Sommaire

Liste des figures

Liste des tableaux

Introduction générale

La convergence vers tout IP et les avancées technologiques favorisent la migration vers l'IPTV. La télévision transmise par le protocole Internet présente de nombreuses possibilités tant pour les utilisateurs que pour les fournisseurs de services. En effet, dans un contexte concurrentiel féroce, l'adoption de nouveaux services est un élément de différenciation majeur. Maroc Telecom, étant l'unique fournisseur du service IPTV actuellement au Maroc vise dans sa stratégie de migration vers les réseaux NGN de diminuer les coûts et d'augmenter les revenus en transportant tout type de flux sur la même architecture pour les différentes technologies d'accès (xDSL, GPON).

La technologie IPTV permet d'utiliser un réseau IP existant pour transmettre le contenu télévisuel ou multimédia qui peut être visualisé sur des télévisions standards en passant par un encodeur (STB) ou sur les PC directement. Ce flux multimédia exige plus de ressources réseau en termes de bande passante pour répondre au besoin croissant de ce service, dans ce sens et pour satisfaire ses clients et augmenter la QoS de l'IPTV, l'opérateur historique a confié le projet de l'optimisation de la solution de bout en bout à Huawei Technologies pour optimiser davantage la bande passante et réduire le taux de perte des paquets, ainsi que le délai du zapping.

En récupérant le flux provenant des satellites par les paraboles placées à SHOUL dans la région de Rabat-Salé-Kenitra, Huawei se charge de le transformer en un flux IP multicast à l'aide de la plateforme IPTV qui contient le Head-end. Comme la plateforme IPTV ne fait pas l'objet de l'optimisation dans mon PFE, toute l'architecture responsable de cette transformation sera illustrée dans les chapitres étudiants la solution, comme un serveur IPTV qui génère le flux IP. C'est ce flux IP que je vais prendre en charge pour le transporter sur le réseau de l'opérateur en cherchant à optimiser l'architecture existante et à adapter les protocoles déployés.

Pour organiser ce rapport qui synthétise mon travail tout au long de ces cinq mois de stage, quatre chapitres sont mis en place. Le premier chapitre présente la multinationale Huawei Technologies et les missions qui m'ont été accordées au sein de son département NT (Network Technologies). Le second chapitre décrit le cadre général de l'IPTV en citant les services et les fonctionnalités qu'il offre et l'architecture de sa plateforme. Puis, le 3éme chapitre donne une description de la solution IPTV existante et en fin le 4éme et dernier chapitre cible une partie de cette architecture et la détaille pour l'optimiser.

Chapitre 1 : Contexte général du stage

Dans ce premier chapitre, je vais présenter l'organisme d'accueil. Puis, je donnerai une idée sur le contexte général du stage ainsi que sur les taches à réaliser. Et pour finir je donnerai une description du plan du stage.

1. Présentation générale de l'organisme d'accueil

Huawei Technologies est une entreprise dont le siège social est situé à Shenzhen en Chine. Créé en 1988, Huawei est devenu un fournisseur dominant en Chine, puis s'est lancée pour les marchés internationaux en adoptant une politique de prix très agressive.

Huawei Technologie est une entreprise active dans le secteur des technologies de l'information et de la communication (ICT). Elle fournit le matériel, les logiciels et les prestations de services pour les réseaux de télécommunications des opérateurs et les réseaux informatiques des entreprises.

Ses principaux concurrents économiques sont Cisco Systems, Alcatel-Lucent, Ericsson, Nokia, Nortel, NEC et ZTE. Ces derniers ont vu leurs parts de marché en Asie s'effriter et ont assisté à la montée en puissance du groupe chinois sur les marchés émergents et occidentaux.

Depuis son implémentation au Maroc en 1999, en tant que bureau représentatif de Huawei Technologies, le volume d'activités de Huawei Maroc n'a cessé d'augmenter. Son portefeuille clientèle s'est largement diversifié, grâce à ses produits de qualité et au niveau supérieur de service qu'elle assure pour ses clients. Huawei Maroc occupe actuellement une place de leader dans le marché marocain de télécommunication grâce à une étroite collaboration avec les principaux opérateurs marocains, à savoir Maroc Telecom, Meditel et Inwi.

Huawei sous-traite le déploiement de ses solutions aux sous-traitants suivants : SIRECOM – MRS - DIMENSION DATA – TIBCO - …

Mon stage a été effectué au sien de département NT (Network Technology) de Huawei Maroc dans son bureau de Rabat, ce département a pour mission d'assurer la maintenance des services pour leur partie réseau.

2. Contexte du stage

Dans le cadre de sa stratégie de diversification de services et pour faire face à la concurrence et garder sa place de leader du marché des télécommunications, Maroc Telecom a introduit le service de l'IPTV, qui en exploitant la même infrastructure existante permet d'augmenter le revenu moyen par abonné (ARPU).

Maroc Telecom a confié le déploiement d'IPTV à Huawei Technologies en 2005. Un projet d'extension a été aussi mis en place en 2010 pour répondre au nombre d'abonnés désirant bénéficier de ce service. Huawei Technologies, actuellement s'occupe de la maintenance de ce service côté plateforme IPTV et côté transport.

L'équipe du Réseau fixe cherche actuellement à optimiser cette solution dans le but d'augmenter la QoS et satisfaire le client final, pour enfin la proposer à Maroc Telecom et la convaincre de l'adopter. C'est dans ce cadre que s'inscrit mon PFE effectué au sein du département NT de Huawei Technologies et qui a pour objectif de mener une réflexion collective avec l'équipe pour trouver la bonne optimisation.

Après la première réunion avec l'équipe, les missions qui m'ont été accordées sont les suivantes :

- Etude de la plateforme IPTV (compréhension complète de la transformation du flux DVB : Digital Video Broadcast en un flux multicast TSoIP : Transport Streaming over IP).

- Etude et description de la solution end-to-end (les protocoles et les technologies utilisées coté Backbone, transport et accès).
- Ciblage d'une partie à optimiser en justifiant ce choix.
- Résultat de la solution d'optimisation proposée en faisant un comparatif entre la nouvelle solution et l'actuelle.

3. Planification du stage

Avant de commencer mon stage PFE, j'ai élaboré un planning prévisionnel à suivre pour réaliser les missions qui m'ont été confiées par l'équipe de maintenance à Huawei Technologies. Ce planning a été plus ou moins respecté parce qu'il y avait des notions qui nécessitaient plus de temps pour les comprendre et d'autres qui ont été facilement assimilables dans une durée plus courte. J'étais amenée aussi à revoir des concepts déjà vus dans le stage pour corriger ce qui a été mal compris ou ajouter d'autres informations pour enrichir mes connaissances.

La figure suivante illustre le planning que j'ai effectué à l'aide des outils de diagramme de Gantt sous MS PROJECT pour la durée de mon stage qui s'étale du 01/02/2016 au 30/06/2016 :

	Nom de la tâche	Durée	Début	Fin
1	Présentation du sujet PFE	1 jour	Lun 01/02/16	Lun 01/02/16
2	Etude de la plateforme IPTV	15 jours	Mar 02/02/16	Lun 22/02/16
3	**Etude de la solution IPTV actuelle**	**42 jours**	**Mar 23/02/16**	**Mer 20/04/16**
4	Etude du protocole IS-IS	6 jours	Mar 23/02/16	Mar 01/03/16
5	Etude du protocole PPPoE	3 jours	Mer 02/03/16	Ven 04/03/16
6	Etude des technologies xDSL	1 jour	Lun 07/03/16	Lun 07/03/16
7	Etude de l'équipement MSAN	3 jours	Mar 08/03/16	Jeu 10/03/16
8	Etude de la technologie GPON	3 jours	Ven 11/03/16	Mar 15/03/16
9	Etude du protocole BGP	2 jours	Mer 16/03/16	Jeu 17/03/16
10	Etude de la technologie MPLS	6 jours	Ven 18/03/16	Ven 25/03/16
11	Etude du protocole DHCP	2 jours	Lun 28/03/16	Mar 29/03/16
12	Etude du protocole VRRP	1 jour	Mer 30/03/16	Mer 30/03/16
13	Etude des protocoles multicast IGMP et PIM	15 jours	Jeu 31/03/16	Mer 20/04/16
14	**Optimisation de la solution existante**	**23 jours**	**Jeu 21/04/16**	**Lun 23/05/16**
15	Optimisation du partage des charge entre les deux liens des CX600 liés au MSAN	15 jours	Jeu 21/04/16	Mer 11/05/16
16	remplacement du PPPoE par Le DHCP	4 jours	Jeu 12/05/16	Mar 17/05/16
17	Minimisation du délai d'acheminement du trafic multicast	4 jours	Mer 18/05/16	Lun 23/05/16
18	Rédaction du rapport	75 jours	Mar 01/03/16	Lun 13/06/16

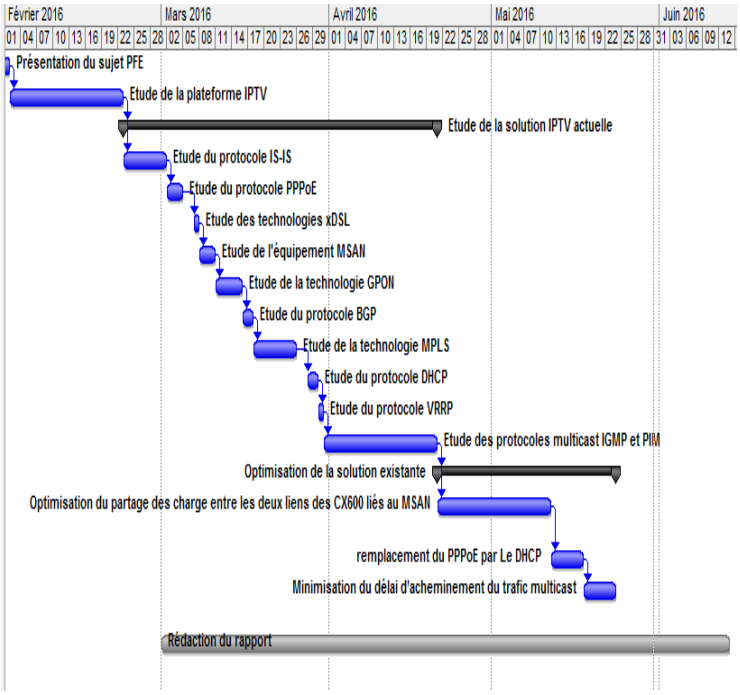

Figure 1: Diagramme de Gantt du PFE.

4. Conclusion

Pour commencer ce rapport qui résume le travail réalisé durant la période de mon PFE. Il a été nécessaire de donner une présentation de la société qui m'a accueilli et de définir en clair le cadre général de mon stage tout en précisant les missions qui m'ont été confiées dès le premier jour. Suite à cette affectation de tâches, j'ai pu élaborer le planning du stage pour bien organiser mon travail et atteindre tous les objectifs tracés.

Chapitre 2 : Etude de la plateforme IPTV de Huawei Technologies

Dans ce chapitre une présentation de la plateforme IPTV sera réalisée. Tout d'abord elle portera sur les services assurés par cette plateforme. Ensuite je donnerai l'architecture détaillée de cette plateforme. Et finalement je m'intéresserai aux problèmes sous-jacents à la solution IPTV.

1. Présentation du service IPTV

IPTV (TV over IP) est un service qui permet aux abonnés de l'opérateur de regarder des chaînes télévisées tout en exploitant la même infrastructure qui leur permet l'accès à Internet. Le client en s'abonnant à un bouquet de chaînes donné (découverte, prestige, évasion) aura accès à toutes les chaînes disponibles dans le bouquet choisi.

Le recours à ce service se justifie côté client, par l'incapacité de la télévision par satellite à assurer une réception sans perte dans les conditions météorologiques défavorables. Le second motif qui est le plus motivant et rend les clients plus intéressés à s'abonner est l'interactivité qu'offre l'IPTV par le biais de ses services sous-jacents. En effet, les parents actuellement peuvent contrôler les chaînes diffusées dans leurs bouquets et les programmes regardées par leurs enfants par une simple configuration. Une description détaillée de tous les services sera le sujet de la section qui suit.

L'adoption de la solution IPTV par l'opérateur historique se justifie par :

- La compétition avec les autres opérateurs l'oblige à diversifier ses services.
- La domination des services mobile large bande sur les services fixes larges bande.
- Augmentation du revenu moyen annuel par client ou l'ARPU (Average Revenue Per Unit).

2. Services offerts par l'IPTV

2.1. Service VoD

La technologie IPTV introduit le service de la Video on Demand qui permet aux clients de naviguer dans un catalogue de films ou de programmes proposés par l'opérateur, de regarder des bandes d'annonce et de choisir le programme qui leur plait.

Techniquement, quand un client sélectionne un film, une liaison point à point en unicast est établie entre le STB du client et le serveur qui délivre le streaming (HMS).

Figure 2: Service VoD.

2.2. Service TVoD

Le service de TV à la demande est prévu pour visionner des programmes TV récents en choisissant le programme TV à partir de l'archive.

Une chaîne de TV reçue à partir d'un satellite ou d'une station de diffusion est enregistrée sur le serveur. En cherchant dans le contenu média du STB, les informations concernant l'heure du début du programme TV sont affichées. Ces informations sont fournies à partir du guide des programmes (EPG). La recherche des programmes TV enregistrés peut être faite en utilisant les marqueurs du début du programme ou simplement en choisissant une date et heure arbitraires.

Figure 3: Service TVoD.

2.3. Service BTV

Le service Broadcast TV (BTV) est le service de diffusion de la télévision basé sur le réseau IP Broadband.

Maroc Telecom coopère avec les fournisseurs de service pour obtenir la permission de la diffusion des contenus. Actuellement, IAM diffuse 135 chaînes y compris les chaînes radio.

Figure 4: Service BTV.

2.4. Service Radio

Ce service permet au client d'accéder à plusieurs stations Radio via son STB, Maroc Télécom offre jusqu'à 20 stations Radio national et international.

Figure 5: Service Radio.

2.5. Service TSTV

Le service TSTV (Time Shift TV) est l'un des services issus de la fonction BTV, qui utilise la capacité de transmission bidirectionnelle du réseau IP. Le TSTV permet aux utilisateurs de regarder des programmes déjà diffusés. Pendant la lecture des programmes de BTV, les utilisateurs peuvent effectuer des opérations interactives telles que la pause, l'avancement rapide, la recherche et l'affichage de l'état et du temps.

Figure 6: Service TSTV.

2.6. Service PIP

Le service Picture In Picture (PIP) est un service BTV personnalisé. Quand un utilisateur regarde un programme BTV il peut débuter le service PIP, et alors, deux programmes BTV sont présentés sur deux fenêtres de tailles différentes. L'usager peut switcher vers la petite fenêtre et donc choisir son programme préféré.

Figure 7: Service PIP.

2.7. Service Mosaïque

Le Service Mosaïque permet de créer un seul écran de sélection de chaînes qui contient jusqu'à 48 chaînes.

Ce service offre au client la possibilité de sélectionner le contenu qu'il préfère et cela lui permet aussi de suivre un grand nombre de chaînes en même temps.

Figure 8: Service Mosaïque.

2.8. Service PVR

Le Personal Video Recorder est un service personnalisé de la Broadcast TV. Un utilisateur peut enregistrer ses programmes préférés des chaînes BTV sur un disque dur au niveau de son STB. Après l'enregistrement, l'utilisateur peut lire les programmes enregistrés.

Figure 9: Service PVR.

2.9. Service TVMS

La TVMS (TV Message system) envoie des messages de recommandation des programmes, suggestions, votes et TV shopping, vers les STB des clients.

3. Architecture de la plateforme IPTV

La plateforme IPTV est illustrée en couches dans le schéma suivant :

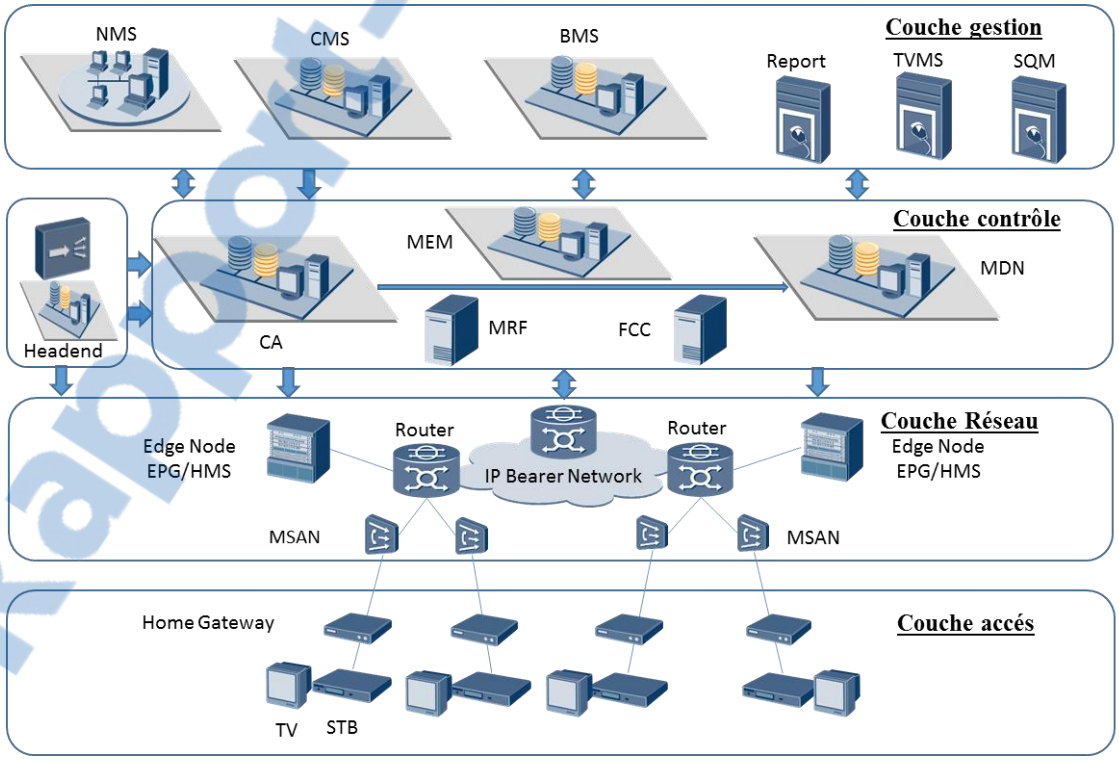

Figure 10: Architecture de la plateforme IPTV. [1]

3.1. Couche de gestion des services

La couche service management s'occupe de la gestion en intégrant des serveurs suivants :

- NMS (Network Management System) : est utilisé pour fournir une gestion unifiée pour les éléments du réseau (BMS, CMS, MDN, MEM). Le NMS comprend l'I2000 (pour la supervision), iCnfg (pour gérer la configuration de tous les modules), et une base de données (pour stocker les données du NMS). A travers les NMS, la plate-forme fournit les fonctions telles que la gestion et la configuration des dispositifs de surveillance de la performance du système IPTV.
- CMS (Content Management System) : gère tout ce qui est en rapport avec le contenu destiné aux utilisateurs.
- BMS (Broadcast Management System) : contient les profils des abonnés.
- report : présente des statistiques sur les demandes des clients et sur les chaînes regardées, ces informations servent de base pour le service de marketing pour gérer les bouquets proposés aux utilisateurs, par exemple les chaînes qui ne sont pas vues par un certain nombre d'abonnés seront remplacées par d'autres.
- TVMS (IPTV Messaging System) : est un service d'affichage de messages de l'opérateur sur l'écran de l'abonné pour l'informer des changements dans son bouquet ou simplement pour faire la publicité d'un nouveau service.
- SQM (Service Quality Manager) : vérifie et assure la qualité du service.

3.2. Couche Contrôle des services

3.2.1. Head-end

Head-end est le site qui reçoit et traite les signaux numériques des satellites, il est composé des éléments suivants :

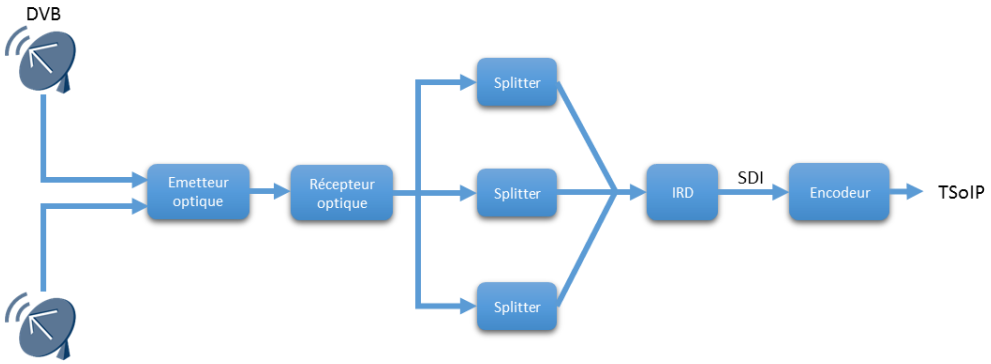

Figure 11: Composants du HeadEnd. [1]

- Système de réception du signal : La réception du signal se fait par un système composé d'antennes, toutes deux antennes sont centrées sur un satellite donné (Hotbird-Nilesat-Badr-astra), soit alors huit antennes au total, la redondance de ces antennes est assurée par une antenne motorisée. Ensuite, le signal passe par un transmetteur optique vers un récepteur optique qui l'injecte dans des splitters. Ces derniers servent à reproduire le même signal dans 16 sorties qui constituent l'entrée du système de décodage.

Le système de réception est muni d'un LNB (Low Noise Block downconverter) servant à convertir toute la bande de fréquence en une bande de basses fréquences supportée par l'IPTV : L-band : 0.950000-2.150000GHz.

- Système de décodage IRD (Integrated Receiver and Decoder) : dont la sortie est en SDI (Synchronous Digital Interface), il se charge de trois opérations :
  - Démodulation du signal en utilisant la norme QPSK.
  - Descrambling qui sert à décrypter les chaînes reçues cryptées depuis le satellite tel qu'Al Jazeera à l'aide des cartes de décryptage spécifiques qu'on peut insérer dans l'IRD.
  - Décodage en utilisant la norme MPEG-2 pour la radio et MPEG-4 pour la vidéo.

Un IRD a pour sortie une seule chaîne si cette dernière est en HD et deux chaînes si elles sont en SD. Il y'en a 3 types :

- IRD PVR2991 : pour le décodage des chaînes SD

- IRD PVR7K : pour le décodage des chaînes HD

- IRD PVR2980 : pour le décodage de l'audio comme pour la radio

- Système d'encodage : Assuré par les encodeurs ENVIVIO, ce système a pour rôle principalement de donner une adresse IP multicast à chaque chaîne après avoir fait la compression du contenu à l'aide de la norme H.264. Le système d'encodage est par la suite le responsable de la génération du flux multicast TSoIP.

3.2.2. CA

CA (Conditional Access) est le système de cryptage qui assure les éléments suivants :

- Cryptage du flux multimédia.
- Gestion de la base de données de clés de cryptage et de décryptage
- Authentification et autorisation des STBs

Le contenu crypté au niveau du système de cryptage CA sera décrypté à sa réception par le STB qui contient la clé de décryptage.

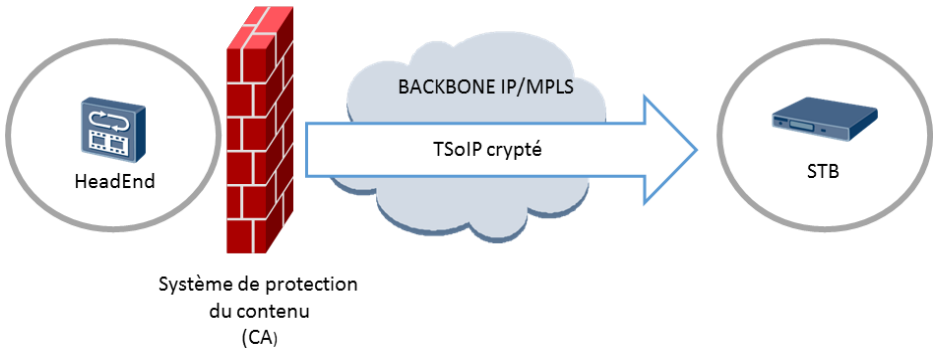

Figure 12: Cryptage du contenu multicast. [9]

3.2.3. MDN

MDN (Media Delivery Network) est un composant qui se trouve dans le site central, il enregistre et distribue tout ce qui est en rapport avec la VOD et la TVOD et TSTV.

Sous-composants du MDN	Description
CMI : Content management interface	Fournit le CMS externe. Ce dernier ajoute le contenu des médias au MDN, supprime le contenu du MDN, interroge le MDN pour le contenu, et modifie le contenu du MDN.
MC : Media Content	Fournit des informations telles que la performance, les alarmes et les journaux du MDN.
MM : Media Manager	Gère le contenu. Après avoir reçu des instructions de gestion du contenu (par exemple, des instructions pour ajouter, supprimer, et interroger le contenu des médias) de la CMI, le MM effectue les tâches de gestion du contenu, par exemple : la publication, l'ajout, la suppression et l'interrogation du contenu.
RRS : Request Routing Server	Cherche le serveur HMS le plus proche du STB de l'abonné. Il surveille aussi l'état, le contenu, et la charge de chaque HMS en temps réel, et équilibre les charges entre HMS.
HMS : Huawei Media Server	Est un serveur de stockage qui fournit directement des services de diffusion pour les utilisateurs
UM : Usage Mediator	Réalise les statistiques et classifie les chaînes selon le taux d'audience.

Tableau 1: Sous-composants du MDN [1]

3.2.4. MEM

MEM (Media Entertainment Middleware) contient les éléments suivants :

Sous-composants du MEM	Description
EPG : Electronic Program Guide	Est un serveur web en java script qui délivre une page EPG qui contient des informations sur les programmes présents dans les bouquets d'IPTV. il est en relation directe avec le STB. on a plusieurs EPG dans chaque région.
Upgrade	Est un serveur de mise à jour de la version du STB, il existe deux serveurs upgrade à rabat pour mettre à jour la version de l'EPG utilisée.
ACS : Application Control Server	Servant à l'authentification et l'autorisation des comptes des abonnés.

EDS : EPG Distributing Server	Permet d'affecter à chaque client un EPG en se basant sur l'adresse IP et le numéro du port.
ECS : EPG Control Subsytem	Gère et maintiens les informations concernant tous les serveurs d'un MEM.
PMS : Product Management Subsystem	Gère les produits et les services, sert aussi à créer les CA.
SMS : Subscriber Management System	Sert à gérer les informations concernant les abonnés.
CIS : Content Injection Subsystem	Permet de gérer le contenu des programmes télévisés.

Tableau 2: Sous-composants du MEM. [1]

3.2.5. MRF

MRF (Media Relay Frame) encapsule le contenu multimédia dans des messages RTP avant de le router au réseau IP/MPLS. Il assure le FEC (Forward Error Correction) et RET (RETransmission). Une copie du flux obtenu est enregistrée au Media Delivery Network (MDN).

3.2.6. FCC

FCC (Fast Change Channel) est un serveur qui fournit la fonction FCC. Lorsqu'un utilisateur bascule entre les chaînes, le serveur FCC accélère la livraison du flux multimédia pour raccourcir le temps de commutation entre chaînes.

Les serveurs cités auparavant sont soit déployés dans les sites régionaux, soit existent seulement dans le site central :

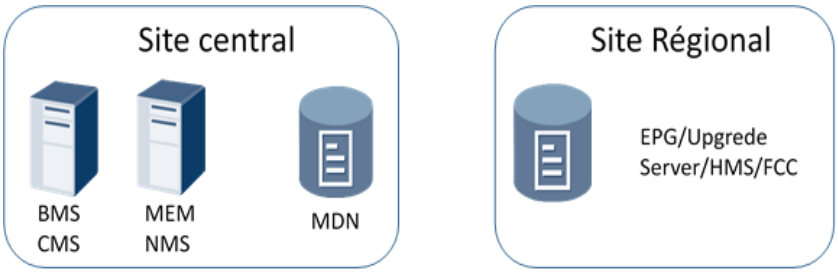

Figure 13: Emplacement des serveurs de la plateforme. [8]

4. Défis sous-jacents à la plateforme IPTV

4.1. Codage du flux

En IPTV, on ne peut pas transmettre toutes les chaînes à la fois aux clients, comme c'est le cas de la télévision traditionnelle, à cause de la bande passante limitée. De ce fait, le changement de chaîne (Zapping) sans coupure de réception, le grand besoin en Bande passante, et la sensibilité aux pertes de paquets et aux paquets erronés s'imposent comme des défis importants à l'IPTV pour assurer la meilleure qualité possible aux clients.

L'encodage en IPTV se fait en H.264 (MPEG-4) pour les chaînes télévisées et en MPEG-2 pour les chaînes radio, pour préserver au maximum la bande passante. Il utilise la structure GOP pour la compression vidéo. GOP est un groupe d'images qui diffèrent légèrement les uns des autres. Il comprend trois types de trames I-Frames, B-Frames, et P-Frames. Chaque trame est une image. Chaque GOP peut avoir une I-Frame et plusieurs B-Frames et P-Frames. Le GOP peut contenir un nombre fixe de trames comme il peut contenir un nombre variable de trames selon le contenu de la vidéo.

- I-Frame : c'est une trame de référence qui contient l'information complète de l'image. C'est la première trame du GOP. Chaque GOP possède une seule I-Frame et ne peut être affiché si celle-ci est perdue. La I-Frame contient le plus du flux de données et consomme plus d'espace par rapport aux autres trames du même GOP. On peut dire simplement qu'elle représente le background de l'image.
- P-Frame : rétablie l'image selon l'I-Frame. Elle est aussi une trame de référence pour le rétablissement de l'image de la B-Frame. Un GOP ne peut être affiché normalement en cas de perte de la P-Frame.
- B-Frame : utilise La I-Frame et les P-Frames pour rétablir une image.

La figure suivante montre les relations entre les différentes trames de ce codage vidéo.

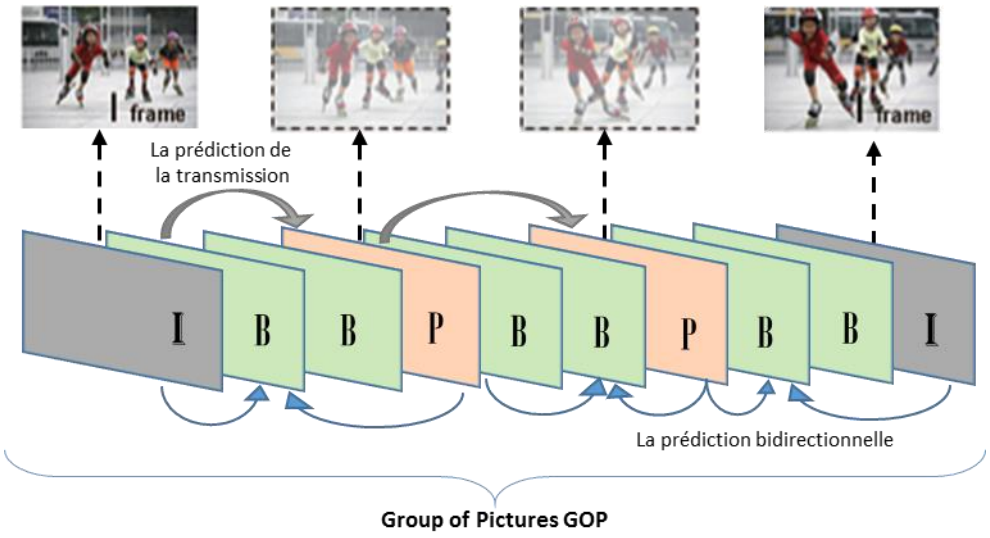

Figure 14: Relations entre les différentes trames du codage vidéo. [6]

Après la compression de la vidéo, elle est découpée en tranches, ces tranches sont encapsulées dans un paquet MPEG-TS de 188 bytes, et chaque groupe de 7 paquets est encapsulé dans un paquet RTP et puis ce dernier sera encapsulé dans un paquet UDP, comme c'est illustré dans la figure ci-dessous.

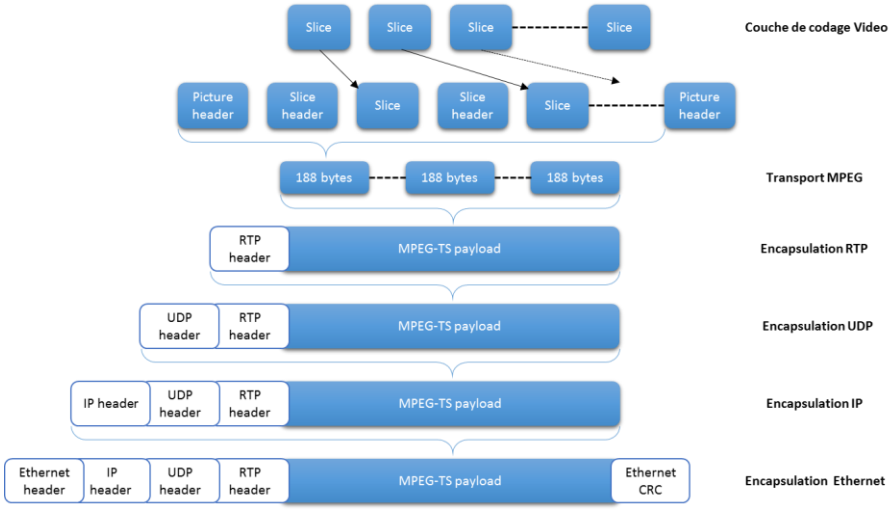

Figure 15: Encapsulation d'un paquet vidéo en IPTV. [6]

Le principe de la compression vidéo montre que le temps d'attente avant le passage à une autre chaîne est très dépendant du temps d'attente d'une I-Frame et du PSI « Program Specification Information ».

PSI est une métadonnée à propos des programmes (chaînes), elle fait partie d'un MPEG-TS. PSI inclus quatre tables :

- PAT (Program Associate Table) : liste tous les programmes disponibles dans le TS. Chacun des programmes est identifiée par un numéro de programme qui sera réservé pour spécifier le PID utilisé pour l'identifier dans la NIT.
- CAT (Conditional Access Table) : spécifie si le contenu a le droit d'être diffusé.
- PMT (Program Mapping Table) : contient des informations concernant chaque programme présent dans le TS. Ces informations incluent le numéro du programme et une liste des flux élémentaires ainsi que d'autres descriptions optionnelles.
- NIT (Network Information Table) : donne des informations sur l'état du réseau.

4.2. Changement de chaîne

Le temps d'attente du PSI et d'une I-Frame rend le temps de changement d'une chaîne instable, car Le PSI est reçu par le STB dans un délai variant entre 100 ms et 500 ms, tandis que l'intervalle de la I-Frame varie selon le contenu de la vidéo et la forme du codage.

Le tableau suivant montre les différents retards lors du zapping :

Facteurs du retard du zapping	Retard typique
IGMP leave	~ 10 to 20 ms
IGMP join	~ 10 to 20 ms
Temps du processus MSAN	~ 30 to 50 ms
retard du DSL	~ 10 ms
retard du réseau Core/Agg	~ 20 to 50 ms
Attente du PAT/PMT	~ 500 ms
Attente de la I-Frame	~ 250 ms to 1.8 s
Décodage	~ 50 ms

Tableau 3: Différents retards lors du changement de chaîne (basé sur les analyses de Huawei).

Le retard cumulatif est de l'ordre de 2.5s. Pour diminuer le temps du zapping en diminuant le temps d'attente du PSI et des I-Frames, le serveur FCC a été mis en place. En effet, le FCC envoi en unicast ces deux trames au STB avec un débit plus grand que l'ordinaire pour une durée de 2.5s. Après cette durée le FCC arrête l'envoi du flux. Le mécanisme du fonctionnement du FCC sera illustré dans ce qui suit.

4.3. Perte de paquets

Le deuxième problème lié à la plateforme IPTV est la sensibilité aux pertes de paquets et aux paquets erronés. Cette perte due à la compression importante du flux vidéo, peut causer l'effet mosaïque (pixellisation de l'image) qui affectera la qualité de l'image. Pour éviter cette dégradation de qualité, Huawei propose le mécanisme de la retransmission automatique RET. Ce mécanisme peut réduire le taux de paquet perdus/erronés comme c'est expliqué par le processus suivant :

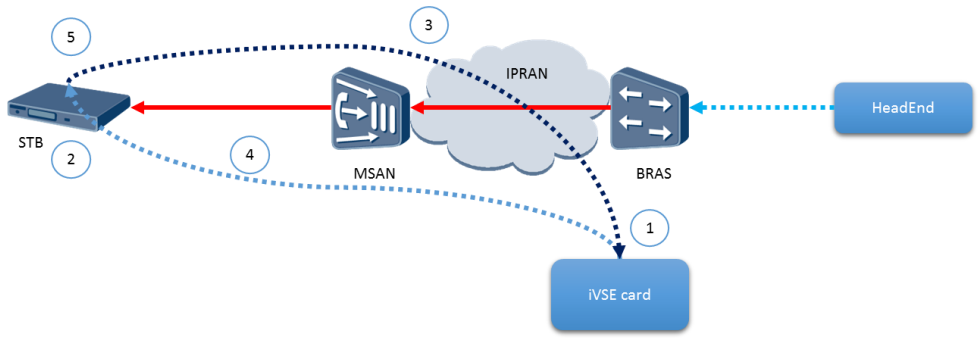

Figure 16: Processus d'implémentation de la RET. [6]

1. La carte iVSE présente au niveau du BRAS enregistre deux seconde ou trois du flux vidéo dans sa mémoire cache.
2. Le STB vérifie la continuité du numéro de séquence SN présent dans l'entête de RTP, et calcule le SN du paquet perdu.

Bit offset	0-1	2	3	4-7	8	9-15	16-31
0	Ver .	P	X	CC	M	PT	Sequence Number
32	Timestamp						
64	SSRC identifier						
96	CSRC identifiers (optional)						
96+(CCx32)	Extension header (optional)						
96+(CCx32)+(Xx((EHL+1)x32))	Data						

Figure 17: Forme de l'entête RTP.

3. Le STB envoie une demande de retransmission (paquet RTCP) à la carte iVSE.
4. La carte iVSE envoie les paquets en cache (paquets RTCP) au STB.
5. Le STB insert les paquets retransmis, qui sont en cache pour la retransmission des paquets perdus, dans le flux vidéo.

4.4. Optimisation de la bande passante

Les vidéos consomment une large bande passante. Donc le grand besoin en bande passante s'impose comme l'un des défis majeurs de la solution IPTV. De ce fait, pour diminuer la consommation de la bande passante Huawei propose d'approcher les serveurs de la plateforme aux abonnés.

Avec cette méthode, le contenu est délivré le plus proche possible à l'utilisateur grâce à l'utilisation des cartes vidéo cache intégrées dans les équipements réseau (BRAS, AGG, MSAN) pour étendre les serveurs de la plateforme (FCC, MDN,…) jusqu'aux utilisateurs.

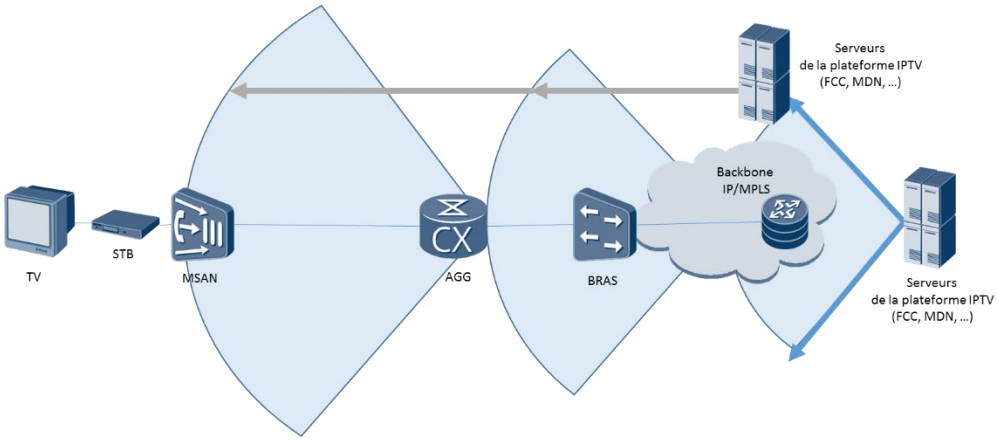

Figure 18: Extension des serveurs de la plateforme.

5. Scénarios de gestion de la plateforme IPTV

5.1. Initialisation du STB

Après l'établissement de la session PPPOE entre le BRAS et le STB, le BRAS envoie l'adresse IP au STB. Ce dernier enregistre dans sa mémoire cache l'adresse IP du serveur EDS et du RRS, il interroge par la suite l'EDS sur l'adresse du serveur UPGRADE pour mettre à jour la version du STB, après l'obtention de l'adresse IP de l'EPG et l'authentification auprès du ACS, l'EPG envoi la page EPG en http, puis il demande la clé de décryptage au CA pour pouvoir déchiffrer le contenu reçu.

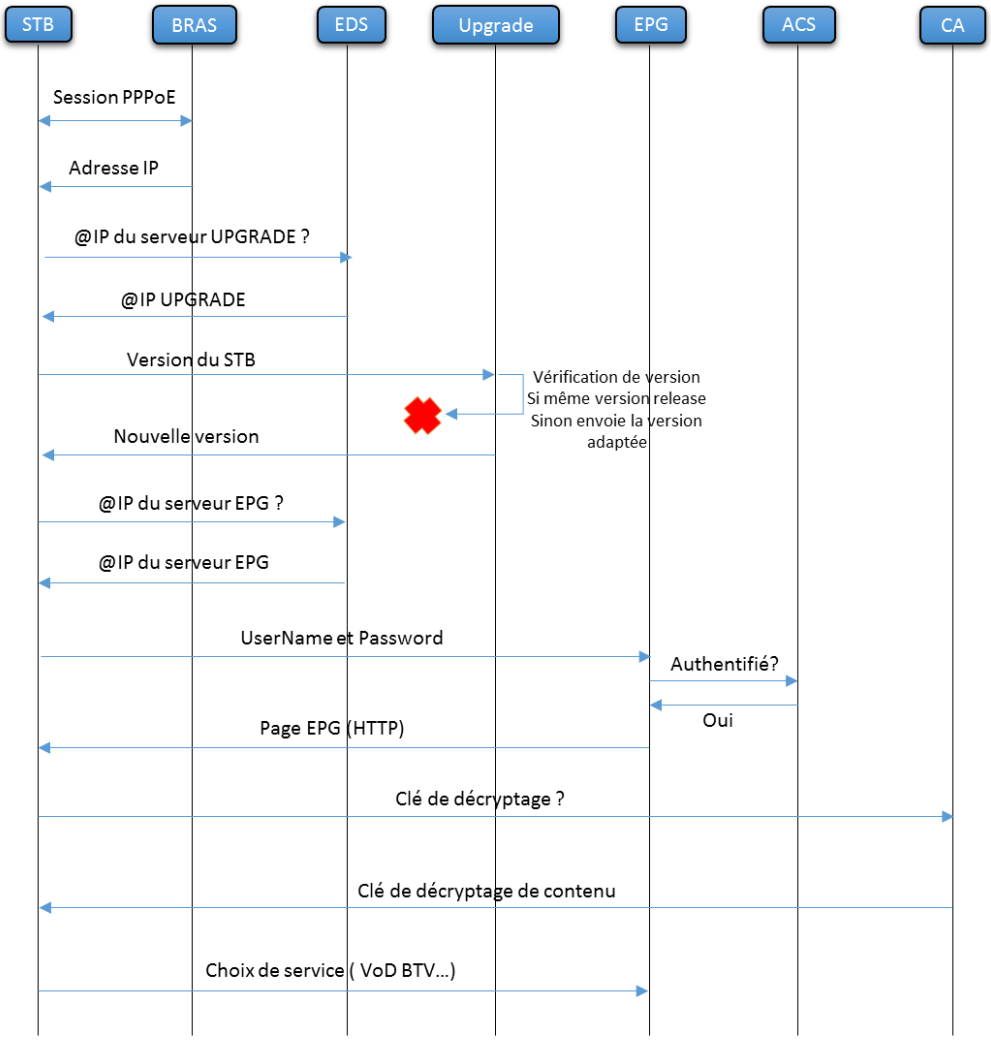

Figure 19: Initialisation STB.

5.2. Service VoD

Le service VOD est un service unicast, il est choisi à partir de la page EPG fourni au STB, le serveur EPG vérifie si l'abonné est inscrit dans ce service, si la réponse est positive le STB demande le flux au RRS qui cherche le serveur HMS le plus proche pour servir le STB.

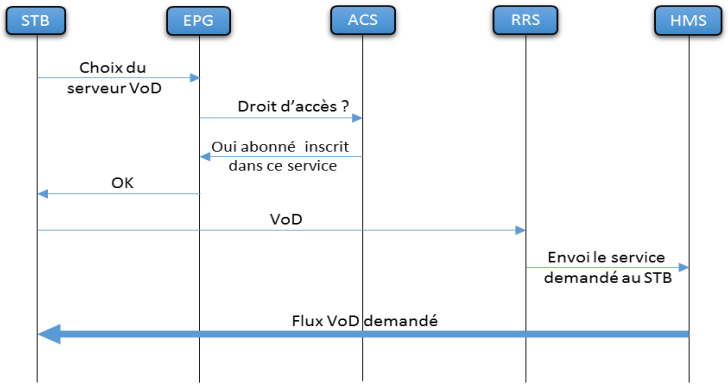

Figure 20: Service VoD.

5.3. Service BTV

- L'EPG demande à l'ACS si la chaîne choisie appartient au bouquet du client avant d'envoyer l'adresse IP multicast de la chaîne demandée.
- le RRS envoi au STB l'adresse du serveur FCC le plus proche à l'utilisateur. Le but c'est d'envoyer le flux multicast demandé en unicast temporairement pour réduire le temps d'attente du client et cela avec un grand débit (1+α) .V. Le temps de recours au serveur FCC en attendant que le flux multicast soit prêt s'appelle le CCT (Channel Change Time)
- Quand le FCC décide que le flux unicast est adapté au flux multicast normal, il envoie un signal RTCP pour informer le STB qu'il doit joindre le groupe multicast de la nouvelle chaîne. Et le FCC diminue la vitesse d'envoi du flux unicast à α .V seulement pour synchroniser les numéros de séquence du RTP.
- Le serveur FCC arrête l'envoi du flux unicast. Les flux unicast et multicast se connectent entre eux. Et l'utilisateur ne se rend pas compte de tout ce processus

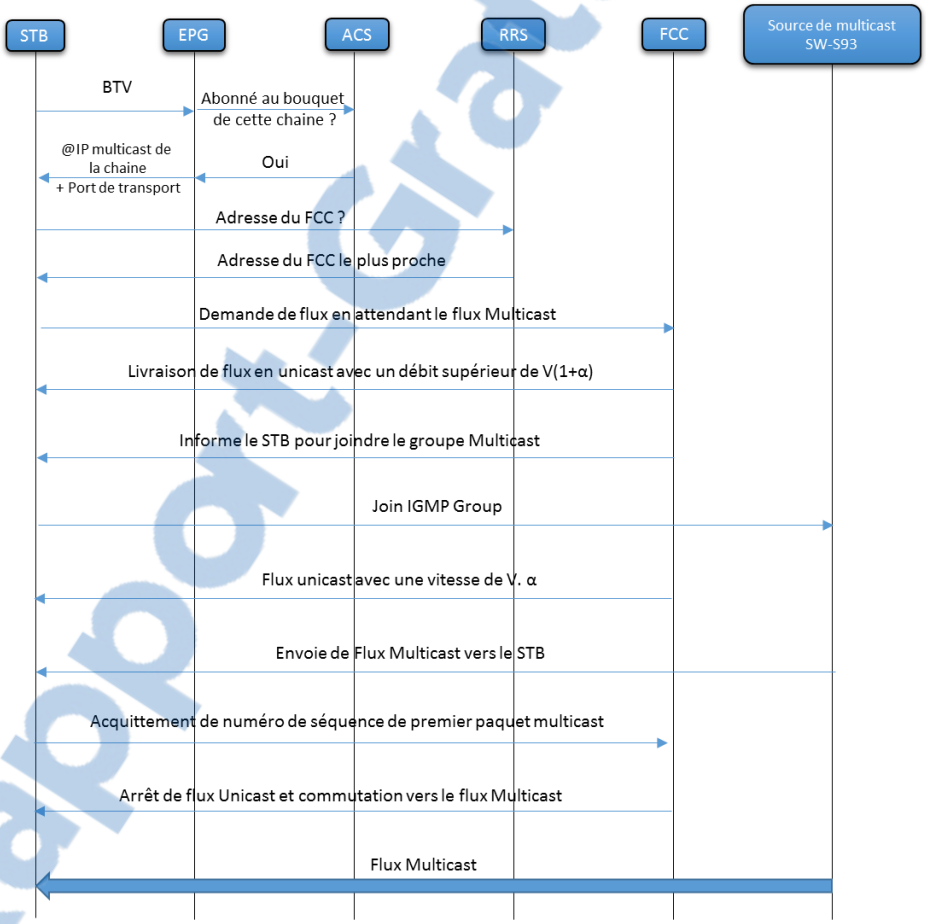

Figure 21: Service BTV.

6. Conclusion

Le présent chapitre donne une présentation générale de l'IPTV en termes de services offerts et de plateforme responsable de la génération du flux multicast, il présente aussi les différents problèmes liés à l'IPTV (changement de chaine - bande passante - perte de paquets). Le prochain chapitre détaillera davantage la solution IPTV déployée actuellement par Huawei au compte de Maroc Telecom.

Chapitre 3 : Description end to end de la solution IPTV de Huawei

La solution IPTV de HUAWEI est implémentée sur l'architecture existante d'IAM qui supporte plusieurs services tournants en parallèles avec le service IPTV. Cette architecture se devise principalement en trois parties : Partie cœur (Backbone IP/MPLS), partie transport (IPRAN), et partie accès.
Ce chapitre sera consacré à la description de chacune de ces parties en termes de technologies et protocoles utilisés pour assurer le fonctionnement de l'IPTV.

1. Introduction

La plateforme IPTV qui a été précédemment détaillée sera illustrée dans le présent chapitre par un serveur nommé « Plateforme IPTV ».

Avant de commencer le descriptif de chaque partie en termes d'équipements déployés et de protocoles utilisés, il est à noter que l'étude de la solution IPTV portera sur deux types de flux : le flux unicast pour le management de l'IPTV et le flux multicast proprement dit pour le transport du flux multimédia.

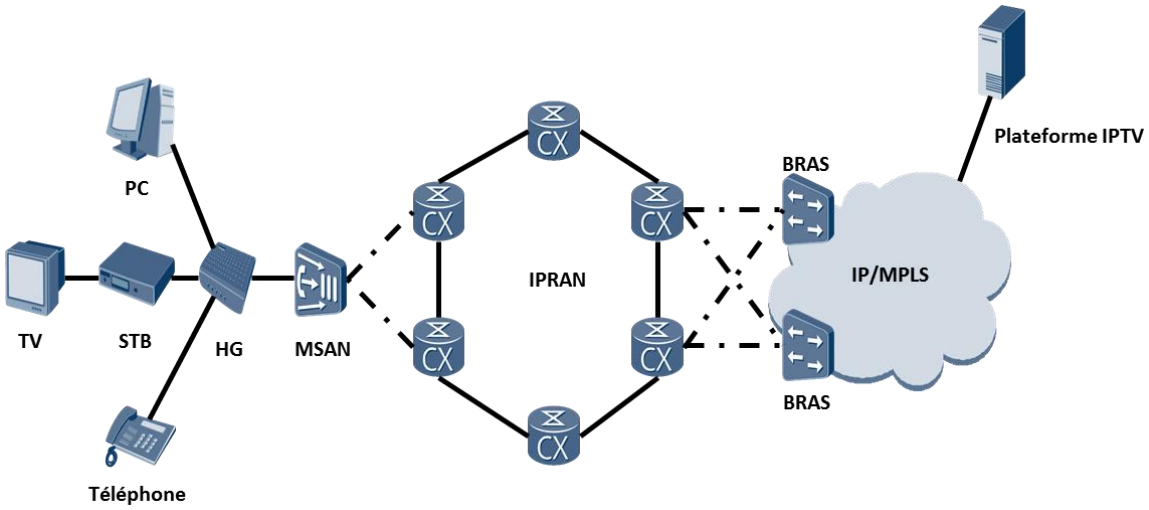

Figure 22: Architecture end-to-end de la solution IPTV.

2. Réseau Backbone IP/MPLS

2.1. Description du Backbone de Maroc Telecom

Le Backbone de Maroc Telecom se base sur la technologie MPLS. Il contient 8P (Providers) distribués sur le royaume, chaque P est connecté à plusieurs PE.

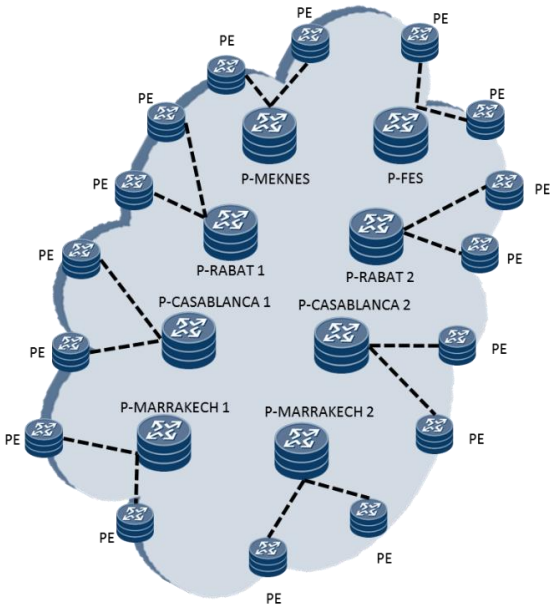

Figure 23: Distribution des P d'IAM sur le royaume.

Pour le flux unicast destiné au management des STBs, l'application L3VPN du MPLS est utilisée. L3VPN permet une séparation sécurisée du flux et une transparence vis-à-vis de l'architecture du Backbone, cette transparence est due au fait que le trafic sera transporté par des tunnels, la technologie L3VPN sera détaillée dans l'annexe F.

Le réseau Backbone IP/MPLS route en multicast les flux de streaming vidéo, injectés par la plateforme IPTV, vers les BRAS connectés aux réseaux d'accès. En effet la plateforme IPTV est la source multicast et les réseaux d'accès sont les récepteurs.

Le Backbone IP/MPLS du Maroc Telecom est connecté à la boucle METRO IP par un équipement qui s'appelle BRAS. Le BRAS de la série des Quidway MA5200G de Huawei établit une session PPPoE avec le STB pour lui allouer une adresse IP de l'un des IP –Pool au STB.

Le Backbone IP/MPLS d'IAM est configuré avec le Protocole Independent Multicast (PIM) qui est un protocole de routage multicast intra-domaine qui fonctionne sur une infrastructure unicast existante.

2.2. Protocole PIM

PIM (Protocol Independent Multicast) est un protocole de routage IP multicast qui permet la diffusion vers un groupe d'hôtes. PIM est dit *Protocol-Independent* car il se base dans ses décisions de routage sur la topologie établie par d'autres protocoles de routage unicast (OSPF, BGP, IS-IS).

Il existe trois modes de fonctionnement du PIM, PIM Dense Mode (PIM-DM) pour les réseaux denses, tels que les LAN, et le PIM Sparse Mode (PIM-SM) pour les réseaux à large échelle, extensible au routage multicast inter-domaines et PIM Source Specific Multicast (PIM-SSM). PIM-SM, est la variante PIM utilisée sur le réseau IAM.

2.2.1. Arbres de distribution

- **Shortest Path Tree (SPT)** : est un "source tree", c'est à dire que chaque source multicast crée un enregistrement (S, G) : (Source, Groupe) concernant ce flux et l'arbre de distribution sera de la source vers les récepteurs du groupe. Il y aura autant d'enregistrement (S, G) et de SPT, dans les routeurs qu'il y a de sources (émetteurs) pour le groupe.
- **Shared Tree (RPT) :** contrairement au Source Tree dont la racine est la source, les Shared Tree ont une racine centralisée, partagée, un point de rendez-vous (RP). Les sources envoient leur flux à la racine (le RP), depuis laquelle le trafic est transféré vers les récepteurs. Comme toutes les sources utilisent un arbre partagé commun, on retrouvera dans les routes la notation (*, G). L'arbre de distribution est dynamique, des branches seront créés ou coupées en fonction des abonnements/désabonnement de récepteurs. Le RP doit être connu par tous les équipements qui supportent PIM, deux méthodes sont utilisées par Huawei dans ce sens, soit le RP est déclaré statiquement soit dynamiquement par le protocole Bootstrap. Le Bootstrap permet à un routeur dit Bootstrap Router (BSR) de collecter les candidatures des routeurs du domaine PIM pour qu'ils soient RP (Condidate RP), et puis diffuser un message Bootstrap contenant les informations sur tous les Condidats RP. Les routeurs utilisent un algorithme commun pour sélectionner le même RP pour un groupe multicast donné. Le RP est déclaré statiquement dans le réseau de Maroc Telecom, il existe un seul RP pour tous les groupes multicast.

2.2.2. RPF

RPF (Reverse Path Forwarding), est l'algorithme de décision de routage pour le multicast. Contrairement à l'unicast où la préoccupation est l'adresse de destination, en multicast il faut également tenir compte de l'adresse source.

Quand le routeur reçoit un paquet, il exécute le mécanisme du « RPF check » qui est expliqué ci-dessous :

- Le routeur consulte sa table de routage unicast, pour déterminer si le paquet a été reçu sur l'interface qui permet de joindre la source dans le chemin inverse.
- Si le test est réussi le paquet sera transféré sur les interfaces de sortie présentes dans la table de routage multicast.
- Sinon le paquet sera détruit afin d'éviter les boucles.

Dans le cas de PIM shared tree, il vérifie le RPF sur l'adresse du RP, en cas de SPT il le fait directement sur l'adresse source (de multicast) IP du paquet.

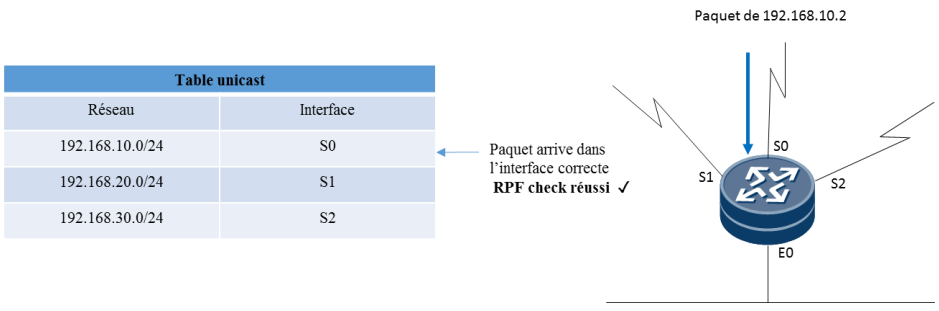

Figure 24: RPF check réussi. [4]

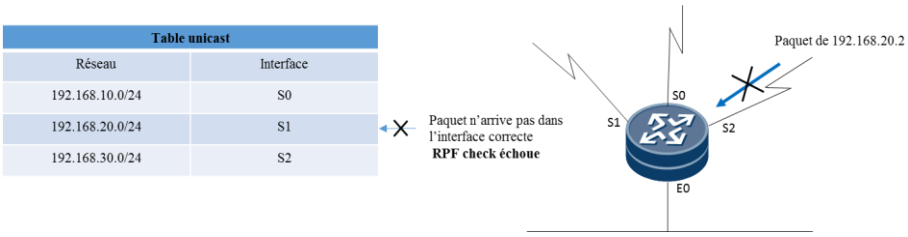

Figure 25: RPF check échoue. [4]

2.2.3. Fonctionnement du PIM-SM

En mode sparse (SM), seuls les clients ayants fait un « IGMP join » (le détail du protocole IGMP sera donné plus tard) sur un groupe feront partie de l'arbre de distribution.

Quand un client rejoint un groupe multicast, son routeur émet un PIM Join vers le point de rendez-vous (RP) le plus proche (si il existe plusieurs routeurs sur le segment du client, une élection du PIM-DR sera réalisé et c'est lui qui sera le responsable de l'envoi du PIM join au RP). Le routeur construit un arbre de distribution partagé (shared tree).

Les sources envoient à un point de rendez-vous (RP), et les clients font une demande explicite auprès de ce RP pour accéder à la source.

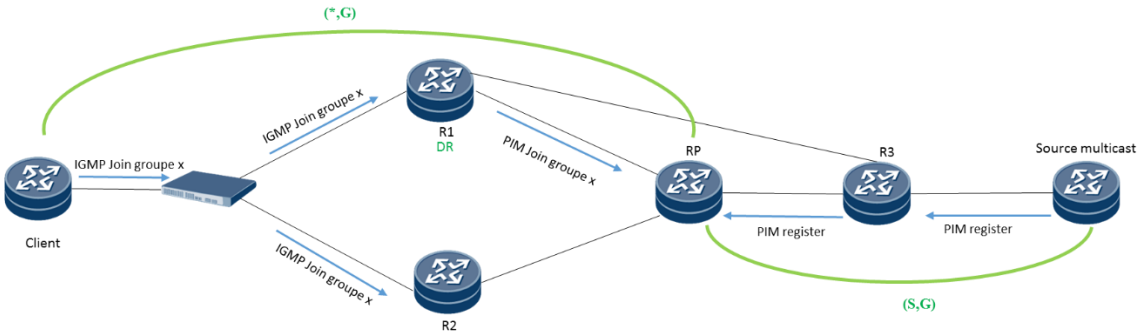

Figure 26: Fonctionnement du PIM-SM.

Le passage par le RP, peut dans certains cas être non optimal, pour cela le mécanisme de Switch Over est implémenté. Ce mécanisme consiste à construire un SPT de la source vers le client, et par la suite réduit le coût de routage.

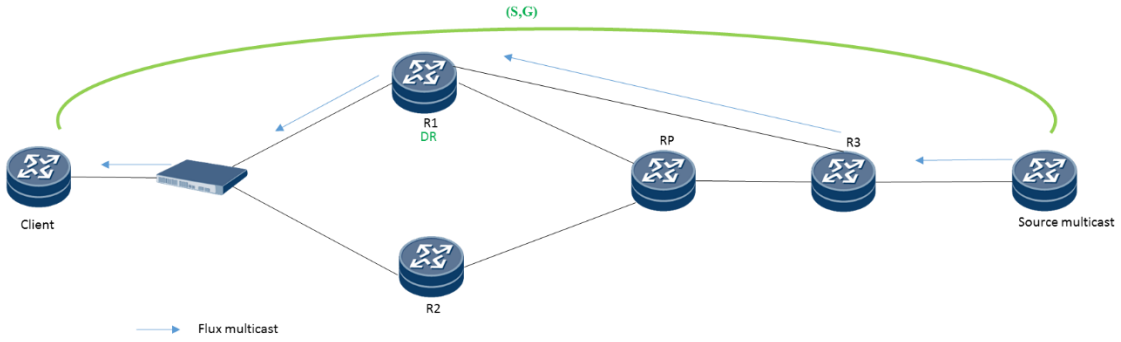

Figure 27: Switch Over.

3. Réseau IPRAN

3.1. Description de la boucle METRO IP

Le réseau METRO IP du Maroc Telecom ou encore IPRAN (IP Radio Access Network) est constitué de plusieurs boucles formés de routeurs de la série CX600 offerts par Huawei. Il existe deux types de CX600 : CX600-8 et CX600-16 dont la simple différence réside en nombre d'interfaces allouées. La connexion entre ces routeurs est assurée par des câbles en fibres optiques de capacité de l'ordre de 10 Gbps. La connexion entre ces routeurs est doublée pour assurer la redondance des liens afin d'éviter la coupure du service en cas d'incident.

3.2. Protocoles utilisés dans la boucle METRO IP

3.2.1. Protocole IS-IS

La boucle métro IP est une partie critique dans l'architecture réseau d'IAM, car elle présente la seule entrée au réseau de l'opérateur de toute une région. Pour cela le protocole BFD est implémenté pour assurer une détection rapide des pannes. Le détail de ce protocole fera l'objet de l'annexe H.

Le protocole de routage qui permet la communication entre les routeurs de la boucle est le même que celui utilisé dans le Backbone, il s'agit du protocole IS-IS. Il existe plusieurs boucles métro pour couvrir tout le territoire national, ainsi chaque boucle présente une zone (area) pour le protocole IS-IS.

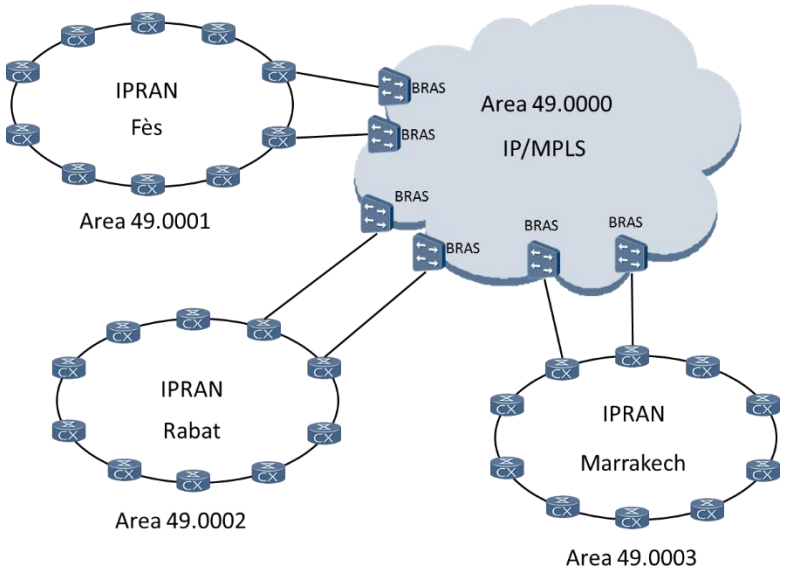

Figure 28: Implémentation du protocole IS-IS.

3.2.2. Protocole VPLS

VPLS est un service Ethernet multipoint-à-multipoint (MP2MP) qui utilise IP ainsi que le mécanisme de tunneling du MPLS pour apporter une connectivité entre plusieurs sites à travers un nuage IP, comme si ces sites sont reliés par un même LAN Ethernet. La technologie VPLS est configurée dans la boucle Métro et par la suite toute cette boucle sera considérée comme un switch.

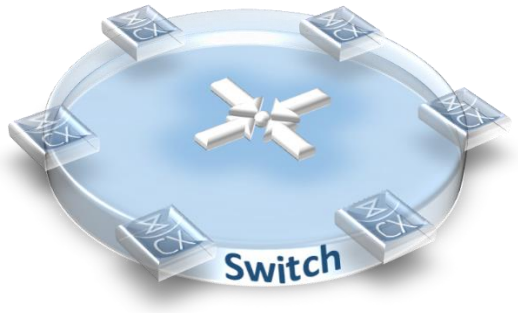

Figure 29: Boucle METRO IP équivalente à un switch.

Pour assurer le bon fonctionnement de ce switch virtuel, il faut instaurer le même mécanisme de travail d'un switch ordinaire. En effet, une fois la trame Ethernet arrive sur un port d'entrée connectant le client, l'adresse MAC destination est recherchée dans la table MAC et la trame est transmise (si l'adresse MAC correspondante se trouve dans la table MAC) à l'intérieur de la boucle au PE adéquat connectant le site distant visé. Si l'adresse MAC n'est pas présente dans la table ou l'adresse destination de la trame est Broadcast, alors la trame sera répliquée et transmise à tous les ports logiques associés à cette instance VPLS excepté le port d'entrée par lequel la trame est arrivée et l'adresse MAC sera enregistrée dans la table. Les adresses MAC n'ayant pas été utilisées après un certain temps sont automatiquement éliminées de la table, exactement comme sur un commutateur Ethernet.

Le VPLS a été mis en place pour pouvoir transporter le protocole PPPoE de couche 2 sur la boucle métro IP. En effet, une fois le STB est connecté au réseau, il établit une session PPPOE avec le BRAS (qui joue le rôle du serveur PPPOE) pour l'obtention de l'adresse IP.

3.2.3. Protocole PPPoE

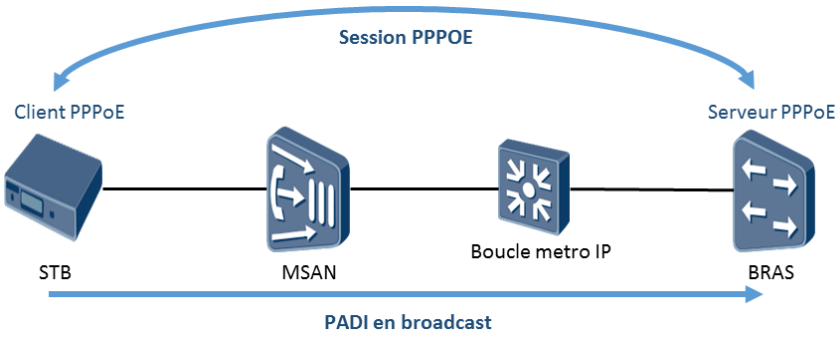

Figure 30: Session PPPOE entre le STB et le BRAS.

- Le STB envoie un message PADI en Broadcast
- Les BRAS répondent par un message PADO, avec des durées différentes.
- Le STB analyse les messages PADO reçus et envoie le PADR au serveur qui a répondu le premier.
- Le BRAS envoi le message PADS au STB pour confirmer l'établissement de la session.
- Session PPP.

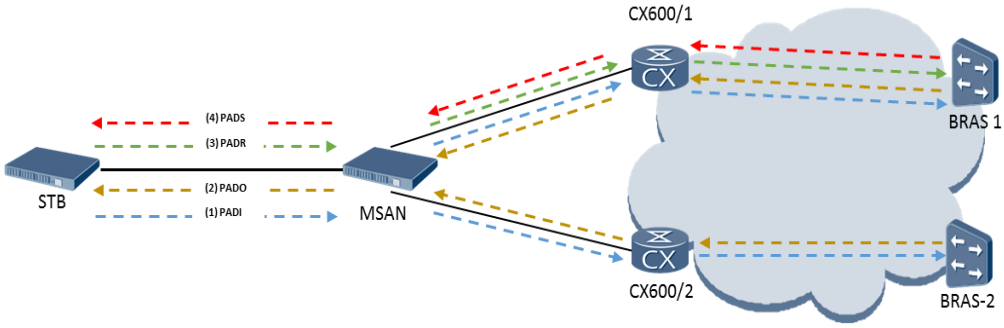

Figure 31: Messages d'établissement de la session PPPOE.

La session est établie donc entre le STB et le premier BRAS qui a répondu, et le flux unicast va suivre le même chemin créé. En général la probabilité pour que le flux unicast passe par le lien reliant le MSAN et le CX600/1 est égale à la probabilité pour que le flux unicast passe par le lien reliant le MSAN et le CX600/2 qui est de 0,5 car soit c'est le BRAS1 qui répond le premier soit c'est le BRAS2.

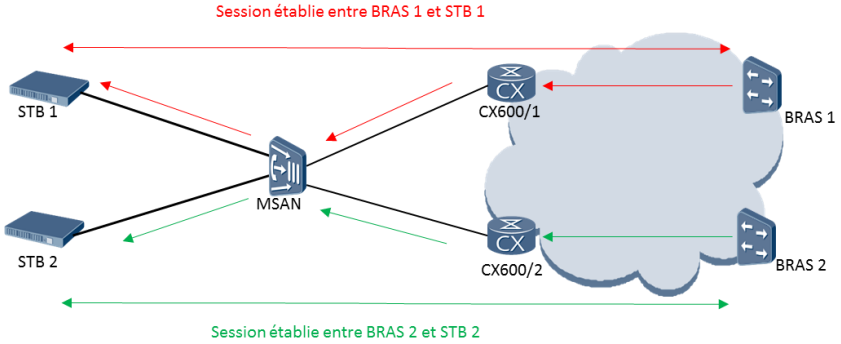

Figure 32: Partage du flux Unicast entre les routeurs CX600/1 et CX600/2.

4. Réseau Accès

4.1. Description de la partie accès

La partie accès est connectée à la boucle Metro IP par le MSAN qui représente le seul point de raccordement des clients au réseau de l'opérateur. La disponibilité de ce réseau est une exigence que l'opérateur doit toujours assurer pour éviter la coupure des services, et la déconnexion de ses abonnés. Afin de pouvoir atteindre ce but, IAM a mis en place un mécanisme de redondance nommé « Dual Homing » qui assure le basculement automatique entre les équipements d'une façon transparente pour l'utilisateur.

La solution «Dual Homing » consiste à raccorder le MSAN aux deux CX600 de la boucle Metro IP qui vont jouer le rôle de maitre/esclave, pour assurer que le trafic échangé entre le routeur CX600-Master et le MSAN sera basculé sur le lien reliant le MSAN avec le routeur CX600-Backup. Le protocole VRRP est utilisé dans les deux routeurs pour chaque instance de service.

Il est à noter que le service IPTV n'utilise plus le VRRP, le flux unicast sortant suit le même chemin établit lors de la création de la session PPPOE entre le BRAS et le STB. L'utilisation du VRRP dans le service IPTV sera discutée plus tard dans le cadre du remplacement de protocole PPPOE par DHCP.

Un MSAN est un équipement qui peut supporter des cartes xDSL, RNIS, Ethernet, FTTx, ou encore X25. De ce fait, au sein d'un seul et même châssis, l'opérateur peut déployer toutes les technologies d'accès envisageables sur son réseau et offrir des services Broadband (l'IPTV, l'internet et la VoIP) et Narrowband (POTS, RNIS, FAX,…).

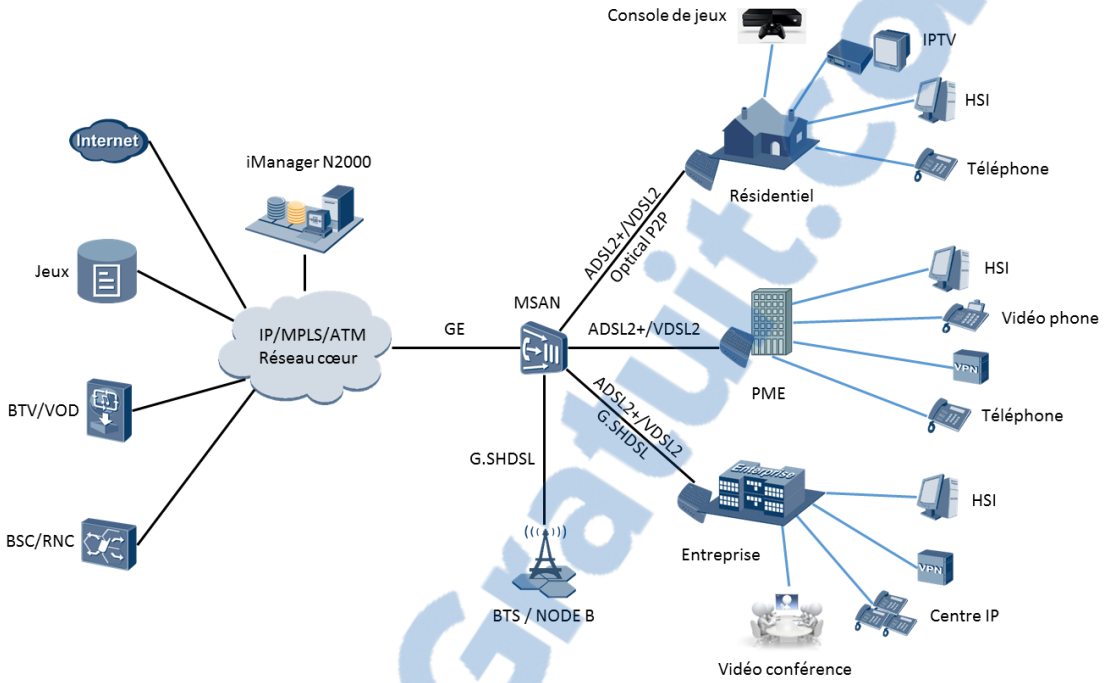

Figure 33: Services supportés par le MSAN.

La technologie déployée actuellement entre le MSAN et la « Home Gateway » est l'ADSL2+ qui utilise l'ATM. L'ATM permet dans le cas d'abandon de cellules dans les techniques de résolution de la congestion, une perte négligeable de données, à cause de la taille fixe des données dans chaque cellule qui est de 48 octets (53 octets avec l'entête). La longueur fixe facilite également l'allocation de la bande passante.

L'ATM est utilisé pour faire transiter les différents types de services sur le même support, depuis le modem de l'abonné jusqu'au MSAN. Les circuits virtuels sont utilisés pour relier l'abonné au MSAN qui prend ensuite en charge le mapping entre le couple (VPI, VCI) associé à chaque service supporté et le VLAN correspondant. Le processus en détail est le suivant :

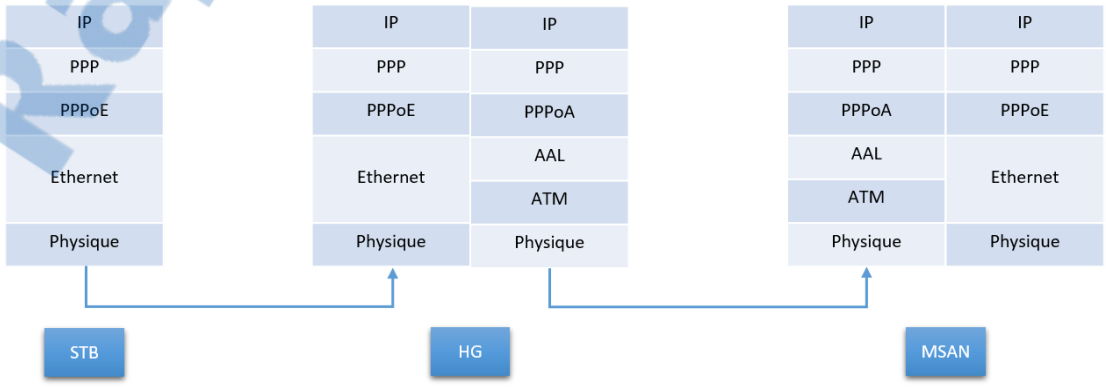

Figure 34: Processus d'encapsulation sur ATM.

1. Le STB envoie ses données au modem (HG) par le biais du protocole Ethernet.
2. Le modem récupère les données provenant du STB et les désencapsule jusqu'au niveau 2 (protocole PPPoE) pour les encapsuler de nouveau dans le protocole AAL (Adaptation à l'ATM) puis dans ATM. Il transmet ensuite les données au MSAN via la technologie ADSL.
3. Le MSAN récupère les données transmises via l'ADSL et fait le mapping entre le couple (VPI, VCI) associé à chaque service supporté et le VLAN correspondant. Il récupère ainsi les données et remonte jusqu'à la couche 3 (IP) afin d'adapter la transmission au réseau reliant le MSAN au réseau de l'opérateur qui est en Ethernet.

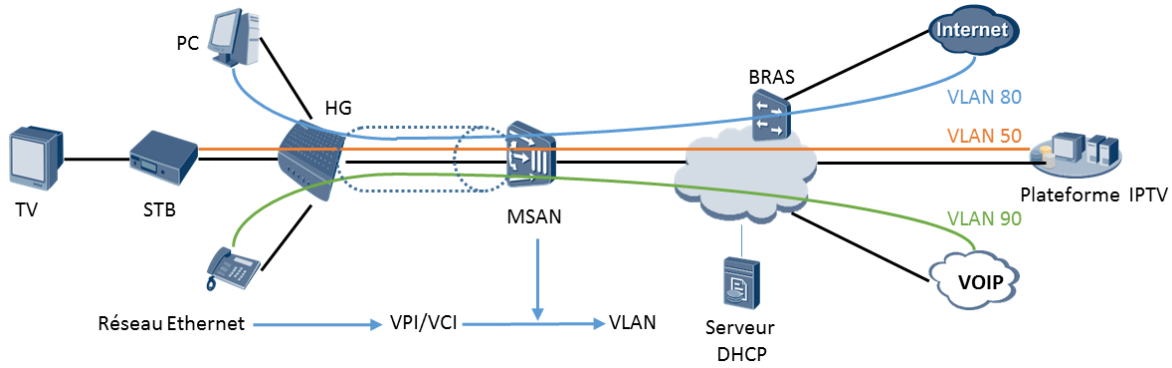

Figure 35: Mapping entre VPI/VCI et VLAN.

4. Le MSAN est configuré statiquement afin d'associer à chaque VPI/VCI le VLAN correspondant.

4.2. Acheminement du flux multimédia au STB

4.2.1. Protocole IGMP

IGMP (Internet Group Management Protocol) est un protocole qui permet d'échanger des informations d'appartenance aux groupes entre les clients qui veulent adhérer un groupe et les routeurs de bordure. Il existe trois versions de ce protocole :

IGMPv1	IGMPv2	IGMPv3
- IGMP membership query : **C'est le message qu'émet le routeur afin de découvrir les hôtes désirant adhérer à un groupe multicast donné. Ce message est envoyé à intervalle régulier sur l'adresse 224.0.0.1 avec une TTL à 1** **- IGMP membership report :** **Paquet envoyé par un hôte donné afin d'adhérer à un**	Cette version est une évolution de la version 1 par intégration de 2 nouveaux messages **- Group Specific query :** Requête émise sur un groupe donné par le querier (qui n'est pas forcément le PIM DR, mais le routeur qui a la plus petite adresse IP), elle permet de s'assurer qu'il reste bien des hôtes qui écoutent le trafic sur ce groupe ou non.	**- Version 3 membership report :** en version 1 et 2, les « membership report » sont émises à destination du groupe multicast. En v3, elles sont émises à destination du 224.0.0.22 et seront interprétés par les routeurs multicast intégrants IGMPv3. 2 modes à distinguer : **- Le mode inclusion :** les paquets multicast d'un groupe donné ne sont acceptés que si les sources ont auparavant été signalées au DR à l'aide du message « Version 3 membership report »

groupe multicast, ce paquet a pour adresse de destination l'adresse du réseau multicast auquel il veut adhérer.	**- Leave group message :** Message émis par un hôte afin de signifier au DR qu'il n'est plus intéressé par le trafic.	**- Le mode exclusion :** tous les paquets d'un groupe donné sont acceptés à l'exception de ceux dont la source fait partie de la liste d'exclusion du DR (source qui est signalée à l'aide d'un message « Version 3 membership report »). Un nouveau type de message est donc intégré et comporte les champs suivants : • Mode • L'adresse du groupe concerné • La liste des sources.

Tableau 4: Versions du protocole IGMP. [3]

IGMPv2 est la version utilisée actuellement dans la solution IPTV, un client final en choisissant une chaîne envoi « IGMP membership report » aux deux CX600 à l'entrée de la boucle METRO IP en traversant le MSAN qui est considéré un équipement couche 2, et par la suite implémente le mécanisme de l'IGMP Snooping.

Le routeur CX600 qui est PIM-DR sera chargé d'envoyer le « PIM join » au RP et par la suite le trafic multicast sera délivré à travers ce routeur élu DR à destination de STB demandeur.

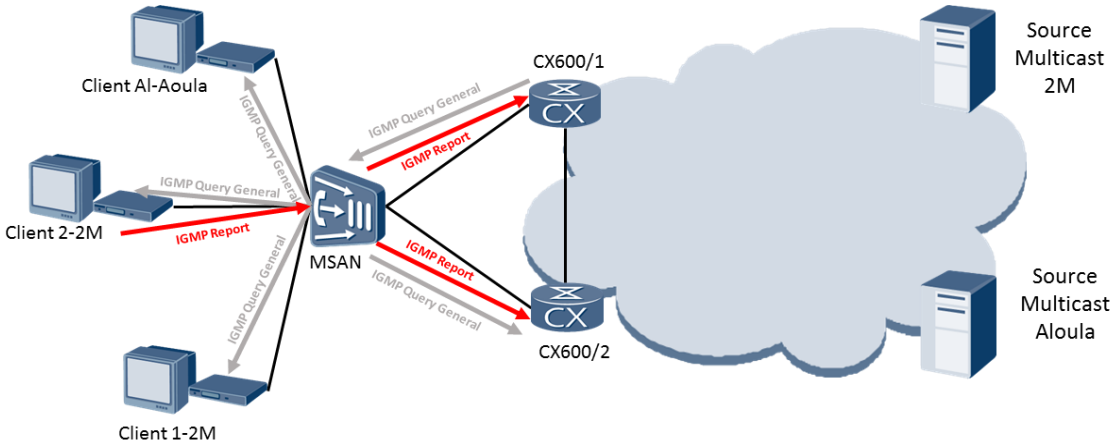

Figure 36: Principe de fonctionnement de l'IGMP.

4.2.2. IGMP Snooping

Un switch niveau 2 considère le flux multicast comme inconnu ou comme Broadcast. Dans tous les cas, cela aura pour conséquence qu'il enverra le flux sur l'ensemble de ses ports, engendrant une congestion du réseau.

IGMP Snooping consiste à donner à un switch une fonctionnalité de niveau 3. Ainsi un switch au niveau duquel l'IGMP Snooping est activé va analyser les trames IGMP qui transitent par lui, afin de déterminer si l'hôte situé dans un port donné doit ou non, recevoir le flux multicast à destination d'un groupe donné. S'il voit passer « IGMP report » pour un groupe donné, il réémettra sur le port concerné tout le flux multicast du groupe correspondant.

4.2.3. IGMP Proxy

IGMP proxy est configuré dans un dispositif de couche 2 entre un routeur et un hôte pour qu'il puisse fonctionner en tant que serveur proxy afin de réduire la charge du routeur.

L'agent IGMP proxy envoie des paquets IGMP query à l'hôte et traite les paquets IGMP response envoyés par l'hôte. En outre, l'IGMP proxy répond aussi aux paquets query envoyés à partir du routeur, résume les messages que l'hôte envoie pour rejoindre ou quitter le groupe multicast, et en informe le routeur.

Pour l'hôte, l'agent IGMP proxy fonctionne comme un routeur. Et pour le routeur, l'agent IGMP proxy fonctionne comme un hôte.

5. Configuration type

Pour la configuration implémentée réellement, le service IPTV est configuré au niveau du MSAN en deux VLANs, VLAN 50 pour le flux multicast et le VLAN 60 pour le flux unicast. Cette configuration suit les étapes suivantes :

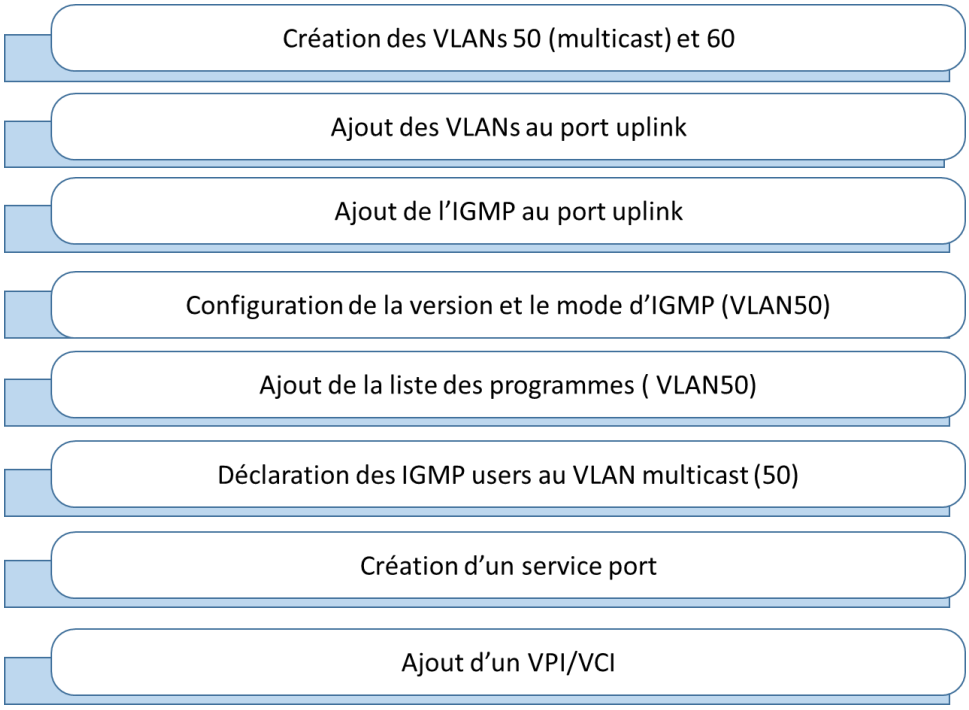

Figure 37: Etapes de configuration du VLAN de multicast au niveau du MSAN.

Pour s'assurer du bon fonctionnement de la solution existante, une simulation du service IPTV a été réalisée grâce au logiciel de simulation eNSP (entreprise Network Simulator Platform) qui est propriété de Huawei. Cette simulation tient en compte les différents protocoles implémentés réellement.

La chaîne 2M a pour adresse multicast 239.0.0.100 et la chaîne AL-Aoula 239.0.0.200.

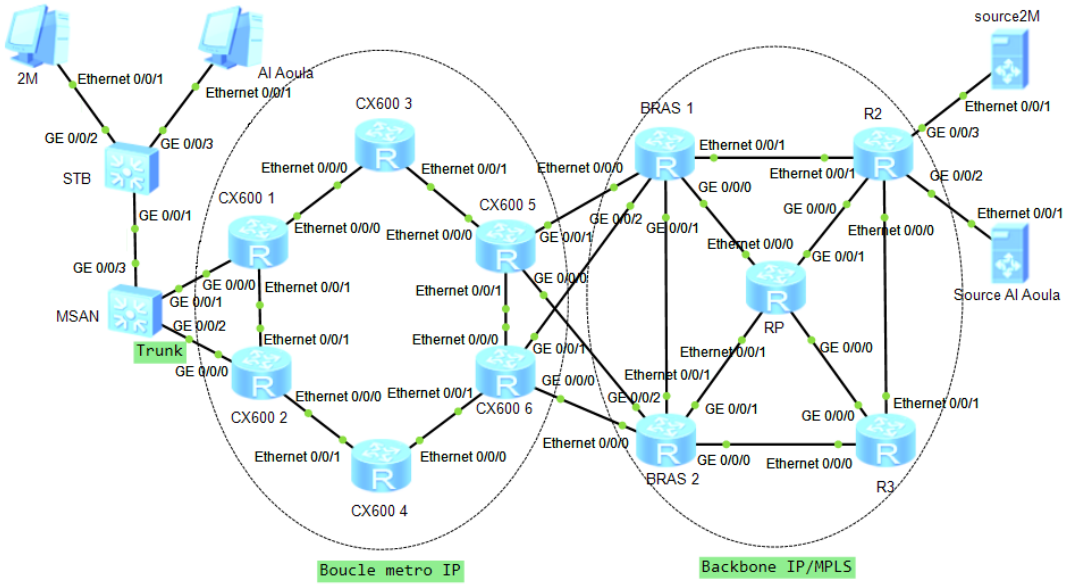

Figure 38: Simulation end-to-end de la solution IPTV.

Le protocole IS-IS est configuré comme IGP dans la boucle METRO IP et aussi dans le Backbone, chaque partie est une area pour le protocole IS-IS.

```
<Huawei>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 28        Routes : 36

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  ISIS-L1 15   10          D   192.168.3.2     GigabitEthernet
0/0/1
       10.0.0.0/24  ISIS-L2 15   30          D   192.168.12.1    GigabitEthernet
0/0/2
       20.0.0.0/24  ISIS-L2 15   20          D   192.168.12.1    GigabitEthernet
0/0/2
       30.0.0.0/24  ISIS-L2 15   20          D   192.168.1.1     Ethernet0/0/0
                    ISIS-L2 15   20          D   192.168.12.1    GigabitEthernet
0/0/2
       40.0.0.0/24  ISIS-L2 15   20          D   192.168.1.1     Ethernet0/0/0
       50.0.0.0/24  ISIS-L2 15   30          D   192.168.1.1     Ethernet0/0/0
       60.0.0.0/24  ISIS-L2 15   40          D   192.168.1.1     Ethernet0/0/0
                    ISIS-L2 15   40          D   192.168.12.1    GigabitEthernet
0/0/2
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     Ethernet0/0/0
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     Ethernet0/0/1
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/1
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet
0/0/1
```

Figure 39: Capture de la table de routage au niveau du BRAS 1.

```
<Huawei>dis multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry

 00001. (192.168.200.11, 239.0.0.100)
       Uptime: 00:01:25
       Upstream Interface: Register
```

Figure 40: Capture de la table de routage multicast dans le RP.

Cette dernière capture montre la création d'un arbre (S, G) qui a comme source l'adresse du serveur 192.168.14.2 et comme groupe 239.0.0.100.

6. Conclusion

Ce chapitre présente l'architecture end to end de la solution IPTV et les différents protocoles mis en places pour assurer son bon fonctionnement. Ce chapitre servira pour la compréhension et l'analyse des différents problèmes détectés au niveau de l'implémentation actuelle et les différentes solutions proposées dans le chapitre suivant.

Chapitre 4 : Solution proposée pour l'optimisation end-to-end de la solution IPTV

Après avoir préparé tous les outils nécessaires pour entamer le sujet de mon PFE, qui est l'optimisation de la solution IPTV déployée actuellement, une partie de cette solution sera ciblée et analysée afin de proposer une optimisation qui améliorera le fonctionnement du service IPTV.

1. Problématique

L'objectif de ce stage PFE est d'analyser de bout en bout l'architecture déployée actuellement pour en sortir les failles et proposer une solution faisable techniquement et d'un coût économiquement acceptable.

Après avoir analysé le principe du fonctionnement du multicast sur l'architecture existante, nous avons détecté un problème de partage de charge entre les deux routeurs CX600 de la boucle Metro IP. En effet, lorsque le protocole PIM est activé dans les routeurs de la boucle IPRAN et dans le Backbone MPLS, un mécanisme d'élection d'un DR est réalisé pour élire le routeur qui va transmettre le « PIM join » message au routeur RP. Sinon les deux routeurs CX600 interfacés avec le MSAN vont recevoir le « IGMP join » et vont générer tous les deux le « PIM join » à destination du RP, donc on aura par la suite deux copies du flux multicast, ce qui encombre la bande passante davantage.

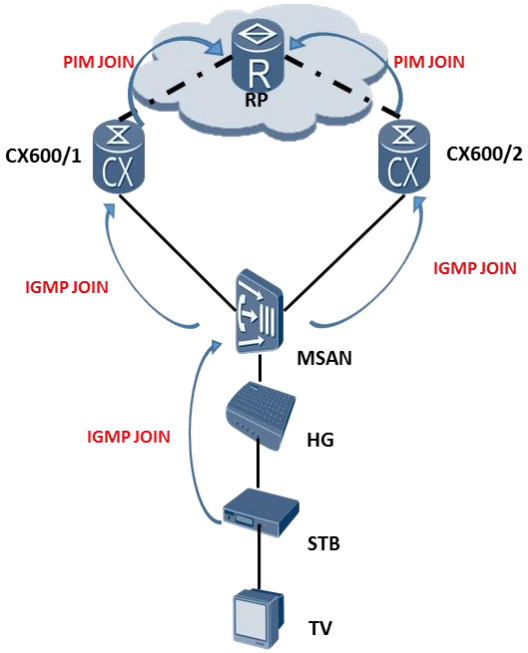

Figure 41: Mécanisme de jointure d'une chaîne.

Une fois le DR est élu (en se basant sur le routeur qui a la plus grande priorité et en cas d'égalité la plus grande adresse IP), c'est lui qui va transmette le PIM join message au RP et par la suite on aura un seul flux multicast envoyé au MSAN.

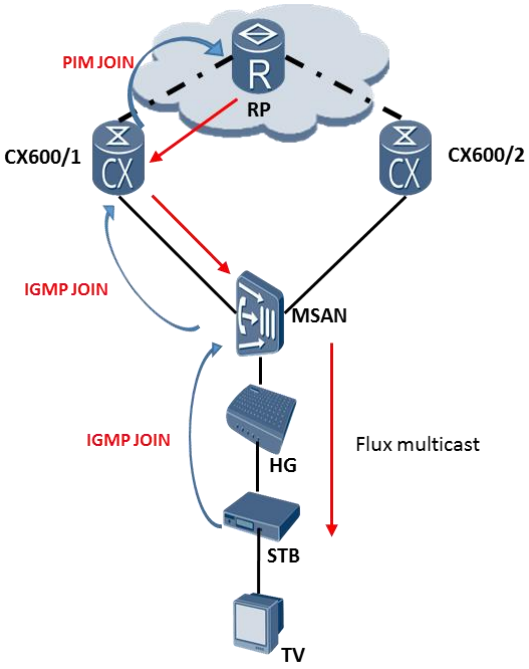

Figure 42: Passage du flux après élection du DR.

Donc si le STB demande n'importe quelle chaîne supportée dans la plateforme IPTV, le flux passera toujours à travers le DR élu, et le lien entre le MSAN et le deuxième routeur CX600 (Non DR) ne sera pas exploité. Cela présente un problème d'équilibrage de charge entre les deux routeurs CX600, surtout que Maroc Telecom vise à faire passer toutes les chaînes en HD et aussi à ajouter de nouvelles chaînes à la plateforme, ce qui demandera des besoins de plus en terme de bande passante et augmentera la charge du lien qui transporte la totalité du flux. D'où la nécessité de rendre le second lien opérationnel aussi et de partager la charge entre les deux routeurs.

2. Solution proposée pour le partage de la charge entre les CX600

La solution que nous avons proposée consiste à séparer les chaînes télévisées en deux VLANs, chaque VLAN sera servi par un routeur CX600 différent, ce qui assurera un partage de charge entre les deux routeurs d'extrémités.

Ce partage de chaînes entre les deux VLANs doit être optimal, pour cela on va utiliser le serveur UM de la plateforme IPTV pour récupérer les statistiques sur le taux d'audience des chaînes déployées dans la plateforme.

Pour la semaine du 18/04/2016 au 24/04/2016, et pour la durée du 19 :00h à 20 :00h, on remarque que c'est 2M qui se retrouve en tête des chaînes les plus regardées. Ces statistiques restent approximativement les mêmes pour les autres périodes de la journée.

Statistics of Weekly Total Viewing Time per BTV channel by region

2016-04-27 15:26:01

Week: 2016-04-18 ~ 2016-04-24 Region: Global
Time period: 19:00:00 ~ 20:00:00 Operator: iptv

Ranking	BTV Channel Name	Total viewing time	Percentage (%) viewing time per channel
1	2 M	6495,50	16,44%
2	Al Aoula	4586,92	11,61%
3	France 2	2952,26	7,47%
4	TF1	2451,07	6,20%
5	M6	1861,26	4,71%
6	Medi1 TV	1318,59	3,34%
7	Nickelodeon	1199,49	3,04%
8	Arryadia TNT	1180,38	2,99%
9	Cartoon Network	1113,56	2,82%
10	MBC4	915,62	2,32%
11	France 3	884,98	2,24%
12	France 24	691,32	1,75%
13	Boomerang	681,94	1,73%
14	Al Maghribia	573,87	1,45%
15	Nickelodeon Jr	548,73	1,39%
16	Saoudi-Quran	520,47	1,32%
17	TV5 Monde	502,62	1,27%
18	I Tele	487,40	1,23%

Tableau 5: Taux d'audience des chaînes télévisées d'IAM.

Le partage doit prendre en considération ces statistiques. En effet, les chaînes populaires ne doivent pas être regroupées dans le même VLAN, parce que si on fait ainsi un seul lien sera surchargé et l'autre lien sera intacte. Pour cela le partage de trafic sera en Zigzag, c'est-à-dire la chaîne de priorité 1 avec les chaînes de priorités impaires (2M – france2 – M6-….) et la chaîne de priorité 2 avec les chaînes de priorités paires (AL Aoula, TF1-, Medi1 TV,…).

La solution consiste à mettre deux VLANs, VLAN 50 pour la moitié des chaînes de priorité impaire et le VLAN 51 pour l'autre moitié de priorité paire.

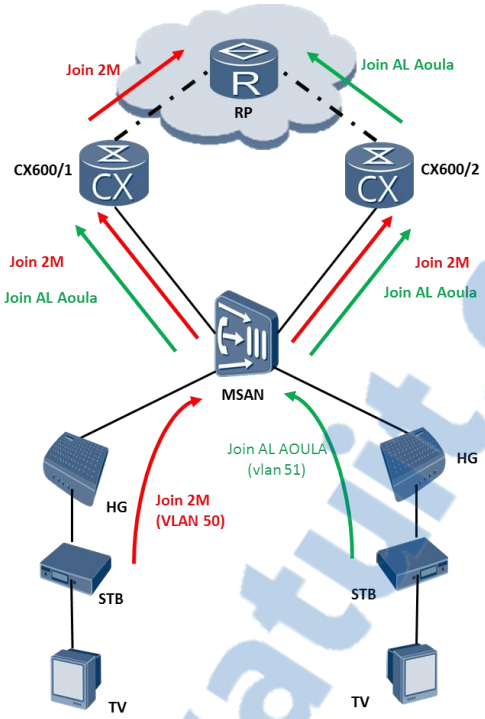

Figure 43: Description de la solution de partage de charge.

Reste maintenant à simuler cette solution à l'aide du logiciel eNSP pour tester son bon fonctionnement. L'architecture simulée est la suivante :

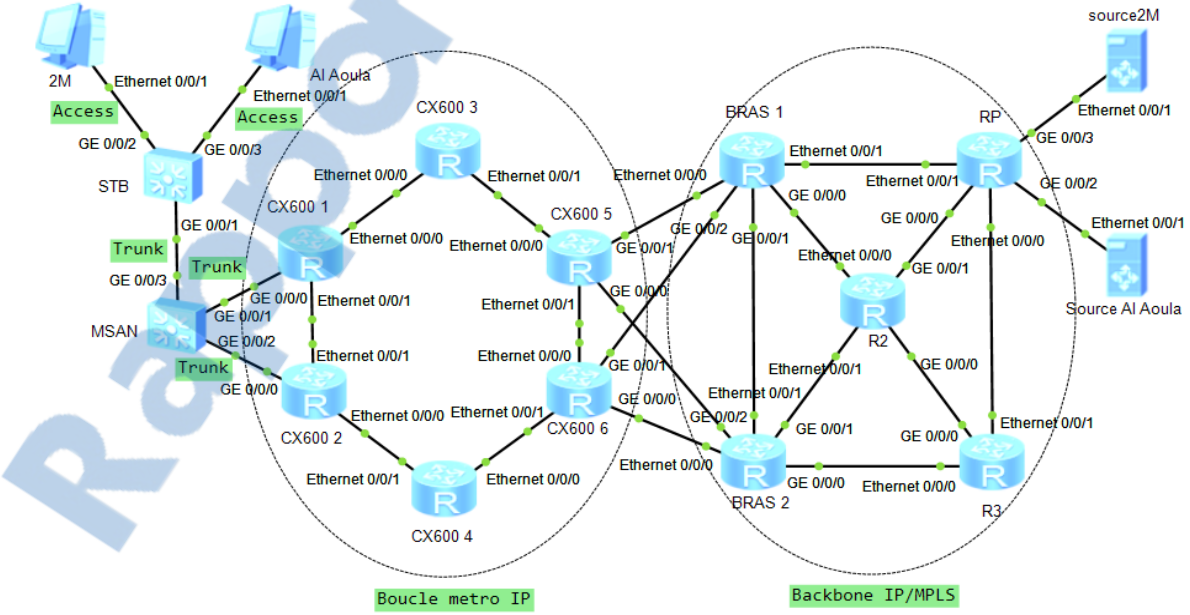

Figure 44: Architecture simulée pour tester la solution de partage de charge.

- Le STB permet de connecter une seule télévision de l'utilisateur final, cet utilisateur a le droit de joindre n'importe quelle chaîne si elle est inscrite dans son bouquet, quel que soit le VLAN auquel appartient cette chaîne. Pour cela nous avons simulé le STB par un switch qui est connecté à deux équipements qui représentent en réalité la même TV, pour simuler le fait de joindre des chaînes dans deux VLANs différents.
- La boucle IPRAN est représentée ici par six routeurs seulement, et le Backbone est allégé dans cette manipulation pour la simplifier.
- Dans la présente manipulation on va simuler une chaîne de chaque VLAN, 2M (239.0.0.100) du VLAN 50 et AL Aoula (239.0.0.200) du VLAN 51.

Etapes d'obtention du flux multicast :

1. Client1_2M appartient au VLAN 50, il envoi IGMPv2 report à l'adresse multicast de la chaîne 2M demandée 239.0.0.100.
2. Les deux routeurs CX600 de la boucle vont recevoir ce message, et seul le routeur élu DR du VLAN 50 va envoyer le PIM join. Ici nous avons forcé le CX600/1 à devenir DR pour le VLAN 50 en changeant sa priorité par la commande : **pim hello-option dr-priority** 150, cette commande est activée dans la sous interface eth0/0/0.50 (pour le CX600/2 la priorité pour la sous interface eth0/0/0.50 est 100). Le flux va donc passer par le CX600/1.
3. En arrivant au MSAN qui est un équipement couche 2, le flux multicast sera diffusé dans l'ensemble des ports. Pour éviter cela, l'IGMP Snooping est activé au niveau du MSAN. Le flux donc est envoyé au client qui l'a demandé.
4. Les mêmes étapes vont être suivies pour joindre AL Aoula en passant par le CX600/2 qui est configuré DR pour le VLAN 51.

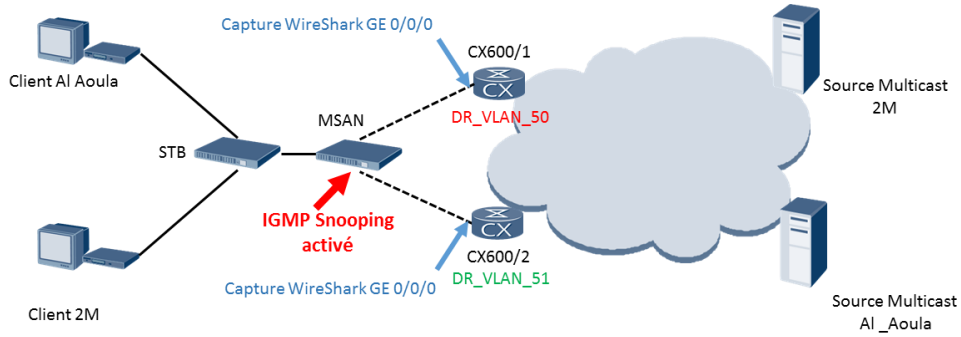

Figure 45: Specification du DR de chaque VLAN.

No.	Time	Source	Destination	Protocol	Length	Info
75	1970-01-01 03:18:35.683000	192.168.10.1	239.0.0.100	IGMPv2	50	Membership Report group 239.0.0.100
76	1970-01-01 03:18:35.715000	192.168.80.3	192.168.80.4	BFD Co…	70	Diag: No Diagnostic, State: Up, Flags: 0x00
77	1970-01-01 03:18:35.855000	192.168.10.4	192.168.10.3	BFD Co…	70	Diag: No Diagnostic, State: Up, Flags: 0x00
78	1970-01-01 03:18:35.980000	192.168.60.2	239.0.0.100	UDP	1374	5893 → 0 Len=1328
79	1970-01-01 03:18:35.980000	192.168.60.2	239.0.0.100	UDP	1374	5893 → 0 Len=1328
80	1970-01-01 03:18:35.980000	192.168.60.2	239.0.0.100	UDP	1374	5893 → 0 Len=1328
81	1970-01-01 03:18:35.980000	192.168.60.2	239.0.0.100	UDP	1374	5893 → 0 Len=1328
82	1970-01-01 03:18:35.980000	192.168.60.2	239.0.0.100	UDP	1374	5893 → 0 Len=1328

Figure 46: Capture à l'interface GE 0/0/0 du CX600/1.

No.	Time	Source	Destination	Protocol	Length	Info
13	4.07900000	80.0.0.1	224.0.0.1	IGMPv2	64	Membership Query, general
14	4.17200000	HuaweiTe_2e:3c:c2	Spanning-tree-(for-	STP	119	MST. Root = 32768/0/4c:1f:cc:2e:3c:c2 Cost
15	4.31300000	80.0.0.10	230.0.0.1	IGMPv2	50	Membership Report group 230.0.0.1
16	4.31300000	70.0.0.10	239.0.0.100	IGMPv2	50	Membership Report group 239.0.0.100
17	4.50000000	80.0.0.2	80.0.0.1	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
18	5.04700000	70.0.0.1	70.0.0.2	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
19	5.28200000	70.0.0.2	70.0.0.1	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
20	5.40700000	80.0.0.1	80.0.0.2	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
21	5.81300000	80.0.0.2	80.0.0.1	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
22	6.57900000	70.0.0.1	70.0.0.2	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
23	6.84400000	70.0.0.2	70.0.0.1	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
24	6.84400000	HuaweiTe_2e:3c:c2	Spanning-tree-(for-	STP	119	MST. Root = 32768/0/4c:1f:cc:2e:3c:c2 Cost
25	7.03200000	80.0.0.1	80.0.0.2	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
26	7.34400000	80.0.0.2	80.0.0.1	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00
27	7.84400000	70.0.0.1	70.0.0.2	BFD Cor	70	Diag: No Diagnostic, State: Up, Flags: 0x00

Figure 47: Capture sur l'interface GE 0/0/0 du CX600/2.

Pour tester le bon fonctionnement de cette solution, nous allons rendre le lien entre le CX600/1 et le MSAN non opérationnel en rendant l'interface eth0/0/0 du CX600/1 shutdown.

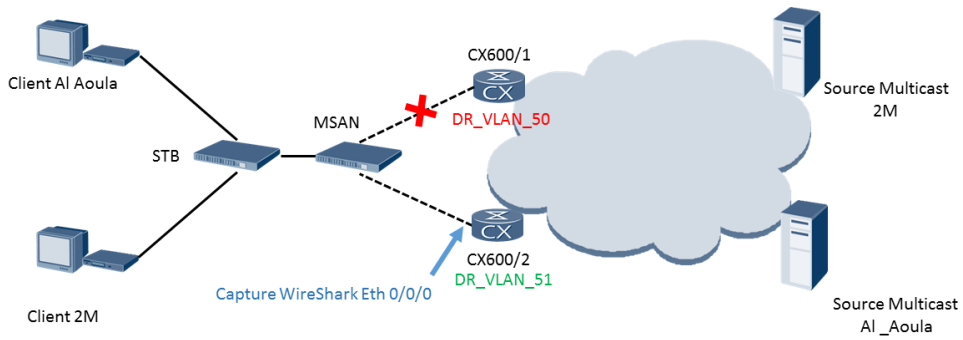

Figure 48: Simulation du basculement vers le nouveau DR.

No.	Time	Source	Destination	Protocol	Length	Info
91	103.390000	HuaweiTe_4b:2d:6b	ISIS-all-level-1-IS	ISIS	1514	L1 HELLO, System-ID: 0000.0000.0003
92	103.453000	50.0.0.1	224.0.0.13	PIMv2	76	Join/Prune
93	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
94	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
95	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
96	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
97	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
98	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
99	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
100	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
101	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
102	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
103	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
104	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0
105	103.984000	192.168.14.2	239.0.0.100	UDP	1370	Source port: cgms Destination port: 0

Figure 49: Capture du trafic sur l'interface Eth 0/0/0 du CX600/2.

D'après la capture, le trafic passe maintenant par le CX600/2 qui est devenu le nouveau DR pour le VLAN 50. En effet, le protocole PIM échange des messages Hello entre les deux interfaces du CX600 pour l'élection du DR (dans le LAN du MSAN). Au bout de 3*hello timer le CX600/2 se déclare DR parce qu'il n'a rien reçu de son voisin PIM.

Le Querier (celui qui a la plus petite adresse IP) va envoyer des messages « IGMPv2 Query-general » périodiquement (chaque 60s) pour s'assurer qu'il y a au moins un membre du groupe qui est encore intéressé par ce flux multicast. Tous les clients dans le LAN qui sont abonnés au même groupe vont recevoir ce message et ils vont déclencher un timer, le client dont le timer a expiré le premier va générer un « IGMPv2 report ». Ainsi le nouveau DR en recevant l'« IGMPv2 report » va envoyer le PIM join et le trafic sera envoyé aux clients.

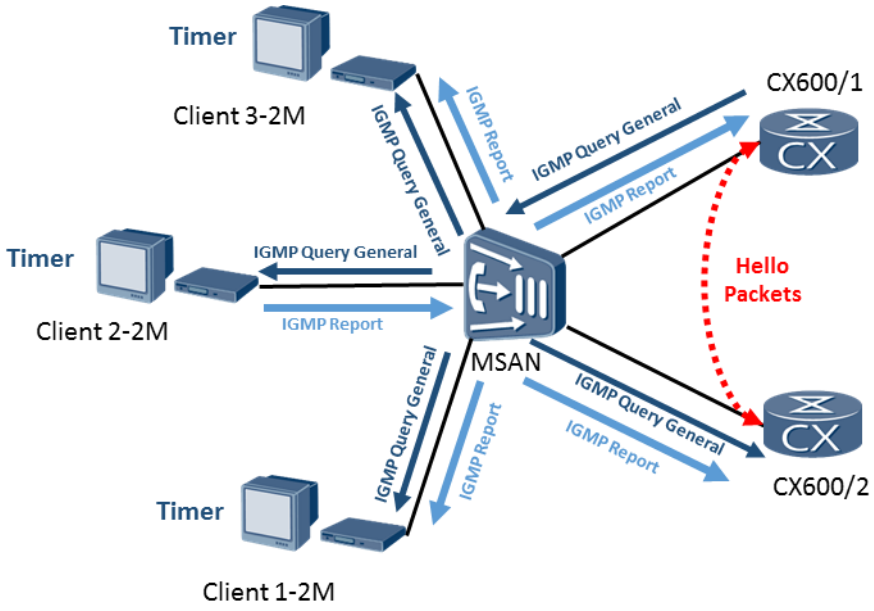

Figure 50: Principe de fonctionnement du protocole IGMP.

3. Solutions proposées pour l'optimisation réseau

3.1. Obtention d'adresse IP avec le protocole DHCP

La solution IPTV déployée actuellement est basée sur le protocole PPPoE pour l'obtention de l'adresse IP, le principal apport du PPPoE est le mécanisme d'authentification qui permet de s'assurer de l'identité du STB avant de le servir (allouer une adresse IP). Cependant, l'authentification des STB est assurée actuellement par le serveur ACS de la plateforme et non pas le protocole PPPoE.

Le protocole PPPoE qui a été introduit pour son mécanisme d'authentification, présente des inconvénients, parmi lesquels :

- Etablissement de la session PPPoE entre le STB et le BRAS, ce qui nécessite le passage par le BRAS pour le transport du flux unicast et par la suite causera l'encombrement du BRAS.
- La nécessité de configurer la boucle Metro IP en VPLS pour pouvoir transporter les paquets couche 2 du PPPoE.
- Complexité du troubleshooting d'un protocole coche 2.

Pour contourner ces points faibles du protocole PPPoE, nous avons proposé de le remplacer par le protocole DHCP. En effet, nous allons nous servir du serveur DHCP présent dans la plateforme IPTV pour allouer les adresses IP aux STBs, en configurant le DHCP Relay et le VRRP au niveau du CX600/1 et CX600/2. Le protocole DHCP est présenté dans l'annexe D.

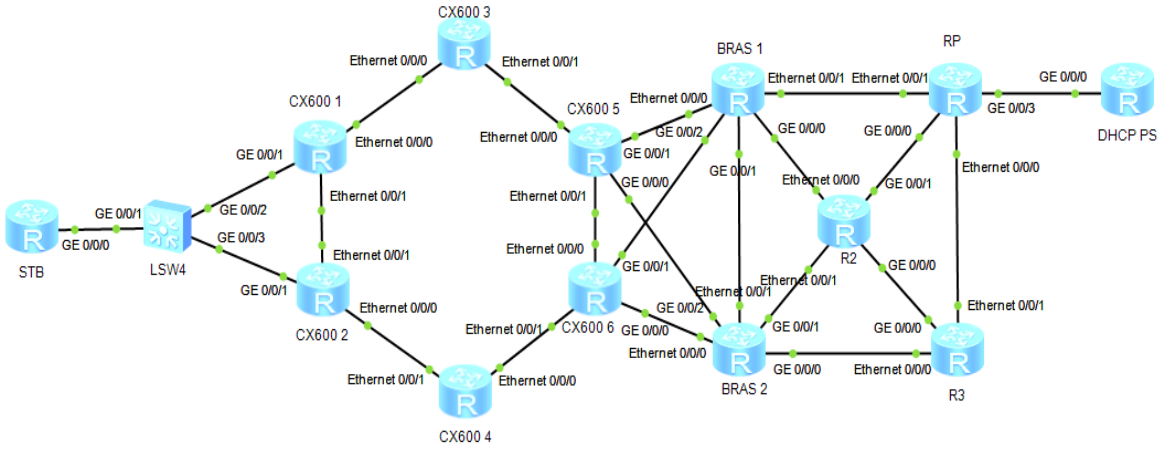

Figure 51: Simulation du protocole DHCP.

La capture suivante montre le résultat :

No.	Time	Source	Destination	Protocol	Length	Moving Picture Experts Group	Info
148	77.859000000	HuaweiTe_d4:20:34	ISIS-all-level-1-IS	ISIS HELLO	1514		L1 HELLO, System-ID: 0000.0000.0002
149	78.328000000	90.0.0.1	224.0.0.18	VRRP	60		Announcement (v2)
150	78.656000000	0.0.0.0	255.255.255.255	DHCP	342		DHCP Discover - Transaction ID 0x3dfff56f
151	79.015000000	192.168.200.10	90.0.0.254	DHCP	342		DHCP Offer - Transaction ID 0x3dfff56f
152	79.015000000	0.0.0.0	255.255.255.255	DHCP	342		DHCP Request - Transaction ID 0x3dfff56f
153	79.234000000	192.168.200.10	90.0.0.254	DHCP	342		DHCP ACK - Transaction ID 0x3dfff56f
154	79.265000000	HuaweiTe_f1:1e:15	Broadcast	ARP	60		Gratuitous ARP for 90.0.0.254 (Request)
155	79.344000000	90.0.0.1	224.0.0.18	VRRP	60		Announcement (v2)

Figure 52: Capture sur l'interface GE0/0/0 du STB.

3.2. Minimisation du délai d'acheminement du trafic multicast

Lors du zapping entre les chaînes, on remarque parfois un crachement d'image qui est dû au fait que le serveur FCC peut arrêter l'envoi du flux unicast avant que le flux multicast soit délivré par la source. Ce comportement du FCC est dû au fait que le serveur FCC ne peut pas attendre le flux multicast à une durée supérieur à 2,5 secondes, il arrête le flux sans attendre la réception d'un acquittement de la part du STB.

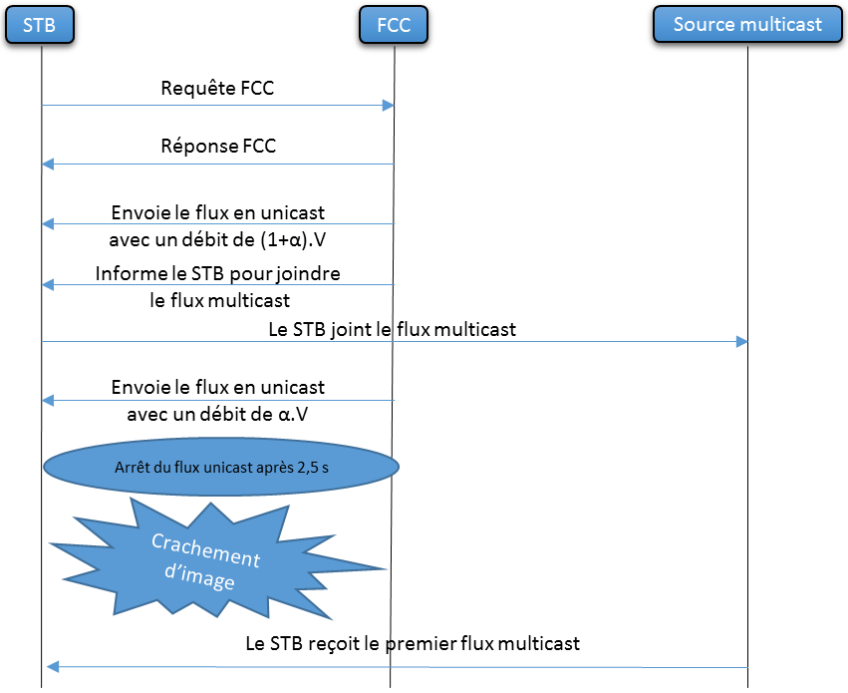

Figure 53: Mécanisme du Zapping.

Pour cela la solution Préjoin a été mise en place. Il s'agit de demander statiquement les chaînes populaires au niveau des deux CX600 interfacés avec le MSAN, ainsi le flux sera présent au niveau des CX600 au lieu d'aller le demander à la source multicast, ce qui diminuera le temps d'acheminement du trafic.

Le choix du préjoin au niveau du CX600 et non pas au niveau du MSAN est expliqué par les deux motifs suivants :

- Ne pas surcharger le lien entre le CX600 et le MSAN et optimiser la bande passante.
- La probabilité pour qu'un utilisateur demande le flux par CX600 est supérieur à la probabilité qu'un utilisateur le demande par MSAN.

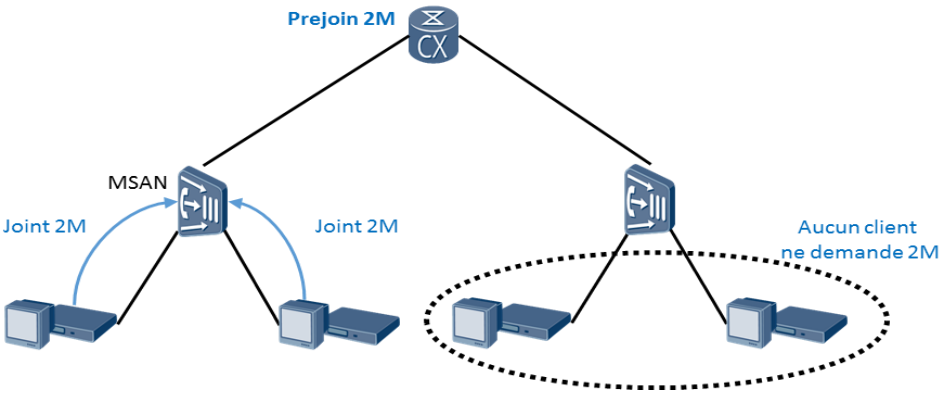

Figure 54: Demande d'une chaîne par MSAN.

La simulation de cette solution a été basée sur la même architecture donnée précédemment :

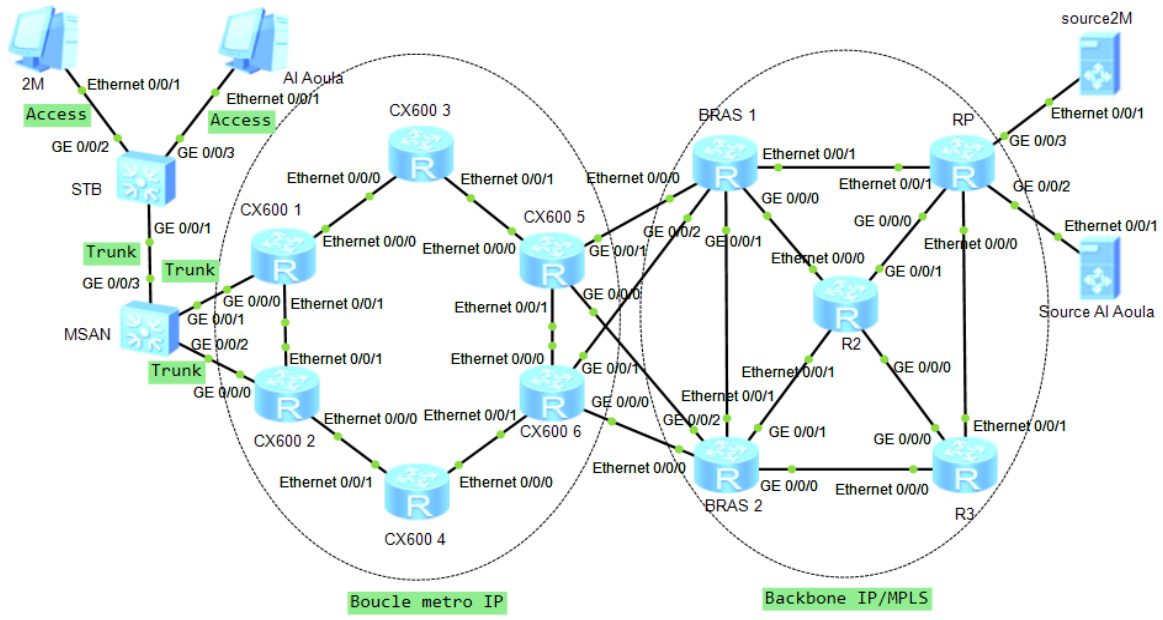

Figure 55: Configuration du prejoin au niveau du CX600/1 et du CX600/2.

La demande statique de 2M et AL-Aoula est configurée au niveau du CX600/1 et CX600/2 par la commande : **igmp static-group** 239.0.0.100**, igmp static-group** 239.0.0.200.

La capture montre que le trafic est présent au niveau du CX600/1 avant qu'un STB demande de joindre la chaîne 2M par exemple.

No.	Time	Source	Destination	Protocol	Length	Moving Picture Experts Group	Info
2669	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2670	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2671	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2672	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2673	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2674	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2675	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2676	24.516000000	192.168.14.2	239.0.0.200	UDP	1370		Source port: 9743 Destination port: 0
2677	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2678	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2679	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2680	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2681	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2682	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0
2683	24.578000000	192.168.200.11	239.0.0.100	UDP	1370		Source port: 8984 Destination port: 0

Figure 56: Capture sur l'interface Eth0/0/0 du CX600/1.

4. Conclusion

Ce chapitre constitue le cœur de mon stage PFE, il cible le raccordement de la partie accès avec le réseau d'IAM, en cherchant à optimiser la bande passante allouée au service IPTV et ce en partageant la charge entre les deux routeurs CX600 de la boucle METRO IP interfacés avec le MSAN.

Conclusion générale

Ce rapport synthétise le travail de cinq mois de stage au sein de Huawei Technologies, qui a été réalisé sous l'intitulé « Optimisation end-to-end de la solution IPTV de Huawei Technologies ».

Suite à l'étude détaillée de la solution IPTV déployée actuellement par Huawei pour le compte de Maroc Telecom, plusieurs limitations ont été remarquées. Pour cela la mission maitresse de ce stage était de chercher une alternative et compléter les insuffisances de cette solution.

Pour atteindre cette fin, j'ai été amené, dans un premier lieu, à établir une étude de la plateforme IPTV qui est responsable de la transformation du flux DVB en un flux IP multicast, et de la gestion du flux multimédia. Par la suite, j'ai élaboré une étude détaillée de la solution existante en parcourant tous les protocoles utilisés réellement, puis je me suis focalisé sur le problème de partage de charge entre les routeurs CX600 interfacés avec le MSAN afin d'en trouver une solution faisable techniquement. Et finalement j'ai proposé d'autres optimisations complémentaires pour assurer une meilleure qualité et une disponibilité continue du service.

Ce projet m'a permis d'élargir mes connaissances et de renforcer mes compétences dans le domaine des réseaux. Il m'a été aussi une occasion pour découvrir le métier de l'ingénieur réseau et surtout celui d'un ingénieur de maintenance en réseau, qui doit localiser et diagnostiquer rapidement les alarmes. Cette tâche n'est pas toujours facile, car elle nécessite un troubleshooting approfondi de tous les éléments du réseau.

Comme perspective j'envisage de faire l'étude de la migration complète du service IPTV sur IPv4 vers IPTV sur IPv6, vue que la migration vers tout IPv6 est actuellement la préoccupation de tous les opérateurs marocains qui cherchent à transporter tous leurs services à travers un réseau totalement en IPv6.

Bibliographies

[1]. IPTV Solution. Huawei Internal.

[2]. ODC020001 IP Multicast Basis ISSUE1.2 Huawei Internal.

[3]. ODC020002 IGMP Protocol Principle ISSUE1.2 Huawei Internal.

[4]. ODP500019 PIM-SM Protocol Principle ISSUE1.0_20061229_A Huawei Internal

[5]. PPPoE Protocol. Huawei Internal.

[6]. VDSL2 Technical Training -20100713-A. Huawei Internal.

[7]. ME60 Feature Description-IP Multicast (V600R005C00_02). Huawei Internal.

[8]. Huawei IPTV System NMS Training Slides. Huawei Internal.

[9]. Huawei IPTV Solution V100R003C28 System Description. Huawei Internal.

[10]. Configuration Guide - Basic Configurations (V800R002C01_01).

[12]. Configuration Guide - IP Routing (V100R006C00_01 & V200R002C00_02).

[13]. Configuration Guide – MPLS (V100R006C01_01 & V600R003C00_02 & V800R002C01_01).

[14]. Huawei, MA5600T Feature Description (V800R007C01_06, MSAN).

[15]. CCIE Routing and switching v5.0 –volume 2-.

[16]. Les tunnels point à point – Christian Caleca-.

[17]. Huawei BFD principles. Huawei Internal.

[18]. Huawei GPON Training Slides. Huawei Internal.

Acronymes

A

AAA: Authentication, Authorization, Accounting
AAL: ATM Adaptation Layer
AC: Access Concentrator
ACS: Application Control Server
ADSL: Asymmetric digital subscriber line
AES: Advanced Encryption Standard
AGG: Aggregation
ARP: Address Resolution Protocol
ARPU: Average Revenue Per Unit
ATM: Asynchronous Transfer Mode

B

B-Frame: Bidirectional Frame
BCP: Bridge Control Protocol
BFD: Bidirectional Forwarding Detection
BGP: Border Gateway Protocol
BMS: Business Management Subsystem
BRAS: Broadband Remote Access Server
BSC: Base Station Controller
BSR: BootStrap Router
BTS: Base Transceiver Station
BTV: Broadcast Television

C

CA: Conditional Access
CAT: Conditional Access Table
CCT: Channel Change Time
CDN: Content Delivery Network
CE: Customer Edge
CHAP: Challenge Handshake Authentication Protocol
CIS: Content Injection Subsystem
CLNP: Connectionless Network Protocol
CMI : Content Management Interface
CMS: Content Management System
CRC: Cyclic Redundancy Code
CS: Central Server
CSNP: Complete Sequence Number PDU

D

DBA: Dynamic Bandwidth Assignment
DIS: Designated IS
DHCP : Dynamic Host Configuration Protocol
DNS: Domain Name System
DR: Designated Router
DSL: Digital Subscriber Line
DSLAM: Digital Subscriber Line Access Multiplexer
DVB: Digital Video Broadcast

E

ECS: EPG Control Subsystem
EDS: EPG Distributing Server
EIGRP: Enhanced Interior Gateway Routing Protocol
eNSP: enterprise Network Simulation Platform
EPG: Electronic Program Guide

ES: Edge Server

F

FAX: télécopieur
FCC: Fast Channel Change
FCS: Frame Check Sequence
FEC: Forward Error Correction
FEC: Forwarding Equivalent Class
FIB: Forwarding Information Base
FTTB: Fiber To The Building
FTTC: Fiber To The Curb
FTTH: Fiber To The Home
FTTx: Fiber To The x

G

G.SHDSL: Global.Standard High-Bit-Rate Digital Subscriber Line
GE: Gigabit Ethernet
GEM: Gpon Encapsulation Method
GoP: Group of Pictures
GPON: Gigabit Passive Optical Network

H

HD: High Definition
HDSL: High-bit-rate Digital Subscriber Line
HE: HeadEnd
HG: Home Gateway
HMS: Huawei Media Server
HSI: High Speed Internet

I

I-Frame: Intracoded Frame
IAM: Ittisalat Al Maghreb
ICT: Information and Communication Technology
IGMP: Internet Group Management Protocol
IGP: Interior Gateway protocol
IOS: Internetwork Operating System
IP: Internet Protocol
IPCP: Internet Protocol Control Protocol
IPRAN: internet Protocol Radio Access Network
IPTV: Internet Protocol Television
IPv6: Internet Protocol version 6
IPX: Internetwork Packet Exchange
IPXCP: Internetwork Packet eXchange Control Protocol
IRD: Integrated Receiver and Decoder
IS: Intermediate system
IS-IS: Intermediate system to Intermediate system
iVSE: integrated Value-added Service Enhancement

L

L3VPN: Layer 3 Virtual Private Network
LAN: Local Area Network
LCP: Link Control Protocol
LCP: Link Configuration Packet
LDP: Label Distribution Protocol
LER: Label Edge Router
LFIB: Label Forwarding Information Base
LIB: Label Information Base
LLC: Logical Link Control
LMP: Link Maintenance Packet

LNB: Low Noise Block converter
LSDB: Link-State Database
LSP: Label Switched Path
LSP: Link State Packet
LSR: Label Switch Router
LTP: Link Termination Packet

M

MAC: Medium Access Control
MC: Media Content
MDN: Media Delivery Network
MDU: Multiple Dwelling Unit
MEM: Media Entertainment Middleware
MM: Media Manager
MP2MP: Multipoint-to-Multipoint
MPEG-2: Moving Picture Experts Group 2
MPEG-4: Moving Picture Experts Group 4
MPEG-TS: Moving Picture Experts Group Transport Stream
MPLS: Multiprotocol Label Switching
MP-BGP: Multiprotocol BGP
MRF: Media Relay Frame
MSAN: Multiservice Access Node

N

NCP: Network Control Protocol
NIT: Network Information Table
NGN: New Generation Networks
NMS: Network Management System
NSAP: Network Service Access Point
NT: Network Technologies

O

ODN: Optical Distribution Network
OLT: Optical Link Terminal
ONU: Optical Line Unit
OSI: Open Systems Interconnection
OSPF: Open shortest path first

P

P: Provider
P-Frame : Predicted Frame
P2P: Pear to Pear
PAD: PPPoE Active Discovery
PADI: PPPoE Active Discovery Initiation
PADO: PPPoE Active Discovery Offer
PADR: PPPoE Active Discovery Request
PADS: PPPoE Active Discovery Session-confirmation
PADT: PPPoE Active Discovery Termination
PAP: Password Authentication Protocol
PAT: Program Associate Table
PC: Personal Computer
PDU: Packet Data Unit
PE : Provider Edge
PFE : Projet de Fin d'Etude
PHB: Pen-Ultimate Hop Popping
PID: Program Identifier
PIM: Protocol Independent Multicast
PIM-DM: PIM Dense Mode
PIM-SM: PIM Sparse Mode

PIM-SSM: PIM Source Specific Multicast
PIP: Picture In Picture
PMS: Product Management Subsystem,
PMT: Program Map Table
PON: Passive Optical Network
POTS: Plain Old Telephone Service
PPP: Point to Point Protocol
PPPoA: Point to Point Protocol over ATM
PPPoE: Point to Point Protocol over Ethernet
PPPoE+: Point to Point Protocol over Ethernet Plus
PRC: Partial Route Computation
PSI: Program-Specific Information
PSNP: Partial sequence number PDU
PVR: Personal Video Recorder

Q

QoS: Quality of Service
QPSK: quadrature phase shift keying

R

RD: Route Distinguisher
RET: RETransmission
RFC: Request For Comment
RIB: Routing Information Base
RNC: Radio Network Controller
RNIS: Réseau numérique à intégration de services
RP: Rendezvous Point
RPF: Reverse Path First
RRS: Request Routing Server
RSVP-TE: Resource Reservation Protocol-Traffic Engineering
RT: Route Target
RTCP: Real-time Transport Control Protocol
RTP: Real-time Transfer Protocol

S

SD: Standard Definition
SDI: Synchronous Digital Interface
SDSL: Symmetric Digital Subscriber Line
SHDSL: Single-pair High-speed Digital Subscriber Line
SMS: Subscriber Management System
SN: Sequence Number
SQM: Service Quality Manager
SPF: Shortest Path first
SPT: Shortest Path Tree
STB: Set Top Box

T

T-CONT: Transmission Container
TCP: Transmission Control Protocol
TDMA: Time division multiple access
TE: Traffic Engineering
TLV: Type Length Value
TS: Transport Stream
TSoIP: Transport Stream over Internet Protocol
TSTV: Time Shift TV
TTL: Time to live
TV: Television
TVMS: TV Message System
TVoD: Television on Demand

U

UDP: User Datagram Protocol
UM: Usage Mediator

V

VCI: Virtual Channel Identifier
VDSL: very-high-bit-rate Digital Subscriber Line
VLAN: virtual local area network
VoD: Video on Demand
VoIP: Voice over IP
VRF: Virtual Routing and Forwarding
VPLS: Virtual Private LAN Service
VPN: Virtual Private Network
VPI: Virtual Path Identifier
VRRP: Virtual Router Redundancy Protocol

W

WDM: Wavelength-division multiplexing

X

xDSL: x Digital Subscriber Line

ANNEXE -A- PPP

Point to Point Protocol (PPP) ou Le protocole Point à Point propose une méthode standard pour le transport de datagrammes multiprotocoles sur une liaison simple point à point.

PPP comprend trois composants principaux :

- Une méthode pour l'encapsulation

L'encapsulation PPP permet le multiplexage de différentes connexions protocolaires, au niveau réseau, simultanées sur la même liaison physique. Cette encapsulation a été conçue dans l'exigence d'une excellente compatibilité avec la plus grande variété de matériels.

- Protocole de contrôle de liaison (LCP)

Afin d'être suffisamment souple pour pouvoir être porté dans de nombreux environnements, le protocole PPP dispose d'un protocole de contrôle de liaison. Le LCP est utilisé pour effectuer la négociation automatique des options de format, la gestion de la taille variable des paquets, la détection d'une boucle de liaison ainsi que d'autres erreurs courantes de configuration. Il gère, de même, la rupture de liaison. Les autres fonctionnalités apportées concernent l'authentification de l'identité de l'hôte dans lequel il est implémenté, ainsi que la détection de fautes de fonctionnement sur la liaison.

Les trames LCP :

- Trame LCP d'établissement de liaison. (LCP)
- Trame LCP de fermeture de liaison. (LTP)
- Trame LCP de maintenance de liaison. (LMP)

- Protocole de gestion réseau (NCP)

Une famille de protocoles de contrôle du réseau pour l'établissement et la configuration de plusieurs protocoles de la couche "réseau" :

- IPCP (Internet Protocol Control Protocol).
- IPXCP (Internetwork Packet eXchange Control Protocol).
- BCP (Bridge Control Protocol).

Une trame PPP est de la forme :

Drapeau	Adresse	contrôle	Protocole	Données	FCS
1 octet	1 octet	1 octet	2 octets	Taille variable	2 ou 4 octets

Figure 57: Forme d'une trame PPP. [16]

- **Drapeau** : Indicateur de début ou fin de trame (Valeur = 01111110).
- **Adresse** : Adresse de Broadcast standard (Valeur = 11111111), car PPP n'attribue pas d'adresse d'hôte (Couche 2).
- **Contrôle** : Fourniture d'un service non orienté connexion (Valeur = 00000011).
- **Protocole** : Identification du protocole encapsulé (IP, IPX, etc.).
- **Données** : Contient soit la valeur zéro, soit des données (1500 octets maximum).
- **FCS** : Séquence de contrôle de trame pour une vérification des erreurs.

Le lien PPP rencontre un certain nombre d'états, dans les processus de configuration, de maintien et de clôture d'une liaison point-à-point. Le diagramme suivant décrits brièvement ces états.

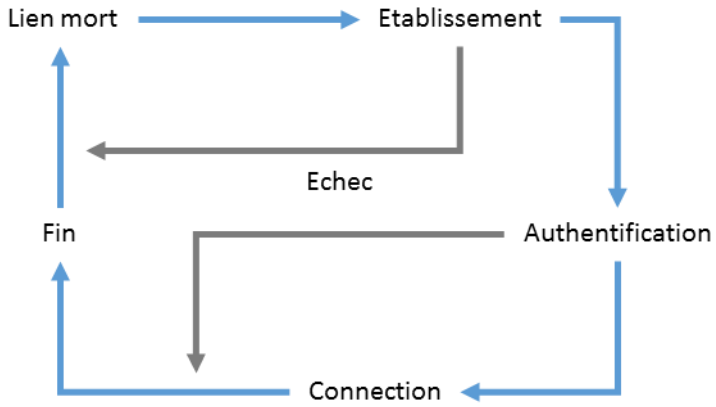

Figure 58: Diagramme d'états de la session PPP. [16]

- Lien mort (Couche physique non prête)
  Une communication débute et se termine nécessairement dans cet état. Lorsqu'un événement extérieur (comme une détection de porteuse ou la configuration par l'administrateur réseau) indique que le niveau physique est en état pour un processus de connexion, PPP passera la liaison en phase d'établissement.

- Establishment de lien
  Le protocole de liaison (LCP) est utilisé pour établir la connexion grâce à l'échange de paquets de Configuration. Cet échange est totalement résolu, et le mécanisme LCP entre dans l'état Ouvert, lorsque des paquets d'acquittement sont reçus des deux côtés.

- Authentification
  Sur certaines liaisons il peut être pertinent d'imposer une authentification du correspondant avant de permettre toute négociation protocolaire au niveau réseau. Il y a deux types d'authentification :

  - PAP : protocole d'identification par mot de passe. Il fonctionne de la même manière qu'un identifiant normal où le client s'authentifie en envoyant au serveur son nom d'utilisateur et son mot de passe (optionnellement crypté). Le serveur comparera ces données à ceux stockées dans une base de données secrète. Cette technique est vulnérable devant les attaques individuelles et les erreurs.
  - CHAP : Consiste en une vérification périodique de l'identité de l'utilisateur basée sur une clé secrète partagée entre le client et le serveur. Le serveur envoi au client un défi (une valeur aléatoire), le client en recevant ce défi déduit l'empreinte qui est calculée grâce à une fonction de hachage appliquée sur le défi et la clé et l'envoi au serveur qui la compare avec l'empreinte qu'il a calculé lui. Si c'est identique, le client est authentifié.

- Connection (Phase de négociation réseau)
  Une fois que PPP a achevé les procédures précédentes, chaque protocole réseau (tels qu'IP, IPX, ou AppleTalk) doit être configuré séparément via un protocole NCP. Chaque NCP devrait pouvoir être Ouvert et Fermé à tout moment.

- Fin de la liaison (Fermeture de liaison)
  PPP peut fermer la liaison à tout moment. Ceci peut survenir suite à une perte de porteuse, l'échec d'une authentification, la détection d'une qualité de liaison insuffisante, la chute d'une temporisation d'attente, ou la fermeture de la liaison décidé par l'administrateur réseau.

ANNEXE -B- PPPoE

Le protocole PPP fonctionne pour les liaisons point à point. Mais il n'est pas applicable pour le Broadcast Ethernet et tout autre réseau d'accès multipoint. De ce fait, Le protocole PPPoE a été mis en place.

PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de connecter un réseau d'hôtes (clients) à un concentrateur « AC » (serveur). Il assure non seulement l'accès des utilisateurs Ethernet avec un moyen d'accès à large bande, mais fournit aussi des solutions pratiques de contrôle d'accès et de traçabilité.

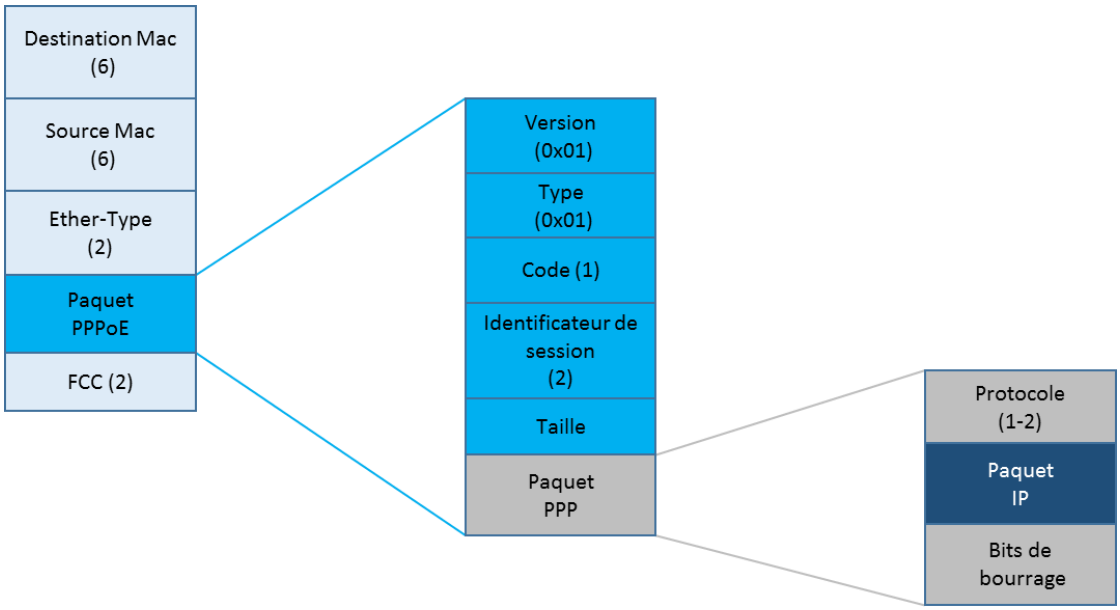

Figure 59: Forme du paquet PPPoE. [5]

Une session PPPoE passe par deux étapes différentes : étape de découverte « discovery stage » et étape de la session PPP « PPP session stage ».

Chaque utilisateur doit établir une unique session PPP. Mais avant cela, l'hôte doit connaître l'adresse MAC du serveur et cela se fait dans l'étape de découverte.

- l'étape de la découverte :
  Cette étape permet à un hôte de découvrir tous les ACs et d'en choisir ensuite un.
  Cette étape s'effectue en quatre sous étapes :
  - Emission en broadcast d'un paquet d'initialisation (PADI) par l'hôte.
  - Emission de paquets d'offres (PADO) en unicast par un ou plusieurs serveurs.
  - Emission en unicast d'un paquet de requête de session (PADR) par l'hôte.
  - Emission d'un paquet d'acquittement (PADS) par le serveur.

- Les différents types de paquets de l'étape de la découverte :
  - Le paquet Initialisation (PADI) :
    L'hôte envoie ce paquet en Broadcast, le champ « identificateur de session » doit contenir 0x0000 et le champ « code » est mis à 0x09. Il doit contenir un TAG « non de service » qui indique le service que l'hôte demande. Le PADI entier (l'entête PPPoE incluse) ne doit pas dépasser 1484 octets pour laisser suffisamment d'espace à un agent relais pour ajouter un TAG « Identificateur de session relais »

  - Le paquet Offre (PADO) :
    Quand un serveur reçoit un paquet PADI qu'il peut servir, il répond en envoyant un paquet PADO en unicast. Le champ « code » est mis à 0x07 et le champ « identificateur de session » doit contenir 0x0000. Le PADO doit contenir un TAG nom du serveur, un TAG « non du service » identique à celui du PADI et d'autres TAGs du nom de service indiquant des services que le serveur peut offrir. Si le serveur ne peut pas servir le PADI, il ne doit pas répondre avec un PADO.

  - Le paquet Requête (PADR) :
    Puisque le PADI est envoyé en Broadcast par l'hôte, ce dernier peut recevoir plus d'un PADO. Il en choisit donc un selon le non du serveur ou selon le service offert. L'hôte envoie alors en unicast un paquet PADR au serveur qu'il a choisi. Le champ «identificateur de session » doit contenir 0x0000 et le champ « code » est mis à 0x19. Le PADR doit contenir exactement un TAG de type « nom du service » qui indique le service que l'hôte demande, et un nombre quelconque de TAGs d'autres types.

  - Le paquet Confirmation de Session (PADS) :
    Quand le serveur reçoit un paquet PADR, il prépare le commencement d'une session PPP. Il génère un « identificateur de session » unique pour la session PPPoE et répond l'hôte par un paquet PADS envoyé en unicast. Le champ « identificateur de session » doit contenir la valeur unique générée pour la session PPPoE et le champ « code » est mis à 0x65. Le PADS contient exactement un TAG de type « nom de service » qui indique le service pour lequel le serveur a accepté la session PPPoE, et un nombre quelconque de TAGs d'autres types. Si le serveur n'accepte pas le « non de service » demandé dans le PADR. Il doit répondre dans ce cas par un PADS qui contient un TAG de type « nom de service-Erreur » (et un nombre quelconque de TAGs d'autres types). « L'identificateur de session » doit alors être mis à 0x0000.

  - Le paquet Terminaison (PADT):
    Ce paquet peut être envoyé à tout moment après l'établissement de la session pour indiquer que celle-ci est terminée. Il peut être envoyé, soit par l'hôte ou par le serveur, en unicast. Le champ « code » est mis à 0xa7, et «l'identificateur de session » doit indiquer quelle session est à terminer. Aucun TAG n'est nécessaire. Quand un PADT est reçu, aucun autre trafic utilisant cette session PPP ne peut être envoyé. Même les paquets normaux PPP de fin de la liaison ne peuvent être envoyés après l'envoie ou la réception d'un PADT. Une extrémité PPP devrait utiliser le PPP lui-même pour arrêter une session PPPoE, mais le paquet PADT peut être utilisé quand PPP ne le peux pas.

Après l'acquittement, on passe à l'étape suivante qui est l'étape de la session PPP

- l'étape de la session PPP :
  Lors de l'ouverture de la session PPPoE, Les données PPP sont envoyées de la même manière que pour toute autre communication PPP.

Le schéma suivant résume les étapes citées ci-dessus :

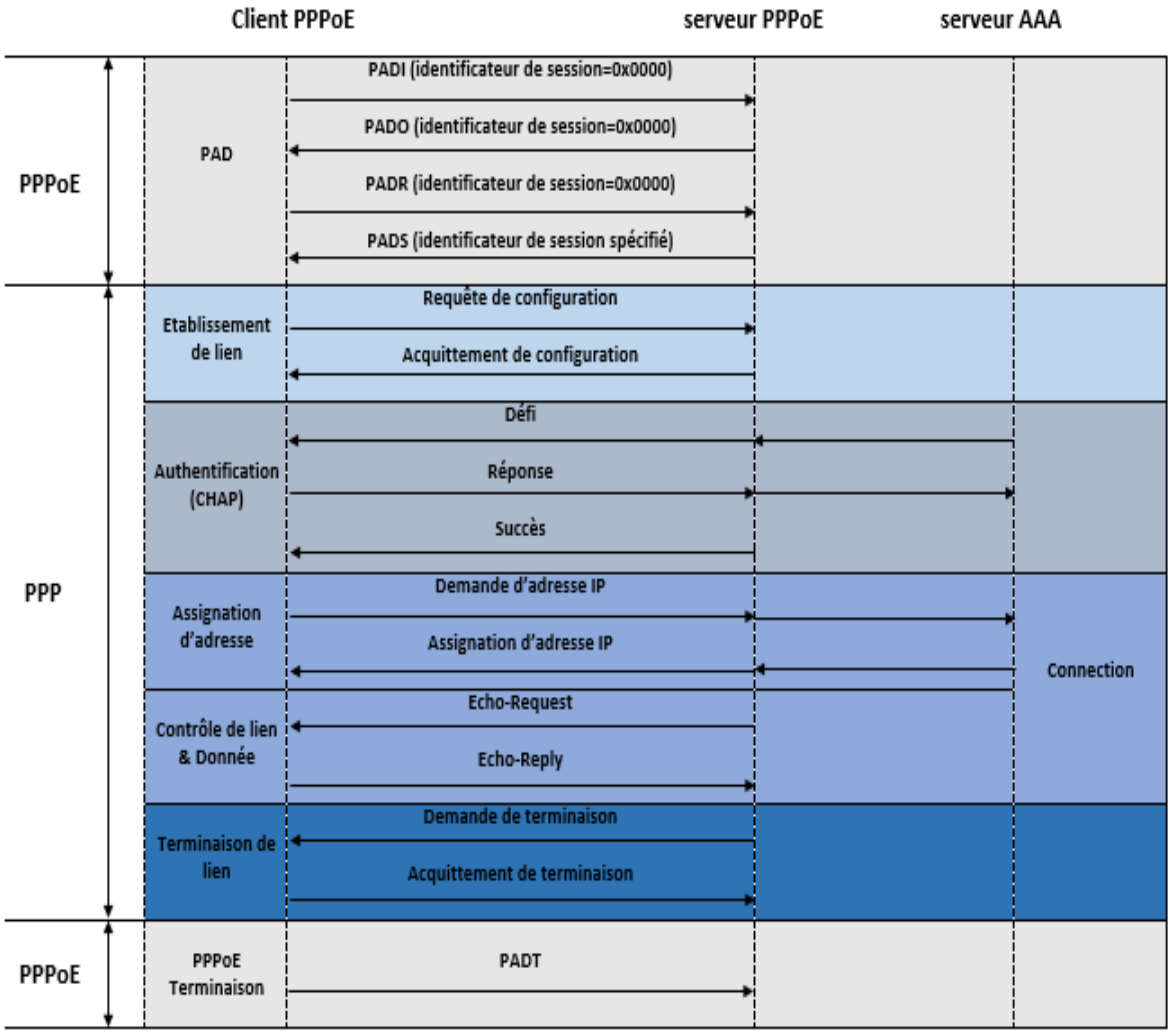

Figure 60: Cycle de vie d'une session PPPoE. [5]

ANNEXE -C- PPPoE+

PPPoE possède un mécanisme de sécurité évolué. Néanmoins, il présente lui aussi des insuffisances. Le serveur PPPoE authentifie l'utilisateur à la base des comptes utilisateur (PAP ou CHAP), mais si ce compte est piraté, le pirate récupèrera aussi une adresse IP et il aura accès au service en question. D'où la nécessité d'introduire une nouvelle fonctionnalité de sécurité et cela était l'objectif de l'introduction du PPPoE+.

PPPoE+ ou l'agent intermédiaire du PPPoE est déployé dans un équipement couche 2 qui est situé entre l'utilisateur et le BRAS comme montre la figure ci-après.

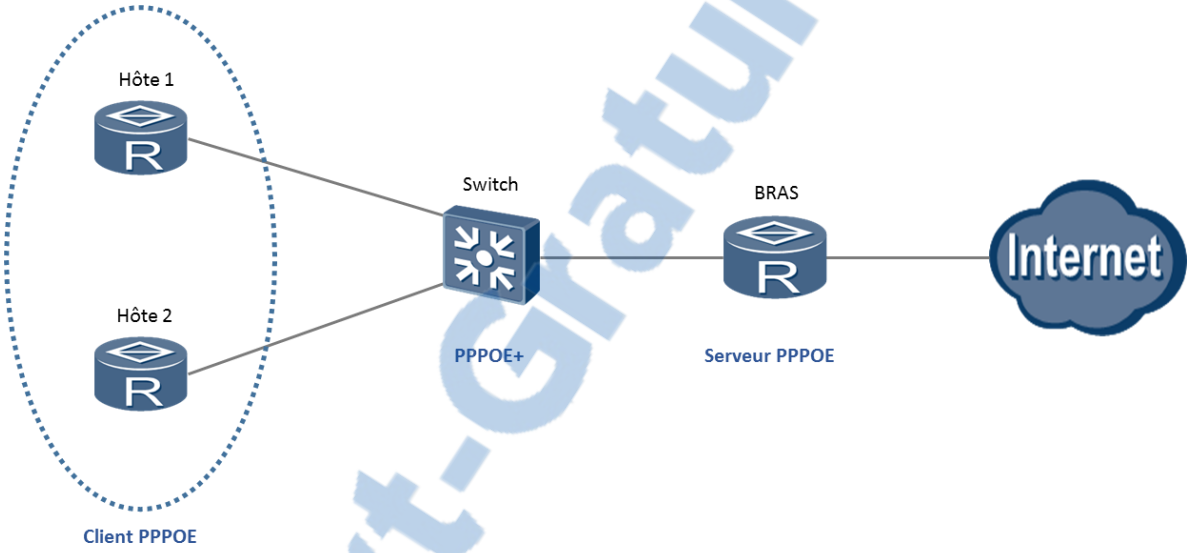

Figure 61: Réseau PPPoE+.

L'équipement dans le réseau réel d'IAM est le MSAN qui est présenté ici par un simple switch.

Le MSAN envoie les PAD reçus de l'utilisateur (notamment PADI et PADR) au serveur après avoir ajouté un TAG contenant des informations sur l'interface connectée au client PPPoE comme Le numéro d'interface, l'identifiant du VLAN, et l'adresse MAC du serveur PPPoE. Les informations du compte utilisateur et de l'interface d'accès sont authentifiées pour prévenir toute tentative de piratage du compte utilisateur.

La figure suivante montre le processus de fonctionnement du PPPoE+.

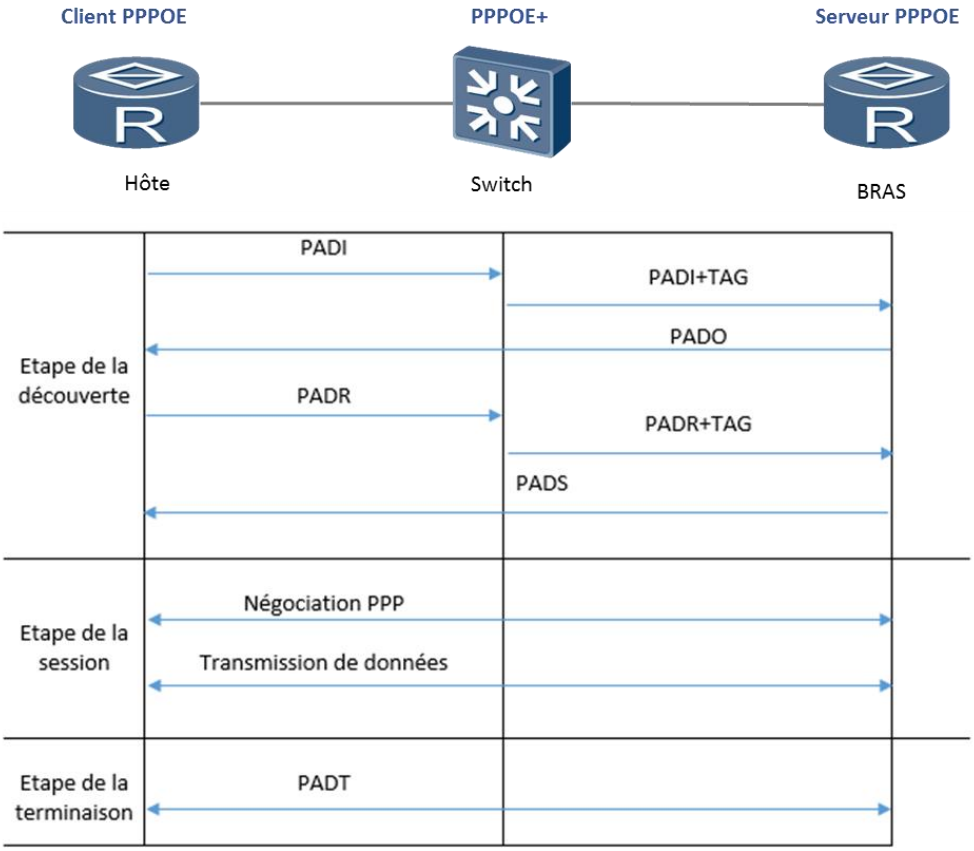

Figure 62: Le processus de fonctionnement du PPPoE+.

ANNEXE -D- DHCP & DHCP Option 82

Protocole de configuration dynamique « Dynamique Host Configuration Protocol » est un protocole permettant d'affecter automatiquement des adresses IP aux clients d'un serveur pour une durée limitée (la durée du bail). Cela facilite la configuration des réseaux, surtout pour les réseaux les plus complexes, car au lieu de configurer manuellement chaque hôte, c'est à dire lui donner une adresse IP ainsi que tous les paramètres d'accès dont il a besoins à savoir le masque, la passerelle par défaut et l'adresse du DNS, un serveur DHCP offre au client un bail d'accès au réseau et lui donne toutes les information dont il a besoin pour la durée du bail.

Le processus d'affectation d'adresse IP est le suivant :

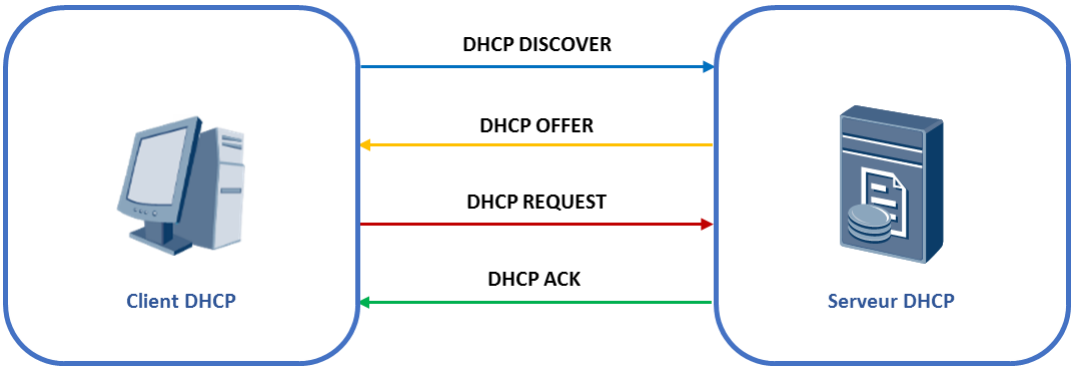

Figure 63: Processus d'affectation d'adresses IP en utilisant DHCP.

- Quand le client DHCP démarre, il cherche un serveur DHCP en envoyant en Broadcast une demande de bail IP « DHCP Discover » avec une adresse d'émission 0.0.0.0 qu'il adopte puisqu'il n'a pas encore d'adresse IP, il fournit aussi son adresse MAC pour être identifié par le serveur.
- Le ou les serveurs DHCP ayant des adresses IP non affectées vont répondre, en Broadcast, par un message « DHCP Offer » qui contient une proposition de bail, l'adresse IP du serveur et l'adresse MAC du client. Le client, en temps normal, accepte la première réponse.
- Dans ce cas, le client répond en Broadcast à tous les serveurs par un « DHCP Request » contenant l'adresse IP choisi et l'adresse IP du serveur choisi pour à la fois demander cette adresse IP ainsi que les autres paramètres de configuration à ce serveur et informer les autres de ce choix pour qu'ils libèrent les adresses IP proposées.
- Le serveur choisi répond donc en unicast par un acquittement « DHCP Ack (DHCP Acknoledgement) » qui comporte l'adresse IP allouée, Le masque, l'adresse du DNS et l'adresse de la passerelle. Le server ajoute aussi trois autres champs contenant le temps du bail, la date de demande de renouvellement et la période durant laquelle le client a la possibilité de rediffuser des recherches de DHCP dans le cas où le serveur DHCP ne répond pas.

Les autres messages du DHCP qui ne sont pas présents dans le scenario cité ci-dessus :

- DHCPNACK : « DHCP Negative ACKnowledgment » est un message envoyé par le serveur au client indiquant que la notion d'un client pour les adresses réseau est incorrecte. Par exemple si le client change de sous réseau ou au cas où son bail a expiré.

- DHCPDECLINE : c'est un message du client au serveur qui indique que l'adresse réseau est déjà utilisée.
- DHCPRELEASE : c'est un message du client au serveur dont le but est de libérer l'adresse réseau et d'annuler le bail.
- DHCPINFORM : c'est un message envoyé par le client au serveur pour demander uniquement les paramètres locaux de configuration car le client dans ce cas a déjà une configuration d'adresse réseau externe.

Le client DHCP tente de renouveler le bail quand ce dernier arrive à environ 50% de son temps de vie, en communiquant directement avec le serveur qui le lui a donné (en unicast), donc les seuls messages échangés sont un DHCPREQUEST et un DHCPACK. Si cette tentative échoue, à 87.5% du bail, le client envoi en Broadcast à tous les serveurs un DHCPREQUEST, ces derniers répondent soit par un DHCPACK ou un DHCPNACK.

Quand le client reçoit un message DHCPNACK ou lorsque le bail expire, il ne doit plus utiliser l'adresse IP et il doit demander un nouveau bail en utilisant le processus cité auparavant. S'il n'obtient pas une autre adresse et que le bail est expiré, la communication TCP/IP est rompue.

Dans le cas où le serveur DHCP et son client ne sont pas dans le même domaine de diffusion, un serveur appelés relais DHCP prend en charge la mission de relayer les requêtes et les réponses :

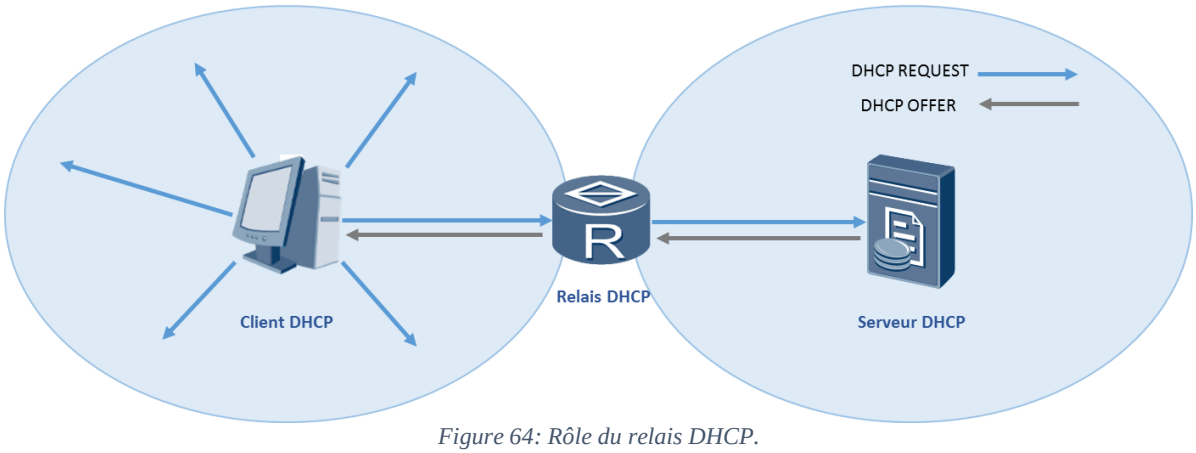

Figure 64: Rôle du relais DHCP.

Malgré les avantage qu'offre le protocole DHCP qui facilite la configuration du réseau, simplifie la configuration des machines portables et économise l'utilisation des adresses, il reste imparfait et l'un de ses plus importants défauts est sa vulnérabilité face aux attaques, vue que tout utilisateur peut avoir une adresse IP s'il envoie un message DHCPDISCOVER sans authentification. C'est pour cela que le DHCP Option 82 a été mis en place.

DHCP Option 82

DHCP Option 82 est utilisé dans des switchs pour éviter les attaques du serveur DHCP. Il consiste à ajouter dans le message DHCPREQUEST envoyé par le client le port et l'adresse du point d'accès au passage par ce point d'accès. Dans notre cas le switch est le MSAN et c'est lui qui va assurer le rôle de relais de confiance en ajoutant le port où le client est physiquement connecté. De cette façon le serveur connait les abonnés et la provenance des messages et il sera donc plus sécurisé contre toute tentative d'attaque. Cette méthode présente des similarités avec l'option PPPOE+.

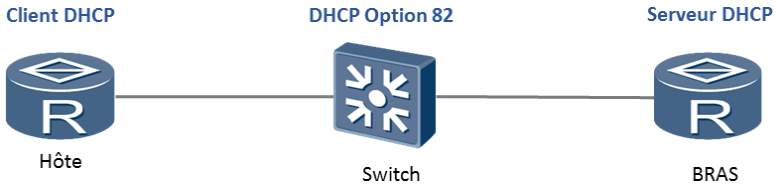

Figure 65: Relais DHCP Option 82.

Le tableau suivant montre la différence entre les protocoles d'accès PPPoE, PPPoE+, DHCP et DHCP Option 82.

	PPPoE	DHCP	PPPoE+	DHCP option 82
Attribution d'adresses	✓	✓	✓	✓
Authentification	✓		✓	✓
Principe de session	✓		✓	
Localisation du client			✓	✓
Difficulté de gestion	Difficile (couche 2)	Simple (couche 7)	Difficile (couche 2)	Simple (couche 7)

Tableau 6: Comparaison entre PPPoE, PPPoE+, DHCP et DHCP Option 82.

ANNEXE -E- IS-IS

Intermediate System to Intermediate System Protocol est un protocole de routage pour les fournisseurs d'accès internet moderne, il a été créé et déployé pour la pile OSI. Puis cette implémentation originale du protocole ISIS a été modifiée pour qu'elle soit adaptée au modèle TCP/IP sous nom d'Integrated IS-IS.

1. Caractéristiques du Protocole

- Protocole de routage de type état de lien.
- Utilise l'algorithme de Djikstra pour le calcul de chemin le plus court.
- Utilise les messages Hello pour la découverte des voisins.
- Plus efficace que l'OSPF.
- Facile à adapter à l'IPV6.

2. Composants d'architecture du protocole IS-IS

- Un IS (intermidiate system) est un routeur qui appartient à une seule aire.
- Les routeurs Level 1 sont des routeurs qui gardent les informations de routage à l'intérieur des aires dont ils font partie.
- Les routeurs Level 2 gardent seulement les routes du Backbone.
- Les routeurs L1/L2 sont utilisés pour le routage entre les aires, les routeurs L1 utilisent le routeur L1/L2 le plus proche pour quitter l'aire.

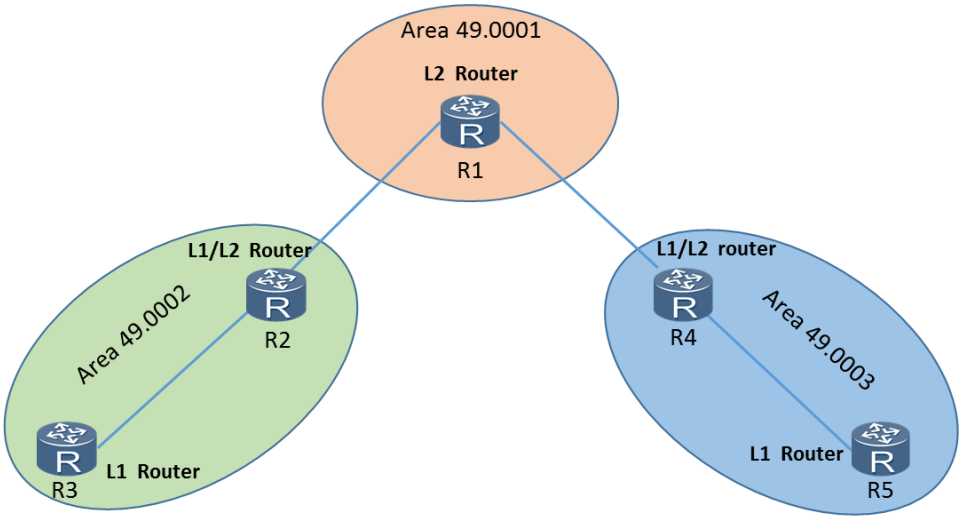

Figure 66: Exemple d'une architecture ISIS sur GNS3.

- La métrique du protocole IS-IS n'est pas basée sur la bande passante comme c'est le cas pour le protocole OSPF, la valeur de la métrique varie entre 0 et 63 avec une valeur de 10 par défaut. IS-IS introduit 4 types de métriques :
  - Cost : la métrique par défaut.
  - Delay : elle mesure le retard de transit.

- Expense : mesure le coût financier de l'utilisation d'un lien.
- Error : Mesure la probabilité d'erreur associée à un lien.

3. L'adressage NSAP

Le protocole OSI utilise l'adresse CLNP (Connection Less Network Protocol).

Quand on assigne une adresse CLNP à un routeur, on l'appelle NSAP (Network Service Access Point). Cette adresse est donné à un nœud et non pas à l'une de ses interfaces. La taille maximale de cette adresse est 20 Octets.

L'implémentation originale d'OSI définit 5 Champs dans l'adresse NSAP, le protocole IS-IS utilise seulement 3 champs :

- Area ID
- System ID
- NSAP selector

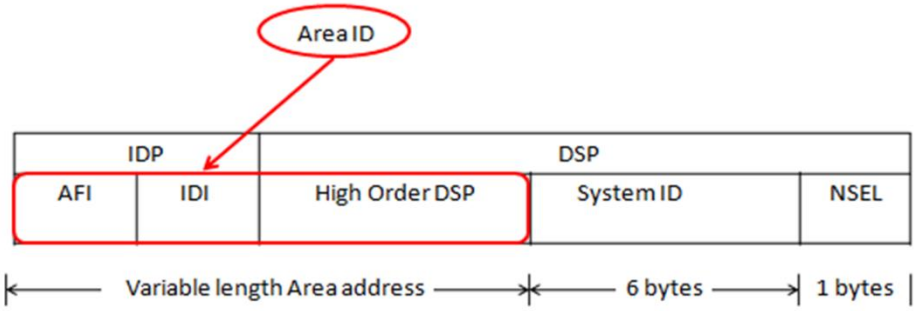

Figure 67: Format de l'adresse NSAP. [15]

Exemple:

Area ID: 49.126 System ID: aa15.b254.1841 Nsap selector: 00

L'adresse NSAP de ce routeur est: 49.126.aa15.b254.1841.00

4. Type des Réseaux IS-IS

Deux types de réseaux sont supportés :

- Broadcast
- Point-to-Point

Dans le mode Broadcast la connectivité avec les autres IS est totale, c'est-à-dire que chaque IS est lié directement avec les autres IS. Ce mode nécessite l'élection d'un Disignated IS (DIS) qui joue le même rôle qu'un DR de l'OSPF.

Dans le mode Point-to-Point on a une connectivité partielle, on n'a pas besoin d'utiliser un DIS.

Le mode Broadcast utilise l'adressage multicast alors que le mode Point-to-Point utilise l'adressage unicast.

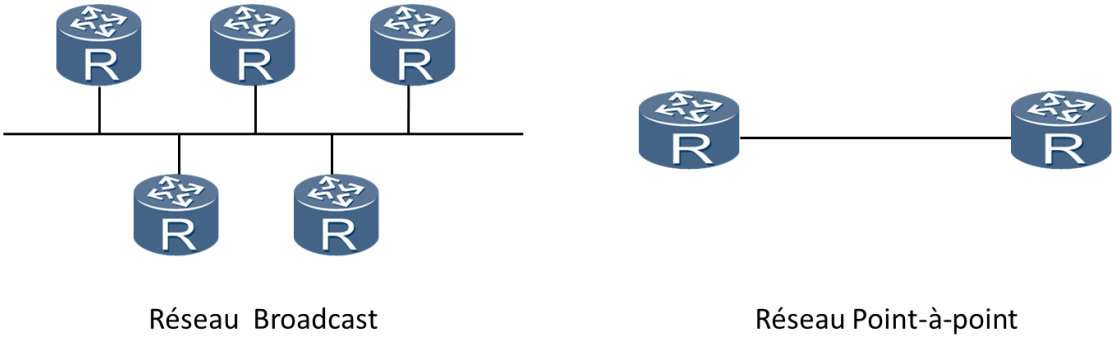

Figure 68: Types des réseaux IS-IS.

5. Types de paquets IS-IS

Le protocole ISIS introduit 4 types de paquets

- Hello : Détection des voisins et création des relations d'adjacence
- Link state packet LSP : 4 types
  - Level1 pseudonode
  - Level1 non pseudonode
  - Level2 pseudonode
  - Level2 non pseudonode
- Complet Sequence Number PDU (CSNP) : donne la liste des LSPs présents dans la LSDB de l'émetteur, il informe les autres ISs sur les LSPs expirés ou perdu dans le cas d'un réseau Broadcast. Pour les réseaux poindre à point, le CSNP est généré lors de la phase d'établissement de l'adjacence tandis que pour les réseaux Broadcast il est généré périodiquement.
- Partial Sequence Number PDU (PSNP) : utilisé pour demander un LSP ou accuser la réception d'un LSP dans les réseaux point à point. Et seulement pour demander un LSP dans le cas d'un réseau Broadcast.

6. Mécanisme de fonctionnement

Dans une architecture réseau où le protocole IS-IS est activé, la découverte des voisins et la création de la table de routage suivent les étapes suivantes :

- ⇨ Chaque IS dans le réseau envoie des paquets HELLO pour découvrir ses voisins.
- ⇨ Chaque IS s'identifie par une annonce qui contient ses interfaces actives et ses voisins directement connectés.
- ⇨ Chaque IS garde une copie de l'annonce reçu puis transmet cette annonce à son voisin aval.
- ⇨ Chaque IS commence à construire sa base de données une fois qu'il reçoit toutes les copies des annonces des autres ISs.
- ⇨ Chaque IS alors commence à calculer précisément les routes des différentes destinations en se basant sur l'algorithme de Djikstra du plus court chemin (SPF).

7. Exemple de simulation :

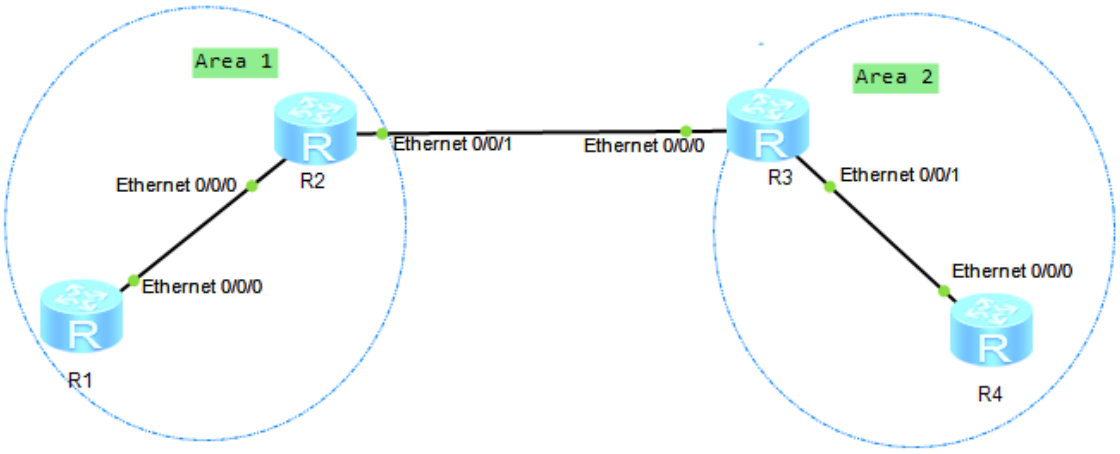

Figure 69: Simulation du protocole IS-IS.

Les configurations faites au niveau de chaque routeur :

```
<Huawei>dis current-configuration
#
sysname Huawei
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher OOCM4m($F4ajUn1vMEIBNUw#
 local-user admin service-type http
#
isis 1
 is-level level-1
 network-entity 49.0001.0000.0000.0001.00
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.10.1 255.255.255.0
 isis enable 1
#
```

Figure 70: Configuration au niveau du routeur R1.

```
isis 1
 network-entity 49.0001.0000.0000.0002.00
 import-route isis level-2 into level-1
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.10.2 255.255.255.0
 isis enable 1
 isis circuit-level level-1
#
interface Ethernet0/0/1
 ip address 192.168.20.1 255.255.255.0
 isis enable 1
 isis circuit-level level-2
#
```

Figure 71: Configuration au niveau du routeur R2.

```
isis 1
 network-entity 49.0002.0000.0000.0001.00
 import-route isis level-2 into level-1
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.20.2 255.255.255.0
 isis enable 1
 isis circuit-level level-2
#
interface Ethernet0/0/1
 ip address 192.168.30.1 255.255.255.0
 isis enable 1
 isis circuit-level level-1
#
```

Figure 72: Configuration au niveau du routeur R3.

```
isis 1
 is-level level-1
 network-entity 49.0002.0000.0000.0002.00
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
 ip address 192.168.30.2 255.255.255.0
 isis enable 1
```

Figure 73: Configuration au niveau du routeur R4.

La table de routage de R1 et R4 ne contient pas la route pour sortir de la zone :

```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   ISIS-L1 15   10          D   192.168.10.2    Ethernet0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  Direct  0    0           D   192.168.10.1    Ethernet0/0/0
   192.168.10.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0

<Huawei>
```

Figure 74: Table de routage du routeur R1.

Pour cela on ajoute la commande suivante au niveau des deux routeurs R2 et R3 pour activer l'option de « route Leaking » :

import-route isis level-2 into level-1

```
<Huawei>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   ISIS-L1 15   10          D   192.168.10.2    Ethernet0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  Direct  0    0           D   192.168.10.1    Ethernet0/0/0
   192.168.10.1/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
   192.168.20.0/24  ISIS-L1 15   20          D   192.168.10.2    Ethernet0/0/0
   192.168.30.0/24  ISIS-L1 15   30          D   192.168.10.2    Ethernet0/0/0

<Huawei>
```

Figure 75: Table de routage du routeur R1 après la configuration du « route Leaking ».

ANNEXE -F- MPLS & MPLS VPN

MPLS (Multi Protocol Label Switching) est une technologie 2.5, dont le rôle principal est de combiner les concepts du routage IP de niveau 3, et les mécanismes de la commutation de niveau 2.

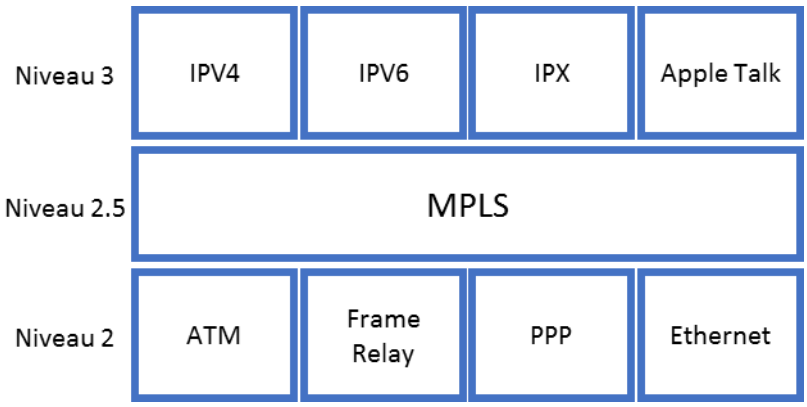

Figure 76: MPLS dans la pile TCP/IP. [15]

L'objectif initial du MPLS est de réduire le temps de traitement des paquets dans les équipements réseau, car le routage couche 3 consomme du temps pour analyser l'entête IP qui contient des informations inutiles pour le routage, par l'introduction d'un label inséré par le protocole MPLS entre les couches 2 et 3. Ainsi chaque routeur possède une table associant un port/label d'entrée à un port/label de sortie. Cette table est rapide à parcourir, ce qui a pour but d'accroître la rapidité du routage par rapport à un réseau IP. Actuellement le principal apport de cette technologie est d'offrir de l'ingénierie de trafic (MPLS-TE (TE : Trafic engineering)) et la mise en œuvre de VPN efficaces.

Le format de l'entête MPLS :

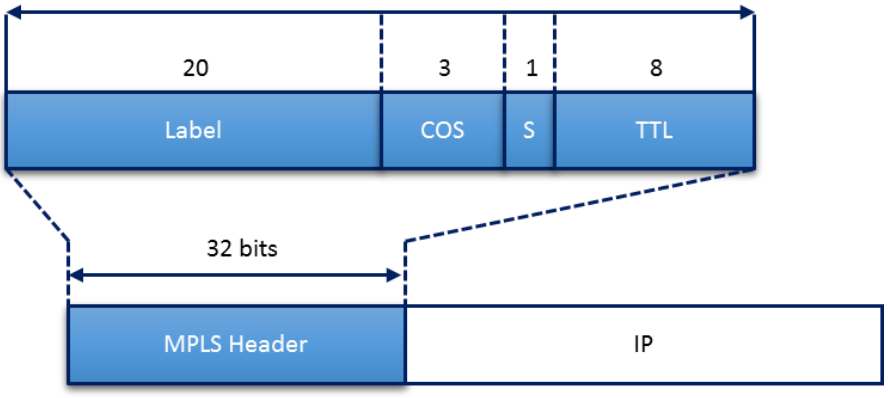

Figure 77: Format de l'entête MPLS. [15]

- Cos ou Exp = Experimental.
- S = Indique le bas de pile, permet d'empiler des labels

- TTL = Time to live, le même qui est présent dans l'entête IP, il est décrémenté à chaque passage par un routeur qui supporte MPLS puis recopié dans l'entête IP à la sortie du domaine MPLS.

MPLS fonctionne en deux plans : le plan de contrôle qui est en mode non connecté et le plan de données qui fonctionne en mode connecté. Le plan de contrôle a pour mission de construire le chemin que vont emprunter les paquets dans le plan de donnée, ce chemin est appelé le LSP (Label Switching Path).

Principe de fonctionnement du MPLS :

- Plan Contrôle :

Dans le plan de contrôle nous avons besoin d'un protocole de routage IGP (OSPF, ISIS, EIGRP,…) et d'un Protocol de distribution des labels (LDP ou RSVP-TE).

IGP permet de construire une table de routage RIB (Routing Information Base) que le LDP par exemple va utiliser pour assurer sa fonction.

Les paquets IP entrant sur le réseau MPLS sont associés à une FEC : Forwarding Equivalent Class, Pour classifier un paquet dans une FEC, MPLS se base sur le protocole de distribution utilisé, dans le cas de LDP chaque label est affecté à la FEC correspondante par préfixe réseau présent dans la table de routage du routeur.

LDP permet de construire deux tables :

- FIB (Forwarding information Base) qui est utilisée par un routeur pour commuter un paquet si le paquet reçu n'est pas labélisé, l'action dans ce cas est un PUSH.
- LFIB (Label Forwarding Information Base) qui est utilisée par un routeur pour commuter un paquet labélisé, et l'action est soit un SWAP soit un POP.

Ces deux tables sont construites à base de :

- LIB (Label Information Base) : C'est la première table construite au niveau d'un LSR, elle contient pour chaque sous-réseau IP la liste des tables reçus par les voisins. Ses entrées sont de la forme (réseau de destination, LSR, Label) où LSR est le nœud qui a généré le label.
- RIB (Routing Information Base) : C'est une table de commutation complète qui contient les mêmes informations que la table de routage et qui permet au routeur de prendre ses décisions d'acheminement. Les routeurs utilisent toujours un IGP pour calculer le meilleur chemin. Avec l'aide de la RIB, on peut déterminer le meilleur label à utiliser pour un préfixe donné (le nexthop figure dans la LIB).

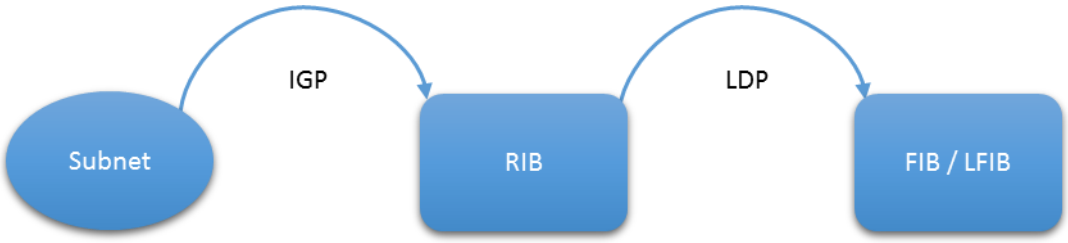

Figure 78: Processus de construction de la table LFIB.

➢ Plan de données :

Dans le schéma suivant, sont présentés l'architecture du réseau MPLS et le principe de commutation par label :

- Ingress_LER : le premier point de contact avec le réseau MPLS, responsable d'insérer un label à l'entrée ➔ PUSH
- Egress_LER : la sortie du domaine MPLS, il est responsable d'enlever le label ➔ POP
- LSR : tout routeur qui supporte MPLS, les LER sont des LSR, le LSR du cœur MPLS permet de changer un label d'entrée par un autre de sortie ➔SWAP.

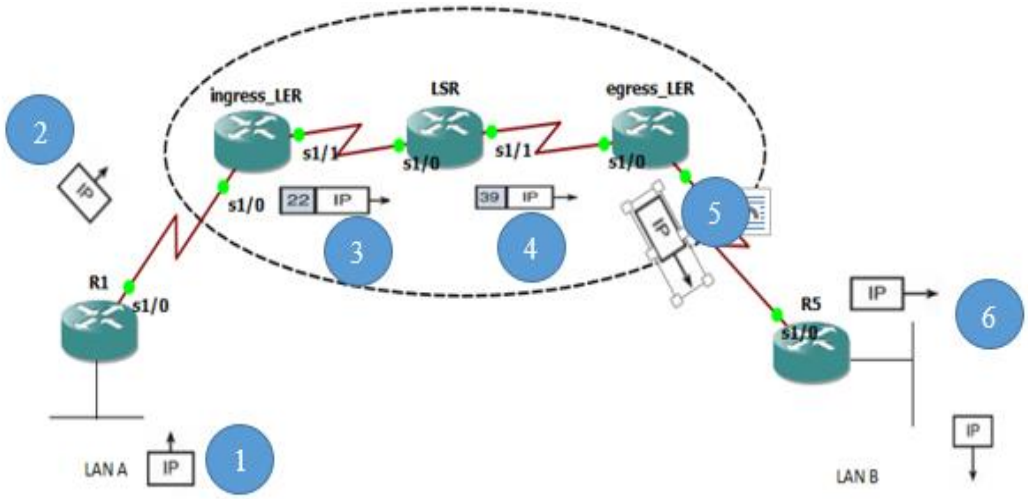

Figure 79: Simulation du MPLS.

1- Un host dans le LAN A envoi un paquet IP à son destinataire dans le LAN B
2- Le routeur R1, qui ne contient aucune configuration MPLS, route le paquet en se basant sur sa table de routage.
3- L'ingress_LER reçoit le paquet non labélisé, et lui ajoute un tag à partir de la table FIB
4- Le LSR fait le swap du label 22 en un autre label, ici 39
5- L'egress_LER ensuite se charge d'enlever le label et l'envoyer à R5
6- R5 se base sur sa table de routage pour transmettre le paquet à sa bonne destination.

Il est à noter que le LSR au lieu d'annoncer un « vrai » label, annonce un label « implicit null », l'egress_LER lorsqu'il reçoit ce binding, sait qu'il doit réaliser une opération « pop » au lieu d'une opération « swap ». Le label Implicit-Null n'apparaît en fait jamais sur le lien. Cela évite que le dernier routeur ait à analyser un label puis à regarder sa LFIB, c'est l'option PHB (Pen-Ultimate Hop Popping) qui est intégré par défaut sur Cisco IOS et sur les IOS Huawei aussi.

MPLS VPN :

Dans le MPLS VPN, une terminologie particulière est utilisée :

- ingress_LER + egress_LER ➔ PE (Provider Edge)
- LSR_coeur ➔ P (Provider)

Les protocoles et les standards définis par MPLS VPN résolvent le problème de conflits d'adresses si deux sites connectés utilisent le même adressage privé en définissant le concept de plusieurs tables de routage sous le même routeur nommée VRF (Virtual Routing and Forwarding) comme le montre l'exemple suivant, les deux LAN connectés respectivement à CE_A2 et CE_B2 :

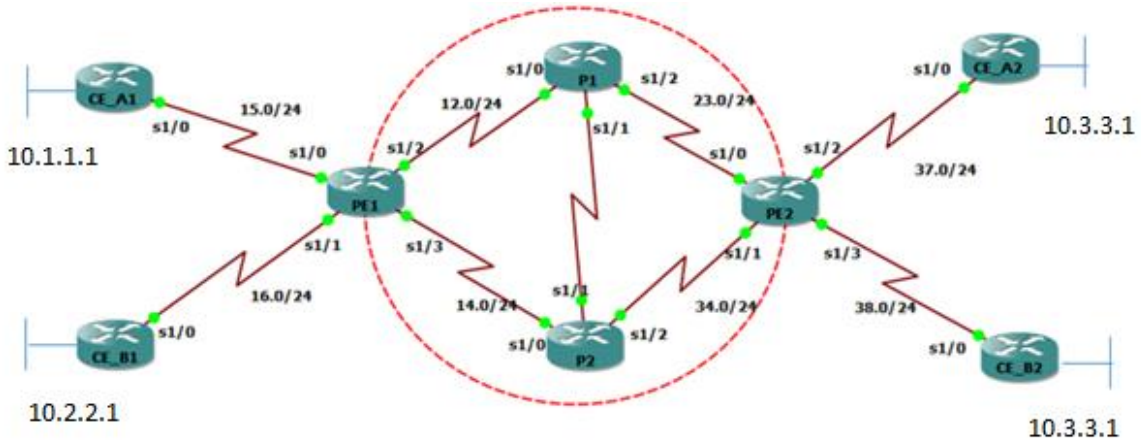

Figure 80: Simulation de l'application L3VPN.

Plan contrôle :

Trois notions sont ajoutées :

- VRF : cette option est utilisée pour enregistrer les routes de différents clients séparément, elle est configurée dans chaque PE. Une VRF par client est exigée pour isoler complètement le trafic des clients.
- RD (Route Distinguisher) : c'est une option de MP-BGP qui permet de distinguer les routes de clients différents. Le RD a une taille de 8 octets (il est configuré manuellement par l'opérateur). On obtient une adresse VPNv4 de 96 bits.
- RT (Route Target) : une option de MP-BGP qui permet l'échange de route entre différents site d'une même entité. En effet, un routeur PE annonce les routes d'une VRF avec les RT spécifiés en **export** et les autres routeurs PE importent ces routes dans les VRF qui sont configurées pour **importer** ces valeurs de RT.

Plan de données :

L'ingress PE dans MPLS VPN a un travail supplémentaire à faire, il doit insérer deux labels :

- Outer-mpls header, avec le bit S=0, qui permet au paquet d'être commuté jusqu'à l'egress PE.
- Inner-mpls header, avec le bit s=1, qui identifie l'egress PE.

La configuration complète est la suivante :

1- Tous les routeurs du domaine MPLS supportent OSPF comme IGP, tous les liens et les interfaces loopback des routeurs sont annoncés.

2- Les interfaces à l'intérieur du domaine sont configurées pour supporter MPLS. Pour cela on utilise ➔ **mpls ip** pour chaque interface.

3- Création du VRF, RD, RT de chaque client et les associées à l'interface correspondante :

 # ip vrf vrf-name
#rd rd-value
#route-target {**import**|**export**} rt-value
#ip vrf forwarding vrf-name (à l'intérieur de chaque interface)

4- EIGRP est configuré entre les PE et CE comme IGP :

- CE :

#router eigrp num
 # network @rx

- PE :

#router eigrp num
 # address-family ipv4 vrf vrf_name
#autonomous-system num
#network @interface_liée au CE @masque_générique
no auto-summary

5- Redistribution entre EIGRP et BGP :

- PE:

#router bgp num
#address-family ipv4 vrf vrf_name
#redistribute eigrp num

#router eigrp num
#address-family ipv4 vrf vrf_name
#**redistribute bgp** bande-passante délai charge fiabilité MTU

6- Configuration de MP-BGP entre PE :

#router bgp num
#neighbor @loopback PE_distant remote-as num
#neighbor @loopback PE_distant update-source loopback0
#address-family vpnv4
neighbor @loopback PE_distant activate
#neighbor @loopback PE_distant send-community

ANNEXE -G- VRRP

VRRP est un protocole qui fournit une solution de continuité de service principalement pour la redondance des passerelles par défaut. Cette redondance est mise en place par le biais du protocole ARP. Lorsque le PC doit envoyer une trame à sa passerelle, il émet une requête ARP et celle-ci répond en fournissant son adresse MAC.

VRRP utilise la notion du routeur virtuel, auquel est associée une adresse IP virtuelle ainsi qu'une adresse MAC virtuelle particulière sous la forme **00:00:5E:00:01 : XX** (où XX est le numéro du groupe VRRP). Dès lors, pour le PC, quoi qu'il arrive, ce sera cette adresse MAC qui identifiera sa passerelle. De leur côté les routeurs dialoguent par multicast (224.0.0.18) afin de négocier et de savoir qui devra se charger de traiter la trame destinée à l'adresse MAC VRRP. C'est-à-dire désigner le routeur Master (celui qui a la plus grande priorité) pour exécuter cette tâche et désigner le deuxième routeur comme Slave réalisant le rôle de backup.

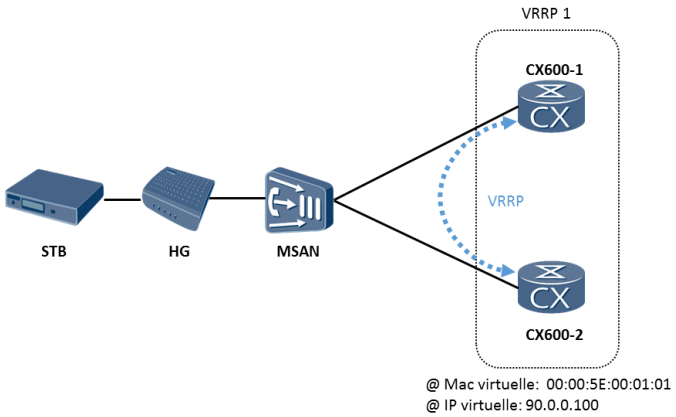

Figure 81: Implémentation du VRRP entre les deux routeurs CX600 de la boucle METRO IP.

Les captures suivantes montrent le bon fonctionnement de ce mécanisme :

```
[Huawei]disp vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Master
    Virtual IP : 90.0.0.100
    Master IP : 90.0.0.1
    PriorityRun : 200
    PriorityConfig : 200
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2016-05-17 10:47:49 UTC-08:00
    Last change time : 2016-05-17 10:50:52 UTC-08:00
```

Figure 82: CX600-1 joue le rôle du Master.

```
<Huawei>disp vrrp
  GigabitEthernet0/0/1 | Virtual Router 1
    State : Backup
    Virtual IP : 90.0.0.100
    Master IP : 90.0.0.1
    PriorityRun : 150
    PriorityConfig : 150
    MasterPriority : 200
    Preempt : YES   Delay Time : 0 s
    TimerRun : 1 s
    TimerConfig : 1 s
    Auth type : NONE
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Create time : 2016-05-17 10:50:19 UTC-08:00
    Last change time : 2016-05-17 10:51:21 UTC-08:00
```

Figure 83: Routeur CX600-2 joue le rôle du Backup.

```
<Huawei>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 27        Routes : 30

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  ISIS-L1 15   40           D   10.0.0.2        Ethernet0/0/0
       10.0.0.0/24  Direct  0    0            D   10.0.0.1        Ethernet0/0/0
       10.0.0.1/32  Direct  0    0            D   127.0.0.1       Ethernet0/0/0
       20.0.0.0/24  ISIS-L1 15   20           D   10.0.0.2        Ethernet0/0/0
       30.0.0.0/24  ISIS-L1 15   30           D   10.0.0.2        Ethernet0/0/0
       40.0.0.0/24  ISIS-L1 15   30           D   60.0.0.1        Ethernet0/0/1
                    ISIS-L1 15   30           D   90.0.0.2        GigabitEthernet
0/0/1
       50.0.0.0/24  ISIS-L1 15   20           D   60.0.0.1        Ethernet0/0/1
                    ISIS-L1 15   20           D   90.0.0.2        GigabitEthernet
0/0/1
       60.0.0.0/24  Direct  0    0            D   60.0.0.2        Ethernet0/0/1
       60.0.0.2/32  Direct  0    0            D   127.0.0.1       Ethernet0/0/1
       90.0.0.0/24  Direct  0    0            D   90.0.0.1        GigabitEthernet
0/0/1
       90.0.0.1/32  Direct  0    0            D   127.0.0.1       GigabitEthernet
0/0/1
     90.0.0.100/32  Direct  0    0            D   127.0.0.1       GigabitEthernet
0/0/1
      127.0.0.0/8   Direct  0    0            D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0            D   127.0.0.1       InLoopBack0
    192.168.1.0/24  ISIS-L1 15   40           D   60.0.0.1        Ethernet0/0/1
                    ISIS-L1 15   40           D   90.0.0.2        GigabitEthernet
```

Figure 84: Routeur CX600-1 qui est Master a une route directe vers l'adresse IP virtuelle.

ANNEXE -H- BFD

1. Protocole BFD

Les réseaux transportant la vidéo, la voix et les données sont sensibles et exigent une haute disponibilité. D'où la nécessité de détecter rapidement les pannes de liens.

Le protocole BFD (Bidirectional Forwarding Detection) accélère la détection des failles sur le lien entre deux systèmes. Si le système ne reçoit pas des messages BFD control, alors on suppose qu'il y a une panne le long du lien, du coup le service ou bien le protocole lié au BFD et mis au courant pour qu'il réagisse face à cette panne.

D'un point de vue plus simple, BFD est similaire à un protocole Hello utilisé par un IGP avec une différence majeur de vitesse avec laquelle les paquets BFD sont générés.

2. Avantages du protocole BFD

- Protocole indépendant du media, des données ou du protocole de routage.
- la rapidité de détection des erreurs (environ 50ms)
- la période des paquets BFD control peut être ajustée dynamiquement pour éviter les messages erronés

3. Paquet BFD control

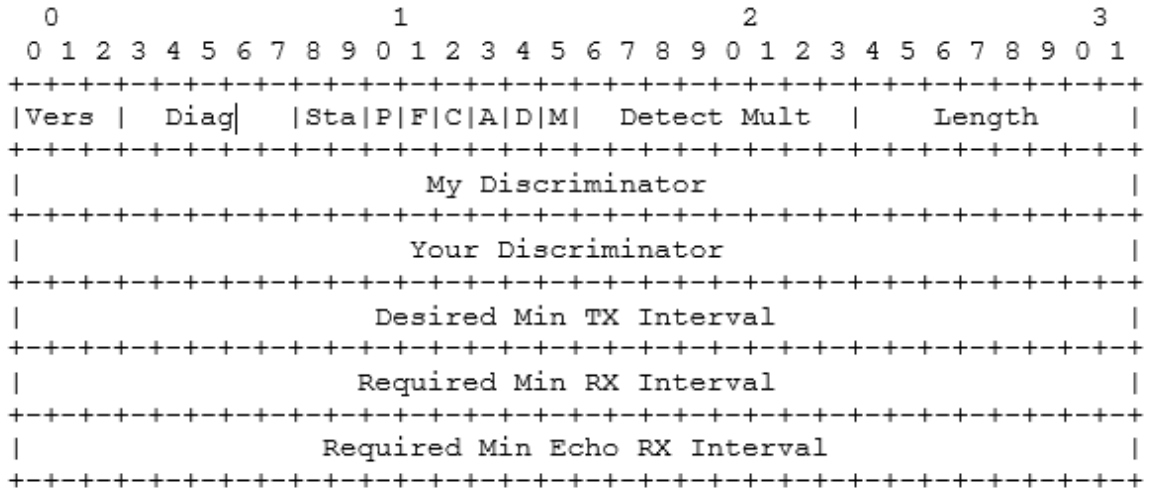

Figure 85: Format du paquet BFD. [17]

- **vers** : version du protocole BFD.
- **Diag** (Diagnostics) : le code de diagnostique qui indique la cause du dernier changement d'état d'une session BFD.
- **Sta** (State) : l'état courant de la session BFD.
- **P** (Poll) : un bit indiquant que le système demande une vérification de connectivité.
- **F** (Final) : un bit indiquant que le system qui transmet répond à un message BFD control avec le bit P configuré à 1.

- **C** (Control Plane Independent) : bit indiquant que l'implémentation de la session BFD dépend du plan contrôle.
- **A** (Authentication Present) : bit indiquant qu'une session BFD doit être authentifiée.
- **D** (Demand) : bit indiquant que le mode demande est activé, ce mode permet de savoir si la session est active dans les deux directions.
- **M** (Multipoint) : bit réservé aux futures point-to-multipoint extensions du BFD.
- **Detect Mult** (Detection time multiplier) : l'intervalle de transmission négocié multiplié par une valeur définie par défaut de 3.
- **Length** : longueur du paquet BFD control.
- **My Discriminator** : unique, non nul champ généré par le système de transmission. Il est utilisé pour démultiplier des sessions BFD multiples.
- **Your Discriminator** : discriminateur reçu par le système à distance, ce champ reflette la valeur reçu de champ My Discriminator ou bien il est à zéro si cette valeur est inconnu.
- **Desired Min TX Interval** : l'intervalle du temps minimum en millisecondes que le système de transmission adopte pour l'envoie périodique des messages BFD control.
- **Required Min RX Interval** : l'intervalle du temps minimum en millisecondes entre deux paquets BFD control reçu que le système peut supporter.
- **Required Min Echo RX Interval** : l'intervalle du temps minimum en millisecondes entre l'écho de deux paquets BFD reçu que le système peut supporter.

4. Simulation

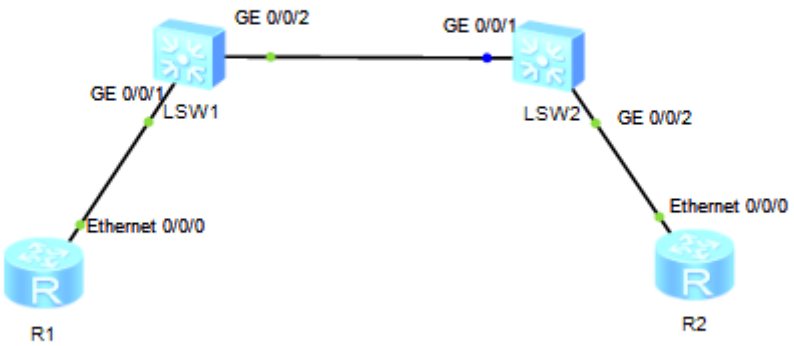

Figure 86: Simulation du protocole BFD sous eNSP.

Après avoir configuré le protocole PIM dans les routeurs R1 (choisi comme DR) et R2, nous allons configurer le protocole BFD pour le PIM dans chaque interface des deux routeurs.

Par la suite nous activerons le protocole BFD dans chaque routeur en utilisant les commandes suivantes :

```
[Huawei]BFD
[Huawei-bfd]interface ethernet 0/0/0
[Huawei-Ethernet0/0/0]pim bfd enable
[Huawei-Ethernet0/0/0]
May 17 2016 11:12:18-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5
```

Figure 87: Etapes de configuration du BFD dans R1 et R2.

Verification de la configuration:

```
<Huawei>display pim interface eth 0/0/0 verbose
 VPN-Instance: public net
 Interface: Ethernet0/0/0, 192.168.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 192.168.1.1 (local)
     PIM DR Priority (configured): 100
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM join attribute (negotiated): enabled
     PIM generation ID: 0XEF5B1A8E
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: enabled
     PIM BFD min-tx-interval: 1000 ms
     PIM BFD min-rx-interval: 1000 ms
```

Figure 88: Vérification de la configuration du protocole PIM dans R1.

À l'aide de WireShark, on prend une capture de trames entre les switches :

2436	1573.09400	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2437	1573.32800	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2438	1574.21900	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2439	1574.45300	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2441	1575.36000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2442	1575.56300	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2444	1576.54700	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2445	1576.67200	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2447	1577.65600	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2448	1577.84400	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2449	1578.84400	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2450	1578.96900	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2452	1579.95300	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2453	1580.11000	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
2454	1581.12500	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00

Figure 89: Capture WireShark des messages BFD.

Nous remarquons un échange de messages BFD control entre les deux routeurs, le champ **state** est **up** ce qui indique que les deux sessions sont établies avec succès.

Le contenu de chaque trame :

```
BFD Control message
    001. .... = Protocol Version: 1
    ...0 0000 = Diagnostic Code: No Diagnostic (0x00)
    11.. .... = Session State: Up (0x03)
  Message Flags: 0x00
      0... .. = Poll: Not set
      .0.. .. = Final: Not set
      ..0. .. = Control Plane Independent: Not set
      ...0 .. = Authentication Present: Not set
      .... 0. = Demand: Not set
      .... .0 = Multipoint: Not set
    Detect Time Multiplier: 3 (= 3000 ms Detection time)
    Message Length: 24 bytes
    My Discriminator: 0x00002000
```

Figure 90: Contenu du message BFD.

Nous allons essayer maintenant de désactiver le service multicast sur le routeur R1 en utilisant la commande : **#undo multicast routing-enable**

462	313.078000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
463	314.188000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x00
464	314.297000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: Control Detection Time Expired, State: Down, Flags: 0x00
465	314.328000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: Control Detection Time Expired, State: AdminDown, Flags: 0x00
555	500.016000	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Down, Flags: 0x00
556	500.110000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Init, Flags: 0x00
557	500.578000	192.168.1.2	192.168.1.1	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x20
558	500.625000	192.168.1.1	192.168.1.2	BFD Cor	66 Diag: No Diagnostic, State: Up, Flags: 0x20

Figure 91: capture WireShark des messages BFD après désactivation du PIM.

Après l'arrêt du service de multicast dans le routeur R1, nous constatons un changement d'état dans le paquet BFD control pour les deux routeurs. Lorsque le detect time est expiré, le routeur R1 envoie un BFD control avec l'état **Down**. Par la suite, R1 envoie un autre paquet BFD control avec l'état **AdminDown**, ce paquet va mettre le BFD du routeur R2 en état **down** aussi.

Nous activons à nouveau le service multicast, le routeur R1 envoie un BFD control avec l'état **Init** pour indiquer au routeur R2 qu'il veut passer à l'état **Up**.

Ensuite les paquets envoyés par les deux routeurs passent à l'état **Up** indiquant que la session est bien établie.

ANNEXE -I- xDSL

Depuis qu'on a découvert la possibilité d'utiliser la totalité de la bande passante du cuivre pour transmettre à la fois la voix et les données, plusieurs technologies ont vu le jour pour assurer cette transmission. Parmi ces technologies la famille xDSL (Digital Subscriber Line) a été mise en place.

Il existe deux types de transmission en technologies xDSL :

- La transmission symétrique

Certaine technologies xDSL utilisent ce mode de transmission appelé aussi duplex pour transmettre avec le même débit les données soit dans le sens montant ou descendant.

- La transmission asymétrique

Elle utilise contrairement aux technologies symétriques deux débits différents pour les deux sens montant et descendant. Elle utilise un débit descendant plus grand que le débit montant pour éviter la surcharge des équipements coté fournisseur.

Les technologies xDSL les plus connue sont explicitées dans le tableau suivant :

Technologies xDSL	Symétrique	Asymétrique	Débit montant Max	Débit descendant Max	Porté Max (Km)	Nombre de paires	IPTV
SDSL	✓		2 Mbps		3	1	
HDSL	✓		1.5Mbps /2 Mbps		3	2/3	
SHDSL	✓		2,3 Mbps / 4,6 Mbps		6.5	1/2	
ADSL		✓	896 kbps	8 Mbps	5	1	
ADSL2		✓	1200 kbps	12 Mbps	5	1	
ADSL2+		✓	1 Mbps	24 Mbps	5	1	✓
VDSL	✓	✓	52 Mbps	52 Mbps	1.5	1	
VDSL2	✓	✓	100 Mbps	100 Mbps	0.35	1	✓

Tableau 7: Différentes technologies xDSL.

Les technologies xDSL ont prouvé leur efficacité de transfert des données sur le même support de cuivre appartenant à l'infrastructure déjà installée. Néanmoins elles ont quelques limitations qui se résument principalement dans une distance maximale limitée entre l'abonné et le centre de rattachement et dans le débit qui ne satisfait plus le besoin croissant des services. C'est pour parer à ces inconvénients que les opérateurs ont adopté une stratégie de migration vers la technologie GPON.

ANNEXE -J- GPON

La technologie GPON est une nouvelle technologie optique venue pour remplacer les technologies xDSL. Elle est basée sur l'utilisation du PON qui est un réseau passif constitué des OLT (Optical Line Terminal), ONU (Optical Line Unit) et du splitter qui est passif. L'utilisation de ces équipements passifs se justifie par leur faible consommation. Pour assurer un passage total à la fibre optique, le déploiement de la technologie FTTx est passé par plusieurs étapes : FTTC, FTTB, FTTH.

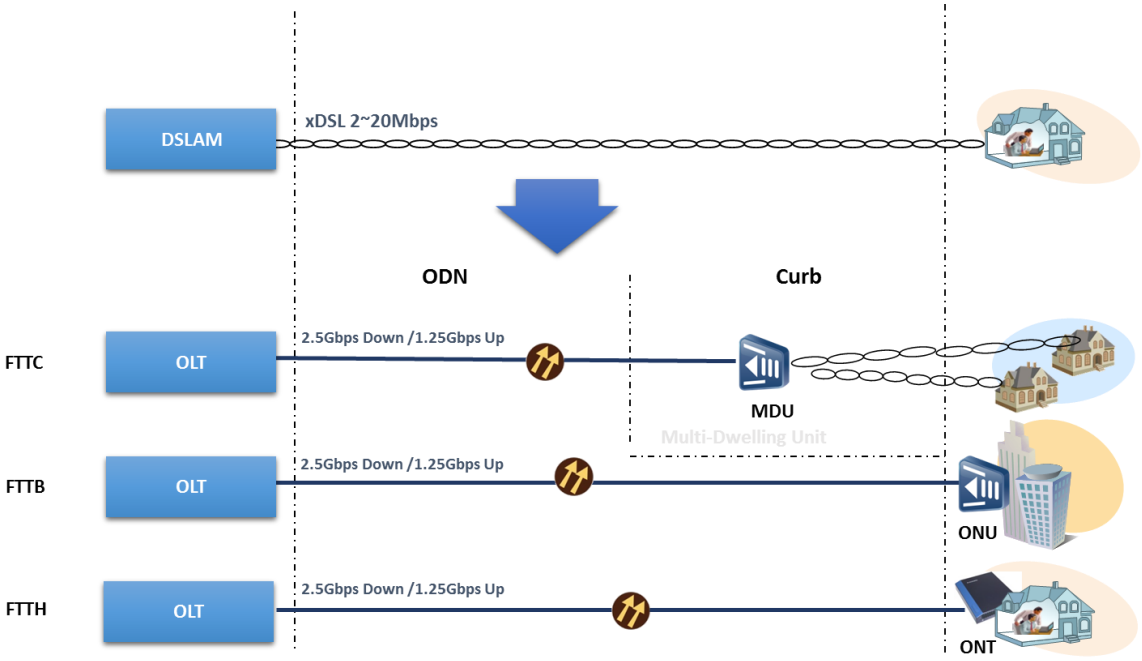

Figure 92: Passage d'une architecture d'accès xDSL aux architectures optiques FTTx. [18]

Le GPON utilise une architecture point à multipoint au lieu d'une architecture point à point pour économiser au maximum l'utilisation des fibres optiques.

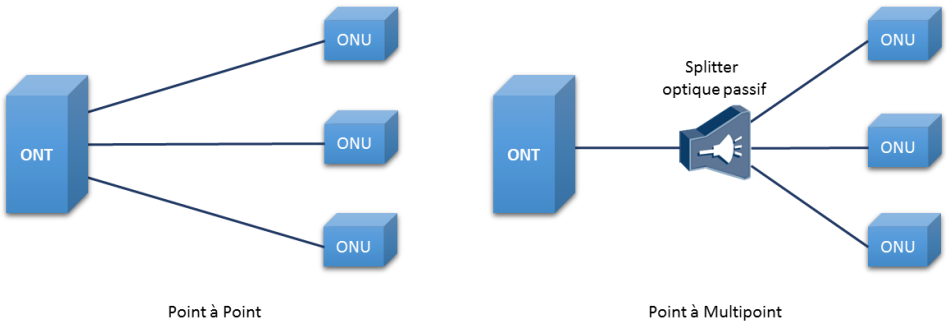

Figure 93: Architecture point à point et architecture point à multipoint.

Le GPON utilise la transmission sur fibre optique et adopte le WDM pour utiliser la même fibre en upstream et en downstream. Dans ce sens trois longueurs d'ondes ont été réservées (1490 nm pour le downstream, 1310 nm pour le upstream, 1550 nm pour le câble TV, à noter que ce service n'est pas encore déployé au Maroc).

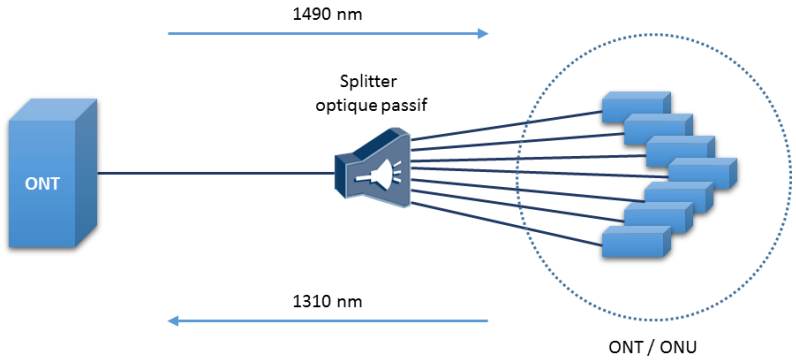

Figure 94: Multiplexage WDM en GPON.

Pour transmettre les données relatives à chaque service aux clients demandeurs, le splitter envoie en Broadcast tous les services aux ONU. Et chaque ONU prend le trafic qui lui est destiné.

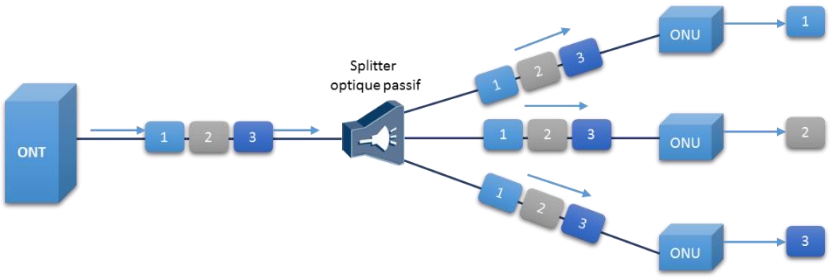

Figure 95: Transmission des services. [18]

Pour s'assurer que le client ne lit que les paquets des services qui lui sont destinés, le contenu transmis en downstream est crypté en utilisant le cryptage AES : Advanced Encryption Standard. En effet, l'OLT crypte les paquets grâce à une clé partagée avec l'ONU, qui prend ensuite en charge le décryptage de ces paquets. Donc même si les ONU reçoivent tous les services, ils n'arrivent à décrypter que le flux qu'ils ont droit à voir.

Pour la transmission en UPLINK la technique TDMA est utilisée :

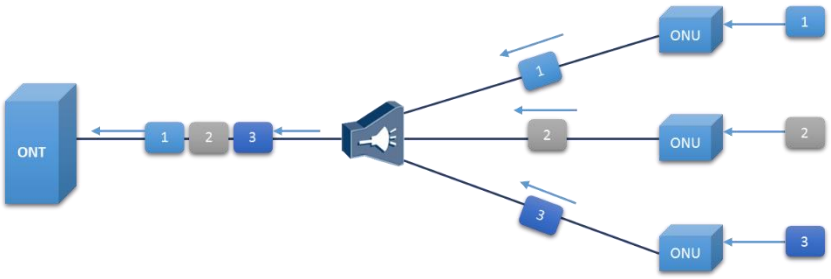

Figure 96: Transmission en upstream en TDMA. [18]

Pour le flux montant, le risque de collision entre les paquets des différents utilisateurs est fortement probable à cause de la distance différente entre le MSAN et les clients. C'est là où intervient le principe du ranging qui consiste en l'égalisation des délais de transmission pour éviter ce problème.

Chaque interface GPON du MSAN accepte plusieurs ONU identifiés par un ONU-ID qui représente un client chaque client est abonné à un ou plusieurs services qui représentent les Ports identifiés par le Port-ID et dont la bande passante est géré par des T-CONT qui sont identifiés par le Alloc-ID.

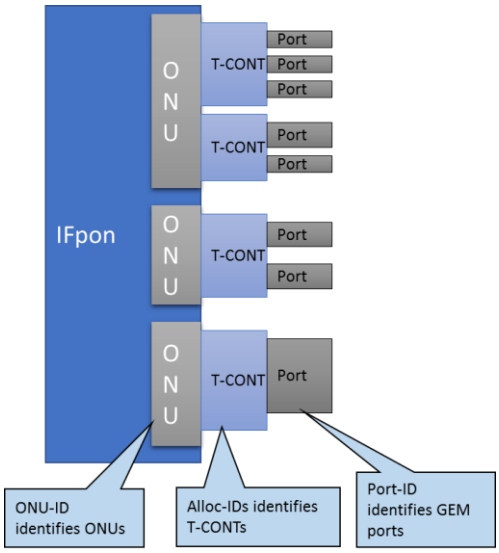

Figure 97: Architecture de multiplexage en GPON. [18]

Les types de T-CONT et de Bandes passantes sont résumés dans le tableau suivant :

Bandes passantes			Types de T-CONT				
Types		description	Type 1	Type 2	Type 3	Type 4	Type 5
Garanteed	Fixed	Allouée d'une manière permanente	✓				✓
	Assured	Alloué à la demande		✓	✓		✓
Additional	Non-Assured	Permet le partage de la bande passante selon un pourcentage relatif à la demande de l'utilisateur			✓		✓
	Best Effort	Permet le partage équitable de la bande passante entre les utilisateurs				✓	✓
Max.		Rassemble tous les types précédents			✓	✓	✓

Tableau 8: Relations entre les types de bandes passantes et les types de T-CONT.

La trame GPON est constituée de deux parties. La première est l'entête qui contient le champ upstream bandwidth map où sont définis les T-CONT. La deuxième partie est le payload.

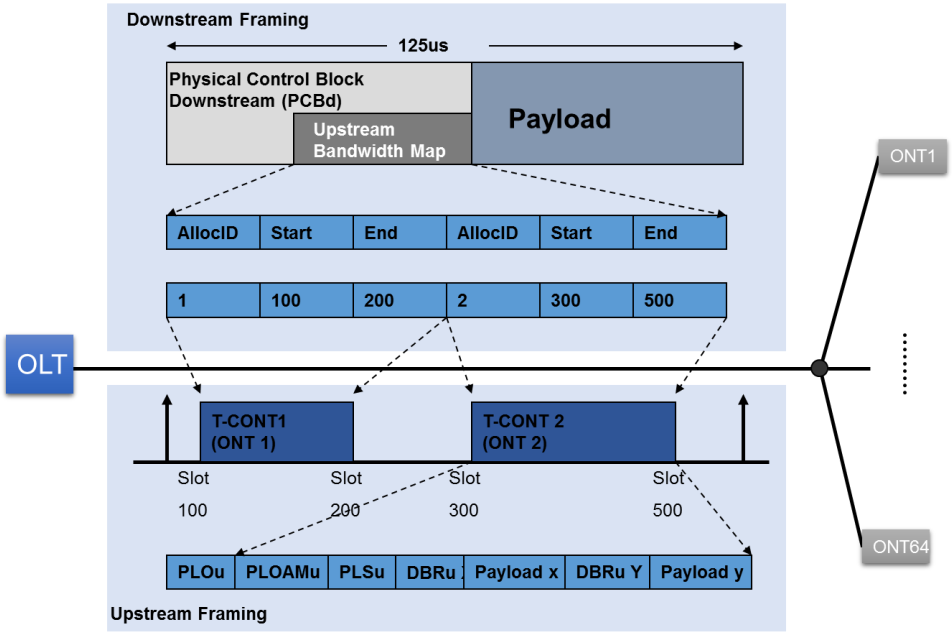

Figure 98: Structure de la trame GPON. [18]

En downstream, le champ upstream bandwidth map contient les Alloc-ID identifiant les T-CONT. Chaque Alloc-ID est suivi du début et de la fin de l'envoie c'est à dire les timeslots alloués à ce T-CONT.

En upstream, les T-CONT envoyés contiennent plusieurs champs d'informations identifiant le T-CONT ainsi que le champ DBRu qui identifie le DBA c'est-à-dire l'état du T-CONT. Le payload contient le DBA Repport qui englobe les informations essentielles pour l'allocation dynamique de la bande passante.

La bande passante est allouée dynamiquement par l'OLT pour le flux montant en utilisant le mécanisme DBA (Dynamic Bandwidth Assignment) qui est basé sur les informations du DBA report sous forme de bandwidth Map.