN (NordVPN, SurfShark, GhostVPN, etc.) sur le marché.

Avec un abonnement mensuel, l'objectif est totalement différent des deux types évoqués précédemment.

Ces solutions ouvertes à tous sont utilisées principalement pour :

La protection de la vie privée sur Internet grâce au surf anonyme, plus ou moins vrai en fonction des fournisseurs.

**Contourner les restrictions géographiques pour l'accès à certains contenus**, tiens tiens le protéger devient pirate ... MDR

Cela permet d'accéder au catalogue vidéos d'un autre pays ☺

L'internaute établit une connexion VPN à partir de son ordinateur vers un serveur VPN du fournisseur VPN, et ensuite il peut naviguer sur Internet via ce tunnel.

Côté du fournisseur VPN, **différents mécanismes et rebonds sur plusieurs serveurs permettent d'anonymiser l'utilisateur.**

Il est ainsi possible de naviguer sur Internet comme si l'on était localisé à Hawaï, à Tahiti, et autres paradis fiscaux ...

Un seul inconvénient, quand vous regardez par la fenêtre vous ne voyez pas ...



Mon avis sur ce genre de VPN... Quand je vais sur Internet ce n'est pas pour pirater et je soupçonne les fournisseurs de ces VPN de vendre un produit qui ne profite qu'à eux... Mais cela n'est que mon avis ☺

Qui apporte des grands posters à coller sur les fenêtres de la salle 406 ... ?

## 5 Les protocoles des VPN

Une liste non exhaustive mais une liste qu'en même ☺

### 5.1 Le protocole PPTP

Le protocole PPTP (*Point-to-Point Tunneling Protocol*) est une méthode **historique** pour mettre en place tunnel VPN, développé à la base par Microsoft.

Je vous en parle surtout pour *votre culture personnelle*, car ce protocole n'est plus recommandé à cause de plusieurs failles de sécurité.

Il présente l'avantage d'être compatible avec les vieux appareils, mais il a des "lacunes" en matière de sécurité, et il y a des protocoles plus sécurisés qu'il est préférable d'utiliser.

**PPTP est un protocole historique, mais obsolète.**

Si vous voulez jouer les "vieux" et le mettre en place avec un routeur Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/PPTP>

C'est très facile à mettre en place ☺

Si vous voulez creuser le domaine je vous conseille ce site :

### 5.2 Les protocoles L2TP/IPsec

Conçu par Microsoft, le protocole L2TP pour *Layer 2 Tunneling Protocol*, s'appuie sur un autre protocole pour fonctionner IPsec (*Internet Protocol Security*).

Chacun de ces 2 protocoles à un rôle bien spécifique.

1. L2TP a pour objectif d'établir la connexion VPN en elle-même.
2. IPsec assure la sécurité par le chiffrement des données en transit dans le tunnel VPN.

Avec ce type de tunnel VPN, il y a une double authentification, car il y a un tunnel L2TP dans un tunnel IPsec, ce qui apporte un plus d'un point de vue sécurité, mais les performances sont très impactées, car les flux sont plus lourds à gérer.

Il est délaissé et remplacé par OpenVPN bien plus rapide, OpenVPN est un protocole que nous allons voir dans la suite de ce cours

Si vous voulez jouer les "vieux" et le mettre en place avec un routeur Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/L2TP>

C'est très facile à mettre en place ☺

Si vous voulez creuser le domaine je vous conseille ce site :

<https://www.frameip.com/l2tp-pppoe-ppp-ethernet/>

### 5.3 Les protocoles IKEv2/IPsec

Le protocole **IPsec** vu précédemment est aussi associé à un autre protocole : **IKEv2** (*Internet Key Exchange version 2*).

Il est plus récent que L2TP, et s'en inspire, d'ailleurs il s'appuie sur IPsec pour les mêmes raisons : bénéficier de la sécurité et du chiffrement des données.

IKEv2 est une collaboration entre deux grands de l'informatique et du réseau, Microsoft et Cisco.

La version 2 est disponible depuis 2005. La première version date de 1998...

Quand un tunnel IKEv2 est monté entre 2 hôtes, il y a tout d'abord une authentification mutuelle entre les 2 hôtes avec une clé partagée, la négociation des paramètres cryptographiques et la création de clés de session, c'est la phase 1.

Puis vient la phase 2, déclenchée pour négocier d'autres paramètres, notamment les réseaux accessibles au travers du tunnel VPN.

La connexion IKEv2 est réputée comme étant rapide, ce qui facilite l'usage de ce VPN sur les téléphones portables.

Si vous voulez jouer les "vieux c.." et le mettre en place avec un routeur Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/IPsec>

C'est très difficile et pénible à mettre en place ☹

### 5.4 Le protocole OpenVPN

**OpenVPN est encore le leader dans le monde des VPN mais pour combien de temps encore ?**

C'est un protocole open source. Il existe depuis 2001 et bénéficie d'une très bonne réputation.

Il est implémenté au sein du logiciel OpenVPN, mais aussi compatibles avec de nombreux équipements réseaux tels les routeurs Mikrotik.

Si on parle d'un VPN SSL, on fait référence à OpenVPN, car il s'appuie sur le protocole SSL pour chiffrer les échanges.

L'algorithme de chiffrement symétrique utilisé est l'**AES 256 bits**, un algorithme très fiable et très robuste.

OpenVPN est à la fois simple à configurer, rapide et sécurisé, alors forcément il plaît.

Il fonctionne en **UDP sur le port 1194**, mais il peut fonctionner sur d'autres ports, ainsi qu'en TCP. Même si cela va forcément affecter les performances, c'est intéressant pour contourner certains pare-feu.

Contrairement aux VPN L2TP/IPsec et IKEv2 qui sont régulièrement bloqués par les Firewall.

**Le site officiel :** <https://openvpn.net/>

Un excellent Tuto pour l'installer et l'utiliser dans votre VM :

<https://www.it-connect.fr/debian-11-et-openvpn-comment-creeer-son-propre-serveur-vpn/>

Une petite capture wireshark entre un serveur 192.168.56.102 et un client 192.168.56.103

Je ne vais pas la détailler ☺

Juste voir

— qu'on est en **UDP** sur le port **1194**

— et qu'au dessus on a de **TLS** : *Transport Layer Security*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.103	192.168.56.102	OpenVPN	84	MessageType: P_CONTROL_HARD_RESET_CLIENT_V2
2	0.003189	192.168.56.102	192.168.56.103	OpenVPN	96	MessageType: P_CONTROL_HARD_RESET_SERVER_V2
3	0.004815	192.168.56.103	192.168.56.102	OpenVPN	92	MessageType: P_ACK_V1
4	0.005863	192.168.56.103	192.168.56.102	OpenVPN	184	MessageType: P_CONTROL_V1 (Message fragment 1)
5	0.005873	192.168.56.103	192.168.56.102	OpenVPN	184	MessageType: P_CONTROL_V1 (Message fragment 2)
6	0.005880	192.168.56.103	192.168.56.102	TLSv1	110	Client Hello
7	0.006143	192.168.56.102	192.168.56.103	OpenVPN	92	MessageType: P_ACK_V1
8	0.007420	192.168.56.102	192.168.56.103	OpenVPN	92	MessageType: P_ACK_V1

Frame 6: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF\_{81A5C9C1-2E04-47CE-...}

Ethernet II, Src: PcsCompu\_bb:22:84 (08:00:27:bb:22:84), Dst: PcsCompu\_4a:be:45 (08:00:27:4a:be:45)

Internet Protocol Version 4, Src: 192.168.56.103, Dst: 192.168.56.102

User Datagram Protocol, Src Port: 33198, Dst Port: 1194

OpenVPN Protocol

Type: 0x20 [opcode/key\_id]

Session ID: 9311214641221158445

HMAC: 4d8bfb13d3bc971a68a4a82950e8240786861b2

Packet-ID: 5

Net Time: Jan 23, 2013 00:52:12.000000000 CET

Message Packet-ID Array Length: 0

Message Packet-ID: 3

Message fragment (26 bytes)

[3 Message fragments (226 bytes): #4(100), #5(100), #6(26)]

Transport Layer Security

TLSv1 Record Layer: Handshake Protocol: Client Hello

Si vous voulez jouer les “jeunes” et le mettre en place avec un routeur Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/OpenVPN>

C'est facile à mettre en place ☺

Si vous voulez configurer un client OpenVPN sous ubuntu, il suffit de lire des tutos☺

<https://fr.support.smartdnsproxy.com/article/166-vpn-setup-for-ubuntu-openvpn-protocol>

## 5.5 Le protocole WireGuard

Dans l'histoire des VPN, le protocole WireGuard est très récent, en version stable que depuis mars 2020.

Il est compatible avec l'ensemble des OS tels Windows, Linux, BSD, macOS, Android et iOS. Il est aussi disponible sur les routeurs et c'est lui que nous utiliserons en TP.

En comparaison des solutions vues précédemment comme OpenVPN et IPSec, il se veut plus simple dans son fonctionnement et surtout **beaucoup plus rapide** : les débits proposés sont plus élevés.

WireGuard fonctionne en mode **peer-to-peer** et **l'authentification entre deux clients s'effectue par un échange de clés (publique/privé)**.

La sécurité est assurée par différents algorithmes par exemple, il utilise **l'algorithme de chiffrement symétrique ChaCha20**, l'authentification des messages est effectuée avec **Poly1305**.

Voilà ce que ça donne avec wireshark (Capture du TP...)

No.	Time	Source	Destination	Protocol	Length	Info
19	43.631226	193.199.103.1	193.199.103.33	WireGuard	190	Handshake Initiation, sender=0x08CD6DBF
20	43.636144	193.199.103.33	193.199.103.1	WireGuard	134	Handshake Response, sender=0xE00A390E, receiver=0x08CD6DBF
21	43.638286	193.199.103.1	193.199.103.33	WireGuard	170	Transport Data, receiver=0xE00A390E, counter=0, datalen=96
22	43.640727	193.199.103.33	193.199.103.1	WireGuard	170	Transport Data, receiver=0x08CD6DBF, counter=0, datalen=96
27	53.769834	193.199.103.1	193.199.103.33	WireGuard	74	Keepalive, receiver=0xE00A390E, counter=1

Frame 19: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface -, id 0

Ethernet II, Src: 0c:77:d2:37:00:01 (0c:77:d2:37:00:01), Dst: 0c:38:0d:b4:00:00 (0c:38:0d:b4:00:00)

Internet Protocol Version 4, Src: 193.199.103.1, Dst: 193.199.103.33

User Datagram Protocol, Src Port: 61664, Dst Port: 61664

WireGuard Protocol

Type: Handshake Initiation (1)

Reserved: 000000

Sender: 0x08cd6dbf

Ephemeral: rBfVhSeuhnWRBwZP8GpV9p8KSH6KEuH9x/oK7lHsTCM=

Encrypted Static

Static Public Key: Aq2f/W9U7RHboYm7SZAYgLIJCvxmm2w3QPhb8sXmwFI=

Encrypted Timestamp

Timestamp: Mar 2, 2023 16:23:45.754974720 UTC

mac1: 0288a3b021989ec4c468d9e847da1b4c

[Receiver Static Public Key: AsVHGZjtmF2t1z+DWkx256EyGwWNY1D8D+Como4nPho=]

mac2: 00000000000000000000000000000000

**Clef publique CE1**

Si vous voulez jouer les “jeunes étudiants de L3” et le mettre en place avec des routeurs Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/WireGuard>

C'est facile à mettre en place ☺

Une autre méthode, venir au dernier TP ☺

## 5.6 ZeroTier

ZeroTier est un logiciel de réseau virtuel privé (VPN) qui permet aux utilisateurs de créer et de **rejoindre des réseaux virtuels décentralisés**.



Il utilise un **protocole de réseau propriétaire** pour permettre aux ordinateurs distants de se connecter les uns aux autres comme s'ils étaient sur le même réseau local. Il est utilisé pour la connectivité de réseau dans les entreprises, les écoles et les organisations à but non lucratif.

Il est aussi utilisé pour

- les jeux en ligne,
- les connexions à distance
- les applications IoT. (Les objets connectés)

Si vous voulez jouer les “**experts** étudiants de L3” et le mettre en place avec des routeurs Mikrotik :

<https://help.mikrotik.com/docs/display/ROS/ZeroTier>

C'est possible à mettre en place ☺

Je ne sais pas (encore...) le faire, car je n'ai jamais pratiqué mais avec un peu de temps ça doit pouvoir se faire ☺

## 6 Les MPLS L2VPN et L3VPN

Les VPN MPLS se configurent sur les PE et permettent de créer des VPN d'un site à un autre site et pour tout un ensemble de machines !

Il n'y a pas de notion de chiffrement !!!

Avec les L2VPN on va pouvoir faire passer les VLAN au travers d'Internet, oui oui les VLAN au travers d'internet !!

**Ce sont des VPN créés par l'ISP pour le client ayant plusieurs sites !!!**

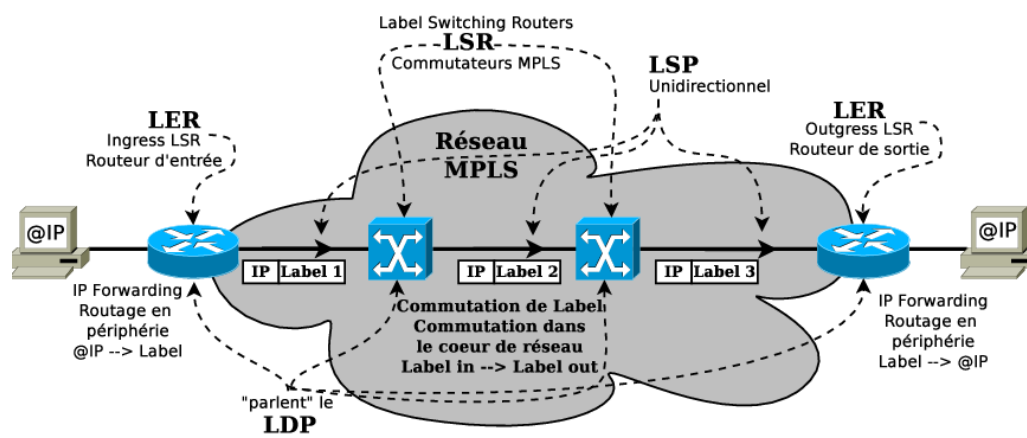
Les universités en France utilisent ce genre de VPN et sont fournis par leur FAI, Renater.

<https://services.renater.fr/vpn/index>

Ces VPN s'appuient sur une technologie que l'on nomme MPLS . Une technologie très récente puisqu'elle a moins de 25 ans... N'oubliez pas que le routage est “vieux” de plus de 40 ans...

MPLS, **MultiProtocol Label Switching** ou **MultiProtocole de Commutation d'Étiquette** est un ensemble de spécifications définies par l'**IETF** (*Internet Engineering TaskForce*) en 1997, qui consiste à doter les **trames** circulant sur le réseau, d'un **Label** servant à indiquer aux **routeurs** le chemin que la donnée doit emprunter.

Je ne vais pas vous faire un cours sur MPLS non non, juste vous l'expliquer en une image



Quand on va d'un site à un autre site, on entre par un PE appelé aussi LER et on ressort par un PE appelé aussi LER. Les routeurs que l'on traverse ne font pas office de routeurs puisqu'ils ne s'occupent pas des @IP mais des Labels. Un label correspond à une route.

Pour s'échanger les Labels les routeurs utilisent un protocole de routage nommé LDP.

Les LSR émettent périodiquement des messages “Hello” à l'aide de l'@IP de multicast 224.0.0.2 comme OSPF. Les LSR voisins se présentent en communiquant simplement leur @IP et leur **LSR Identifier (LSR-ID)**. Le LSR ayant le LSR-ID le plus petit ouvre alors une session TCP sur le port 646 comme BGP : LDP Initialisation avec son voisin et c'est parti les labels sont échangés...

**C'est un vrai cocktail... un mélange d'OSPF et de BGP...**



MPLS seul ne sert à rien!!!

Mais il permet

- **L'ingénierie de trafic** ou *Traffic Engineering* qui permet d'optimiser l'utilisation des ressources d'un réseau afin d'éviter la congestion. C'est la prise en compte de la bande passante disponible sur un lien lors des décisions de routage qui rend possible cette optimisation.
- **La gestion de la Qualité de Service** (QoS : elle dépend du débit minimal garanti, du débit maximal, de la latence et de la gigue ) en définissant 5 classes de services (**Classes of Service** : CoS) :
  1. **Vidéo** : La classe de service pour le transport de la vidéo possède un niveau de priorité plus élevé que les classes de service de données.
  2. **Voix** : La classe de service pour le transport de la voix possède un niveau de priorité équivalent à celui de la vidéo, c'est-à-dire plus élevé que les classes de service de données.
  3. **Données très prioritaires** (D1). Il s'agit de la classe de service possédant le plus haut niveau de priorité pour les données. Elle sert notamment aux applications ayant des besoins critiques en terme de performance, de disponibilité et de bande passante.
  4. **Données prioritaires** (D2). Cette classe de service correspond à des applications non critiques possédant des exigences particulières en terme de bande passante,
  5. **Données non prioritaires** (D3), représentant la classe de service la moins prioritaire.
- La mise en place de tunnel VPN de couche 2 et 3.

Remarque : si vous voulez plus d'informations sur MPLS : Poursuivez vos études dans le domaine des réseaux et allez travailler chez un FAI ☺

## 6.1 Le L3VPN

Une image de **Renater** : Tiens un PE et des CE ☺

Figure 2 - Connexion via un lien de niveau 2 fourni au travers d'un réseau de collecte (L2VPN MPLS ou VLAN...)

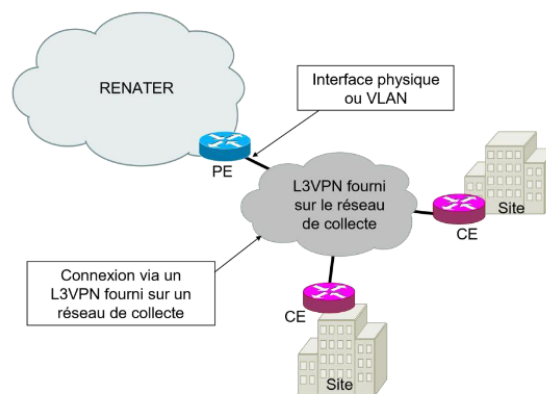


Figure 3 - Connexion via un VPN de niveau 3 fourni sur un réseau de collecte (VRF-to-VRF - RFC 4364 - 10.a)

Extrait du document PDF : [https://services.renater.fr/\\_media/vpn/doc-l3vpn\\_20190321.pdf](https://services.renater.fr/_media/vpn/doc-l3vpn_20190321.pdf)

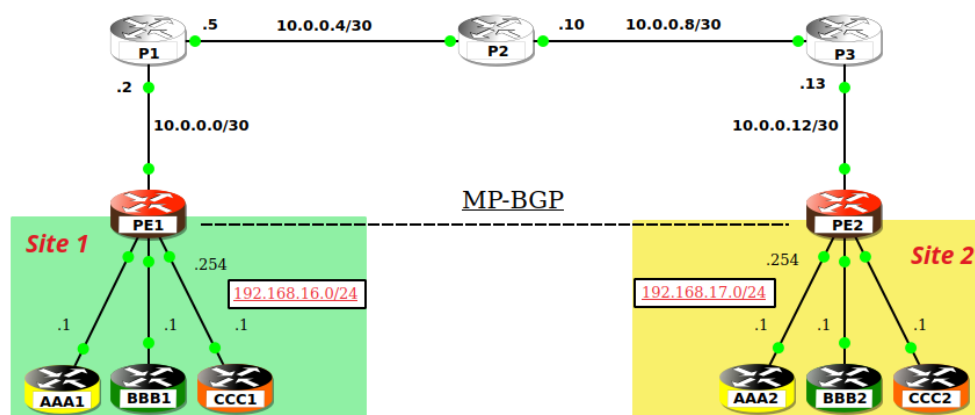
Voici celui du TP

On a 2 site, le site 1 et le site 2 ☺

Il peut y avoir autant de sites qu'il y a de PE chez un FAI!!!

Le faire avec n entreprises ayant chacune m sites allant de 2 à 1000 n'est pas un problème, des @IP privées en 10.0.0.0/8 il y en a **16 777 214** ça devrait être suffisant ☺





### 6.1.1 Les entités physiques des VPNs MPLS de couche 3 et leur fonctions :

#### Le CE (*Customer Edge router*)

- Routeur client connecté au backbone IP via un service d'accès.
- Il route en IP le trafic entre le site client et le PE
- Ce routeur appartient au client et **n'a aucune connaissance des VPN et de la notion de Label**.
- Tout routeur traditionnel peut être un routeur CE.
- Il est en **@IP privée**, pénurie d'@ IPV4 oblige!

#### Le P (*Provider device*) ou LSR

- Routeur ou commutateur de cœur de backbone chargé de la commutation de labels des trames MPLS.
- Il n'intervient pas dans la mise en place du VPN, **tout est transparent pour lui**.
- Aucune configuration à modifier ou à ajouter!

#### Le PE (*Provider Edge router*) ou LER

- Routeur backbone de périphérie auquel sont connectés des CE.
- C'est au niveau des PE qu'est déclarée l'**appartenance d'un CE à un VPN donné**.
- Le **PE gère les VPN** en coopérant avec les autres PE et commute les trames avec les P.
- Le PE a la capacité de gérer **plusieurs tables de routage** grâce à la notion de VRF.

## 6.2 Les entités logiques des VPNs MPLS et leurs fonctions

Le **VPN implique l'isolation du trafic entre sites clients n'appartenant pas aux mêmes VPN**, d'où :

### 6.2.1 La ou le<sup>1</sup> VRF

- Le VRF (*Virtual Routing and Forwarding* table) est un routeur virtuel se trouvant dans un routeur réel!
- Il est constitué :
  - d'une table de routage,
  - d'une FIB (*Forwarding Information Base*)
 toutes **spécifiques et indépendantes** des autres VRF et de la table de routage globale.
- Chaque VRF est désigné par un nom sur les PE.  
Les noms sont affectés localement et n'ont aucune signification vis-à-vis des autres routeurs.
- Chaque interface de PE, reliée à un site client, est rattachée à une VRF particulière. Lors de la réception de paquets IP sur une interface client, le routeur PE procède à un examen de la table de routage du VRF auquel est rattachée l'interface et donc **ne consulte pas sa table de routage globale**.
- Cette possibilité d'utiliser **plusieurs tables de routage indépendantes** permet de gérer un plan d'adressage par sites, même en cas de **recouvrement d'adresses** entre VPN différents.
- Chaque PE associe, de manière statique, un VRF appelé LIB (*Label Information Base*) dans la norme MPLS à chacune de ses interfaces utilisateur.
- Le VRF est un routeur virtuel associé à un VPN qui donne les routes vers les réseaux IP faisant partie de ce VPN.

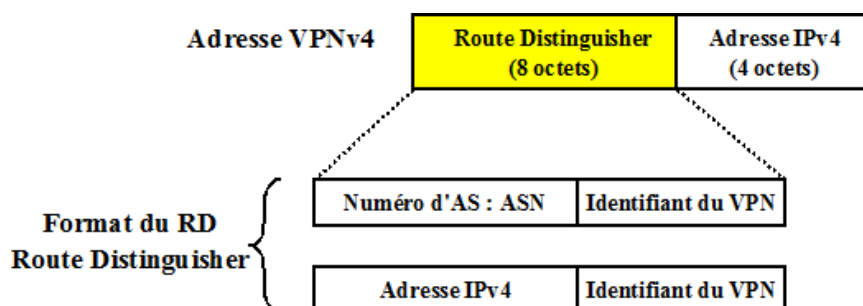
1. selon que l'on parle du routeur ou de sa table de routage...

- Le VRF assure le routage dans le VPN, **il considère le réseau MPLS comme un lien point à point entre le PE d'entrée et le PE de sortie**. Le PE de sortie est considéré comme étant le prochain saut (*Next Hop*) dans le réseau dans le réseau VPN.

### 6.2.2 Adresses VPN-IPv4

Un client VPN peut appartenir à plusieurs VPN et l'utilisation de plus en plus fréquente par les clients d'@IP privées de la RFC 1918 conduit à un chevauchement d'adresses. L'unicité d'adresse ne peut être garantie, **on a donc introduit la notion d'adresses de Ip de type VPN, les adresses VPN-IPv4**.

- Elle est codée sur 12 octets (96 bits) ce qui est mieux que les 32 bits d'IPv4..., commençant par un **identifiant unique de route choisi arbitrairement par le FAI, la RD (Route Distinguisher)** sur 8 octets et se terminant par une adresse IPv4 sur 4 octets.
- Une route VPNv4 est formée d'une RD et d'un préfixe IPv4, s'écrit ainsi sous la forme **RD :Subnet/-Masque**.  
Ex : **1664 :33 :192.168.16.0/24**.



**C'est comme cela que l'on différencie AAA1 de BBB1 et de CCC1 dans la partie TP !!!**

Voir la partie TP pour les configurations etc ...

## 6.3 Le L2VPN

Une image de **Renater** : Tiens un PE et un CE ☺

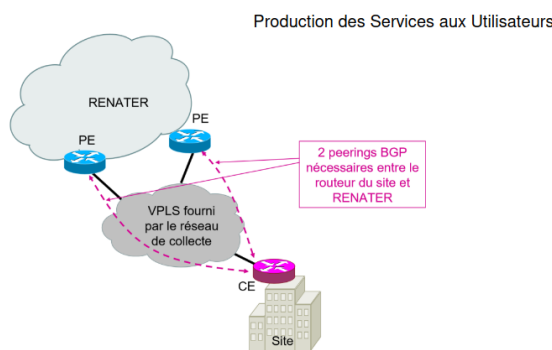
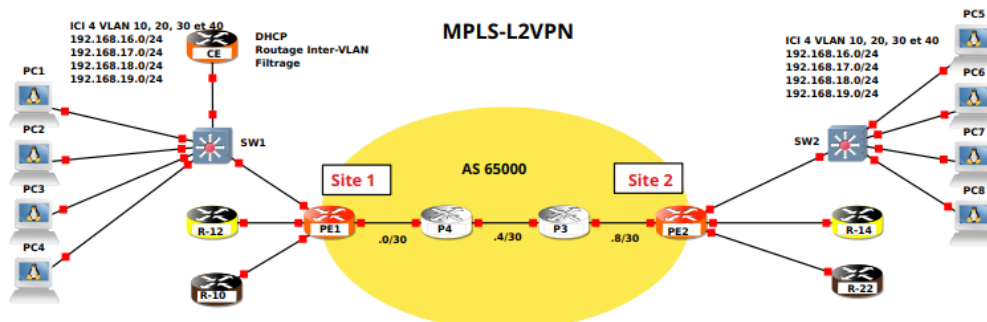


Figure 5 - Connexion redondée via un service VPLS fourni par un réseau de collecte

Extrait du document PDF : [https://services.renater.fr/\\_media/vpn/doc-l2vpn\\_20190322.pdf](https://services.renater.fr/_media/vpn/doc-l2vpn_20190322.pdf)

Voici celui du TP

On a 2 site, le site 1 et le site 2 ☺



Les 2 sites communiquent ici grâce à 3 VPN de couche 2, c'est à dire que le BB représenté ici en jaune est équivalent à 3 switches, un pour chaque site!!!

L'objectif des L2VPN est de connecter des sites clients, les CE, par l'intermédiaire d'un niveau 2 virtuel.

Pour cela, aucun niveau 3 n'est nécessaire entre le routeur de l'opérateur, le PE et celui du client le CE.

OUI OUI vous avez bien lu, les interfaces des PE n'ont pas d'@IP v4 ou v6

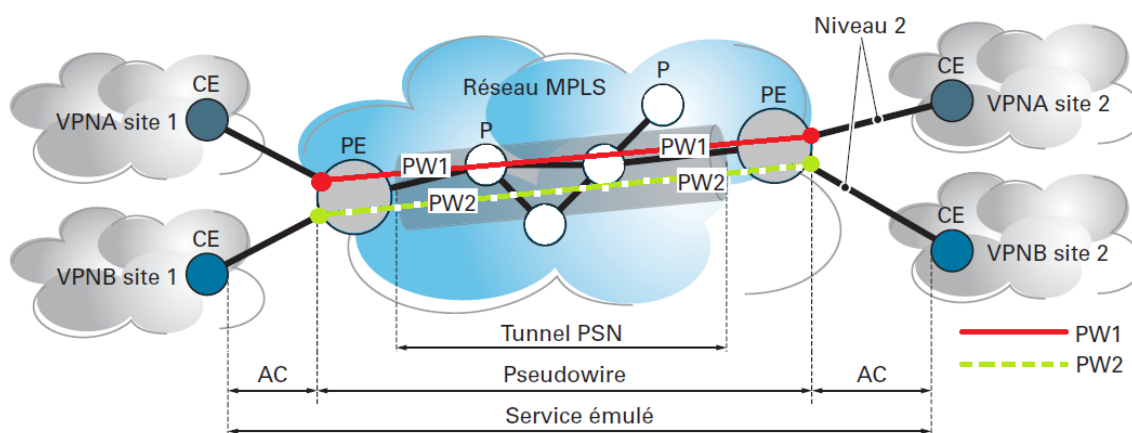
On en manque et bien on n'en met plus ☺

Une image valant mieux qu'un long texte , voilà ce que ça peut donner

Cette partie est à comprendre, pour comprendre la suite!!!

La figure suivante illustre ce qu'est un L2VPN et les éléments qu'il contient.

Dans ce cas de figure, nous avons 2 **pseudowires** PW1 et PW2 reliant les 2 sites A et les 2 sites B.



- Les Équipements **PE** (**Provider Edge**) : les routeurs de périphérie du réseau cœur (**backbone**). Ils sont situés en entrée et sortie du réseau ;
- Les Équipements **CE** (**Customer Edge**) : l'équipement du client, un routeur, un pont, un switch, voir directement un hôte ;
- Circuit d'attachement **AC** (**Attachment Circuit**) : il connecte le CE du réseau client au PE du réseau de l'opérateur. Cet AC peut être soit un circuit **physique** (un câble **RJ45**, une **FO** etc.), soit un circuit **logique**.  
Exemples : **Ethernet port**, **Ethernet VLAN**, connexion **PPP**... ;
- Le **PW** (**Pseudowire**) : c'est une émulation de connectivité **point à point** sur un réseau **PSN** permettant l'interconnexion de 2 nœuds quel que soit leurs technologies de niveau 2. Un **pseudowire** est établi de routeur **PE** à routeur **PE** ; Le **Pseudowire** doit émuler le **comportement** et les **caractéristiques** du service original afin que cela soit transparent pour le client.
- Le tunnel **PSN** (**Packet Switched Network Tunnel**) : tunnel, sur un réseau à **commutation de paquets**, qui relie des routeurs PE. Les PSN sont divers et variés, tels les tunnels **L2TP** (**Layer 2 Tunneling Protocol**), **IpSec** (**Internet Protocol Security**) et **MPLS**.
- L'**Emulated Service**, le service émulé : le service offert de bout en bout comprenant les **AC** et les **PW**.
- le **Payload du service** ou charge utile : ce niveau présente le flux des données transporté dans un paquet **PW**

La technologie la plus à la mode dans les L2VPN c'est VPLS

## VPLS

Je vais essayer d'être concis... VPLS c'est très très compliqué et seuls les 3 points suivants sont à apprendre ☺

1. VPLS est un **VPN multipoint de couche 2** basé sur un cœur en MPLS et Ethernet et des routeurs PE ayant des fonctionnalités spécifiques. Et ces fonctionnalités spécifiques, les routeurs dont on dispose les ont ...



2. Ces fonctionnalités spécifiques vont permettre de créer un service qui a son tour permet de créer un **segment de LAN** émulé pour un groupe de clients
3. Donc si on a un segment de LAN alors on obtient un **domaine de broadcast de niveau 2** capable d'**apprendre des adresses MAC** et de les **utiliser pour forwarder des données**.

**Avec VPLS, les routeurs dans le WAN entre 2 sites sont équivalent à des switches!!!**

J'ai écrit équivalent !!!

## 7 En pratique

Par faute de temps... Nous n'allons pas tout voir

Je vous propose de voir 3 types de VPN,

- 2 VPN non chiffrés MPLS-L3VPN et MPLS-L2VPN
- 1 VPN chiffré : Wireguard

Pourquoi ces 3 là ?

Car ils ne sont pas trop longs à mettre en place et à étudier et que je préfère faire des VPNs de site à site, vu que c'est la matière réseau

Pour créer un VPN il faut :

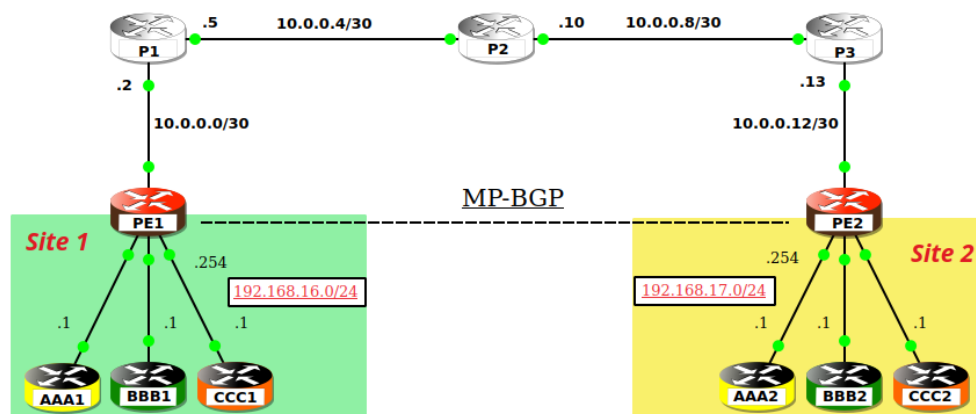
- Si c'est un VPN de couche 2, créer une **couche physique virtuelle** ... Mince alors même la couche physique devient virtuelle, mais où va-t'on, au secours, ce cours devient complément fou ☹. On appelle cela un **pseudowire**
- Si c'est un VPN de couche 3 et plus, créer une **interface virtuelle** ... ça on sait faire et bien sur une table de routage spécifique à cette interface virtuelle.

### 7.1 MPLS-L3VPN

La maquette n'a pas de grandes ambitions. Nous avons 3 entreprises ayant chacune 2 sites.

Il peut y avoir autant de sites qu'il y a de PE chez un FAI!!!

Le faire avec n entreprises ayant chacune m sites allant de 2 à 1000 n'est pas un problème, des @IP privées en 10.0.0.0/8 il y en a **16 777 214** ça devrait être suffisant ☺



Comment ça fonctionne ?

Sur les 2 PE on déclare 3 VRF.

Qu'est-ce qu'une VRF ?

Cela veut dire **Virtual Routing Forwarding**

#### 7.1.1 Conf d'un PE

Conf de PE1, pour la conf de PE2 changer 11 en 22, 16 en 17 et 10.0.0.0 en 10.0.0.12

```
/interface bridge add name=lo0
/ip dhcp-client remove 0
/routing bgp instance set default as=1664
```



```

/routing ospf instance set [ find default=yes ] router-id=11.11.11.11
/ip address
add address=11.11.11.11 interface=lo0 network=11.11.11.11
add address=10.0.0.1/30 interface=ether1 network=10.0.0.0
add address=192.168.16.254/24 interface=ether2 network=192.168.16.0
add address=192.168.16.254/24 interface=ether3 network=192.168.16.0
add address=192.168.16.254/24 interface=ether4 network=192.168.16.0
/ip route vrf
add export-route-targets=1664:33 import-route-targets=1664:33 interfaces=\
ether2 route-distinguisher=1664:33 routing-mark=AAA
add export-route-targets=1664:86 import-route-targets=1664:86 interfaces=\
ether3 route-distinguisher=1664:86 routing-mark=BBB
add export-route-targets=33:86 import-route-targets=33:86 interfaces=ether4 \
route-distinguisher=33:86 routing-mark=CCC

/mpls ldp set enabled=yes lsr-id=11.11.11.11
/mpls ldp interface add interface=ether1
/mpls ldp neighbor add transport=11.11.11.11
/routing bgp instance vrf
add redistribute-connected=yes routing-mark=AAA
add redistribute-connected=yes routing-mark=BBB
add redistribute-connected=yes routing-mark=CCC
/routing bgp peer
add address-families=vpn4 name=PE2 remote-address=22.22.22.22 \
remote-as=1664 update-source=lo0
/routing ospf network
add area=backbone network=11.11.11.11/32
add area=backbone network=10.0.0.0/30
/system identity set name=PE1

```

On voit que l'on a une section nommée *ip route vrf*

Cette section permet de faire **du routage statique** ! C'est l'homme qui entre les routes à la main et on obtient des **@VPN-IPv4** grâce au RD et au RT.

```

[admin@PE1] /ip route> export
# mar/06/2023 16:49:40 by RouterOS 6.43.8
# software id =
#
#
#
/ip route vrf
add export-route-targets=1664:86 import-route-targets=1664:86 interfaces=ether3 route-distinguisher=1664:86 routing-mark=BBB
add export-route-targets=33:86 import-route-targets=33:86 interfaces=ether4 route-distinguisher=33:86 routing-mark=CCC
add export-route-targets=1664:33 import-route-targets=1664:33 interfaces=ether2 route-distinguisher=1664:33 routing-mark=AAA
[admin@PE1] /ip route>

```

Ce qui donnera des adresses virtuelles de type VPN-IPv4

### 7.1.2 Les VRF

Si on veut voir la table de routage de PE1

```

[admin@PE1] /ip route> /ip route print
Flags: - disabled, - active, - dynamic, - connect, - static,
      DST-ADDRESS    PREF-SRC    GATEWAY    DISTANCE
0 ADC 192.168.16.0/24    192.168.16.254 ether3      0
1 ADb 192.168.17.0/24    192.168.16.254 22.22.22.22 200
2 ADC 192.168.16.0/24    192.168.16.254 ether4      0
3 ADb 192.168.17.0/24    192.168.16.254 22.22.22.22 200
4 ADC 192.168.16.0/24    192.168.16.254 ether2      0
5 ADb 192.168.17.0/24    192.168.16.254 22.22.22.22 200
6 ADo 1.1.1.1/32        10.0.0.2      110
7 ADo 2.2.2.2/32        10.0.0.2      110
8 ADo 3.3.3.3/32        10.0.0.2      110
9 ADC 10.0.0.0/30        10.0.0.1      ether1      0
10 ADo 10.0.0.4/30       10.0.0.2      110
11 ADo 10.0.0.8/30       10.0.0.2      110
12 ADo 10.0.0.12/30      10.0.0.2      110
13 ADC 11.11.11.11/32     11.11.11.11  lo0         0
14 ADo 22.22.22.22/32    10.0.0.2      110
[admin@PE1] /ip route>

```



**On a** les 3 réseaux des CE 192.168.16.0/24 et 192.168.17.0/24

**Remarquez** la passerelle : 22.22.22.22 qui est l'autre PE donc PE2 !

Et ces routes sont apprises en iBGP on le voit par la distance administrative qui vaut 200

Si un PE veut pinguer un CE il doit choisir la bonne table de routage. Comme le montre la figure suivante

```
[admin@PE1] > ping 192.168.16.1
0
1
2
sent=3 received=0 packet-loss=100%

[admin@PE1] > ping 192.168.16.1 routing-table=
AAA BBB CCC main
[admin@PE1] > ping 192.168.16.1 routing-table=AAA
0 192.168.16.1 56 64 1ms
1 192.168.16.1 56 64 3ms
sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=2ms max-rtt=3ms

[admin@PE1] > █
```

### 7.1.3 Et les P dans tout ça !

Si on veut voir la table de routage de P2

```
[admin@P2] > /ip route print
Flags: - disabled, - active, - dynamic, - connect, - static,
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 ADo 1.1.1.1/32 10.0.0.5 110
1 ADC 2.2.2.2/32 2.2.2.2 lo0 0
2 ADo 3.3.3.3/32 10.0.0.10 110
3 ADo 10.0.0.0/30 10.0.0.5 110
4 ADC 10.0.0.4/30 10.0.0.6 ether1 0
5 ADC 10.0.0.8/30 10.0.0.9 ether2 0
6 ADo 10.0.0.12/30 10.0.0.10 110
7 ADo 11.11.11.11/32 10.0.0.5 110
8 ADo 22.22.22.22/32 10.0.0.10 110
[admin@P2] > █
```

**On n'a pas** les 3 réseaux des CE 192.168.16.0/24 et 192.168.17.0/24

Ils ne font pas de routage quand ça vient d'en dehors du backbone mais du switching de Labels, c'est du MPLS.

On a bien 3 VPN de couche 3, un L3-VPN entre les 2 PE, les P n'ont aucune connaissance des 3 réseaux des CE 192.168.16.0/24 et 192.168.17.0/24

**Remarque :** Il est impossible de faire un traceroute de AAA1 vers AAA2

```
[admin@AAA1] > tool traceroute 192.168.17.1
# ADDRESS LOSS SENT LAST AVG BEST WORST STD-DEV STATUS
1 100% 2 timeout
2 100% 1 timeout
3 100% 1 timeout
4 100% 1 timeout
5 100% 1 timeout
```

```
[admin@AAA1] > █
```

C'est logique non ?

Comment découvrir des routeurs sur son passage qui ne savent pas renvoyer 192.168.16.0/24 ?

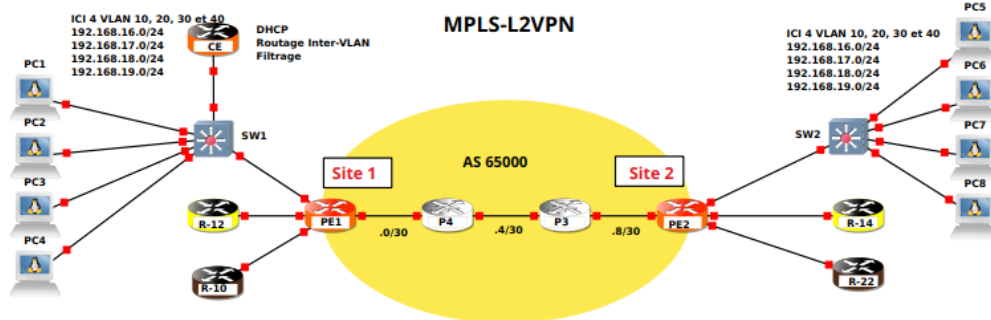
**On en déduit que l'on a des tunnels de couche 3.**

Les P dans le Backbone sont vu par les PE comme des Switch ... **c'est le tunnel entre les 2 PE**  
 ☹ !

## 7.2 MPLS L2-VPN VPLS

On va travailler sur cette architecture





### Quelques explications

- Le FAI a 3 clients CE, R-12 et R-10 d'un côté et R-14 et R-22 de l'autre côté
  - Il y a 2 sites, sur le site 2 on peut voir qu'un site d'une entreprise peut ne pas avoir de CE!
  - Les IP des CE sont 192.168.1.XX/24 avec XX le numéro du routeur. Sauf pour CE qui lui a 4 Réseaux vus dans le TP VLAN2 192.168.16.0/24, 192.168.17.0/24, 192.168.18.0/24 et 192.168.19.0/24
- On pourrait mettre les mêmes IP pour tous les routeurs de chaque site!!!

#### 7.2.1 Conf d'un PE

Conf d'un PE, ici PE1, pour PE2, remplacer 1.1.1.1 par 2.2.2.2, changer les @IP et la partie routing ospf network 10.10.10.8 et surtout site-id=2 !!!

```
/interface bridge
add name=CustA
add name=CustB
add name=CustC
add name=l0
/routing bgp instance set default as=65000 router-id=1.1.1.1
/routing ospf instanceset [ find default=yes ] name="" router-id=1.1.1.1
/interface bridge port
add bridge=CustA interface=ether2
add bridge=CustB interface=ether3
add bridge=CustC interface=ether4
/interface vpls bgp-vpls
add bridge=CustA export-route-targets=65000:1 import-route-targets=65000:1
name=CustA route-distinguisher=65000:1 site-id=1
add bridge=CustB export-route-targets=65000:2 import-route-targets=65000:2
name=CustB route-distinguisher=65000:2 site-id=1
add bridge=CustC export-route-targets=65000:3 import-route-targets=65000:3
name=CustC route-distinguisher=65000:3 site-id=1
/ip address
add address=1.1.1.1 interface=l0 network=1.1.1.1
add address=10.10.10.1/30 interface=ether1 network=10.10.10.0
/mpls ldp set enabled=yes lsr-id=1.1.1.1 transport-address=1.1.1.1
/mpls ldp interface add interface=ether1
/routing bgp peer
add address=families=l2vpn name=peer1 remote-address=2.2.2.2 remote-as=65000
update-source=l0
/routing ospf network
add area=backbone network=10.10.10.0/30
add area=backbone network=1.1.1.1/32
/system identity set name=PE1
```

- On crée 3 interfaces de type VPLS tout comme les interfaces VLAN ou les interfaces wireguard  
*/interface bridge add name=CustA*
- On pontage ces 3 interfaces à 3 interfaces physiques ici ether2  
*/interface bridge port add bridge=CustA interface=ether2*



- On associe ces 3 interfaces à 3 pseudowire  
`/interface vpls bgp-vpls add bridge=CustA export-route-targets=65000 :1 import-route-targets=65000 :1 name=CustA route-distinguisher=65000 :1 site-id=1`
- On échange les 3 adresses des pseudowire entre les 2 PE via BGP  
`/routing bgp peer add address-families=l2vpn name=peer1 remote-address=2.2.2.2 remote-as=65000 update-source=l0`

### 7.2.2 Les interfaces et pseudo-wire

Si sur les PE on tape la commande `/interface vpls bgp-vpls print detail` on obtient :

```
[admin@PE1] > /interface vpls bgp-vpls print detail
Flags:  - disabled,  - inactive
0  name="CustA" route-distinguisher=65000:1 import-route-targets=65000:1 export-route-targets=65000:1 site-id=1 bridge=CustA bridge-cost=50 bridge-horizon=none use-control-word=yes pw-mtu=1500 pw-type=vpls
1  name="CustB" route-distinguisher=65000:2 import-route-targets=65000:2 export-route-targets=65000:2 site-id=1 bridge=CustB bridge-cost=50 bridge-horizon=none use-control-word=yes pw-mtu=1500 pw-type=vpls
2  name="CustC" route-distinguisher=65000:3 import-route-targets=65000:3 export-route-targets=65000:3 site-id=1 bridge=CustC bridge-cost=50 bridge-horizon=none use-control-word=yes pw-mtu=1500 pw-type=vpls
[admin@PE1] > █
```

On voit 3 pw-type = VPLS soit 3 pseudowire entre PE1 et PE2

### 7.2.3 Ping, ARP et traceroute !

Si on fait un ping de PC1 vers PC5 puis un traceroute et qu'ensuite on lance sur PC1 la commande ARP, on constate que

1. les 2 PC se ping
2. PC1 récupère l'@MAC de PC5 qui traverse les routeurs PE1, P3, P4 et PE2 au travers du L2VPN
3. Le traceroute ne montre qu'une seule cible PC5

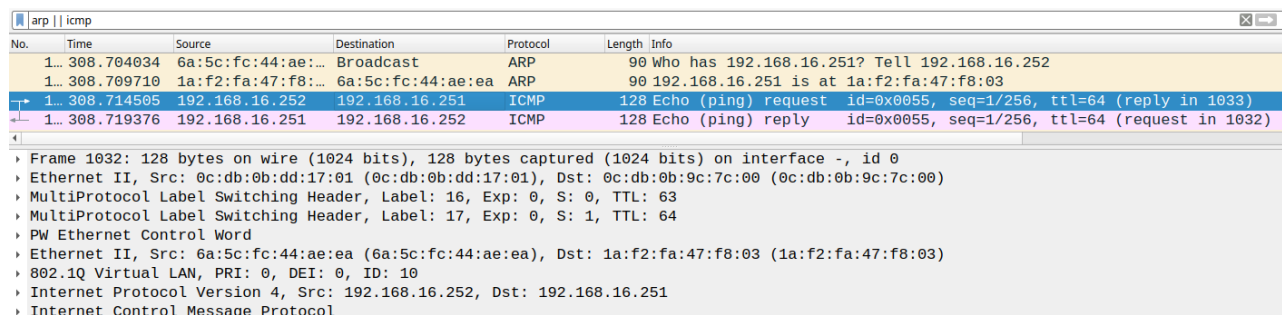
On en conclut que PC1 est relié DIRECTEMENT à PC5 via un VPN de couche 2, un pseudo Wire

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
PC1 console is now available... Press RETURN to get started.
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending select for 192.168.16.252
udhcpc: lease of 192.168.16.252 obtained, lease time 86400
root@PC1:~# arp
Address          Hwtype Hwaddress      Flags Mask      Iface
192.168.16.1     ether  0c:bf:f4:1b:00:00 C              eth0
root@PC1:~# ping -c 1 192.168.16.251
PING 192.168.16.251 (192.168.16.251) 56(84) bytes of data.
64 bytes from 192.168.16.251: icmp_seq=1 ttl=64 time=10.7 ms

--- 192.168.16.251 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.716/10.716/10.716/0.000 ms
root@PC1:~# arp
Address          Hwtype Hwaddress      Flags Mask      Iface
192.168.16.1     ether  0c:bf:f4:1b:00:00 C              eth0
192.168.16.251    ether  1a:f2:fa:47:f8:03 C              eth0
root@PC1:~# traceroute 192.168.16.251
traceroute to 192.168.16.251 (192.168.16.251), 30 hops max, 60 byte packets
 1 192.168.16.251 (192.168.16.251) 16.284 ms 16.834 ms 17.271 ms
root@PC1:~# █
```

Une capture wireshark entre P3 et P4 oui oui entre P3 et P4 dans le BB du FAI montre que l'ARP traverse les routeurs !

**NON ARP ne traverse pas un routeur, ici les routeurs sont transparents à cause du VPN, le Pseudowire**



No.	Time	Source	Destination	Protocol	Length	Info
1...	308.704034	6a:5c:fc:44:ae:...	Broadcast	ARP	90	Who has 192.168.16.251? Tell 192.168.16.252
1...	308.709710	1a:f2:fa:47:f8:...	6a:5c:fc:44:ae:ea	ARP	90	192.168.16.251 is at 1a:f2:fa:47:f8:03
1...	308.714505	192.168.16.252	192.168.16.251	ICMP	128	Echo (ping) request id=0x0055, seq=1/256, ttl=64 (reply in 1033)
1...	308.719376	192.168.16.251	192.168.16.252	ICMP	128	Echo (ping) reply id=0x0055, seq=1/256, ttl=64 (request in 1032)

Frame 1032: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface -, id 0

Ethernet II, Src: 0c:db:0b:dd:17:01 (0c:db:0b:dd:17:01), Dst: 0c:db:0b:9c:7c:00 (0c:db:0b:9c:7c:00)

MultiProtocol Label Switching Header, Label: 16, Exp: 0, S: 0, TTL: 63

MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 1, TTL: 64

PW Ethernet Control Word

Ethernet II, Src: 6a:5c:fc:44:ae:ea (6a:5c:fc:44:ae:ea), Dst: 1a:f2:fa:47:f8:03 (1a:f2:fa:47:f8:03)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10

Internet Protocol Version 4, Src: 192.168.16.252, Dst: 192.168.16.251

Internet Control Message Protocol

- Donc l'ARP traverse un routeur quand on met un PseudoWire!!!
- Le routeur est donc équivalent à 1 switch!

Sur la capture wireshark, on voit apparaître :





- Les 2 labels!
  - 1 pour le LSP qui correspond à la valeur 16
  - L'autre 17 le Label L2VPN!
- **Et la cerise sur le gâteau !**  
 Les couches 2 et supérieures se trouvant entre le CE et le PE sont **ENCAPSULÉS** dans le Pseudo-Wire!!!  
 On peut y voir une seconde couche Ethernet, le VLAN ID qui vaut 10, l'@IP et ICMP  
**On a bien un VPN de couche 2 !**

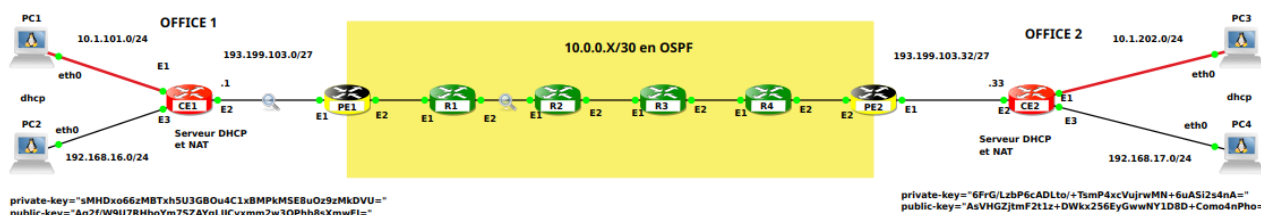
On en déduit que l'on a des tunnels de couche 2.

Le Backbone est vu par les CE comme en Switch ... **c'est le tunnel entre les 2 PE ☺ !**

### 7.3 Wireguard

La maquette n'a pas de grandes ambitions.

Nous avons 2 sites et on a un serveur **Wireguard** de chaque côté comme le montre la figure suivante.



PC1 va pouvoir pinguer PC3 grâce au tunnel chiffré et en utilisant les @IP publiques de CE1 et CE2  
 PC2 ne peut pas pinguer PC4!

**C'est CE1 qui chiffre et CE2 qui déchiffre et vice versa .**

#### 7.3.1 Conf d'un CE

```
/interface wireguard
add listen-port=61664 mtu=1420 name=wireguard1
/ip pool
add name=dhcp_pool0 ranges=10.1.101.2-10.1.101.254
add name=dhcp_pool1 ranges=192.168.16.2-192.168.16.254
/ip dhcp-server
add address-pool=dhcp_pool0 interface=ether1 lease-time=1d name=dhcp1
add address-pool=dhcp_pool1 interface=ether3 lease-time=1d name=dhcp2
/interface wireguard peers
add allowed-address=10.1.202.0/24 endpoint-address=193.199.103.33
endpoint-port=61664 interface=wireguard1
public-key="AsVHGZjtmF2t1z+DWkx256EyGwwNY1D8D+Como4nPho="
/ip address
add address=10.1.101.1/24 interface=ether1 network=10.1.101.0
add address=193.199.103.1/27 interface=ether2 network=193.199.103.0
add address=10.255.255.1/30 interface=wireguard1 network=10.255.255.0
add address=192.168.16.1/24 interface=ether3 network=192.168.16.0
/ip dhcp-server network
add address=10.1.101.0/24 gateway=10.1.101.1
add address=192.168.16.0/24 gateway=192.168.16.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether2
/ip route
add dst-address=10.1.202.0/24 gateway=wireguard1
add dst-address=193.199.103.32/27 gateway=193.199.103.2
/system identity set name=CE1
```



- On voit que l'on crée une interface virtuelle nommée **wireguard1** qui écoute sur le port "pack" : **61664** et on a diminué le MTU de 1500 à **1420** octets  
`/interface wireguard add listen-port=61664 mtu=1420 name=wireguard1`
- On associe (**peer**) cette interface à une autre sur l'autre CE de l'autre côté du backbone en donnant l'IP publique du CE d'en face. Et on autorise **SEULEMENT** le réseau 10.1.202.0/24 à la rejoindre. On donne la clef publique. La clef privée reste bien cachée dans le CE!!!

`/interface wireguard peers add allowed-address=10.1.202.0/24 endpoint-address=193.199.103.33 endpoint-port=61664 interface=wireguard1 public-key="AsVHGZjtmF2t1z+DWkx256EyGwwNY1D8D+Como4nPho="`

On peut voir cette interface qui a une clef privée et une clef publique pour le chiffrement asymétrique.

```
[admin@CE1] > /interface/wireguard/print
Flags: - disabled; - running
0 R name="wireguard1" mtu=1420 listen-port=61664 private-key="sMHDxo66zMBTxh5U3GB0u4C1xBMPkMSE8u0z9zMKDVU=" public-key="Aq2f/W9U7RHboYm7SZAYgLIJCvxmm2w3QPhb8sXmwFI="
[admin@CE1] >
```

Et voici le pire ah non le peer ☺

```
[admin@CE1] /interface/wireguard/peers> print
Columns: INTERFACE, PUBLIC-KEY, ENDPOINT-ADDRESS, ENDPOINT-PORT, ALLOWED-ADDRESS
# INTERFACE PUBLIC-KEY ENDPOINT-ADDRESS ENDPOINT-PORT ALLOWED-ADDRESS
0 wireguard1 AsVHGZjtmF2t1z+DWkx256EyGwwNY1D8D+Como4nPho= 193.199.103.33 61664 10.1.202.0/24
[admin@CE1] /interface/wireguard/peers>
```

Nous avons donc PC1 en @IP privée et derrière un routeur qui fait du NAT qui arrive à pinguer PC3 lui aussi en @IP privée et derrière un routeur qui fait du NAT, si si je vous l'assure ça fonctionne la preuve (Et vous le verrez en TP)

```
root@PC1:~# ping -c 1 10.1.202.252
PING 10.1.202.252 (10.1.202.252) 56(84) bytes of data.
64 bytes from 10.1.202.252: icmp_seq=1 ttl=62 time=5.33 ms
```

```
— 10.1.202.252 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 5.336/5.336/5.336/0.000 ms
root@PC1:~#
```

Voici la capture wireshark correspondant

Mais au fait ping c'est du ICMP, il est passé où l'ICMP ?

Dans le Tunnel ☺

On a 5 paquets IP la première fois!

- 2 pour le **handshake Initiation** et **Response** pour les clefs privées!

Ici c'est la chaîne de caractères : **public-key="Aq2f/W9U7RHboYm7SZAYgLIJCvxmm2w3QPhb8sXmwFI="**

La clef publique de CE1!, puisque Pc1 est rattaché à CE1

- 2 **Transport DATA** correspondant à l'écho request et l'écho reply du ping

- 1 **Keepalive** public-key="Aq2f/W9U7RHboYm7SZAYgLIJCvxmm2w3QPhb8sXmwFI="alive pour dire que c'est terminé

Si on avait eu n pings, il n'y aurait qu'un seul keepalive

Bizarre c'est 10.1.101.248 qui ping 10.1.202.252 et on voit sur Wireshark les @IP 193.199.103.1 et 193.199.103.33 ?



**Est-ce dû au NAT ?****NON!!!**

On peut retirer le NAT, ça ping toujours!!!

Un traceroute de Pc1 à Pc3 renvoie ceci

```
root@PC1:~# traceroute 10.1.202.252
traceroute to 10.1.202.252 (10.1.202.252), 30 hops max, 60 byte packets
 1  10.1.101.1 (10.1.101.1)  1.762 ms  1.691 ms  1.660 ms
 2  * * *
 3  10.1.202.252 (10.1.202.252)  41.505 ms  41.440 ms  41.366 ms
root@PC1:~#
```

Un traceroute de Pc1 à Pc3 renvoie cela ☺

```
root@PC3:~# traceroute 10.1.101.248
traceroute to 10.1.101.248 (10.1.101.248), 30 hops max, 60 byte packets
 1  10.1.202.1 (10.1.202.1)  1.242 ms  1.171 ms  1.110 ms
 2  * * *
 3  10.1.101.248 (10.1.101.248)  21.031 ms  21.004 ms  20.943 ms
root@PC3:~#
```

Les \* \* \* représentent la partie cachée

**On en déduit que l'on a un tunnel chiffré de couche 5.****Le Backbone et les CE sont vus par le LAN comme fil chiffré ... c'est le tunnel entre 2 interfaces virtuelles ☺!**

## 8 Conclusion

Les VPN ça permet

- de passer sous les couches
- de chiffrer
- que des machines derrière du NAT puissent communiquer directement...
- On cache au FAI ce que l'on fait aussi;)