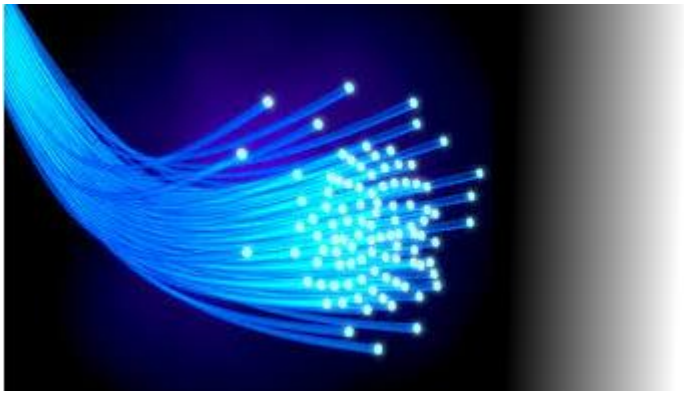
Hes·so FRIBOURG FREIBURG

Haute Ecole Spécialisée de Suisse occidentale

Fachhochschule Westschweiz



« FIBER/LTE »

Documentation de projet

Christophe Perroud, David Rossier–T3

20/01/2015

Résumé

Ce projet a pour but de mettre en place une ligne de backup utilisant la technologie LTE, aux côtés d'une ligne principale qui elle est en fibre optique. Ceci dans l'optique d'amoindrir les couts engendrés par une ligne de backup en fibre optique. La transition entre les deux lignes doit être transparente et le lien entre nos différents lieux géographiques doit être assuré par un lien VPN de "couche 2". Nous avons donc le même sous-réseau de toutes parts du VPN.

Les premiers efforts ont été concentrés dans l'analyse de l'état de l'art. Des informations plus précises sur le fonctionnement des différentes technologies ont été trouvées et assemblées dans l'analyse.

Nous nous sommes concentrés sur les différents équipements qui permettaient de faire un backup d'une ligne à l'aide de la technologie LTE. Nous avons ensuite analysé les besoins concernant les diverses technologies VPN et encapsulations nécessaires dans l'élaboration de notre infrastructure.

Nos choix ont été dictés par les conditions suivantes :

- Lorsque l'on fait une connexion avec le réseau LTE, les adresses IP changent. Pour continuer à assurer un service de "couche 2", il faut utiliser un VPN de couche 2. Pour cela, nous avons utilisé L2TP.
- En ce qui concerne la sécurité sur Internet, nous avons mis en place IPsec sur la ligne de backup, afin de crypter les messages passant par cette ligne. Etant donné que la ligne de fibre optique est directement établie entre les lieux géographiques (ligne louée), IPsec n'a pas été mis en place sur la ligne de fibre optique.
- Les adresse IP offertes par Swisscom aux clients LTE sont privées et se trouvent derrière un NAT avant de "sortir" sur Internet. Elles ne permettent pas une connexion directe d'un client LTE à un autre. C'est pour cela que nous avons mis en place un routeur faisant office de relai dans la DMZ de l'Ecole d'Ingénieurs et d'architectes de Fribourg. Ce routeur va rediriger le trafic depuis un de nos clients jusqu'à l'autre, établissant ainsi la ligne de backup.
- Etant donné que le "switch" en cas de coupure doit se faire rapidement, nous avons utilisé le protocole de routage OSPF et optimisé son temps de convergence afin de répondre aux besoins du projet.

Suite à la mise en place de cette infrastructure, nous avons effectué une batterie de tests afin de valider le cahier des charges.

Abstract

The main goal of this project is to set up a backup line, using the LTE technology, with a main line using the optical fiber. We use this infrastructure to have less costs than using a backup line with optical fiber. The transition between these two lines has to be transparent and the link between our differents geographical locations has to be assured by a layer 2 VPN link. With this kind of VPN, we have the same subnet at each side of the tunnel.

The first efforts we made were fort the art state analysys. More specifical informations about the differents technologies were found and meet in this part.

We concentrated our job on the differents amenities that can have a backup line, using the LTE technology. Then, we have made an analysis about the VPN technologies the many necessary encapsulations.

Our choices were made following theses conditions :

- When we make a connexion with the LTE network, the IP addresses change. To assure the „layer 2“ service, we have to use an layer 2 VPN. We used the L2TP protocole to have this function on our infrastructure.
- To assure the security of the datas on the Internet, we set up an IPsec tunnel on the backup line, to crypt messages. The main line in optical fiber is directly connected (leased line) so we didn't put IPsec on the main line.
- The IP addresses given by Swisscom tot he LTE clients are private and are behind a NAT, before having a public address on the internet. For security reasons, we cannot set up a direct connexion between two LTE clients. For this reason, we set up a router in our school's DMZ. This router acts as a relay and redirects the trafic from a LTE client to another, on the backup line.
- The switch between the two lines (in case of breaking down of the main line), we used the OSPF routing protocol and optimized the convergence timing of OSPF.

Following the establishment of this infrastructure, we conducted a series of tests to validate the specification.

Table des matières

1.Introduction

L'augmentation de capacité de transmission est exponentielle dans 2 technologies d'accès, les fibres optiques et LTE.

Le projet « Fiber avec redondance LTE » consiste à offrir une méthode de lien de backup entre deux sites d'une entreprise. En effet, lorsque le lien fibre est rompu, le but est de se connecter à l'autre succursale en utilisant une connexion se basant sur la technologie 4G / LTE.

Cette documentation détaille la mise en place de ce projet de semestre. Dans un premier temps, nous allons présenter le cahier des charges de notre projet. Nous allons ensuite analyser l'état de l'art, pour ensuite nous concentrer sur les spécifications (infrastructures possibles) et la conception puis de l'implémentation d'une solution fournissant le service susmentionné. Nous comparerons ensuite les capacités de la LTE par rapport à la fibre et tirerons les conclusions sur l'utilisation possible de notre solution dans un environnement de production.

2. Cahier des charges

2.1 Contexte

Toutes les grandes entreprises possèdent des liaisons fibrées entre leurs sites principaux garantissant des communications internes rapides et sûres. Cependant, la rupture d'une fibre peut entrainer la perte totale des connexions. La solution la plus utilisée actuellement est une deuxième connexion en fibre optique sur un tracé géographiquement totalement séparé et très couteuse.

Dans la figure ci-après, on peut voir l'infrastructure classique d'une entreprise avec une ligne de backup en fibre optique. La ligne principale passe par 2 « centrales de quartier » (un pour chaque bâtiment). La ligne de backup, quant à elle, passe par 2 autres centrales de quartier.

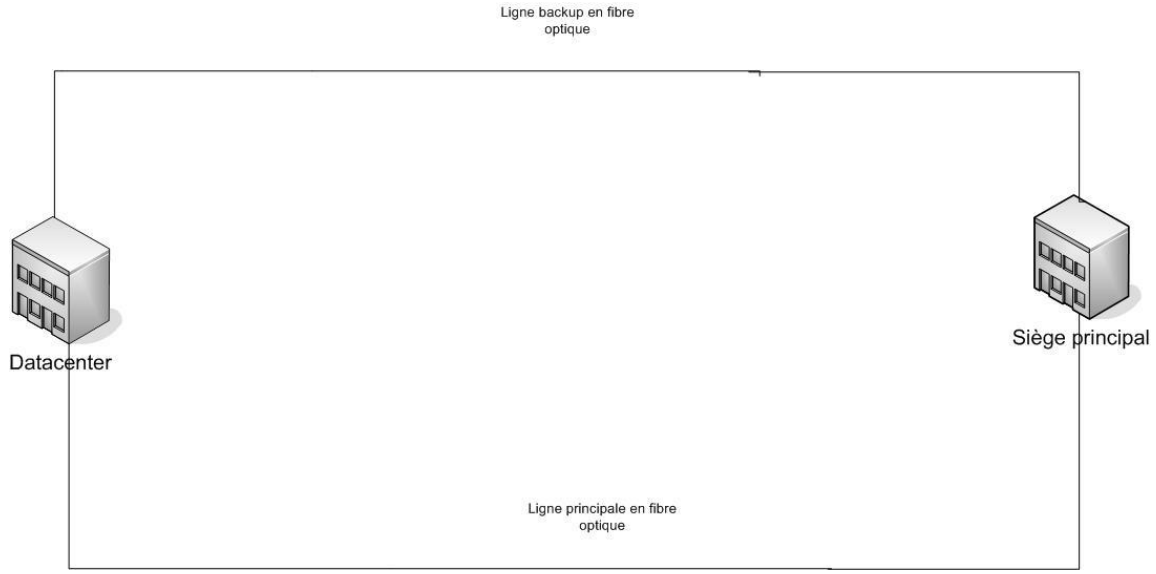


Figure 1 : Infrastructure d'une grande entreprise, avec 2 lignes de fibre optique

Lors de ce travail de semestre, nous devrons proposer et évaluer des liaisons LTE comme redondance aux connexions optiques. Pour ce faire, nous devrons réaliser une liaison point-à-point de 1 Gb/s ou 10 Gb/s 100% optique. La redondance LTE est à organiser avec des VPN (réseaux privés virtuels) et avec des équipements commerciaux du labo Telecom. Des tests de performances vont être effectués en cas de rupture de la fibre optique afin de voir avec quelle vitesse le transfert « fibre/LTE » est fait et afin de mesurer la performance de la ligne de backup.

La figure ci-après illustre l'infrastructure que nous aimerions mettre en place. Une ligne de backup remplace la ligne principale.

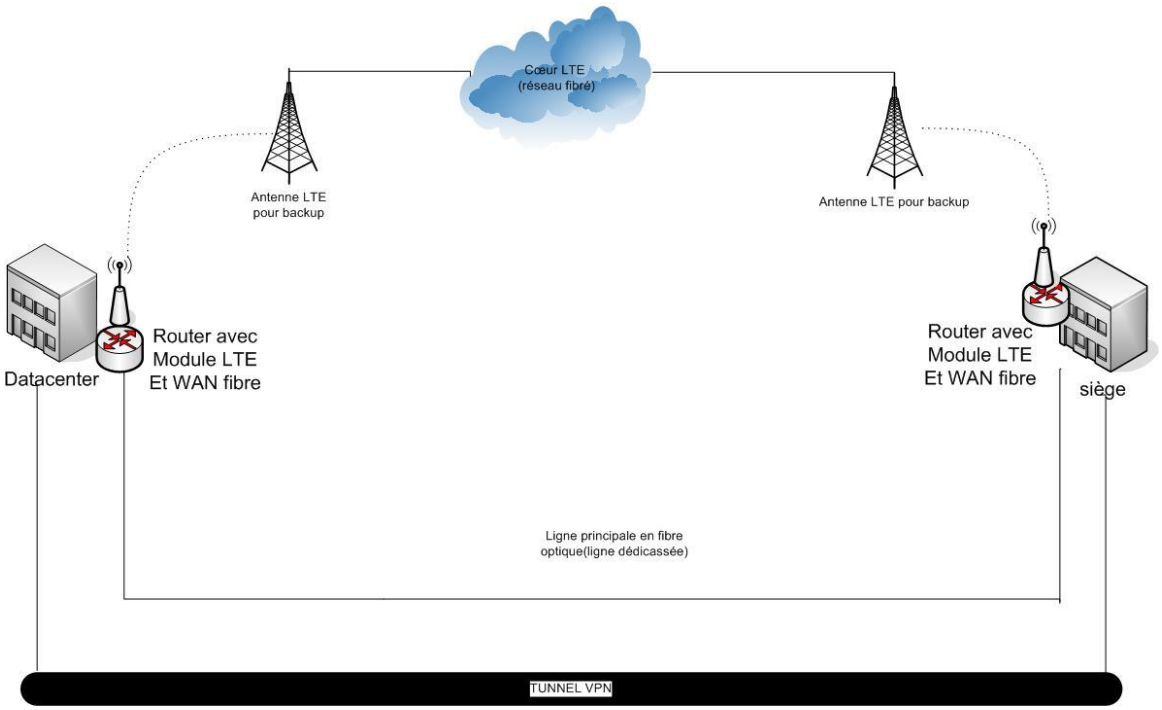


Figure 2 : infrastructure d'entreprise avec ligne de backup via LTE

Après avoir mis en place les deux lignes, il faudra trouver le moyen de commuter entre les 2. C'est-à-dire que lorsque le lien principal de fibre optique tombe, le trafic est automatiquement redirigé sur la ligne LTE et lorsque le lien fibre est à nouveau disponible, le trafic empruntera à nouveau la ligne principale. Cela est important afin de garantir la rapidité et la disponibilité de la ligne en cas de problème.

2.2 Objectifs

- Décrire et concevoir l'architecture du réseau à mettre en place
- Mettre en place, concevoir et configurer le lien optique.
- Mettre en place, concevoir et configurer le lien LTE.
- Générer et mesurer le trafic (LTE et Fibre)
- Mesurer les conséquences d'une coupure de la fibre

La planification de notre projet se trouve dans l'annexe 1.

3. Analyse de l'état de l'art

Dans ce chapitre, nous allons devoir étudier les différentes technologies à disposition, plus particulièrement les lignes de fibre optique, la technologie LTE, les produits et solutions dont on peut disposer en Suisse ainsi que les solutions pour créer un VPN de couche 2.

Finalement, nous comparerons les différentes solutions et produits trouvées, afin de choisir le matériel et les technologies que nous utiliserons.

3.1 Fibre optique

La fibre optique a été inventée en 1970. Le principe est de faire circuler des faisceaux lumineux à travers un cœur en verre ou en plastique. Contrairement aux câbles en cuivre, es données sont véhiculées sous forme lumineuse et non pas électrique, permettant une vitesse de transfert extrêmement élevée.

On dispose également d'une largeur de bande assez élevée, permettant un multiplexage fréquentiel élevé avec plusieurs canaux.

La qualité du transport d'information est également excellente. On subit nettement moins de dégradations que dans les câbles de cuivre.

En Suisse, les constructeurs du réseau optique se sont engagés à louer leurs lignes de fibre optique aux opérateurs. Cela aide à préserver la concurrence et de ce fait, l'offre explose avec de nombreux fournisseurs.

En ce qui concerne les PME, la vitesse devient illimitée ou presque: les opérateurs proposent des débits symétriques allant jusqu'à 10 Gbit/s (c'est-à-dire 500 fois plus qu'une ligne ADSL de base).

Les différences de prix avec le FTTH sont cependant importantes. Chez VTX, une connexion symétrique de 10 Mbit/s coute 460 francs par mois et les prix montent à 690 francs par mois pour du 20 Mbit/s. Des coûts supplémentaires peuvent en outre être facturés en fonction des travaux à effectuer pour l'installation, sont négociés au cas par cas avec les fournisseurs.

3.1.1 Ligne louée en fibre optique

On dispose d'une fibre partant depuis un bâtiment (par exemple un siège d'entreprise, un datacenter, etc..) qui va se connecter à un « central » de fibre optique, qui va avoir le même fonctionnement qu'un DSLAM dans les lignes ADSl. Depuis ce point, on va partir dans le réseau optique du fournisseur, comme montré dans la figure ci-dessous :

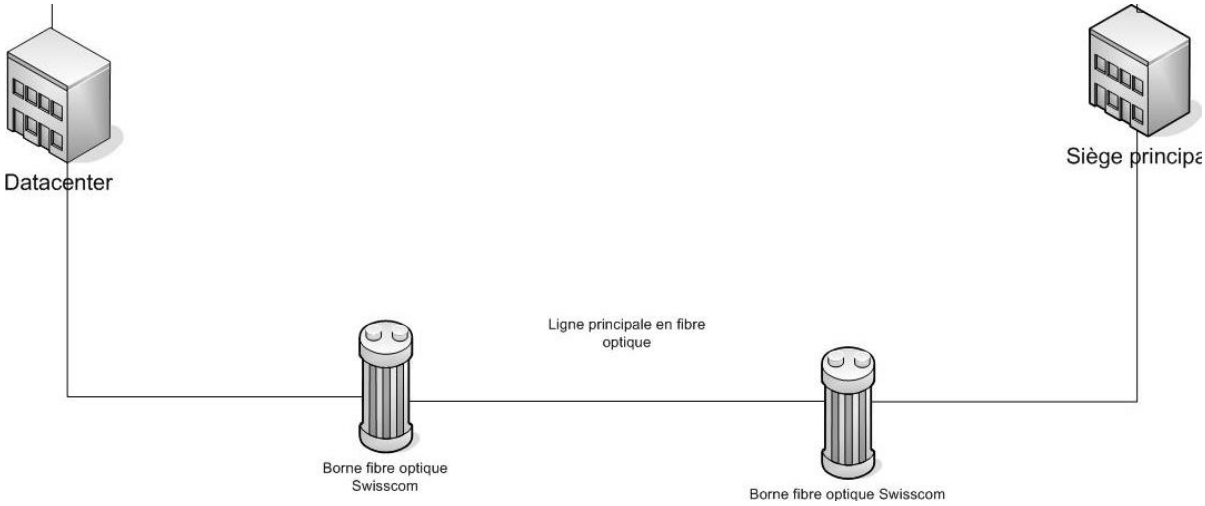


Figure 3 : Schéma de connexion d'une fibre optique

3.1.2 Couts et performances de la fibre optique

Lorsque l'on veut établir une connexion en fibre optique, il faut bien déterminer la différence entre un accès de fibre optique pour accéder à Internet, et une ligne louée entre deux endroits géographiquement distincts.

3.1.2.1 Coûts de l'accès à Internet

	Offre de base pour les PME	Offre pour de fortes attentes	Exploitation par Swisscom	Interconnexion de plusieurs sites
	Business Internet light	Business Internet standard	Business Internet advanced	Mise en réseau
	Commander	Demander offre	Demander offre	Demander offre
Technologie du raccordement	VDSL, fibre optique	VDSL, fibre optique	Dédiée via fibre	VDSL, fibre optique, Dédiée via fibre
Bande passante	Jusqu'à 100/10 Mbit/s	Jusqu'à 100/10 Mbit/s	Jusqu'à 10/10 Gbit/s	Jusqu'à 10/10 Gbit/s
Routeur y c. surveilance & alarme		✓	✓	✓
Terminal de caisse en pure exploitation	✓	✓*		
Alarme en cas d'interruption du service (E-Mail / SMS)		✓		
Liaison de réserve avec redirection IP, sans frais de communication		✓	✓	✓
SLA avec suppression du dérangement dans les 24 heures	✓ (en option)	✓	✓	
Serveur messagerie et Internet Utilisation et exploitation d'adresses IP fixes et service DNS	✓ (en option)	✓	✓	✓
Firewalls pour le trafic entrant et sortant		✓		
Promotion	EXONERATION DE LA TAXE DE MISE EN SERVICE ET DES FRAIS DE BASE JUSQU'À 3 MOIS[1]	EXONERATION DE LA TAXE DE MISE EN SERVICE ET DES FRAIS DE BASE JUSQU'À 4 MOIS[1]		
Coûts	Dès CHF 29.-/mois	Dès CHF 59.-/mois	Sur demande	Sur demande
	Commander	Demander offre	Demander offre	Demander offre
	Détails	Détails	Détails	Détails

Figure 4 : Offres fibres de swisscom pour l'accès à internet

Les coûts varient énormément pour les entreprises. Les opérateurs comme Swisscom ne communiquent pas leurs prix à partir d'une certaine performance en ligne dédiée car de nombreux paramètres interviennent et les prix peuvent énormément varier. On peut observer dans le tableau ci-dessus que les prix de basent sont d'environ 30.- par mois pour un raccordement basique. On peut cependant payer beaucoup plus cher (des centaines voire milliers de francs) pour certaines infrastructures louées.

3.1.2.2 Lignes louées en fibre optique : performances

Les performances d'une ligne louée en fibre optique sont naturellement élevées. La figure ci-dessous montre les performances disponibles sur les lignes louées auprès de Swisscom.

Bande passante disponible

Variante	Downstream/upstream
Fibre optique	30000/3000 kbit/s
	50000/5000 kbit/s
Fibre optique symétrique	2-100 Mbit/s (sur demande)

Figure 5 : Bande passante fibre (ligne dédiée)

3.1.2.3 Coûts de la ligne louée

Selon les indications de M.Robadey, le coût d'une ligne de fibre optique louée est d'environ 2000.- par mois pour 100 Mbits/s de débit, avec une longueur de 4Km (exemple standard d'une connexion fibre pour une entreprise à Zürich).

Pour une fibre de « backup », il faut compter environ 3000.- supplémentaires par mois.

3.2 Technologie LTE

La technologie LTE (Long Term Evolution) est l'évolution la plus récente des normes de téléphonie mobile. Le réseau 4G est l'évolution du réseau mobile de 3ème génération déjà en place. Il est basé sur la norme LTE-Advanced (Long Term Evolution-Advanced). En effet, l'UIT (Union Internationale des Télécommunications) a choisi de considérer la LTE comme système 4G, grâce à ses importantes améliorations par rapport à la 3G.

3.2.1 Couverture en Suisse

À L'heure actuelle, environ 200 communes ont un accès en 4G (ce qui est pour l'instant relativement peu), mais les opérateurs (surtout Swisscom) continuent à mettre en place la 4G à plus large échelle en Suisse.

Sur la figure ci-dessous, on peut observer l'état de l'avancement de la couverture LTE en Suisse :

En bleu, les territoires où la 4G est disponible.

Figure 6 : Couverture 4G par swisscom fin 2014

3.2.2 Performances

Sur la figure ci-dessous, on peut voir l'évolution des performances des divers réseaux mobiles.

Réseau	Norme	Appellation commerciale	Débit théorique descendant	Débit théorique montant	Latence
3G	UMTS	3G	0,384 Mbit/s	0,064 Mbit/s	200ms
3G+ / 3,5G	HSPA	3G+	14,4 Mbit/s	5,8 Mbit/s	70ms
3G++ / 3,75G	HSPA+	Dual carrier / H+	43,2 Mbits/s	11,5 Mbit/s	70ms
3,9G	LTE	4G	300Mbits/s	75 Mbits/s	10ms

Figure 7 : Performances selon technologie

Ce tableau montre bien que la 4G peut atteindre de bien meilleures performances que les normes qui l'ont précédée. Pour atteindre ces débits, on utilise la technologie MIMO (Multi In Multi Out) déjà introduit dans les dernières normes 3G.

Cette technologie MIMO permet d'envoyer plusieurs signaux en même temps avec plusieurs antennes.

3.2.3 Fréquences utilisées par le LTE

Les fréquences utilisées par le LTE varient entre 800 MHz, 1800 MHz et 2600 MHz selon les opérateurs. C'est à 2.6 Ghz que la réception est la meilleure mais le signal contient beaucoup de bruit car les signaux à hautes fréquences sont plus sensibles aux éventuels obstacles.

3.2.4 LTE Advanced

La norme LTE Advanced (lancée par Swisscom en juin 2014) permet d'atteindre des débits descendants d'environ 1Gbits/s. Un débit de cette envergure est possible grâce au « carrier agrégation » (agrégation de porteuses) qui permet d'atteindre une largeur de bande de 100 Mhz maximum contre 20 pour la norme LTE.

Cela veut dire que 2 bandes de fréquences différentes pourront être couplées afin d'offrir de meilleurs débits. La technologie MIMO, déjà présente dans la précédente norme, connait une évolution : il sera possible d'utiliser jusqu'à 8 antennes côté base de transmission, pour atteindre des débits de l'ordre de 3Gbits/seconde.

3.2.5 LTE dans les routeurs Cisco

Dans la figure ci-dessus, nous pouvons voir le fonctionnement par couche de la LTE.

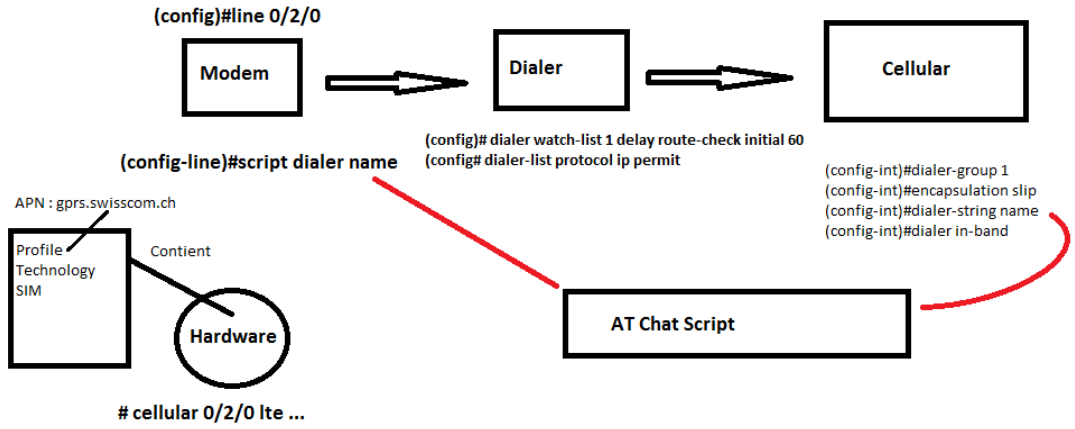


Figure 8 : Fonctionnement LTE

La configuration du Hardware permet de configurer différents paramètres liés à la LTE, comme le profile, qui contient l'APN de l'opérateur, la technologie choisie (LTE / UMTS / …) ainsi que l'accès à la carte SIM (Déblocage, blocage, changement de PIN).

Le modem représente la couche physique. C'est lui qui s'occupe d'établir une ligne de connexion vers l'antenne LTE la plus proche. Il utilise pour cela le chat script et les informations contenues dans le hardware. Il peut être configuré à l'aide dans la configuration de la ligne correspondant au module LTE.

L'interface Dialer représente la couche de liaison de données. C'est elle qui permettra à la carte Cellular d'accepter les protocoles des couches supérieures telles qu'IP, CLNS, etc. Elle définit également les délais de connexion et de route. Elle utilise le AT Chat script et les informations contenues dans la carte SIM, en plus de l'APN, pour se connecter au réseau mobile de Swisscom.

L'interface Cellular correspond à la couche réseau. C'est elle qui va gérer la réception notamment des adresses IP, à l'aide du DHCP reçu par Swisscom. C'est également sur cette interface qu'il est possible de configurer un tunnel IPSec. Elle peut-être configuré au travers de l'interface Cellular du module LTE.

3.3 Choix du matériel LTE

Afin d'établir une connexion LTE de backup entre nos deux sites, il nous a fallu étudier différents matériel qui permettent d'interconnecter plusieurs sites distants à l'aide de la technologie LTE.

Nous allons tout d'abord étudier les différents matériels à disposition et nous finirons par les départager à l'aide d'une analyse multicritère pour nous orienter vers la solution qui sera implémentée.

3.3.1 Netgear MBR1515

Ce modèle de l'entreprise Netgear peut remplir les fonctions de relai entre la ligne ethernet câblée et le LTE. On peut mettre une carte SIM à l'intérieur et ainsi le faire communiquer en LTE. Il est également possible de paramétrer le failover (prise en main de la connexion par le LTE en cas de problème sur la ligne principale).

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.2 D-Link DWR-921

Le D-Link DWR 921 est aussi un routeur possédant une connectique LTE pouvant être utilisée comme backup. Il possède de nombreuses caractéristiques en commun avec le Netgear MBR 1515.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.3 Module LTE de Cisco

Le module Cisco 4G LTE WWAN EHWIC est le premier module pour entreprises utilisant le 4G comme WAN développé par Cisco. Il peut être utilisé comme backup vis-à-vis d'une ligne WAN standard mais aussi comme ligne WAN principale.

Il peut être intégré dans un routeur Cisco 2900, ce qui est un avantage dû au fait qu'on dispose de routeurs de ce type à l'école d'ingénieurs.

Il existe plusieurs variantes de ce module, avant tout aux états unis, notamment en fonction des opérateurs américains. Cependant, il existe une version européenne qui travaille avec ces fréquences :

- 800 MHz

- 900 Mhz
- 2100 MHz
- 2600 MHz

Figure 1. Cisco 4G LTE WWAN EHWIC for Cisco ISR G2

Figure 9 : Carte d'extension LTE pour routeur Cisco

Via la technologie 4G intégrée dans le routeur, on gagne de la rapidité au niveau de l'installation et du management. La qualité de service peut être gérée comme sur n'importe quelle autre interface Ethernet de Cisco. De plus, le temps d'installation est court. Le backup peut être facilement configuré avec cette solution. Le fait de mettre en place un routage utilisant cet adaptateur comme « route secondaire » pourrait être une bonne solution dans ce projet.

3.3.3.1 Avantages

- Simple à mettre en place
- Coûts
- Solution plus professionnelle
- Solution réutilisable pour des projets futurs
- Solution compatible avec le matériel dont on dispose (routeurs Cisco 2900)

3.3.3.2 Désavantages

- Une seule carte SIM par adaptateur (possibilité d'en acheter deux et de faire du partage de charge entre les 2 cartes)

3.3.4 Huawei USB Modem E3276 4G

Ce modèle de Huawei proposé par Swisscom est une clé USB supportant la 4G / LTE. Il pourrait être utilisé comme backup à condition d'être connecté à un routeur ou un modem avec un slot pour une clé USB 4G.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.5 EG860 CPE

L' EG860 est un CPE externe, accédant au réseau LTE et transmettant les données par Ethernet ou wifi.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.6 Huawei USB Modem E3272 LTE (Cat4)

Ce module USB est fourni par l'opérateur Sunrise. Il supporte le LTE, en fournissant un débit pouvant atteindre 150 Mbit/s en downstream et 50 Mbit/s en upstream.

Il n'a pas été retenu car il n'est pas compatible avec le matériel du laboratoire.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.7 Router avec module LTE intégré Swisscom

Swisscom a lancé récemment une solution de backup avec LTE pour les clients privés. Cependant, une solution pour les entreprises va être mise en place début 2015.

Le produit que Swisscom commercialise s'appelle « Internet Box ». Il contient un module LTE permettant d'utiliser la connexion LTE en cas de problèmes sur la connexion WAN principale.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel».

3.3.8 Bintec RS353jv-4G

Ce routeur est un routeur orienté professionnel équipé d'un module LTE. D'après le fabricant, il peut atteindre 100 Mb/s en download et 50 Mb/s en upload. Il peut aussi utiliser la technologie 3G au cas où celle-ci serait utilisable en lieu et place de la 4G. Il peut accueillir une carte SIM (situé en bas du châssis). Ce routeur dispose aussi de 5 ports de type GigabitEthernet.

Il est également possible de mettre en place un tunnel IPSec avec ce routeur, ce qui peut nous être utile dans ce projet.

Ce modèle est documenté de façon plus détaillée dans l'annexe «complément d'analyse: matériel ».

3.3.9 Conclusion

Notre analyse multicritère (disponible dans l'annexe) nous a permis de choisir le module LTE pour routeurs Cisco. En effet, ce dernier nous permettait une simplicité de configuration et une disponibilité que n'offraient aucun des autres appareils.

3.4 Tunnel VPN

En partant du principe que la société échangera des données confidentielles entre les deux sites, nous devons être à même de garantir l'intégrité et la confidentialité des données qui transiteront par notre liaison.

3.4.1 Types de VPN

Afin de garantir la confidentialité et la sécurité du trafic inter-sites, il est possible de crypter les données à plusieurs niveaux :

Couche OSI	Exemple d'application
Couche 7	HTTPS – S/MIME
Couche 4	SSL/TLS – SSH
Couche 3	IPsec – MPLS
Couche 2	L2TP – VPLS-EoMPLS
Couche 1	Wireless encryption

3.4.2 Différences entre un VPN de couche 2 et un VPN de couche 3

Dans un VPN de couche 2, les trames (souvent Ethernet) sont transportées de façon similaire que lorsqu'un simple câble physique est directement connecté entre 2 switchs. Ce VPN assure tous les besoins de Ethernet (apprendre les adresses MAC, utiliser des broadcast…). Les tunnels de couche 2 sont en générale un peu plus simples à mettre en place que les tunnels de couche 3. Si le tunnel est bien implémenté, l'utilisateur ne voit absolument rien et a l'impression d'être dans le même sous-réseau que les machines qu'il va atteindre via le tunnel.

Dans un VPN de couche 3, chaque côté de la connexion est dans un sous-réseau différent et les paquets IP sont routés dans le VPN. Il offre plus de sécurité qu'un tunnel de couche 2. Cependant, il n'offre pas le même niveau de « transparence » qu'un tunnel de couche 2.

3.4.3 L2TP

Ce protocole permet de transporter des connexions en conservant les informations du niveau 2 au niveau 7 du modèle OSI. Le transport de ces connexions se fait grâce à des tunnels IP/UDP, le port UDP utilisé en standard est le 1701. Un même tunnel peut transporter plusieurs connexions, en général il n'y a qu'un seul tunnel entre deux mêmes équipements de terminaison.

Au départ, L2TP a été défini pour transporter des connexions PPP avec la RFC 2661, puis L2TP a été généralisé pour transporter n'importe quel protocole de niveau 2 avec L2TPv3

Nous avons une illustration du tunnel L2TP version 3 dans la figure ci-dessous :

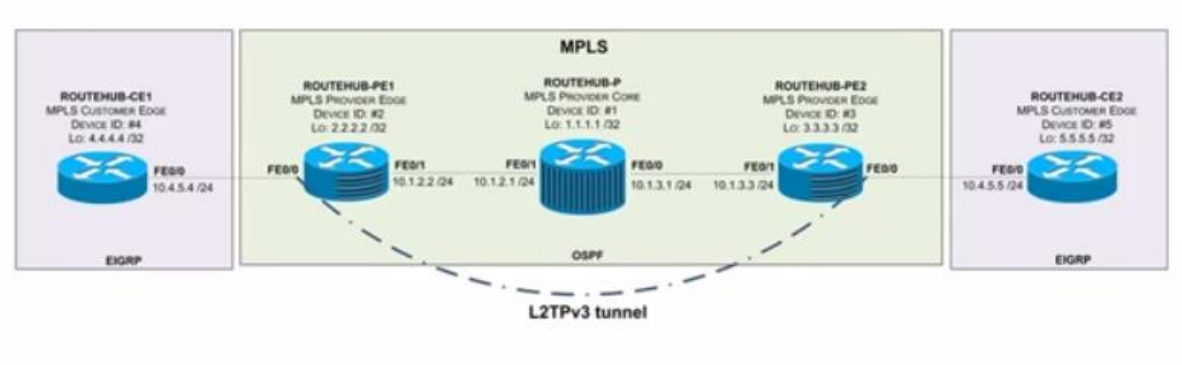


Figure 10: Exemple tunnel L2TP

La version 3 de ce protocole (L2TPV3) permet de mettre plusieurs protocoles dans ce tunnel, contrairement aux versions plus anciennes qui n'autorisaient que du PPP.

3.4.3.1 Encapsulation L2TP

Il existe différentes variantes en ce qui concerne L2TPv3. On peut encapsuler à différents niveaux. On peut directement utiliser L2TPv3 over UDP ou IP. Dans le cadre de notre projet, nous allons utiliser L2TP over IP pour y encapsuler nos paquets à partir de la couche « Ethernet ».

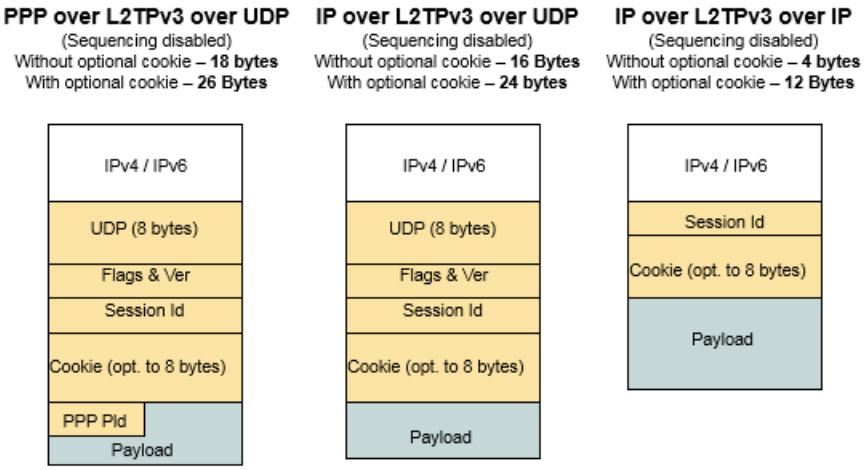


Figure 11 : Encapsulation L2TP

3.4.3.2 Champs principaux

3.4.3.2.1 ID de session

L'id de session est codé sur 32 bits. Il contient une valeur non nulle pour identifier la session. Chaque identificateur de session sera nommé différemment par chaque routeur, ce qui veut dire que la même session pourra recevoir plusieurs session id.

Lors de la création d'une session, les sessions ids sont échangés. Le session id fournit le contexte pour les futurs échanges de données (cookies, taille, type de charge utile…).

3.4.3.2.2 Cookie

Le champ cookie contient une donnée de longueur variable (max 64 bits) qui est utilisée pour contrôler l'association d'une donnée reçue avec le session id. Le cookie

doit être configuré aléatoirement. Le Cookie fournit un niveau supplémentaire de garantie qu'un message a été dirigé sur la bonne session. Le cookie va permettre de prévenir les erreurs de corruption de paquets et d'attaques d'insertion de paquets.

Lorsque le contrôle de connexion est utilisé lors de l'établissement de session, les valeurs des cookies sont choisies et échangées durant la création de session.

3.4.4 MPLS - VPLS

Ces technologies sont utilisées par les opérateurs pour créer des VPN de couche 2 entre plusieurs points d'un réseau. Malheureusement, il est nécessaire d'utiliser le réseau d'un opérateur pour le mettre en place, car chacun des équipements intermédiaires doivent être configurées correctement pour que la technologie fonctionne.

Ils sont décrits plus précisément dans l'annexe « Complément d'analyse : VPN ».

3.4.5 GRE

L'utilisation de GRE dans le cadre d'un tunnel de couche 2 n'est pas applicable car la technologie n'était pas compatible avec nos routeurs. Elle est décrite plus précisément dans l'annexe « Complément d'analyse : VPN ».

3.4.6 Tunnel VPN de couche 3 : IPSEC

IPsec est une suite de protocoles qui permet de sécuriser le trafic IP uniquement. Il garantit ainsi l'authenticité et l'intégrité de chaque paquet d'une communication au travers d'un mécanisme de cryptographie asymétrique. Ces protocoles ont été implémentés après l'arrivée de l'IPv4, car à la base l'IP ne possède aucune notion de sécurité des paquets.

Plusieurs types de tunneling existent :

3.4.6.1 Site to site (routeur du site 1 vers routeur du site 2)

Avantages :	Totalement transparent aux yeux de l'utilisateur
	Gestion des tunnels de manière centralisée
Inconvénients :	La mise en place peut être complexe
	La disponibilité et fiabilité du tunnel sont cruciales

Dans le vocabulaire IPsec, ce type de tunneling est appelé Tunnel Mode.

3.4.6.2 Client to site (client vers le routeur du site distant)

Avantages :	Simplicité de mise en place
Inconvénients :	Le client doit lui-même initier le tunnel
	Difficulté de gestion (beaucoup de tunnels)

3.4.6.3 Client to client (client vers un autre client)

Avantages :	Connexion sécurisée de bout en bout
Inconvénients :	Enormément de tunnels dans le réseau

Les clients doivent eux-mêmes initier les tunnels

Dans le vocabulaire IPsec, ces deux types de tunneling sont appelés Transport Mode.

Comme indiqué précédemment, IPsec est un ensemble de protocoles. On y trouve :

3.4.6.3.1 AH (Authentification Header)
Ce protocole de sécurité fourni l'authentification et le contrôle de sécurité. Il sert également de signature numérique qui permet de garantir que ni le contenu du paquet, ni les en-têtes du paquet n'ont été modifiés. Cependant, il ne garantit pas la confidentialité des données, le contenu des paquets n'étant pas crypté !

3.4.6.3.2 ESP (Encapsulating Security Payload)
Mêmes propriétés que l'AH, mais en plus garanti la confidentialité des données en cryptant le contenu du paquet IP original dans l'ESP.

3.4.6.3.3 IKE (Internet Key Exchange)
IKE est le protocole permettant de créer le tunnel sécurisé entre les deux points au travers de l'échange de clés. Il possède plusieurs phases :

3.4.6.4 Spécification d'IPsec

a) Mode Tunnel vs mode Transport

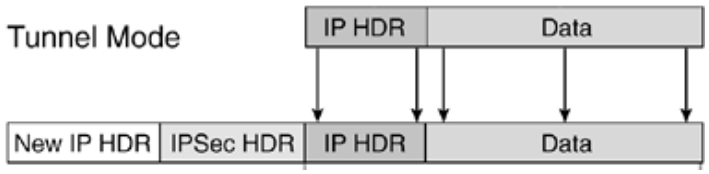


Figure 12 : paquet IPSEC en mode tunnel

En mode Tunnel, l'entier du paquet IP est crypté puis encapsulé dans un paquet IP possédant un nouvel en-tête IP en plus de l'en-tête IPsec.

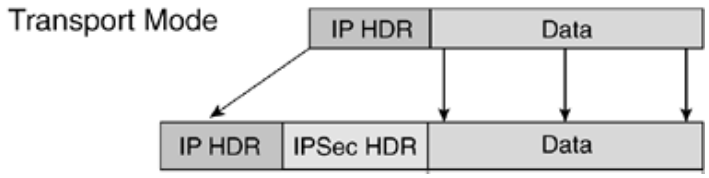


Figure 13 : paquet IPSEC en mode transport

En mode Transport par contre, seule la partie « *données »* du paquet IP original est cryptée. L'en-tête IPsec vient se glisser entre l'en-tête IP du paquet original *(non cryptée)* et la partie *données (cryptée)*.

3.4.6.5 GRE over IPsec

Comme indiqué précédemment, la suite de protocoles IPsec permet de crypter uniquement des paquets de type IP. Mais dans notre cas, nous allons transmettre des paquets de protocoles d'autres couches. Pour pallier à ce problème, il est nécessaire d'encapsuler ces paquets OSPF dans un paquet IP avant de les faire passer dans le tunnel IPsec. C'est ce que l'on appelle le GRE over IPsec.

A la base, le GRE a été développé afin de faire transporter n'importe quel protocole de couche 2 et 3 à travers un réseau IP en encapsulant le paquet de base dans un paquet IP. Il est non sécurisé et ne négocie aucun paramètre avant l'établissement du tunnel. C'est pour cela qu'il est généralement couplé avec l'IPsec afin de garantir l'authenticité et l'intégrité des données qui y transitent.

3.4.7 Spécifications de GRE over IPsec

3.4.7.1 Vue des paquets GRE over IPsec mode tunnel avec ESP

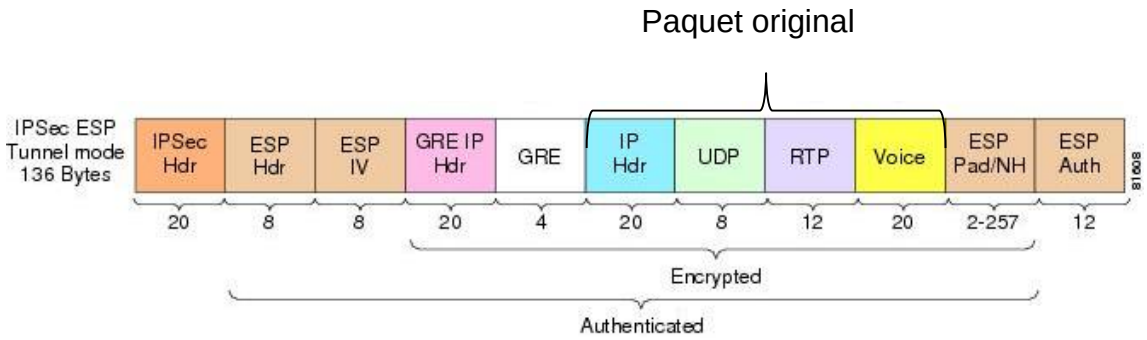


Figure 14 : en-têtes d'un paquet encapsulé avec GRE over IPSEC

On peut donc voir que maintenant, il est possible de faire transiter n'importe quel protocole de couche 3 au sein de notre tunnel IPsec.

3.5 Fragmentations

Etant donné que de nombreuses encapsulations seront mises en place, il faudra être attentif à de possibles fragmentations de paquets. En effet, les en-têtes ajoutés lors des encapsulations vont générer des fragmentations supplémentaires.

3.6 Conclusion

Cette analyse nous a permis d'écarter plusieurs technologies et matériels.

Lors de cette partie d'analyse, nous avons effectué des recherches concernant les différentes technologies concernées par notre projet. Les technologies qui ont été mises en place dans ce projet ont été validées dans le tableau multicritères disponible en annexe. En ce qui concerne les VPN, nos choix ont été dictés par les contraintes du réseau, détaillées dans la suite de ce document.

4.Spécifications

4.1 Introduction

Ce chapitre va détailler les différentes options possibles de notre projet, à savoir quelles infrastructures pourrait-on utiliser pour remplir le cahier des charges.

L'infrastructure globale se base sur 2 points essentiels du cahier des charges :

- Nous avons deux succursales dans l'entreprise dans laquelle nous déployons cette solution.
- Nous devons permettre une communication de couche 2 entre les deux sites géographiques distants.

4.2 Infrastructures possibles.

Dans ce sous-chapitre, les différentes infrastructures possibles seront détaillées.

4.2.1 Solution 1 : VPN sécurité sur la ligne LTE et accès en couche 2 entre les 2 sites

Utilisation d'un tunnel de couche 3 sur la ligne LTE, ainsi que la mise en place des 2 lignes dans un tunnel de couche 2

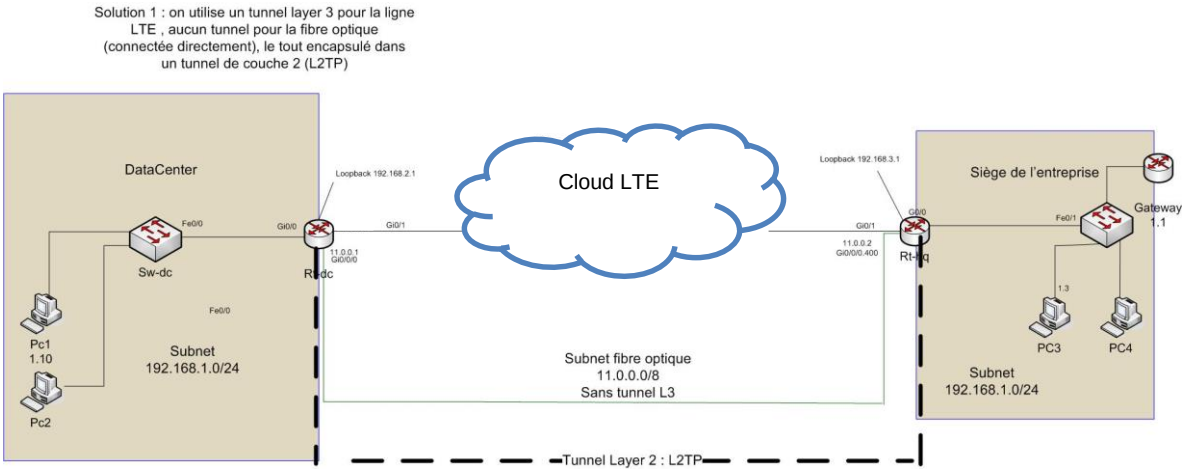


Figure 15 : solution 1 : tunnel de couche 3 sur la ligne LTE et les 2 lignes dans un tunnel de couche 2 L2TP

Dans cette infrastructure, nous allons mettre nos deux lignes physiques (la fibre optique et la ligne LTE) dans un même tunnel logique (tunnel de couche 2 encapsulant les en-têtes Ethernet).

Nous allons également utiliser un tunnel de couche 3 pour la ligne LTE. En effet, l'intérêt d'assurer une certaine sécurité est très important pour la ligne LTE car toutes nos données vont transiter par Internet. Avec cette solution, nous avons notre passerelle par défaut qui se situe sur un autre routeur (d'un côté ou de l'autre du

réseau, cela n'a pas d'importance). Cela facilite l'implémentation et ne nécessite pas de routeur virtuel.

Le 2ème intérêt de cette solution est dû au fait que nous n'utilisons pas de tunnel de couche 3 sur la ligne optique. En effet, cette dernière étant une ligne louée directement tirée entre les 2 sites, le risque d'une attaque de type « man in the middle » est faible.

4.2.2 Solution 2 : 2 tunnels sécurisés

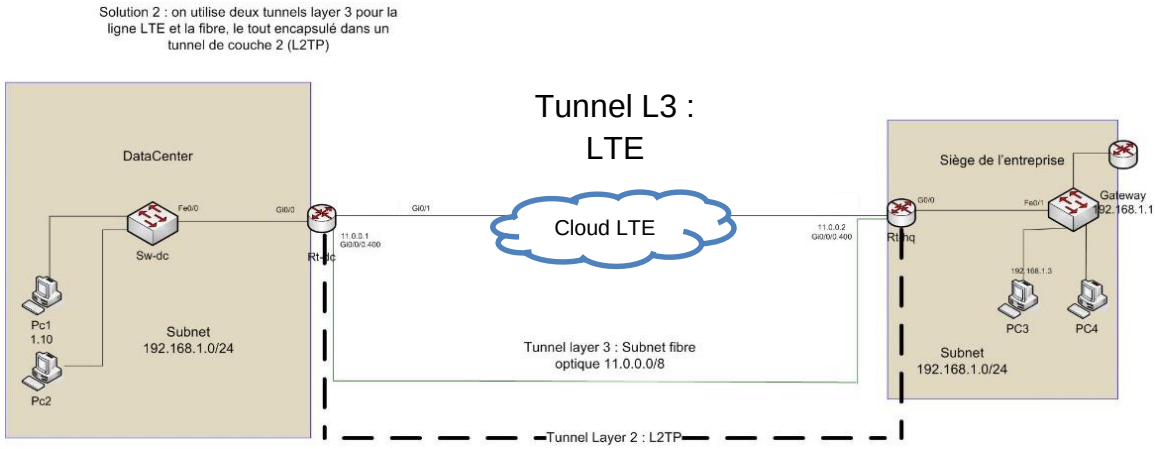


Figure 16 : solution 2 : utilisation avec 2 tunnels de couche 3 (un pour la fibre et l'autre pour le LTE)

La seconde solution ne diffère que très peu de la première. La différence se situe dans le fait que l'on encapsule la ligne de fibre optique dans un tunnel de couche 3. Cela renforce la sécurité de la ligne fibre optique mais complique légèrement l'implémentation des équipements de cette ligne. Un tunnel de couche 3 sur la ligne LTE doit cependant subsister. Il est en effet indispensable pour garantir la sécurité du trafic ainsi que pour transiter dans les multiples sous-réseaux du « nuage » LTE.

4.2.3 Solution 3 : Gateway dans l'un des deux routeurs

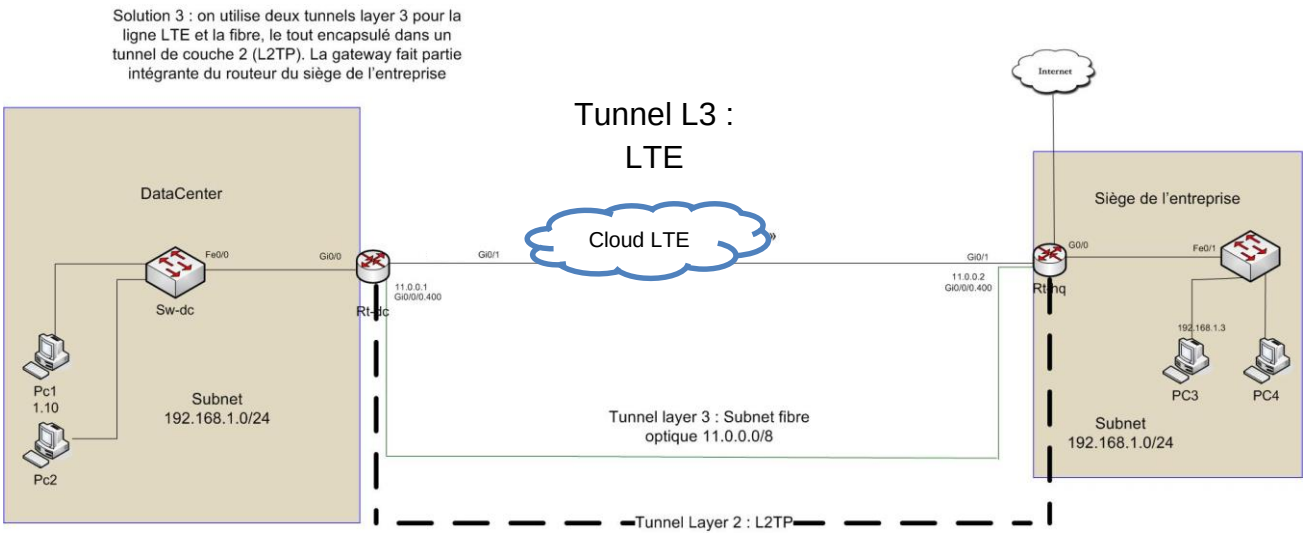


Figure 17 : solution 3 : passerelle par défaut dans un des 2 « switches fibre/LTE »

Contrairement aux solutions précédentes, nous n'utilisons pas de routeur supplémentaire faisant office de passerelle par défaut. Cette passerelle par défaut (donc routeur faisant un lien avec Internet, rt-hq dans le schéma ci-dessus). Est directement intégrée dans un de nos deux routeurs (côté datacenter ou coté headquarter).

Cette solution demande donc l'ajout d'un switch « virtuel » dans le routeur équipé de la passerelle par défaut. Cela demande une implémentation plus complexe mais permet d'économiser un routeur, au cas où nous n'en aurions pas suffisamment ou que les couts seraient un point très important.

4.2.4 Infrastructure globale : conclusion

Ces quatre implémentations d'infrastructures sont toutes réalisables. On pourrait les créer « à la demande » en fonction des exigences du client (veut-il un routeur supplémentaire pour la gateway ou non ? Veut-il que la ligne de fibre optique soit encapsulée dans un tunnel de façon à sécuriser les données ou non ?)

4.3 Infrastructures LTE possibles

L'objectif de la liaison via LTE est évidemment de faire communiquer nos deux routeurs (comme 2 appareils mobiles) en passant par une liaison LTE.

L'infrastructure de Swisscom en ce qui concerne la LTE ressemble à celle-ci :

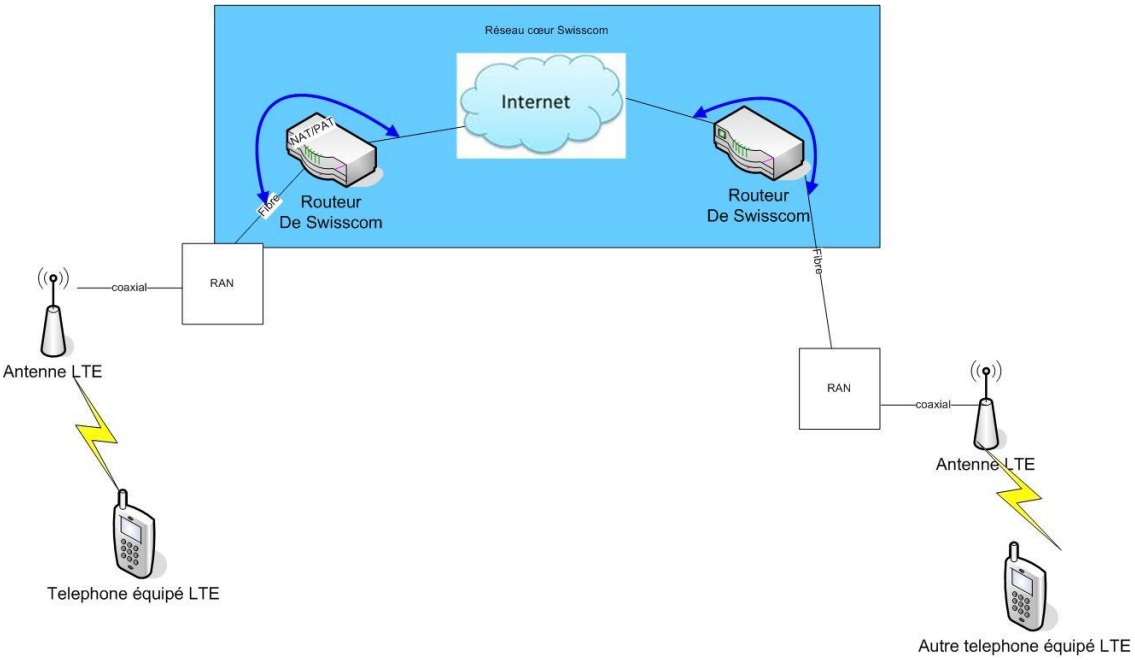


Figure 19: Infrastructure (simple) LTE Swissocm

Chaque client LTE reçoit une adresse « privée », ensuite « natée » dans le routeur de l'opérateur (routeur de Swisscom dans la figure 19). Le principal problème dans ce réseau est dû au fait que l'on ne peut pas directement accéder d'un client à l'autre, les routeurs bloquant certains accès dus à des impératifs de sécurité

Nous avons donc plusieurs options possibles afin de faire transiter des données entre nos deux clients.

4.3.1 Solution 1 : routeur « relai »

La première solution consiste à mettre un routeur sur internet (Routeur backbone dans la figure ci-dessous), afin de faire transiter le trafic envoyé sur le LTE par ce routeur. L'avantage de cette mise en place réside dans le fait que nous passons par un routeur appartenant à l'EIA-FR et donc que nous sommes relativement indépendants des différents providers.

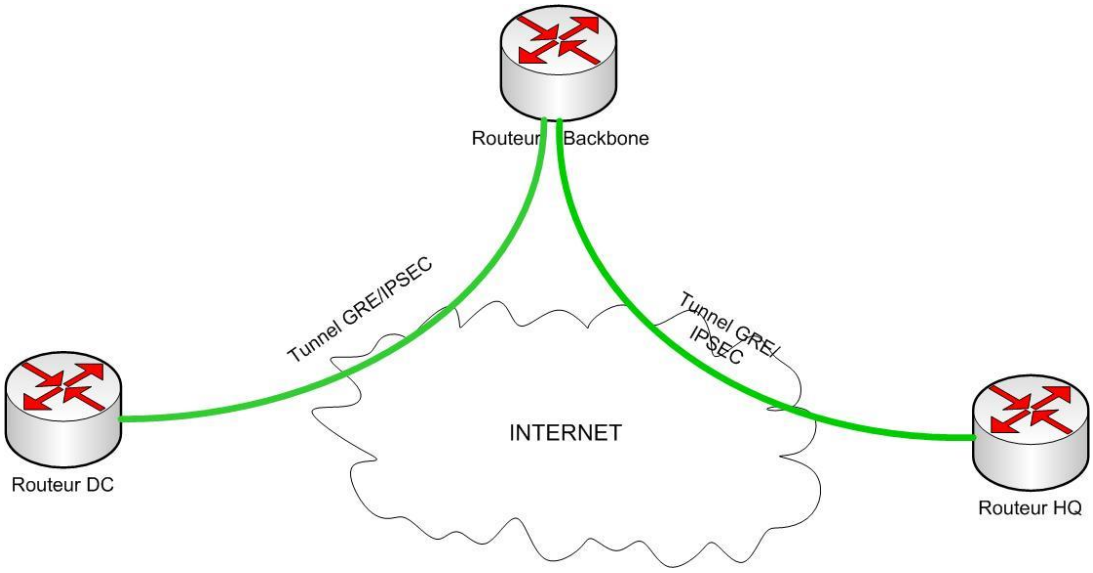


Figure 20: solution 1 : utilisation d'un routeur « backbone » faisant relai sur la ligne LTE

Au niveau de l'encapsulation, le schéma ci-dessous traduit ce qu'il se passe lors de la première moitié du « chemin » entre le PC émetteur et le routeur situé sur Internet. Pour transiter sur le web, les données devront être encapsulées dans GRE et dans IPSEC afin d'assurer l'encryption des données transitant sur Internet.

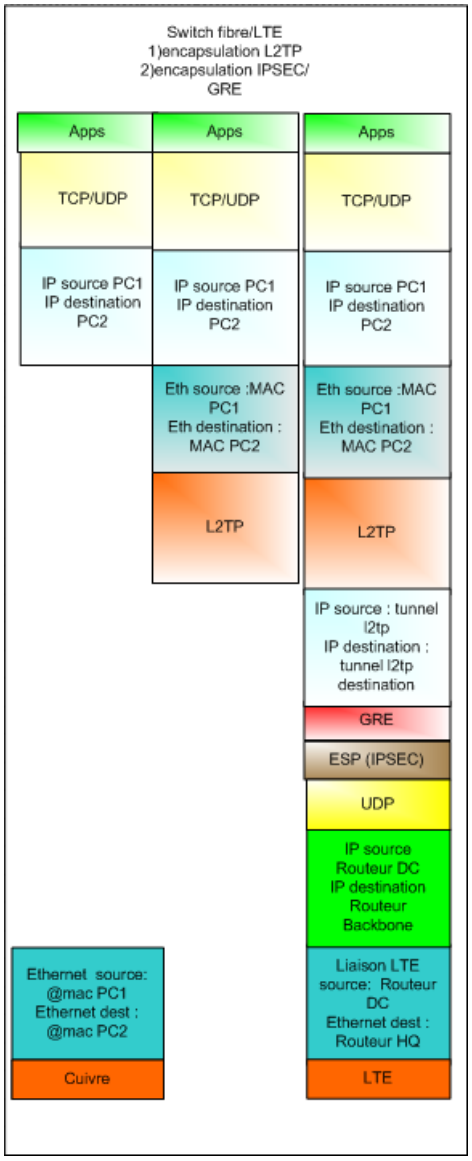


Figure 21: encapsulation des paquets sur la ligne LTE

4.3.2 Solution 2 :

La seconde solution se traduit par la mise en place d'une infrastructure utilisant la technologie DMVPN.

DMVPN (Dynamic Multiploint Virtual Private Network) est une fonctionnalité dans l'IOS de Cisco. Elle permet aux routeurs de créer des tunnels IPSEC entre des routeurs dynamiquement en utilisant les technologies :

1. Multipoint GRE (mGRE)
2. Next-Hop Resolution Protocol (NHRP)
3. Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP)
4. Dynamic IPsec encryption

Le grand avantage de DMVPN est qu'il évite d'avoir besoin de créer de multiples configurations IPSEC. Ceci réduit le degré d'administration (très automatique) et permet de gérer facilement la « scalability » (possibilité d'avoir un plus grand réseau).

Dans la figure ci-dessous, nous avons une petite illustration de l'utilisation de DMVPN. Tous les clients (les 3 routeurs 2,3 et 4) vont utiliser un tunnel DMVPN pour se connecter au routeur central « HUB ». Cela va aussi permettre d'avoir un seul tunnel « virtuel » entre deux routeurs clients.

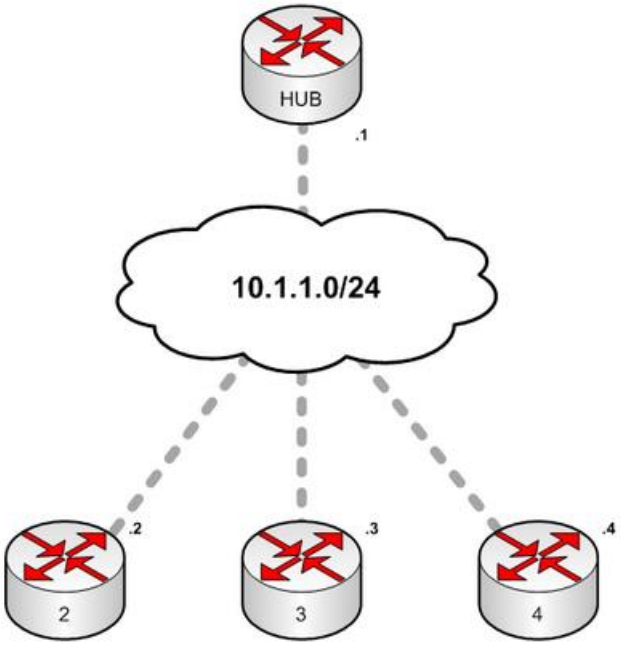


Figure 22: schéma de DMVPN

4.3.3 Solutions LTE possibles : conclusion

Suite à des recherches effectuées sur le DMVPN, nous avons pu voir que cette solution était très intéressante et performante, mais n'était peut-être pas applicable dans notre contexte. En effet, les adresses privées distribuées par Swisscom aux clients LTE passent certainement par un PAT (port address translation) pour obtenir une adresse IP publique. Bien que nous n'en ayons pas la certitude, le fait d'utiliser un PAT est un problème car DMVPN n'est pas conçu pour le supporter.

La meilleure solution pour contrer cette problématique est donc de mettre un routeur sur Internet (dans la DMZ de l'Ecole d'ingénieurs) et de faire passer le trafic LTE par ce routeur. Nous utiliserons donc deux tunnels de couche 3 pour faire passer notre trafic d'un point à un autre, comme le montre la figure 20.

Dans un second temps, l'implémentation avec DMVPN serait envisageable.

5.Conception

Ce chapitre a pour but de déterminer les choix effectués pour résoudre les problèmes liés au cahier des charges et de déterminer les schémas logiques et physiques de l'infrastructure que nous allons implémenter.

5.1 Problèmes et solutions

5.1.1 LTE

Le premier problème lié à une connexion LTE est qu'un lien LTE se trouve en couche 3 (IP) du modèle OSI. Pour conserver une connectivité de couche 2 entre les deux sites, il nous est donc nécessaire d'encapsuler les informations dans un tunnel de couche 2 entre les deux points.

5.1.1.1 Solution

Pour cela, nous utiliserons le protocole L2TP. Ce dernier s'occupe d'encapsuler les informations de couche 2 et supérieures dans le protocole L2TP, et permet un transport de couche 2 par-dessus un réseau de couche 3.

5.1.2 Internet / Security

Le deuxième problème qui pourrait être soulevé est la sécurité.

En effet, lorsqu'un message est envoyé d'une succursale à l'autre, celui-ci transite, soit par l'internet, soit par une fibre optique. L'un comme l'autre peuvent être « sniffées », et il est donc important d'avoir une encryption des données.

5.1.2.1 Solution

Nous utiliserons le protocole IPSec pour sécuriser les données sur la ligne LTE.

5.1.3 Gestion de l'état des liens

Lorsqu'un lien est coupé, il est nécessaire que notre système se rende compte de la panne.

5.1.3.1 Solution

Nous utiliserons le protocole OSPF avec des hello-packets avec un temps très court afin d'assurer la commutation entre les deux lignes. Il faudra faire attention la distance administrative qui devra être plus basse en fibre qu'en LTE.

5.1.4 NAT

Les adresses IP LTE offertes par Swisscom sont privées, et se trouvent derrière un NAT avant de sortir sur internet. Elles ne permettent pas une connexion directe d'un point à un autre du réseau.

5.1.4.1 Solutions

- Adresses IP fixes (dans le range de l'école ou non). Il est possible d'en avoir chez Swisscom, avec un abonnement particulier. Cet abonnement nous donne des adresses publiques fixes, ce qui contournerait la problématique du NAT .

- Routeur dans le backbone servant de relai

5.2 Convention de nommage

5.2.1 Équipement

Préfix	Nom	Description
sw-dc	Switch coté DataCenter	Switch layer 2
sw-hq	Switch coté headquarter	Switch layer 2
Rt-dc	Router coté dataCenter	Routeur de distribution côté datacenter : s'occupe du switch entre la fibre optique et la liaison LTE
Rt-hq	Router coté headquarter	Routeur de distribution côté headquarter : s'occupe du switch entre la fibre optique et la liaison LTE
Relay-lte	Routeur de relai	Relai dans la DMZ de l'école d'ingénieurs
pcX	Personnal Computer	Ordinateur numéro X

Tableau 01: Convention de nommage des équipements

5.2.2 Sites

Sigle	Nom	Description
hq	Headquarter	Succursale principale
dc	Datacenter	Datacenter

Tableau 02: Convention de nommage pour les sites

5.3 Plan d'adressage IPv4

Subnet	IPv4
LAN de l'entreprise	192.168.1.0/24
Ligne de fibre optique	11.0.0.0 /8

Tableau 03: Adresses IP

Les adresses reçues par l'interface LTE sont des adresses privées dans un subnet 10.x.x.x.x. Cependant, elles sont par la suite « natées » pour avoir une adresse IP publique dans le subnet 170.

Nous ne pouvons pas préciser ces adresses davantage car elles changent régulièrement.

5.4 Tunnel de couche 2

Pour le choix du tunnel de couche 2 que nous allons mettre en place, nous nous sommes tout d'abord concentrés sur GRE. GRE est une technologie « passe partout » qui peut encapsuler de nombreux protocoles (de couche 2 et 3). Cependant, implémenter une encapsulation d'Ethernet (puis de la couche 2 de la fibre et du LTE) n'est pas une solution optimale. En effet, cette solution tend à disparaître car de meilleures solutions sont disponibles sur le marché. Les derniers routeurs dont nous disposons empêchent d'ailleurs l'implémentation d'Ethernet over GRE.

Notre choix s'est donc porté sur un protocole que nous n'avons jamais utilisé auparavant : L2TP. Comme vu précédemment, ce protocole permet de transporter des connexions en conservant les informations de couches 2 et supérieures du modèle OSI.

La figure ci-dessous montre l'encapsulation d'un paquet dans un tunnel L2TP

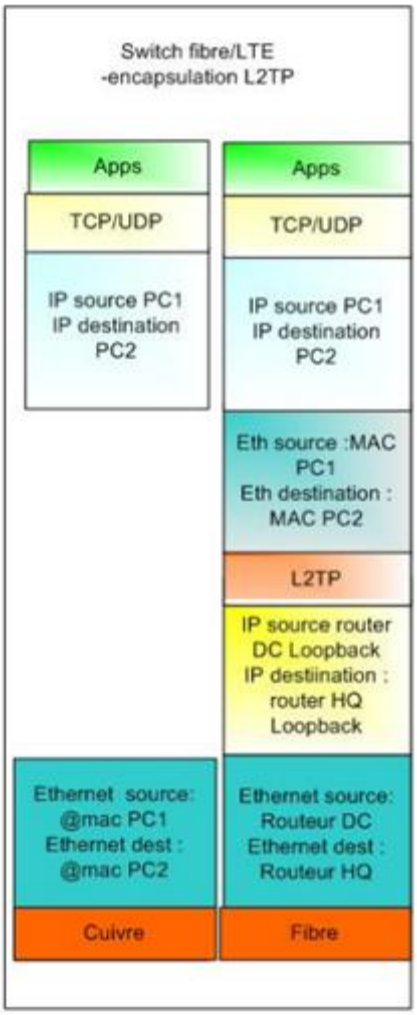


Figure 23: Ajout d'en-tête sur un paquet encapsulé dans un tunnel L2TP

5.5 Plan de l'infrastructure réseau (schema physique)

Suite aux diverses solution proposées, nous avons décidé d'implémenter la solution numéro 1. En effet, nous n'avons pas besoin d'avoir une gateway « interne » au réseau. Cela élimine donc la solution 3. Nous pourrions les implémenter, mais ceci n'est pas spécifié dans le cahier des charges et pourrait apparaitre en tant qu'ajout.

Le fait d'avoir une ligne de fibre optique directement connecté nous assure un minimum de sécurité. Par conséquent, nous allons utiliser un seul tunnel de couche 3 dans la ligne LTE, sans faire de même pour la ligne de fibre optique. Le tout sera encapsulé dans un tunnel de couche 2 comme le montre la figure ci-dessous :

5.5.1 Schéma physique de notre émulation

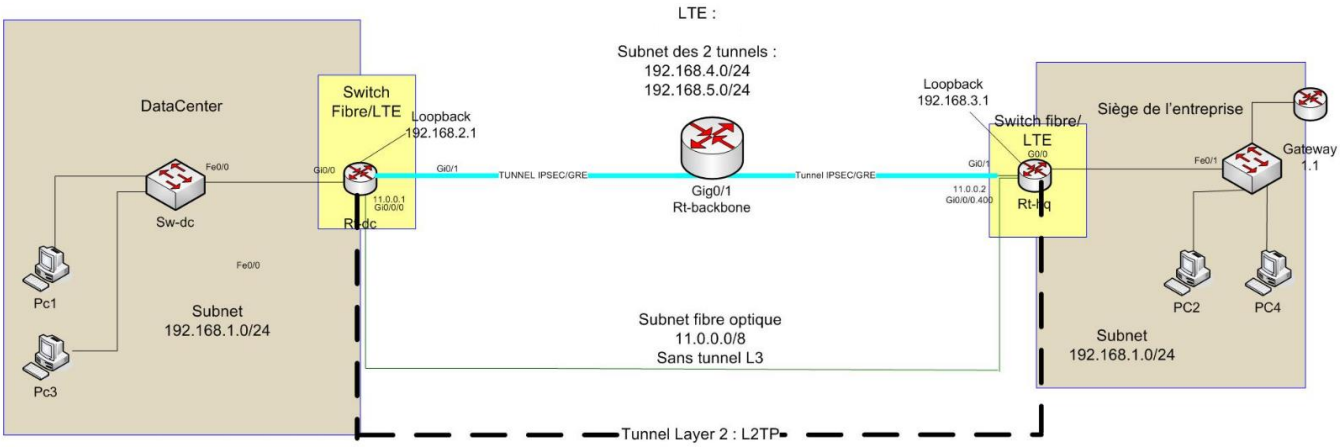


Figure 24: Schéma physique

5.5.2 Encapsulation d'un paquet passant par la ligne LTE

L'encapsulation des paquets est importante à bien comprendre. En effet, nous aurons un tunnel de couche 2 qui encapsulera deux autres tunnels de couche 3 sur la ligne LTE. La figure ci-dessous montre les différentes étapes de l'encapsulation (ajout et suppression d'en-têtes dans les équipements) d'un paquet passant par le LTE. On peut avoir une vue plus précise de ce schéma dans l'annexe « schéma d'encapsulation sur la ligne LTE »

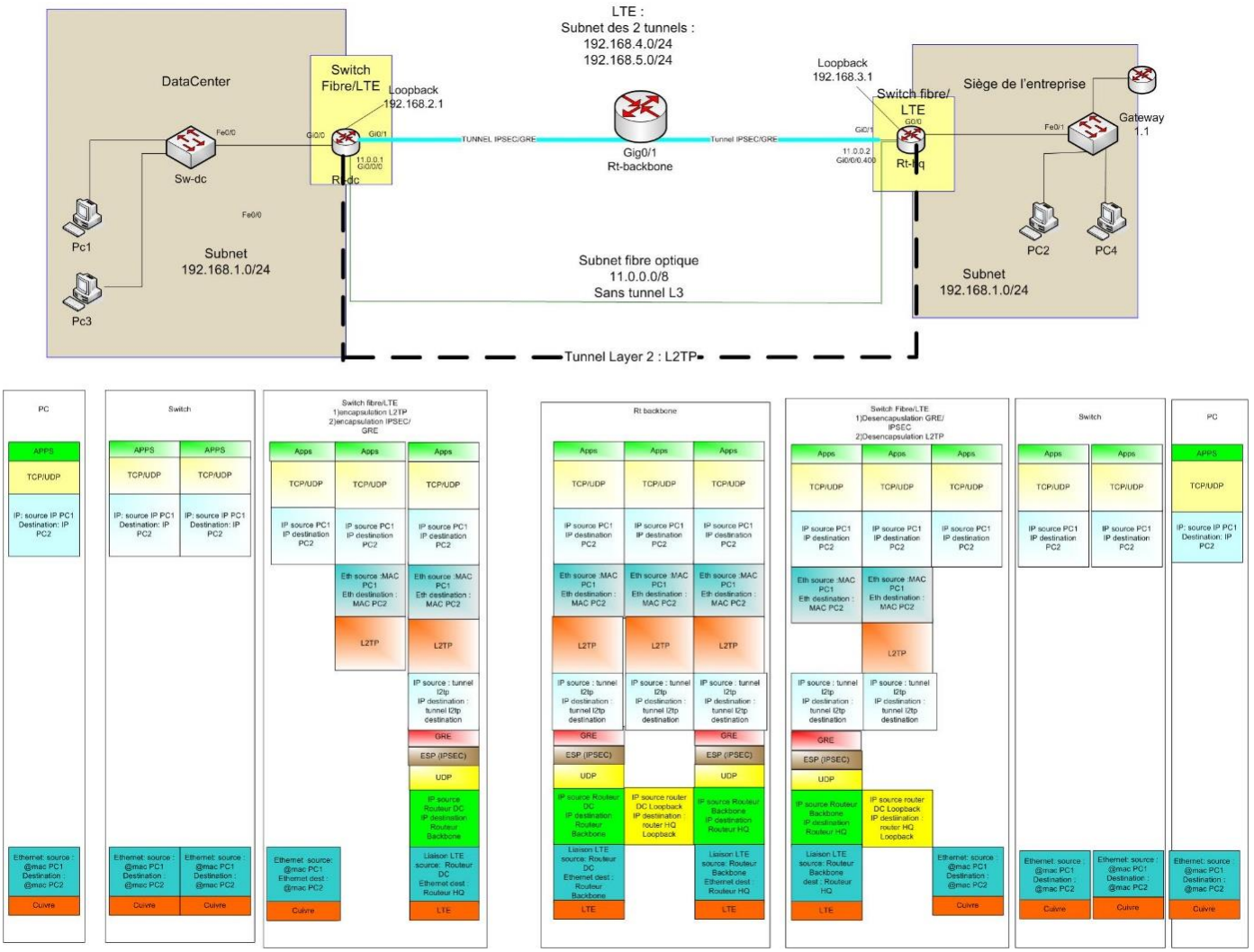


Figure 25: encapsulation d'un paquet passant par la ligne de backup LTE

5.5.3 Encapsulation d'un paquet passant par la fibre optique

Comme le montre la figure ci-dessous, l'encapsulation d'un paquet passant par la fibre optique se fera de la même manière que pour la ligne LTE, à la différence près qu'il n'y aura pas d'encapsulation dans IPSEC. Nous avons en effet jugé qu'IPSEC n'était pas indispensable sur cette ligne. Cependant, nous pourrions l'ajouter aisément. Ce schéma est disponible dans une meilleure qualité dans l'annexe « schéma d'encapsulation : fibre optique ».

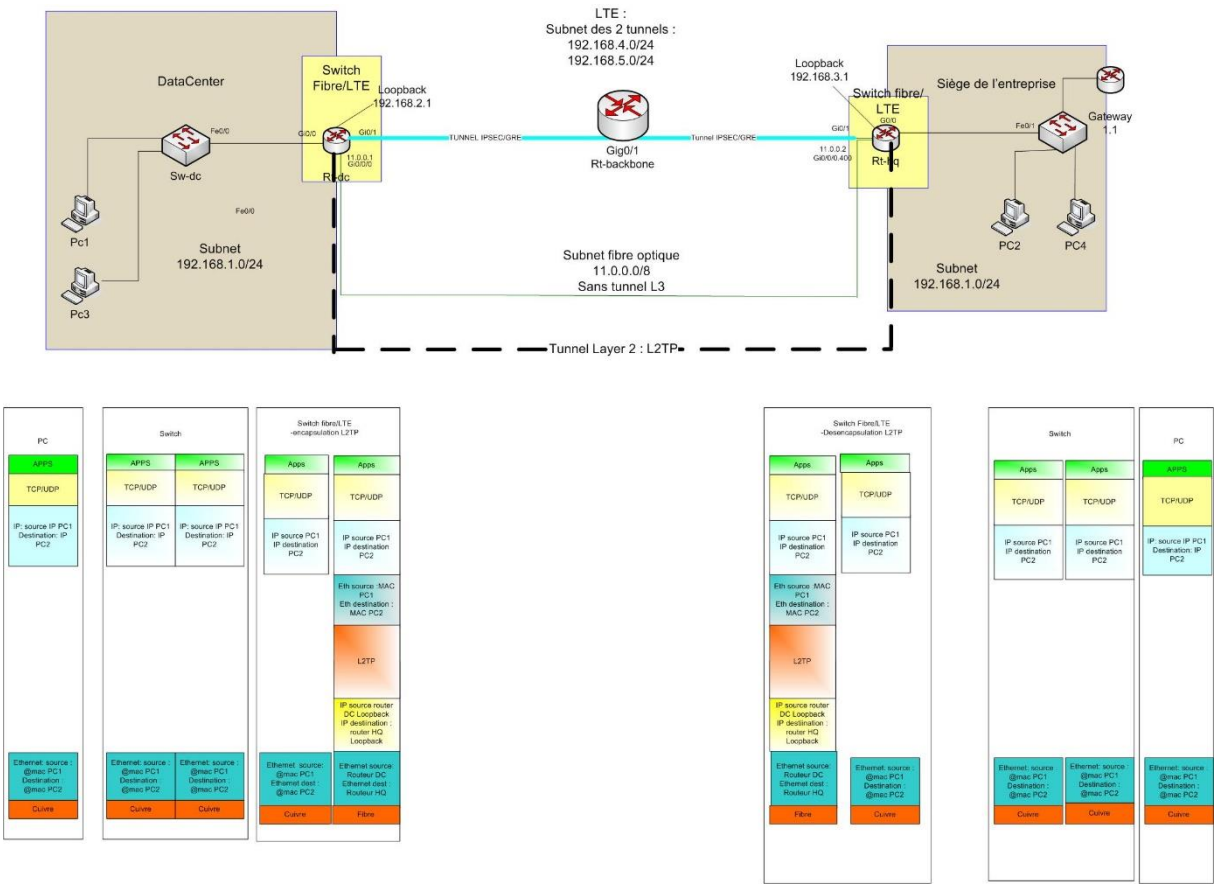


Figure 26: encapsulation d'un paquet passant par la ligne principale en fibre optique

Tous les schémas d'encapsulation sont disponibles en annexe.

5.6 Schéma logique

Du point de vue de l'utilisateur, le schéma logique est très simple. Les deux équipements rt-dc et rt-hq font office de switches, répartis entre deux lieux géographiques différents. Etant donné que le subnet est le même, l'utilisateur n'aura virtuellement qu'un câble entre les deux switches. Il ne se souciera en aucun cas du chemin (et de la liaison LTE ou fibre) que ses données vont emprunter.

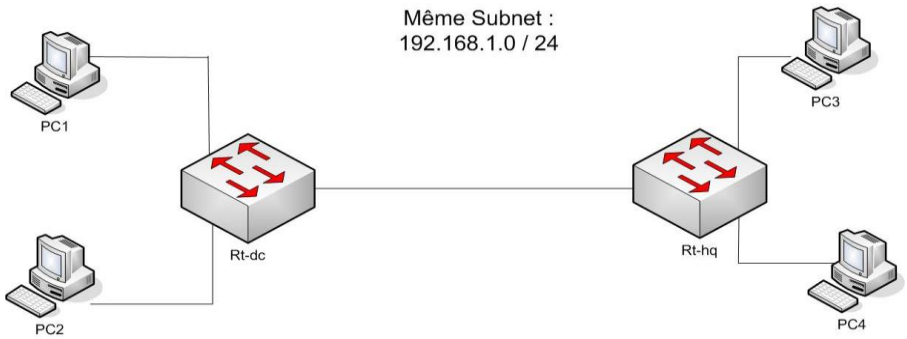


Figure 27: schéma logique

5.7 Tests qui seront mis en place sur l'émulation :

La prochaine étape consiste à créer une émulation de l'infrastructure, afin de tester différents aspects tels que :

- Mettre en place la ligne de fibre optique uniquement et tester la liaison entre les 2 routeurs via le tunnel L2TP
- Mettre en place une connexion LTE et tester la sortie sur internet
- Implémenter la solution de backup. Monter les 2 lignes (fibre optique et la ligne de « simulation LTE » en Ethernet) et contrôler que le switch s'effectue correctement
- Mettre en place le routeur « central » sur le backbone de l'école (possédant une adresse « officielle » publique sur Intenet)
- Mettre en place les tunnels de couche 3 sur la ligne LTE (pour protéger le trafic). Puis tester la totalité de l'infrastructure en passant de la fibre à la LTE si l'on enlève la fibre optique.
- Tester les applications supportées et les changements de bande passante

5.8 Conclusion

Cette partie de conception nous a permis de bien mettre les bases de notre configuration en évidence. L'implémentation en sera facilitée. Cette partie a été d'autant plus importante car nos paquets transférés (tant sur la ligne LTE que via la fibre optique) subissent de nombreuses encapsulations. Il est donc important de connaître le comportement des différents tunnels et les en-têtes que contiendront les paquets.

6. Implémentation

L'implémentation a été réalisée par étapes. Voici les principales:

- Mise en place de la ligne de fibre optique
- Mise en place d'une ligne de backup par Ethernet
- Mise en place de la solution de « switch » entre les 2 lignes
- Mise en place de la ligne LTE

6.1 Configurations

Toutes les configurations des routeurs se trouvent dans l'annexe « configuration des routeurs ».

Les tests réalisés pour la mise en place de la ligne de backup en LTE ont été documentés dans l'annexe « tests effectués sur l'émulation».

6.2 Conclusion

L'implémentation a été conforme à notre conception. Les tests effectués avec M.Buntschu ont été très utiles et nous ont permis de mettre en place une infrastructure fonctionnelle à partir de notre émulation.

7.Tests et validation

Ce chapitre détaille les tests que nous avons effectués sur le projet. Afin de mettre en place l'infrastructure, une émulation a été précédemment créée. Tous les tests de mise en place effectués avec cette émulation se trouvent dans l'annexe « tests sur l'émulation ».

7.1 Test 1 : coupure d'une liaison lors d'un appel en voip

7.1.1 Description

Nous allons tout d'abord mettre en place un serveur Asterisk pour gérer le trafic en VOIP. Nous allons ensuite effectuer un appel entre 2 utilisateurs puis couper la fibre optique. Suite à la coupure de la fibre optique, le trafic va utiliser la ligne de backup et nous pourrons observer le temps de coupure et si la parole subit un grand décalage. Ce test reste évidemment très subjectif (valeurs difficilement calculables) mais permet de mettre en avant l'aspect purement pratique.

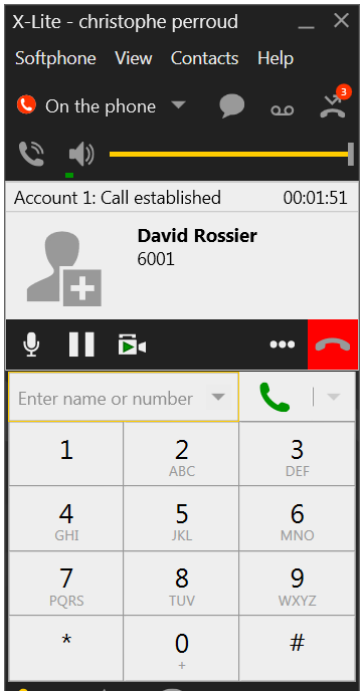


Figure 28 : appel d'un bout à l'autre de l'infrastructure : interface X-lite

7.1.2 Résultats du test

Lorsque le trafic passe par la fibre optique, le décalage est d'environ une demi-seconde entre le moment où l'émetteur parle et le moment où le récepteur entend le message. Lorsque l'on enlève la fibre optique, il n'y a qu'une coupure d'environ une seconde, avant de réobtenir un débit correct et une conversation tout à fait

acceptable. Le décalage entre le moment où l'on parle et le moment où l'on reçoit la parole de l'autre côté reste le même. Bien sûr, ce test est très subjectif car il ne peut pas vraiment être mesuré.

7.2 Test 2 : Transfert d'un fichier important

Pour ce test, nous avons utilisé nos 2 PC connectés respectivement du côté datacenter et du coté headquarter, puis démarré le transfert d'un fichier important d'un PC à l'autre et mesuré le débit. Cette mesure de débit a été faite tout d'abord avec la fibre optique, puis nous avons retiré la fibre et continué le transfert.

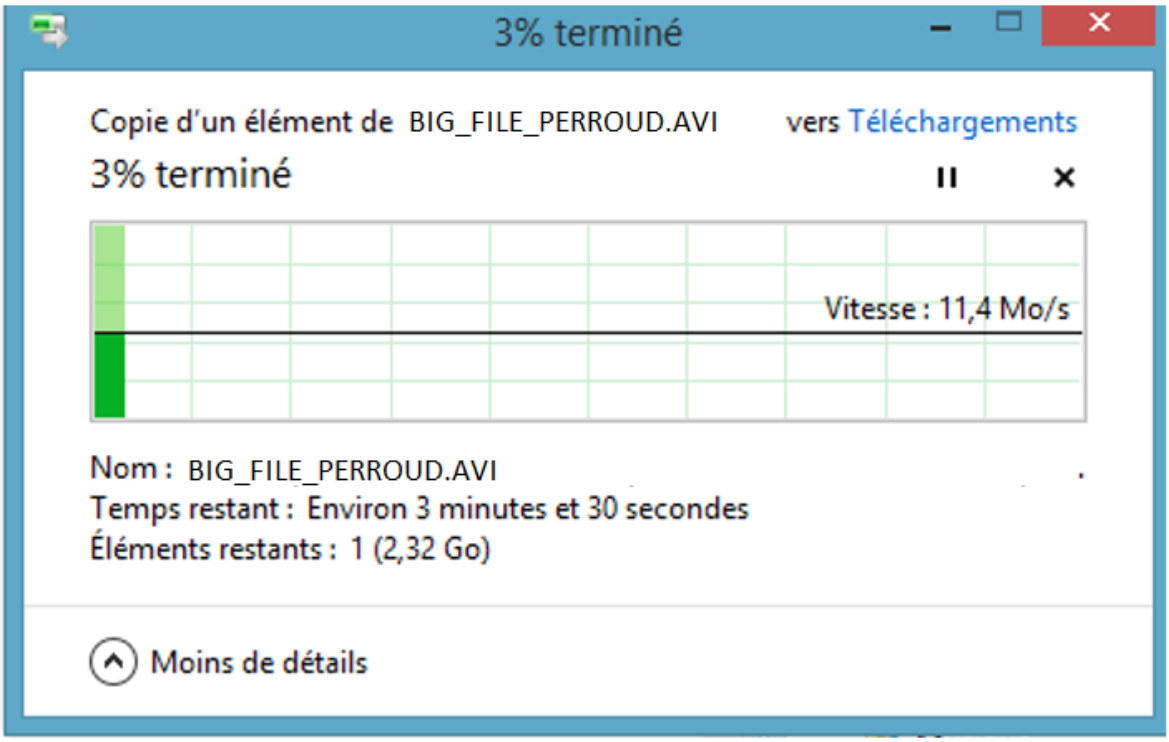


Figure 29 :Transfert d'un gros fichier en passant par la fibre

Comme on peut le voir sur la figure ci-dessus, le transfert lorsque la liaison en fibre est utilisée est relativement rapide. Le transfert est d'environ 11 Mo/s. Ceci est dû au fait que les switches ne peuvent pas travailler plus vite. Le « goulet d'étranglement » ne se situe pas au niveau de la fibre optique mais au niveau des switches.

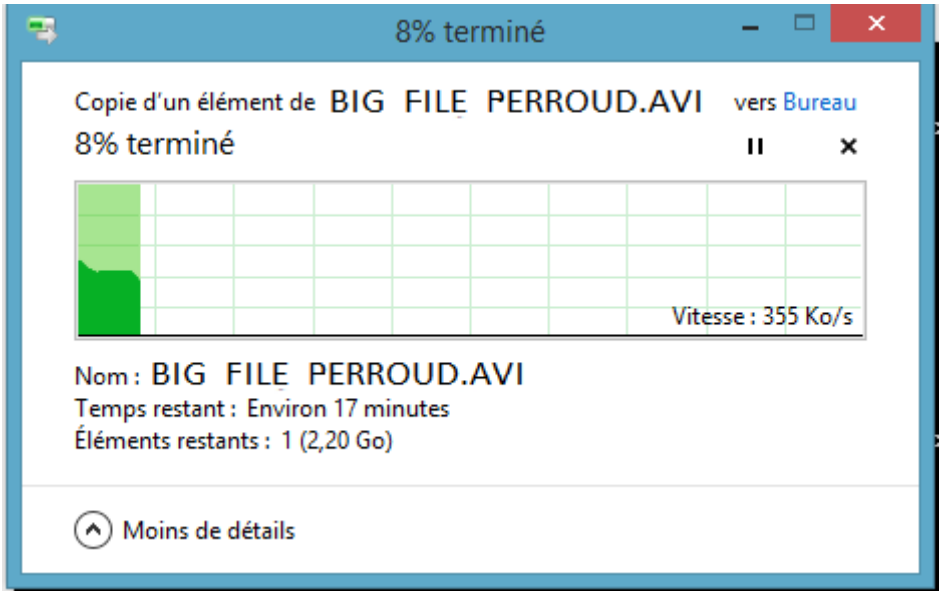


Figure 29 :Transfert d'un gros fichier en passant par la ligne LTE

La figure ci-dessus montre la vitesse de transfert du même fichier lorsque la fibre est retirée et que la liaison est maintenue par la ligne de backup en LTE. Nous avons un débit relativement faible (355 Ko/s). Cela est, cette fois, dû au fait que la ligne de backup représente le goulet d'étranglement. En effet, bien que notre vitesse en upstream soit acceptable en 4G, le problème réside dans le fait que les débits en downstream sont très limités pour les abonnements « grand public ». On peut donc constater que le transfert continue (donc la ligne est maintenue, ce qui est un bon point par rapport au cahier des charges), mais à une vitesse très lente.

7.3 Test 3 : résultats dans jperf

Figure 30 :Vue du changement de débit dans jperf au moment de la coupure de fibre

On observe que le débit diminue fortement. Si l'on conserve l'échelle utilisée lors du transfert en fibre optique, on pourrait même croire que la ligne de backup en LTE n'est pas opérationnelle. Cependant, même si la vitesse a fortement diminué (de 60Mb/s en fibre optique à environ 600Kb/s en LTE), la ligne de backup fonctionne tout de même.

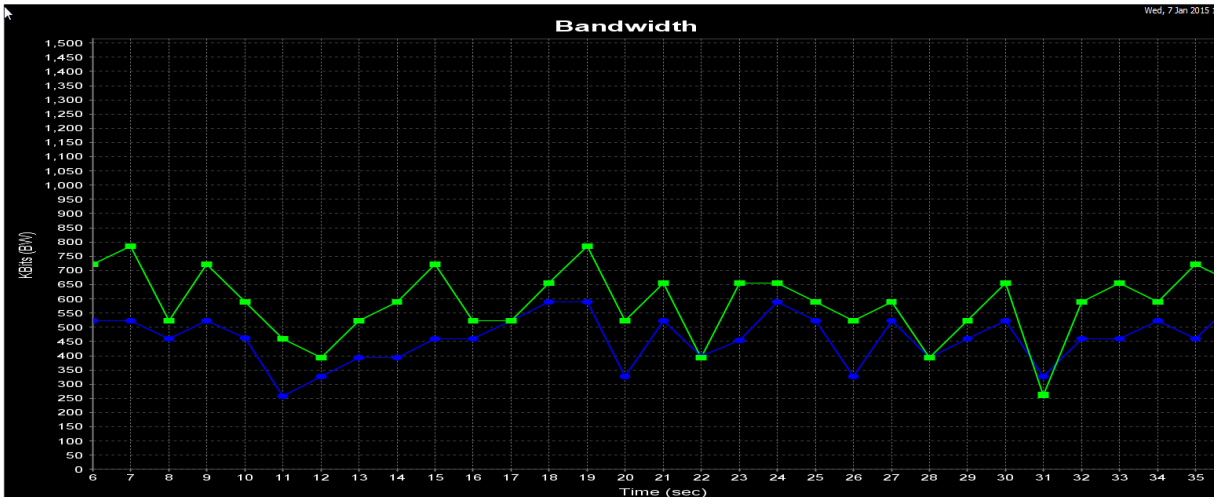


Figure 31 :Graphe de la vitesse sur la ligne LTE (upload en vert, download en bleu)

Lorsqu'on adapte l'échelle à la vitesse de la ligne de backup. On peut observer que les débits sont d'environ 600 Kbit/s.

```
[244] 33.0-34.0 sec  72.0 KBytes   590 Kbits/sec
[260] 33.0-34.0 sec  64.0 KBytes   524 Kbits/sec
[260] 34.0-35.0 sec  56.0 KBytes   459 Kbits/sec
[244] 34.0-35.0 sec  88.0 KBytes   721 Kbits/sec
[244] 35.0-36.0 sec  80.0 KBytes   655 Kbits/sec
[260] 35.0-36.0 sec  72.0 KBytes   590 Kbits/sec
```

Figure 32 :Débits sur la ligne LTE

Nous avons constaté que les débits sont faibles. Ceci est en grande partie dû au fait que l'abonnement utilisé lors de ce test ne propose qu'un upstream maximum de 2 Mbits/s. Le fait que nous ayons effectué ce test dans un endroit relativement isolé diminue aussi l'exposition au réseau 4G.

7.4 Test de lecture de film en streaming

Pour ce test, nous nous sommes connectés au réseau de l'Ecole d'ingénieurs. La mise en place est simple car il suffit de brancher un câble Ethernet entre un de nos deux switches et le port LAN de l'école.

http://tlabs.tic.eia-fr.ch/streaming.php

Nous avons ensuite regardé le début d'une vidéo en utilisant la ligne principale en fibre optique, avant de la retirer et d'observer les changements de qualité lorsque l'on utilise la ligne LTE.

La figure ci-dessous nous montre une image d'un film lorsqu'on le voit en utilisant la fibre optique. L'image est de bonne qualité et le film est fluide.

Figure 33 :Vue d'un film en streaming en passant par la ligne de fibre optique

Lorsque l'on passe sur la ligne LTE, la qualité d'image se détériore. On voit apparaître de façon régulière de gros pixels sur l'image. Le film devient nettement moins agréable à regarder. Certaines images restent statiques au lieu de disparaître. Ceci est dû au codage de la vidéo (MPEG-1). Lorsque l'on perd une image, l'image précédente qui aurait dû être remplacée par l'information reçue reste affichée. Ceci crée donc cet effet visuel où l'on voit encore les « anciennes » images du film (ici, l'oiseau en vol).

Figure 34 :Vue d'un film en streaming en passant par la ligne LTE

7.5 Test d'envoi de données de n'importe quelle application en se connectant au réseau de l'école

Pour bien confirmer que la liaison logique est assurée, nous avons connecté un des deux switches (côté Datacenter ou Head quarter) au LAN de l'école. Nous avons remarqué que les clients des deux côtés reçoivent une adresse IP de l'école, ce qui confirme donc le fonctionnement de notre infrastructure pour recevoir une adresse du serveur DHCP de l'école d'Ingénieurs.

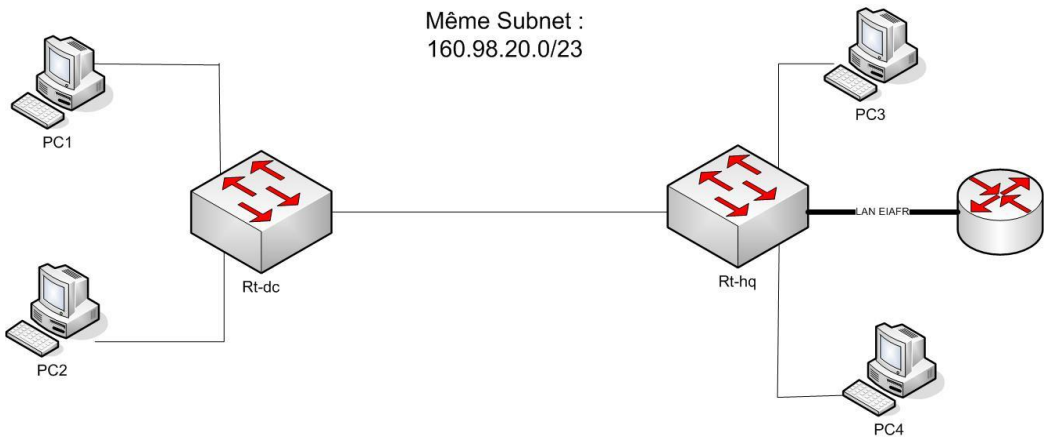


Figure 35 :Plan logique de l'infrastructure

Lorsque nous envoyons des données depuis une application sécurisée (https par exemple), le bit « don't fragment » est fixé à « 1 » lors de l'envoi des paquets, ce qui interdit la re-fragmentation du paquet. La seule solution pour éviter que nos transactions soient bloquées est de diminuer le MTU côté client. On le fait à l'aide de la commande windows suivante :

```
netsh interface ipv4 set subinterface "Local Area Connection" mtu=1400
store=persistent
```

Cette commande va modifier le mtu à 1400 au lieu de 1500, afin de diminuer la taille de la charge utile par paquet et permettre aux en-têtes supplémentaires d'être insérées sans fragmentation dans le paquet.

De plus amples informations sur ce problème sont dans l'annexe « problèmes rencontrés ».

7.6 Résumé des résultats des tests sur l'émulation et sur l'infrastructure

No	Description	Résultat
1	Mise en place d'un tunnel de couche 2 (L2TP)	OK
2	Mise en place et configuration du module LTE sur les routeurs CISCO et communications sur Internet	OK
3	Mise en place de la solution de backup en Ethernet	OK
4	Optimisation du temps de convergence du protocole de routage OSPF	Satisfaisant (1.5 seconde environ)
5	Mise en place d'un routeur « relai » dans la DMZ de l'Ecole d'ingénieurs	OK
6	Passer un PAT avec un tunnel IPSEC en Ethernet	OK
7	Passer le PAT de Swisscom avec un tunnel IPSEC sur LTE	OK

8	Mise en place correcte de la solution de backup sur la ligne LTE	OK
9	Fonctionnement de la réception d'une adresse IP de l'Ecole d'ingénieurs sans problème	OK
10	Lecture d'un flux streaming en passant par la fibre	OK
11	Lecture d'un flux streaming en passant par la ligne LTE	Subit quelques problèmes dus au faible débit
12	Transférer un protocole sécurisé dans notre infrastructure	Nécessite d'adapter le MTU au cas où on ne pourrait pas fragmenter
13	Transférer les messages d'un protocole non sécurisé dans l'infrastructure : DHCP, FTP, http…	OK

8. Conclusion

8.1 Conclusion du projet

Nous avons pu développer une solution fonctionnelle, grâce à un bon approfondissement des technologies de tunnel. Le protocole L2TP nous a permis de mettre en place un tunnel de couche 2. Ce dernier offre la possibilité de relier deux réseaux de couche 2 (Switchs) en traversant un réseau de couche 3 (IP – Internet dans notre cas). Le protocole IPSEC (combiné avec GRE) nous a permis de sécuriser le trafic cheminant par la ligne LTE. Le switch entre les deux lignes a été assuré par le protocole OSPF, que nous avons pu optimiser afin que le temps de convergence soit le plus rapide possible.

En ce qui concerne la sécurité, le point primordial est le routeur « relai-lte » situé dans la DMZ de l'école d'ingénieurs. En effet, c'est le point central de notre infrastructure et si ce routeur subit une défaillance le backup entre nos deux succursales n'est plus assuré. De plus, s'il subit une attaque de type « man-in-the middle », la confidentialité des données pourrait être compromise.

La partie de tests nous a permis de valider tous nos choix quant à la configuration de l'infrastructure finale. Grâce à un protocole de tests structuré, nous avons une solution fonctionnelle. Malheureusement, les débits offerts par la LTE sont assez lents. La solution fonctionne mais ne satisfait pas les exigences que l'on aimerait. En effet, la LTE n'offrant que des débits très faibles, la solution ne pourrait pas être utilisée dans un environnement de production. Néanmoins, les différentes analyses et configurations que nous avons utilisées ouvrent la voie à d'autres projets que nous exposeront dans le chapitre « Opportunités ».

8.2 Conclusion personnelle

Ce projet fut très intéressant pour nous deux. Il nous aura permis d'approfondir nos connaissances, tant dans le domaine du réseau que dans le domaine de la sécurité (il a fallu paramétrer de nombreuses configuration IPSEC). Nous avons également pu découvrir deux technologies avec lesquelles nous n'avions jamais travaillé en projet ou en travail pratique, à savoir le LTE et la fibre optique.

8.3 Opportunités de développement

Ce projet nous a prouvé que le backup via une ligne LTE pouvait fonctionner. Cependant, nous avons aussi pu observer que la vitesse est lente en LTE par rapport aux performances que l'on pourrait atteindre avec la fibre optique.

Nous pourrions donc utiliser une seconde ligne de backup en utilisant une autre technologie. Nous pourrions, par exemple, utiliser le câble, via un abonnement chez CableCom. Une solution utilisant une ligne ADSL ou tout autre média est également

envisageable. La contrainte principale, qui doit être discutée avec les fournisseurs d'accès, est le chemin emprunté par chacun des médiums. Pour assurer une connectivité, il faudrait que les chemins d'une entreprise à l'autre soient totalement séparés.

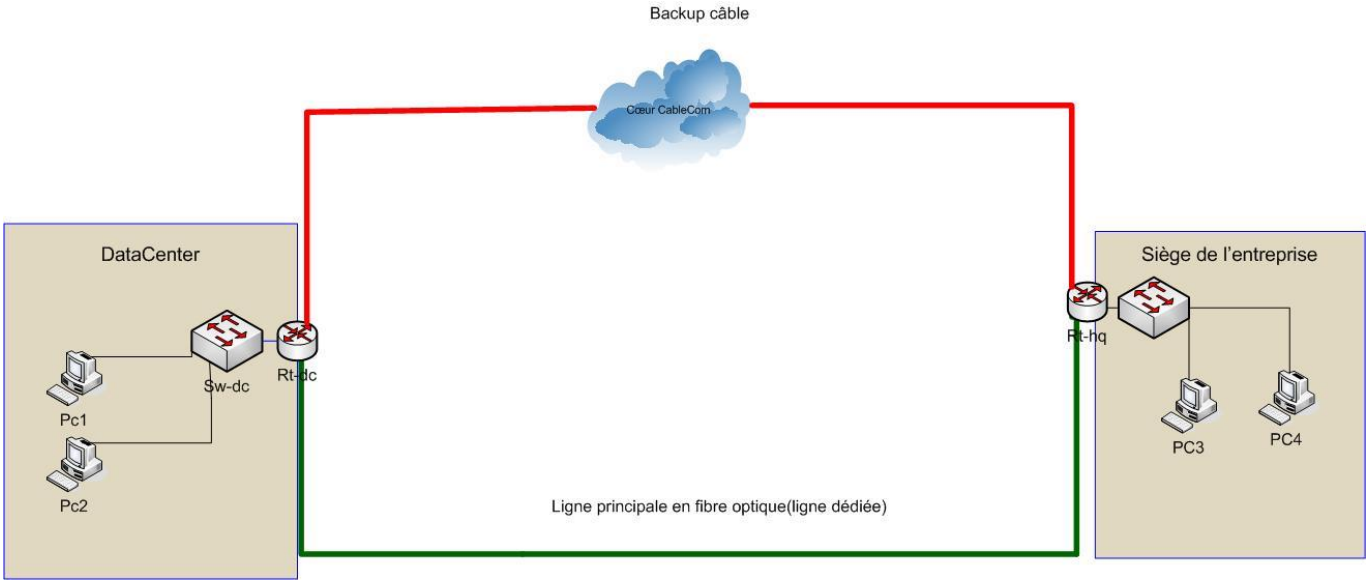


Figure 36 : Contexte avec une ligne de backup via le câble

8.4 Remerciements

Nos premiers remerciements vont à Messieurs François Buntschu et Patrick Gaillet, qui nous ont éclairés sur de nombreux points technologiques, dans le domaine des réseaux en général et également dans les domaines de la sécurité.

Nous tenons également à remercier Messieurs Rupp et Mathys pour leur visite à l'Ecole d'Ingénieurs en début de projet et pour leur intérêt au cours de ce dernier.

Finalement, nous remercions nos deux mandants M.Wagen et M.Robadey pour avoir donné une ligne directrice tout au long de ce projet, au travers des différentes séances.

8.5 Déclarations sur l'honneur

Nous, soussignés, Christophe Perroud et David Rossier, déclarons sur l'honneur que le travail rendu est le fruit d'un travail personnel. Nous certifions ne pas avoir eu recours au plagiat ou à toutes autres formes de fraudes. Toutes les sources d'information utilisées et les citations d'auteur ont été clairement mentionnées.

Christophe Perroud David Rossier

8.6 Contenu du CD

Administration

- Directives
- Donnée du projet

Gestion de projet

- Invitations
- Procès verbaux
- Planification
- Journaux de travail

Configuration

- Routeur Relay LTE
- Routeur HeadQuarter
- Routeur DataCenter

Documentation

- Rapport final
- Annexes

9.Sources/Références

Les atouts de la fibre optique en entreprise :
http://www.largeur.com/?p=3997
Offres de fibre optique de Swisscom :
http://www.swisscom.ch/fr/business/pme/internet/internet-au-bureau.html
Infrastructures WAN CISCO :
http://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/white_paper_c11-636065.html
Guide de la technologie NEMO par CISCO :
http://www.cisco.com/c/dam/en/us/td/docs/routers/access/interfaces/software/deployment/guide/guide_c07-720263.pdf
Article « Swisscom met le turbo » par Xavier Studer
http://www.xavierstuder.com/2013/05/24/4g-lte-swisscom-met-le-turbo-gare-a-certains-details/
Documentation module Cisco :
http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/4g-lte-wireless-wan-enhanced-high-speed-wan-interface-card/datasheet_c78-710314.html
Bintec RS353 datasheet
http://pim.binteclmeg.com/common/ajax.php?modul_id=101&klasse=produkte_pdf&bereich=admin&com=detail&kanal=xml&system_id=6550&sprache=en
Offres Swisscom
http://www.swisscom.ch/fr/business/pme/internet/internet-au-bureau.html
Documentation Netgear MBR1515
http://www.getwirelessllc.com/support/MBR1515.pdf
Datasheet du bintec RS353jv-4G
http://pim.bintec-elmeg.com/common/ajax.php?modul_id=101&klasse=produkte_pdf&bereich=admin&com=detail&kanal=xml&system_id=6550&sprache=en
Manuel Dlink 921 DWR
ftp://ftp2.dlink.fr/Manuels_Francais/DWR-921_A1_Manual_v1.01(FR).pdf
Description des types de VPNL2
https://www.youtube.com/watch?v=ID7Rw7K7nvU
Configuration MPLS sur des équipements Cisco
http://www.ciscopress.com/articles/article.asp?p=391649&seqNum=4
RFC 3931
http://tools.ietf.org/html/rfc3931
Video expliquant la mise en place de L2TPv3
https://www.youtube.com/watch?v=agXmOl0LY7M
Explications sur le tunnel GRE
http://archive.openflow.org/wk/index.php/Tunneling_-_GRE/L2TP
Principe DMVPN
https://www.fir3net.com/Routers/Cisco/dmvpn-tutorial.html

10.Sources des figures

Figure 4-5 : http://www.swisscom.ch/fr/clients-prives/internet/fibre-optique.html

Figure 6 : http://scmplc.begasoft.ch/plcapp/pages/gis/netzabdeckung.jsf?netztyp=lte&lang=fr

Figure 7 : http://www.reseau4g.info/4g-lte/introduction

Figure 9 : http://www.cisco.com/c/en/us/products/interfaces-modules/4g-lte-wireless-wan-enhanced-high-speed-wan-interface-card/index.html

Figure 10 : http://www.ietf.org/proceedings/65/slides/isoftwire-4/isoftwire-7.ppt

Figure 12 : http://wiki.treck.com/images/9/94/ESP_Position_in_IPv4_and_IPv6.gif

Figure 13: http://wiki.treck.com/images/9/94/ESP_Position_in_IPv4_and_IPv6.gif

Figure 14 : http://www.cisco.com/c/dam/en/us/td/i/000001-100000/80001-85000/81001-82000/81608.ps/_jcr_content/renditions/81608.jpg

Figure 22 : https://www.fir3net.com/Routers/Cisco/dmvpn-tutorial.html

Toutes les figures n'ayant pas été référencées ont été réalisées par M.Rossier et M.Perroud

11.Annexes

1. Planning du projet
2. Complément d'analyse : Matériel
3. Tableau multicritères pour choix du matériel
4. Complément d'analyse : VPN
5. Schéma d'encapsulation LTE
6. Schéma d'encapsulation Fibre
7. Tests effectués avec Swisscom
8. Tests effectués sur l'émulation
9. Changement d'IP sur la ligne LTE
10. Configuration des équipements
11. Problèmes rencontrés
12. Journaux de travail
13. PV des séances

12.Glossaire

- 3-4G : 3ème et 4ème generations de normes pour l'Internet mobile
- ADSL : asymmetric digital subscriber line
- AH: authentication header
- BGP: border gateway protocol
- Datacenter: centre de données
- DHCP : Dynamic host configuration protocol
- DMVPN: Dynamic multipoint virtual private network
- DMZ: demilitarized zone
- Download : téléchargement (depuis le web vers la machine en LAN)
- DSLAM: Digital subscriber line access multiplexer
- EIGRP : Enhanced Interior Gateway Routing Protocol
- ESP: encapsulating security payload
- GRE : Generic routing encapsulation
- GSM: Global system for mobile telecommunications
- HSPA : High speed packet access
- HTTPS : hypertext transfert protocol security
- IGP: interior gateway protocol
- IPSEC:Internet protocol security
- IPv4: Internet protocol version 4
- IS-IS : Intermediate system to intermediate system
- L2TP: Layer 2 tunneling protocol
- LSR: Label switch router
- LTE : Long Term Evolution
- mGRE: multi GRE
- MIME: Multipurpose Internet Mail Extensions

- MPLS : Multi protocol packet switching
- NAT: Network address translation
- NHRP : Next hop resolution protocol
- OSPF : Open Shortest Path First
- OSPF: open shortest path first
- PAT: port address translation
- PPP: point to point protocol
- SIM : Subscriber Identity Module
- TCP: transfert control protocol
- TTL: time to live
- UDP: user datagram protocol
- Upload : transfert vers le web
- VPLS: virtual protocol label switching
- VPN: virtual private network
- WAN : wide area network
- Wireless : sans fil
- WLAN : wireless local area network
- WPA-WPA2 :Wi-fi protected access