Mise à niveau des réseaux de transmission (Réseau de TUNISIE TELECOM en Exemple)

Elaboré par

Mazen ESSMARI

RAPPORT DE PROJET DE FIN D'ETUDES

Filière

Licence Appliquée en Sciences des Technologies de l'Information et des Communications

Université Virtuelle de Tunis

Encadré par

M. Naceur Al Andalosi

Année Universitaire
2010 -2011

- SOMMAIRE -

- INTRODUCTION -

Le monde de l'industrie des télécoms change très rapidement, et les opérateurs se trouvent face à des défis et des contraintes technico-économiques pour assurer la satisfaction de leurs clientèles et faire des économies majeurs en termes d'OPEX[1] et de CAPEX[2].

Avec la compétition féroce qui se produit, les fournisseurs du service doivent défendre leurs revenus du service existant et stimuler l'augmentation de la demande avec les nouveaux services. La compétition impose ainsi la proposition de prix plus attirants, assure la rapidité de création et livraison du service et une offre expérience rehaussée à l'utilisateur.

Les fournisseurs du service se sont rendu compte qu'un client qui prend des services multiples est plus lucratif qu'un client qui prend un service seul. C'est plus lucratif même si la même infrastructure peut être utilisée pour offrir ces services multiples. Ce type de convergence des services crée le changement du modèle économique de l'industrie des télécoms. Cependant, faire réponse au modèle économique changeant ajoute de nouveaux défis sur les infrastructures du réseau:

. Les entreprises demandent des solutions économiques avancées afin de mener une valeur et une efficacité améliorée pour le client.

. Les consommateurs demandent un contenu riche et des services empaquetés.

. Les utilisateurs finaux veulent accéder à leurs services n'importe quand, n'importe où, sur n'importe quel périphérique…

. La multimédia et services convergés exigent que le fournisseur améliore de facturation de ces services.

. Avec les multiples technologies, les services et les périphériques, les communications deviennent de plus en plus complexes; construire la loyauté du client exige qu'il soit satisfait de la qualité du service.

La migration vers des réseaux basés sur les paquets a été une tendance dominante dans l'industrie. Maintenant l'attention est concentrée sur l'optimisation des réseaux de transport pour la livraison de multiservices. Ces réseaux du transport ont été basés historiquement en Réseaux (SDH) et Réseaux (MAN).

Nous verrons dans cet œuvre les tendances de Tunisie Telecom tel qu'un opérateur historique et global, pour moderniser et mettre à niveau son réseau de transmission, et les scénarios adoptés pour satisfaire les applications et les services utilisant ce réseau.

Au premier chapitre, on passe par les différentes solutions de réseaux qui reposent sur la norme Ethernet et qui sont utilisées pour livrer des liens de transport à base de paquet et servant pour l'agrégation des

[1] OPEX: Operational Expenditure.
[2] CAPEX: Capital Expenditure.

données et formant un outil pour le « backhauling » des différents terminaux (**MSAN**, Media Gateway, **DSLAM**, **Node B**, Routeurs, Switch…) vers la partie cœur de l'opérateur.

Au second chapitre, on définit les réseaux à routage en longueurs d'ondes, comme une technique de choix qui peut limiter les dépenses de l'operateur (principalement les dépenses des travaux de génie civil et de la pose de nouveaux câbles **FO**) et d'augmenter le débit sur les boucles.

Au troisième chapitre, on se concentre sur les scenarios de changement et de mise à niveau du réseau de transport de Tunisie Telecom en fonction des nouvelles applications et des nouveaux services qu'offre l'opérateur.

CHAPITRE 1

Les Techniques de Transport basées sur la norme Ethernet

Les réseaux de prochaine génération (communément appelés **NGN** pour Next Generation Networks) à commutation de paquets, et Ethernet en particulier, gagnent de plus en plus la traction dans les réseaux **WAN**, ceci est dû aux avantages intrinsèques, tel que la simplicité du réseau, la haute capacité de la bande passante, l'approvisionnement mesurable et flexible du service, et les économies importantes et considérables dans les investissements du capital en matériels et en déploiements du service. Ethernet est aussi une technologie déjà familière pour les entreprises à travers leurs réseaux locaux **LAN**, ces dernières ne devraient avoir aucun problème en l'adoptant pour les services du réseau. Ainsi, la mise à niveau des services **WAN** d'Ethernet vers le transport Ethernet n'est pas sans défi, avec la diversité existante entre les réseaux d'accès et les réseaux de transport, le besoin d'établir une précision au service de bout-en-bout et des garanties de la performance mesurable, et la condition préalable d'assurer la continuité du service pour les applications de l'héritage à travers le « backhaul » de l'Ethernet.

Ce chapitre fournit l'information essentielle sur les questions clés impliquées dans le déploiement de nouveaux services de Transport à base d'Ethernet. Il examine les caractéristiques pour la connectivité Ethernet, la gestion de service et de trafic et résume les niveaux standards pour Ethernet **OAM** (opération, administration et maintenance).

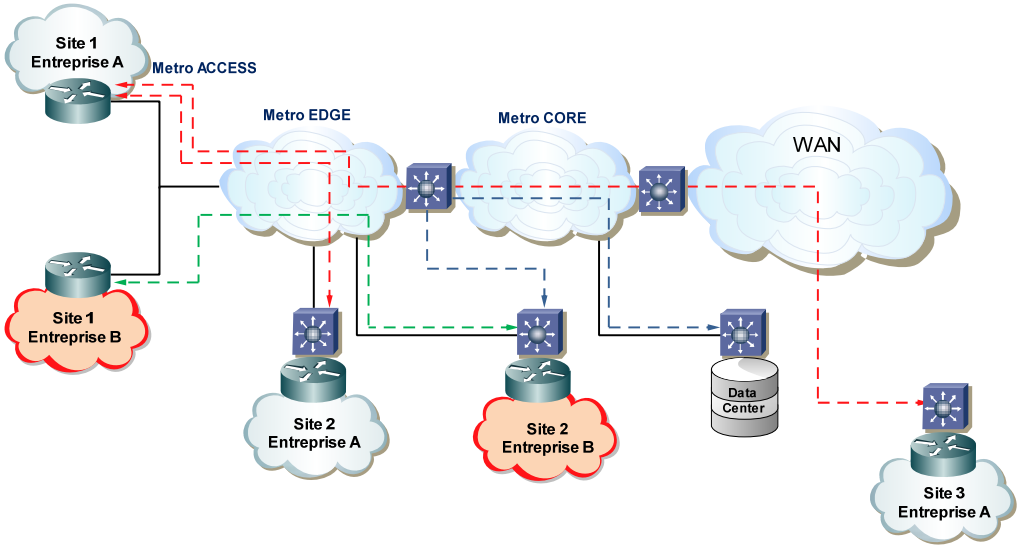
1. Introduction aux données dans le Metro

1.1. Une vue d'ensemble des données du Metro

Une vue d'ensemble des données du Metro met en perspective les différents services de métro et la façon dont ils sont offerts par les différents prestataires.

La Figure 1-1 illustre une vue du réseau Metro en montrant sur les aspects de l'accès des données, l'agrégation des données, et la prestation des services. Comme vous pouvez le voir, le métro est divisé en trois segments:

- **Metro ACCESS**: Ce segment constitue la portion du dernier mile (last mile portion), qui est la partie du réseau qui touche le client final.
- **Metro EDGE:** Ce segment constitue le premier niveau d'agrégation de métro. Les connexions qui quittent les nœuds sont regroupées aux équipements du central **CO** (Central Office) en plus de larges tuyaux transporteurs de données véhiculent les données vers le **WAN** (Wide Area Network).
- **Metro CORE :** - Ce segment constitue un deuxième niveau d'agrégation, où plusieurs « EDGE **CO** » sont regroupés à leur tour puis véhiculés vers le « CORE **CO** », ce dernier est connecté avec un ou plusieurs autres « CORE **CO**» afin de véhiculer les données à travers le **WAN**.



*** Figure 1-1. Une Vue d'ensemble des Données du Metro ***

Les scénarios d'agrégation sont multiples et très variés ce qui engendre parfois une confusion au niveau de la terminologie, par exemple on peur trouver parfois un seul niveau d'agrégation, c'est-à-dire les connexions des nœuds sont directement liés à un routeur du niveau « CORE **CO** », dans d'autres scénarios, le « CORE **CO** » est co-implanté avec le vaste zone **POP**.

1.2. Les services du Metro

Les services du Metro varient en fonction du marché ciblé que ce soit commercial ou résidentiel et s'il s'agit d'un service fourni en vente au détail ou d'un service fourni en vente en gros. La liste suivante donne un résumé de certains des services de Metro qui sont promus:

- Connectivité Internet.
- Service **LAN** transparent (réseau locaux en point à point).
- **L2VPN** (réseaux locaux **LAN** en point à point ou en multipoint à multipoints).
- **LAN** aux ressources du réseau (centre de données distant).
- Extranet.
- Réseaux locaux **LAN** à Frame Relay / **ATM**[1] **VPN**[2].
- Réseaux de stockage (**SAN**[3])
- Transport Metro (backhaul).

[1] ATM : Asynchronous Transfer Mode.
[2] VPN : Virtual Private Networks.
[3] SAN : Storage Area Networks

- **VoIP**[1]

Certains de ces services, tels que la connectivité Internet et les services **LAN** transparents (**TLS**[2]), ont été offerts pendant de nombreuses années. La différence maintenant est que ces services sont fournis avec la connectivité Ethernet, et les operateurs se dirigent vers un modèle dans lequel l'ensemble de ces services peuvent être offerts sur la même infrastructure et peuvent être vendus au même client, sans frais généraux opérationnels majeurs.

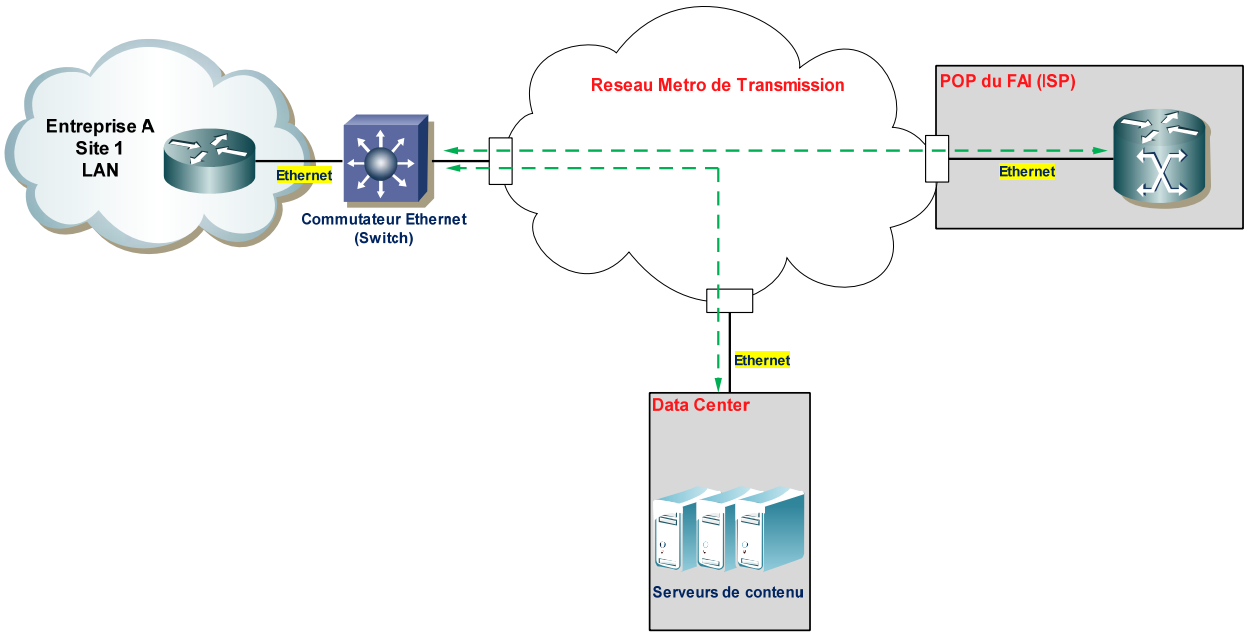
Cela introduit une excellente proposition de valeur pour le client et l'opérateur à la fois. Les services sont fournis par le transport de l'application via des connexions L2 point à point ou multipoint à multipoint. Les sections suivantes décrivent certains de ces services de façon plus détaillée.

1.2.1. LAN aux Ressources réseau

On a vue que les services d'Internet peuvent être délivrés au client par l'installation d'une liaison Ethernet au lieu d'une liaison **E1**[3] **TDM**[4]. Après que la connexion Ethernet soit installée chez le client final, l'opérateur peut vendre différents services au client, tels que le service Réseau Local **LAN** aux ressources du réseau. Un exemple d'un tel service est celle qui permet à une entreprise de sauvegarder ses données dans un emplacement distant et sécurisé en lui permettant de les récupérer en cas de catastrophe.

La figure 1-2 montre qu'en addition du service Internet, le client peut disposer d'une sauvegarde de ses données et du service de récupération des données en cas de défaillance en utilisant le Metro.

[1] VoIP : Voice Over IP.
[2] TLS : Transparent LAN Service.
[3] E1 : c'est le niveau Hiérarchique d'ordre 1 hérité des réseaux PDH (Plesiochronous Digital Hiearchy) classique, et qui vaut 2.048 Mbps.
[4] TDM : Time Division Multiplexing.



*** Figure 1-2. Réseaux locaux **LAN** aux ressources réseau ***

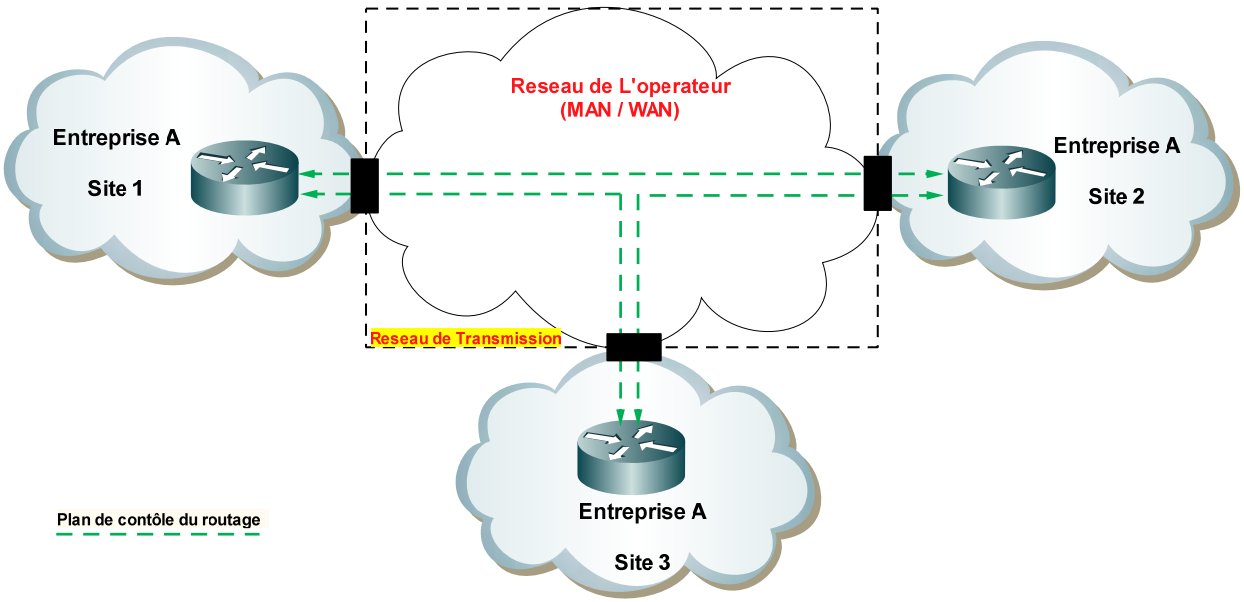
Pour les nouveaux réseaux de données dans lesquelles la connectivité se fait via des liens Gigabit et 10Gigabit[1], le Metro peut être transformé en un réseau local à très haut débit qui offre des applications gourmandes en bande passante et qui ne seraient pas normalement possible de déployer sur l'infrastructure **TDM**.

Comme l'a été mentionné précédemment, le service dans le métro prendra de nombreuses formes en fonction de la clientèle cible. Le même modèle du réseau local **LAN** au réseau des ressources pourrait être appliqué à des applications résidentielles, permettant aux opérateurs à entrer en concurrence avec les entreprises de câblodistribution dans la vente des services multimédia.

1.2.2. Les services Ethernet L2VPN

On remarque que beaucoup de services mentionnés sont des services purement L2 qui offrent une connectivité seulement. Ceci est similaire à l'héritage des services Frame Relay et **ATM**, où la connexion Frame Relay/**ATM** offre une conduite pure L2 et les services **IP** routé peut monter au-dessus de ce lien.

[1] Dès Juillet 2010, IEEE a mis une nouvelle normalisation intitulée IEEE 802.3az qui offre des liens à 40 Gigabit/s et 100 Gigabit/s.



*** Figure 1-3. Les services L2VPN ***

La figure 1-3 représente un opérateur déployant un service Ethernet **L2VPN**. Le réseau de transport se comporte comme un commutateur Ethernet L2 (L2 Ethernet Switch) qui offre une connectivité multipoint à multipoint entre les différents sites clients. Le client peut bénéficier de l'exécution son propre plan de contrôle d'une façon transparente sur le réseau de l'opérateur. Les routeurs du client peuvent échanger leurs propres protocoles de routage sans interférence avec le routage de l'opérateur, et l'opérateur n'est pas obligé à soutenir l'adressage IP du client. Une observation importante, tant que le réseau de l'opérateur se comporte comme un commutateur Ethernet L2 (L2 Ethernet Switch), la technologie sous-jacente et les plans de contrôle différents utilisés dans le réseau de transport ne sont pas nécessairement basées sur Ethernet ou sur un plan de contrôle de la couche 2.

1.2.3.La comparaison entre L'accès Ethernet et Frame Relay

Les services **VPN** du Frame Relay ont été largement acceptés et se sont avérés être très rentables par rapport aux services de ligne privée ou spécialisée point à point. En essence, les services Ethernet peuvent être considérée comme la prochaine génération de Frame Relay, car ils fournissent la plupart des avantages du Frame Relay avec une meilleure évolutivité dans la mesure où ils fournissant une bande passante plus large et des services de connectivité multipoint à multipoint. La liste suivante présente quelques-unes des similitudes et des différences entre un réseau Ethernet et un service de frame Relay:

- Vitesse de L'interface : L'intervalle de vitesse de l'interface du Frame Relay varie de sous-**E1**[1] jusqu'à des vitesses allant à **STM**n[2]. Toutefois, Frame Relay a été largement déployé à basse vitesse sous-**E1**, **E1** et **E3**[3]. Une interface Ethernet peut fonctionner jusqu'à 10 Gbps.

- Services de connectivité au Dernier Mile (Last Mile connectivity) : Les services d'Ethernet trouvent une meilleure acceptation dans les déploiements en réseau (où la fibre arrive jusqu'à l'immeuble), quel que soit le mode de transport. Frame Relay a l'avantage d'être déployé dans des applications hors-réseau sur les lignes de cuivre existantes **E1** et **E3**, qui, jusqu'ici, constitue un pourcentage très élevé de déploiements. Il ya des efforts existants dans les forums, tels que « Ethernet in the First Mile » (**EFM**), pour exécuter Ethernet directement sur les lignes de cuivre existantes.

- Support de circuit Virtuel : Ethernet et Frame Relay offrent une interface multiplexé qui permet au client à un endroit déterminé de communiquer avec d'autres différents endroits en utilisant la même interface physique. La notion de **VLAN**[4] Ethernet est similaire à celle nommé **PVC**[5] du Frame Relay.

- Connectivité multipoint : Une différence évidente entre Frame Relay et Ethernet est que les circuits virtuels du Frame Relay sont des circuits en point à point. Toute connectivité en point à multipoint ou en multipoint à multipoint entre les sites se fait via la fourniture de plusieurs **PVC** point à point et le routage entre ces **PVC** à une couche supérieure, la couche **IP**. Avec Ethernet, le **VLAN** constitue un domaine de diffusion, et de nombreux sites peuvent partager une connectivité en multipoint à multipoint et en L2.

- interface L2 : Un avantage très important que Frame Relay et Ethernet le partage et l'offre, c'est la capacité de maintenir la séparation entre la connectivité réseau en L2 et l'application de plus haut niveau **IP**, y compris le routage L3. Cela permet au client d'avoir le contrôle de ses réseaux existant en L2 ou en L3 et de garder une ligne de démarcation entre le réseau du client et le réseau du transporteur.

2. Les technologies du Metro

[1] Sous-E1 : n × 64 Kbps avec $0 \leq n \leq 32$.
[2] STMn : « Synchronous Transport Module » d'ordre n avec n = 1, 4,16 et 64.
[3] E3 : c'est le niveau Hiérarchique d'ordre 3 hérité des réseaux PDH (Plesiochronous Digital Hiearchy) classique, et qui vaut 34.368 Mbps.
[4] VLAN : Virtual Local Area Network.
[5] PVC : Permanent Virtual Circuit.

Les services et les applications du Metro Ethernet ne nécessitent pas forcément Ethernet comme technologie de transport sous-jacent. Le métro peut être fondé sur des technologies différentes, telles que :

- Ethernet sur **SDH** (**EOS**[1]).
- Resilient Packet Ring (**RPR**).
- Transport Ethernet.

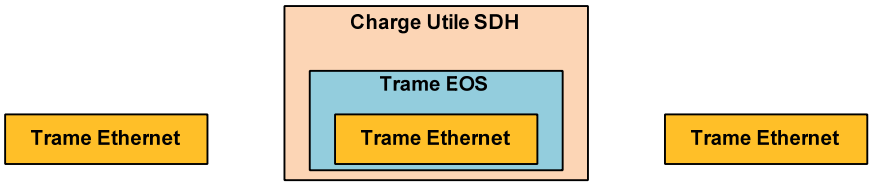
2.1. Ethernet sur SDH

De nombreux opérateurs historiques dans le monde ont déjà dépensé une fortune pour la construction d'une infrastructure de Metro **SDH**. Ces opérateurs voudraient profiter l'infrastructure existante pour fournir des services Ethernet de nouvelle génération. Pour de tels déploiements, la gestion de la bande passante sur le réseau est essentielle, en raison de la faible capacité des anneaux existants **SDH** et le fait qu'ils peuvent être facilement sursouscrits lorsqu'ils sont utilisés pour les services de données.

Traditionnellement, pour les opérateurs, il y a une séparation claire et nette entre le transport et les données. La partie réglementée de l'organisation s'occupe du matériel de transport uniquement, pas de matériel informatique. Avec **EOS**, les fournisseurs d'équipement brisent cette séparation et fondent une ligne entre les données et de transport, ce qui crée un problème pour l'adoption de la nouvelle technologie. Donc, il vaut la peine de temps d'expliquer la technologie **EOS** lui-même.

L'avantage de l'**EOS** est qu'il introduit un service Ethernet tout en conservant tous les attributs de l'infrastructure **SDH**, comme la restauration rapide **SDH**, contrôle da la qualité des liens et l'utilisation du réseau de gestion **OAM&P**[2] existant de **SDH**. Avec **EOS**, la trame Ethernet complète est encore préservée et encapsulée à l'intérieur de la charge utile de **SDH** à l'entrée du réseau et est extraite à la sortie.

Comme le montre la figure 1-4, toute la trame Ethernet est encapsulée dans un entête **EOS** par la fonction **EOS** du terminal à son entrée. La trame Ethernet est ensuite transférée sur l'enveloppe de la charge utile **SDH** (**SPE**[3]) et sont transportées sur l'anneau **SDH**. La trame Ethernet est ensuite extraite par la fonction **EOS** dans l'autre côté.



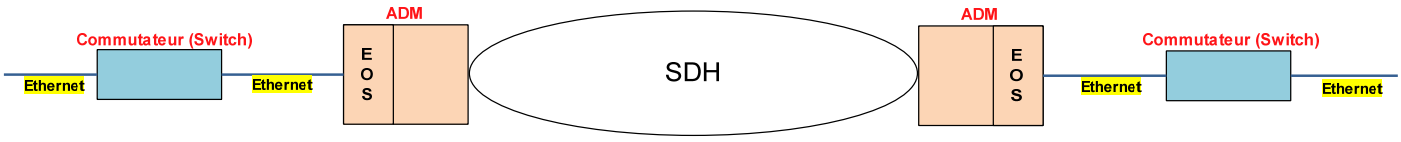
*** Figure 1-4. Ethernet sur **SDH** ***

[1] EOS :Ethernet Over SDH
[2] OAM&P : Operations, Administration, Maintenance & Provisioning.
[3] SPE: Synchronous Payload Envelope

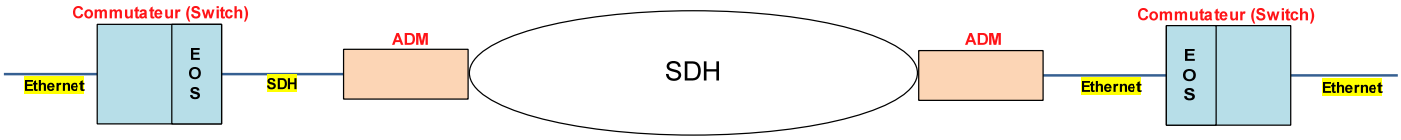
Il existe deux méthodes normalisées pour le transport de trames Ethernet sur un réseau SDH:

- **LAPS** : (Ethernet Over Link Access Procedure **SDH**) qui est définie par l'**UIT-T** selon la norme publiée X.86. **LAPS** est un protocole de connexion similaire à High-Level Data link Control (**HDLC**).
- **GFP** : (Generic Framing Procedure) est également une norme de l'**UIT** qui utilise le protocole de liaison simple de données (**SDL**[1]) comme point de départ. L'une des différences entre la **GFP** et **LAPS** est que la **GFP** peut accueillir des formats de trame autre qu'Ethernet, tels que les **PPP**[2], **FC**[3], **FICON**[4], **ESCON**[5].

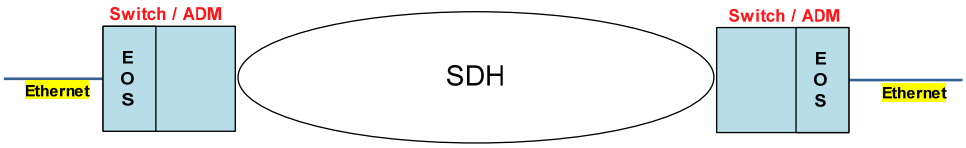
La fonction **EOS** peut résider à l'intérieur de l'équipement **SDH** ou à l'intérieur du commutateur de paquets. Les figures 1-5,1-6 et 1-7 montrent les différents scénarios pour la connexion **EOS**. Dans Figure 1-5, la fonction **EOS** est à l'intérieur du **ADM**[6]. Cela se fait normalement via une combinaison trameur/mappeur qui prend en charge **EOS**. La fonction de mappage **EOS** ajoute un paquetage selon la norme X.86 connu encore par **GFP** autour de l'ensemble de la trame Ethernet, et la fonction de tramage encapsule la trame dans le **SPE** du **SDH**. Dès lors, le **SPE** du **SDH** est transporté à travers l'anneau **SDH** et se détache sur le côté de sortie. L'**ADM** qui contient la fonction **EOS** en addition à d'autres fonctions comme la concaténation virtuelle sont appelés **ADM** de nouvelle génération. Figure 1-6 met la fonction **EO**S à l'intérieur du commutateur.



*** Figure 1-5. La fonction **EOS** à l'intérieur de l'**ADM** ***



*** Figure 1-6. La fonction **EOS** à l'intérieur du commutateur ***



*** Figure 1-7. Les fonctions de l'**EOS** et de commutation groupées à l'intérieur de l'**ADM** ***

[1] SDL : Simple Data Link.
[2] PPP : Point to Point Protocol.
[3] FC : Fiber Channel.
[4] FICON : Fiber Connectivity.
[5] ESCON : Enterprise Systems Connection.
[6] ADM : Add / Drop Multiplexer.

La différence ici est que l'équipement de données et l'équipement de transport ou de transmission sont deux entités différentes qui peuvent être détenus par différents groupes opérationnels au sein du même support. Cela rend plus facile aux entités réglementées et non réglementées de déployer un nouveau service sur support. La seule responsabilité du groupe réglementé est de fournir des circuits **SDH**, comme c'est le cas de la voix traditionnelle ou circuits loués en ligne. Le groupe non réglementée déploie à son tour dans les services de données de la couche supérieure. Il convient également de mentionner que dans ce scénario, le commutateur Ethernet (Ethernet Switch) qui offre les services de données a le contrôle complet des affluents **SDH**. Ceci est en opposition à la figure 1-5, dans laquelle les affluents **SDH** sont terminés à l'intérieur de l'**ADM**, et le commutateur Ethernet (Ethernet Switch) ne voit qu'un lien Ethernet concaténés. La figure 1-7 illustre la combinaison des fonctions de la commutation de paquets, des fonctions de l'**ADM**, et des fonctions **EOS** dans le même équipement fournissant ainsi une efficacité en termes d'équipements.

EOS introduit une certaine inefficacité de la bande passante en déployant les services du Metro Ethernet en raison de l'inadéquation entre les liens **SDH** et les liens Ethernet. La concaténation virtuelle (**VCAT**) est un mécanisme utilisé pour atténuer ces inefficacités, comme nous le verrons la prochaine.

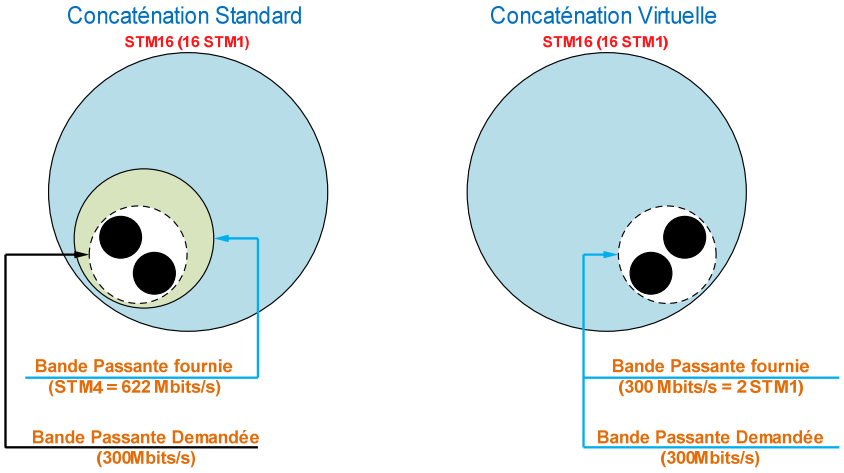
2.1.1. Rôle de la concaténation virtuelle

La concaténation virtuelle est une mesure pour réduire les inefficacités de la bande passante **TDM** sur des anneaux **SDH**. Avec la concaténation standard du **SDH**, les liens **SDH** sont provisionnés avec un léger surdébit qui ne peut pas être adaptés aux besoins en bande passante réelle. Les circuits **TDM** sont soit trop petits ou trop grands pour accueillir la bande passante requise. Sur un anneau **SDH,** une fois le circuit est alloué, l'anneau perd cette quantité de bande passante qu'elle soit utilisée ou non.

Avec **VCAT**, un certain nombre de petits conduits sont concaténées et assemblés pour créer un plus grand conduit qui transporte plus de données par seconde. La concaténation virtuelle se fait sur la couche (L1) du SDH lui-même, ce qui signifie que les différents circuits individuels sont liés et présentés à la couche réseau supérieure comme un seul conduit physique. La concaténation virtuelle permet le regroupement de n***STM** ou de n***VC**, permettant la création de conduits qui peuvent être à la taille bande passante requise.

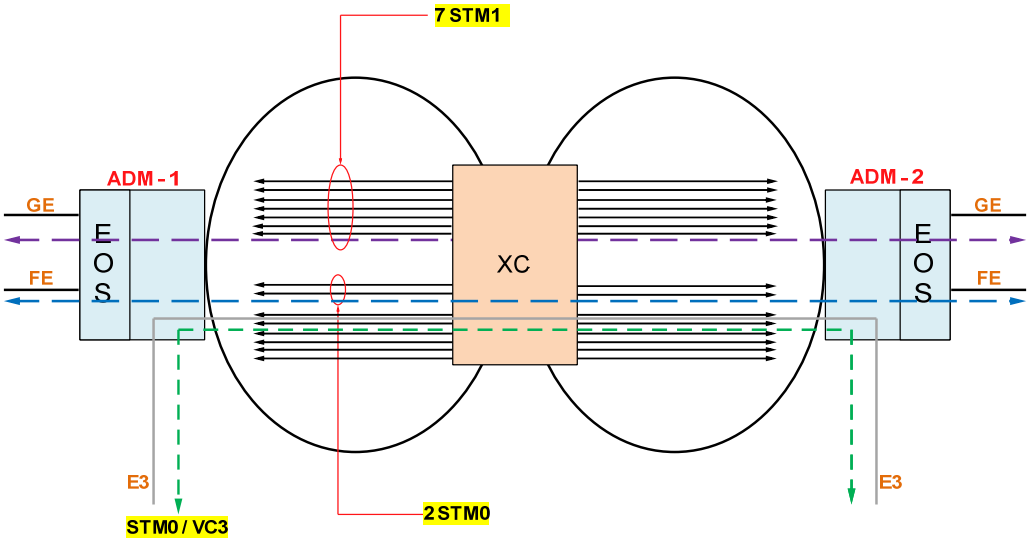
La figure 1-8 met en évidence l'efficacité de la bande passante que peut fournir le mécanisme **VCAT**. On peut allouer au client 2 **STM1** pour lui fournir un débit de 300 Mbit/s, ce qui est inefficace d'une façon générale parce que le coût d'exploitation augmente et la garantie de la totalité de la bande passante n'est pas assurée et met une restriction du débit des paquets à 150 Mbit/s (car les circuits physiques élémentaires sont limités par la bande passante de **STM1**). On peut aussi allouer toute une **STM4**, mais cette méthode peut causer la perte de 2 **STM1** qui ne seront pas exploités et qui ne pourront pas être alloués pour un autre client.

Avec la concaténation virtuelle, l'opérateur peut offrir un conduit au débit de 300 Mbits/s par la fusion de 2 **STM1** engendrant un gros conduit donc on élimine le gaspillage de la bande passante.



*** Figure 1-8. La concaténation virtuelle ***

La figure 1-9 montre un exemple de la façon dont plusieurs services tels que les services de connectivité Ethernet et les services traditionnels de **TDM** peuvent être transmis sur la même infrastructure **SDH**. Si les équipements **SDH** soutiennent le mécanisme **VCAT**, une interface Gigabit Ethernet (**GE**) ou 1000 Mbits/s peut être effectuée par un conduit de 7 **STM1**[1] concaténés, une autre interface Fast Ethernet (**FE**) ou 100 Mbits/s peut être réalisée sur deux **STM0**[2], et une interface **E3** traditionnelle peut être effectuée sur une seule **VC3**. Dans certains cas, la vitesse de l'interface Ethernet ne correspond pas à la vitesse de la côté des réseaux **SDH**.



*** Figure 1-9. Transport Ethernet sur SDH ***

[1] STM1 = 155.520 Mbits/s.
[2] STM0 = 51.840 Mbits/s.

Une interface Fast Ethernet à 100 Mbits/s, par exemple, peut être effectuée sur un seul **STM0**, ou deux **STM0**, ou quelques ou plusieurs **VC12**. Ces scénarios sont utilisés pour arriver à minimiser les pertes de paquets et assurer une bonne gestion de la bande passante.

Les fonctions de l'**EOS** et le mécanisme du **VCAT** sont mises en œuvre aux points d'entrée et de sortie de l'infrastructure **SDH**, et pas nécessairement à tous les stations **SDH** tout au long de l'itinéraire. Dans Figure 1-9, l'**ADM1** et l'**ADM2** supportent les fonctions de l'**EOS** et les fonctions du **VCAT**, tandis que l'équipement du cross-connexion (**XC**) ou de brassage qui relie les deux anneaux reste en état traditionnelle. Cependant, pour que le mécanisme du **VCAT** soit efficace, l'équipement **SDH** sur l'anneau doit être capable d'assurer le brassage les affluents pris en charge par le **VCAT**.

2.1.2. Link Capacity Adjustement Scheme (LCAS)

La concaténation virtuelle est un outil puissant pour le groupement efficace de la bande passante et la création de conduits qui correspondent à la bande passante requise. Cependant, le besoin du client en bande passante peut changer au fil du temps, ce qui nécessite que les conduits **SDH** devront être redimensionnés. Cela pourrait causer des perturbations sur le réseau en tant que les conduits **SDH** chaînes sont ajoutés ou supprimés. Le mécanisme de l'ajustement de la capacité du lien (Link Capacity Adjustement Scheme : **LCAS**) est un protocole qui permet aux conduits d'être redimensionnés à tout moment sans percussions sur le trafic ou sur le lien. **LCAS** exécute également des contrôles de connectivité pour permettre de retirer les liens échoués d'être et d'ajouter de nouveaux liens dynamiquement et sans perturber le trafic sur le réseau.

La combinaison d'**EOS**, **VCAT** et **LCAS** assure une efficacité maximale lors du déploiement des services d'Ethernet sur **SDH**.

NOTE

La concaténation virtuelle et **EOS** sont des technologies orthogonales, ce qui signifie qu'ils sont totalement indépendants. **EOS** est une technologie de mappage qui fonctionne sur la concaténation standard et le mécanisme de la concaténation virtuelle **VCAT**, mais les avantages sont obtenus si elle est faite sur cette dernière.

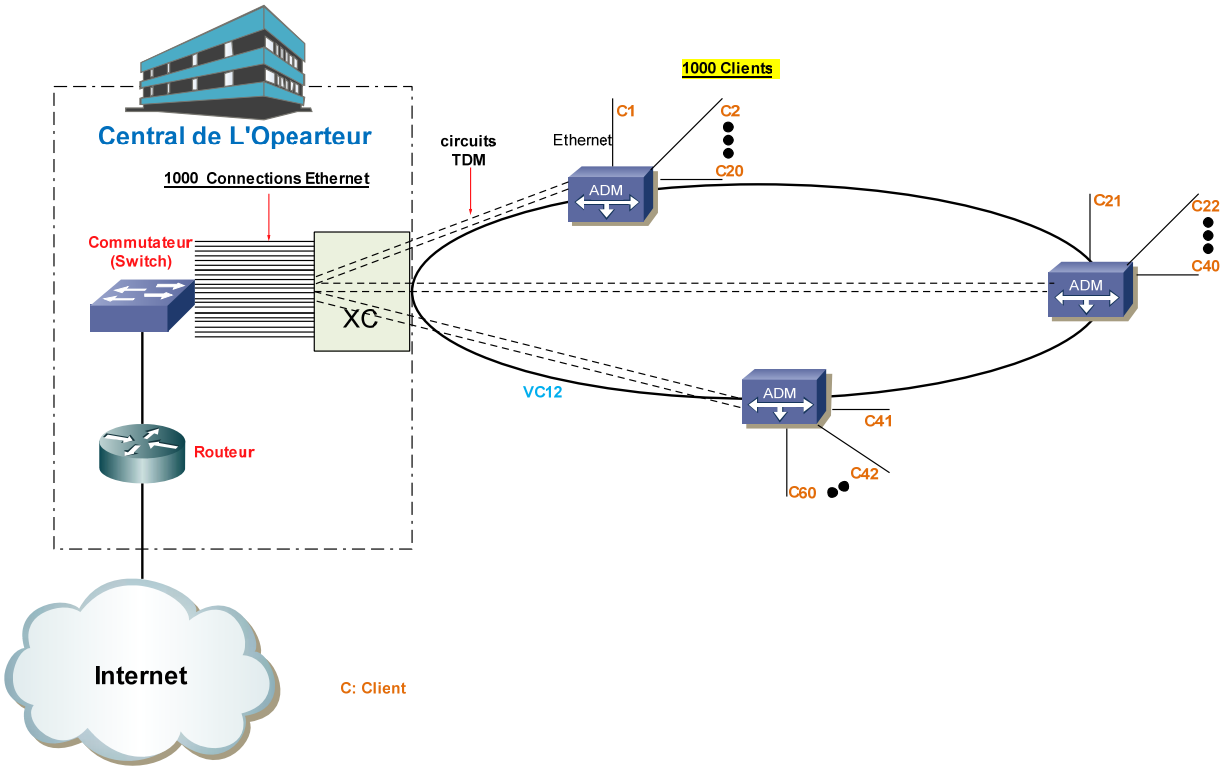
2.1.3. EOS Utilisé comme un service de transport

Ethernet sur **SDH** est encore un service de transport avec une interface Ethernet, similaire au service traditionnel de ligne privée avec des interfaces **E1**, **E3**, ou **STM**n. L'**EOS** offre ce qui est comparable à service de ligne louée point à point en mode paquet. **EOS** est une technologie de mappage des paquets, et non une technologie de "commutation de paquets», et n'offre pas la fonction de multiplexage de paquets qui est

nécessaire pour l'agrégation et la désagrégation des services. Afin de fournir des services de commutation de données améliorés, on a besoin d'introduire des fonctionnalités de commutation de paquets dans l'équipement de Metro.

Le manque de multiplexage de paquets pour le service **EOS** et le fait que des centaines de circuits point à point doivent être fournis entre les clients et le central de l'operateur (**CO**[1]) créent un problème majeur lors de l'agrégation des services dans les déploiements à grande échelle. Chaque circuit individuel **EOS** peut être présenté comme une interface Ethernet distinct dans le **CO**. Avec des centaines de clients utilisant des circuits **EOS**, le **CO** devra mettre fin à des milliers de fils Ethernet individuels.

La figure 1-10 illustre un scénario dans lequel un opérateur utilise **EOS** pour fournir un service de base de connectivité à Internet. Un anneau d'accès Metro **SDH** relie plusieurs entreprises et multiples zones résidentielles au central de l'opérateur (**CO**). L'**ADM** de la prochaine génération fournie des connexions Ethernet à 100 Mbits/s qui se connectent à des routeurs individuels propres aux abonnés. L'anneau lui-même dans cet exemple permet la canalisation des débits inférieurs au niveau de **E1** (2.048 Mbits/s) et chaque connexion est mappée en des circuits formés par (un ou plusieurs n***VC12**).



*** Figure 1-10. **EOS** à l'intérieur de l'équipement de transport ***

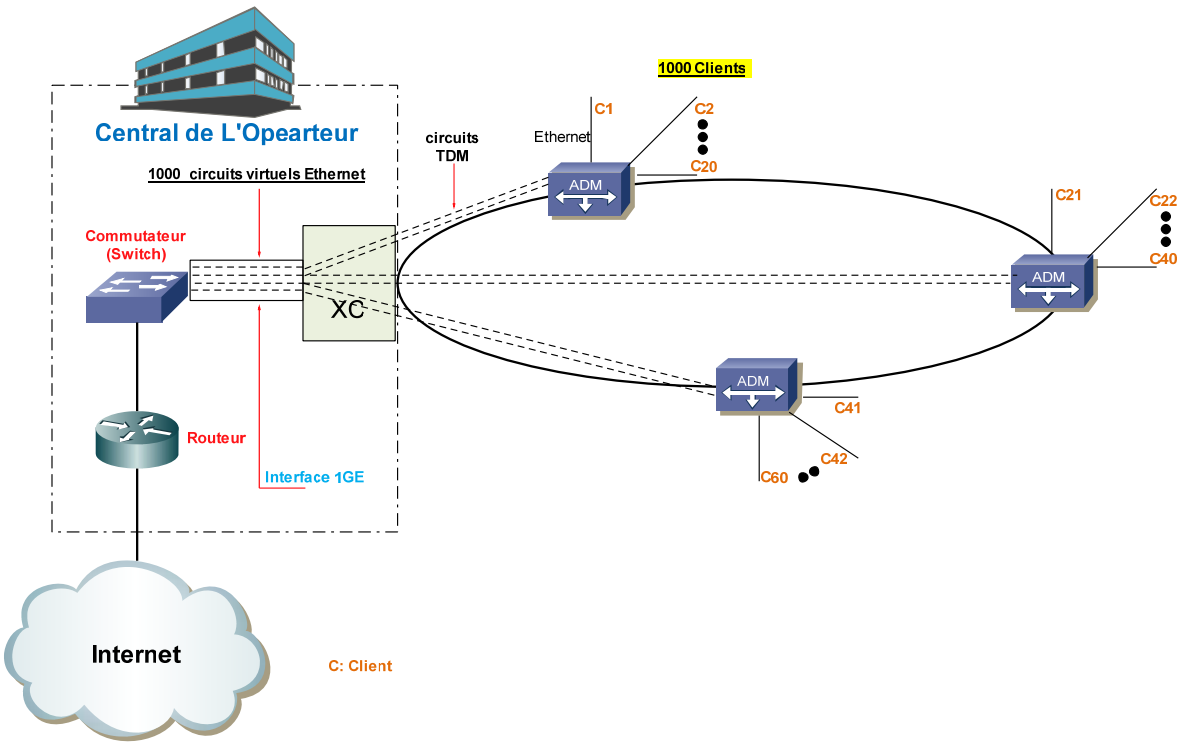
[1] CO: Central Office

Pour chaque client doté d'une interface Ethernet, une interface Ethernet est étendue hors du **XC**[1] au **CO**, et ce pour les spécificités du **XC** qui fonctionne au niveau du **TDM**, et chaque circuit doit être fini d'une façon individuelle. Les interfaces Ethernet individuelles sont ensuite connectées à un commutateur Ethernet «Ethernet Switch» qui agrège le trafic vers le routeur du **FAI**[2]. Cela signifie que si un nœud possède 20 clients, 20 circuits différents doivent être fournis et devrons être étendus hors du **XC** au **CO**. Si le **CO** prend en charge 50 nœuds avec 20 clients par nœud, 1000 circuits **TDM** doivent être fournis, et donc 1000 interfaces Ethernet doivent être étendues au niveau du **CO**. Ce modèle s'avère très inefficace et engendre des problèmes au niveau de la gestion ou en terme d'équipements.

Le **XC** sera chargé par les interfaces Fast Ethernet physiques, et la gestion de la connectivité physique devient très difficile. La solution logique à ce problème consiste à introduire des techniques d'agrégation à l'intérieur du brasseur **XC** en utilisant des **VLAN**[3] Ethernet et d'agréger plusieurs circuits Ethernet sur une seule interface Gigabit Ethernet (**GE**) ou une interface 10Gigabit Ethernet (10**GE**) où chaque circuit est identifié individuellement.

La figure 1-11 montre un exemple dans lequel le **XC** agrège les différents circuits **EOS** sur une seule interface Ethernet qui se connecte à un commutateur Ethernet (Ethernet Switch). Pour ce faire, le **XC** doit être capable d'assurer la séparation logique des circuits individuels **EOS** lors de leur présentation au commutateur Ethernet. Ce ci doit être fait parce que le trafic envoyé à partir du commutateur Ethernet au **XC** sur le port **GE** doit être étiqueté avec l'**ID** du circuit correct pour atteindre la destination correcte. Une méthode est d'avoir l'étiquette des circuits individuels du **XC** avec un **ID** de **VLAN** avant d'envoyer le flux vers le commutateur Ethernet. D'autres implémentations actuelles mettent l'ensemble de la fonction de raccordement à l'intérieur du **XC** lui-même, pour permettre à plusieurs flux **EOS** à être regroupés sur une seule interface à la sortie de l'équipement de transmission.

[1] XC: Cross-Connect Equipment : Brasseur.
[2] FAI: Fournisseurs d'Accès Internet
[3] VLAN : Virtual Local Area Network.

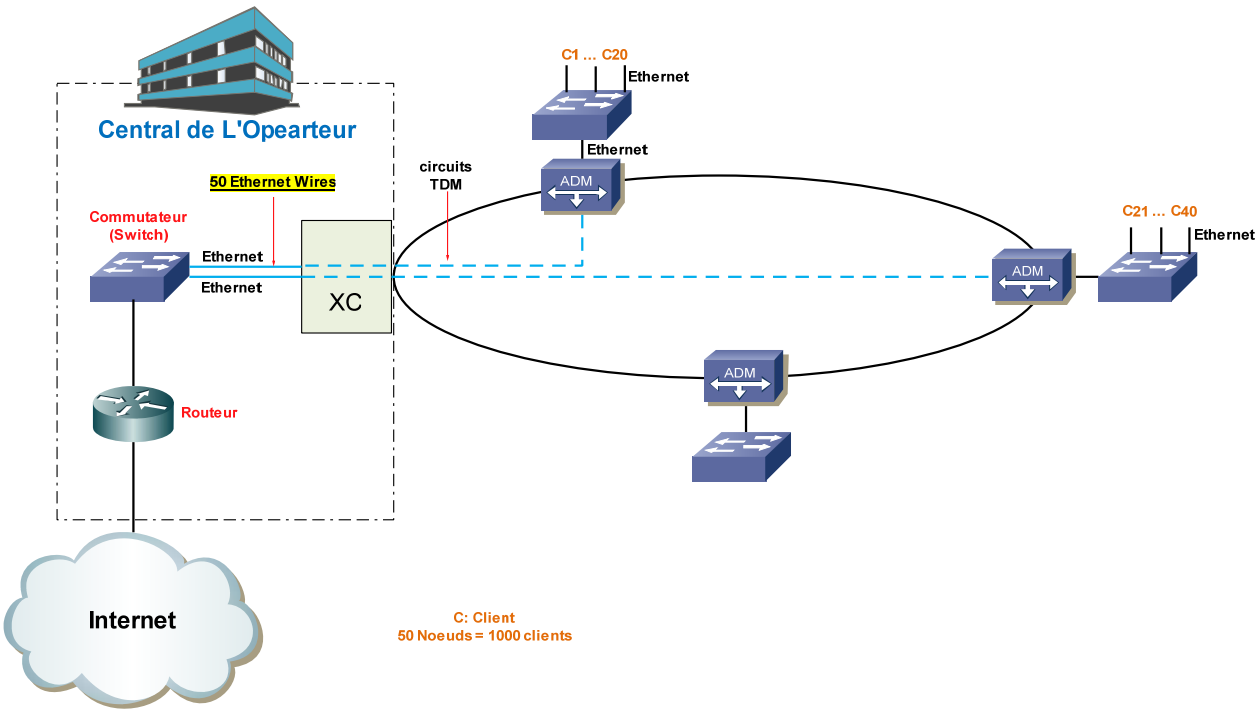


*** Figure 1-11. Agrégation **EO**S à intérieur de l'équipement de transmission. ***

2.1.4. EOS avec multiplexage de paquets à l'accès

L'exemple précédent suppose que chaque client du nœud prend un circuit individuel **TDM**. Une autre solution pour le fournisseur de services consiste à introduire de multiplexage de paquets dans le commutateur d'accès. Le prestataire de services peut réaliser des économies en ayant plusieurs clients partagent le même circuit **TDM**. Ces économies se traduisent par une baisse des coûts pour le service de connectivité de base fournis à la clientèle.

La figure 1-12 montre un scénario où, dans les mêmes 50 nœuds en Metro, chaque nœud possède une **STM0** lien qui est partagée par l'ensemble des 20 clients dans chaque nœud. Ceci réduit considérablement le nombre de circuits **TDM** qui doivent être fournis, parce que tous les clients de du même nœud partagent le même circuit **STM0** vers le central de l'opérateur, ce qui réduit l'ensemble des circuits **TDM** de 1000 à 50. Il est à noter que 50 ports Ethernet doivent encore être étendus dans le CO si le brasseur n'a pas la faculté de d'étiqueter ou d'assurer le multiplexage de paquets.



*** Figure 1-12. **EOS** avec multiplexage de paquets à l'accès ***

Le multiplexage des paquets dans le dernier mile (last mile) est encore un autre pas de plus que les opérateurs Metro aurait à adopter pour migrer vers la prestation les services d'Ethernet commuté. Le trafic provenant de plusieurs clients se battrait pour le lien en **STM0**, et un client avec une interface Fast Ethernet (100 Mbit/s) pourrait facilement surmonter le lien de 50 Mbits/s. L'opérateur aurait besoin d'utiliser des techniques telles que la politique de trafic et la mise en forme de trafic pour qu'il soit capable de fournir à ses clients plusieurs niveaux de bande passante.

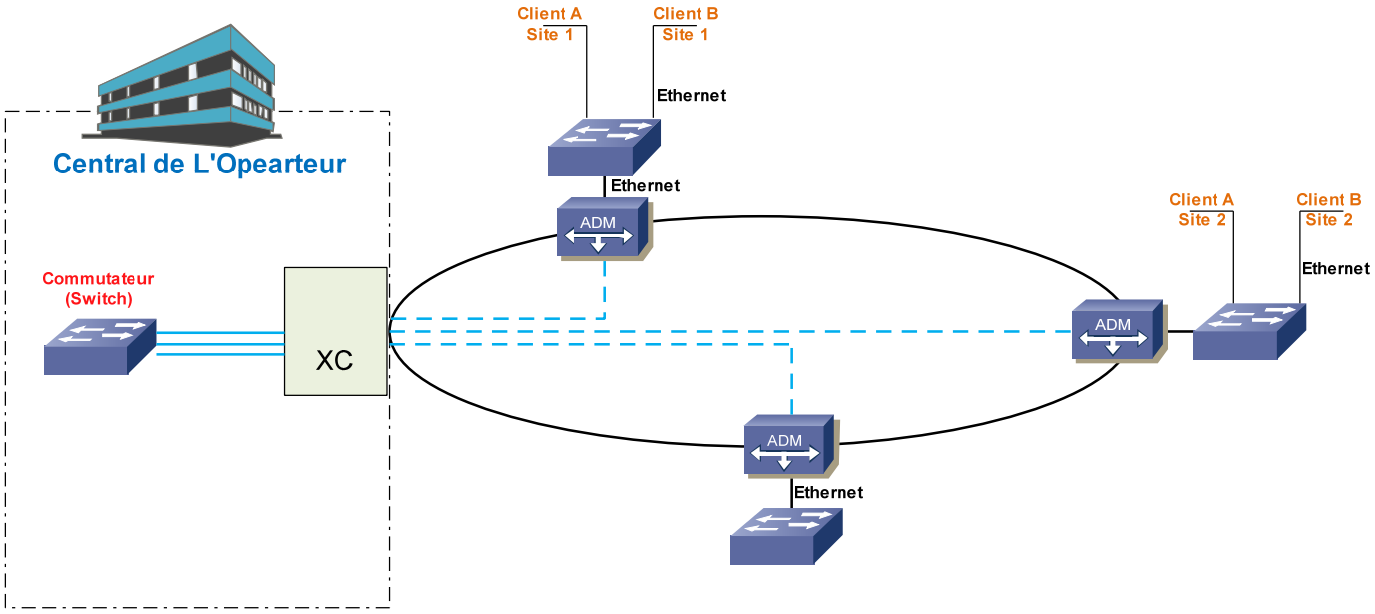
2.1.5. EOS avec commutation de paquets

Jusqu'ici, La discussion a abordé la faculté de fournir des lignes louées de base en point à point ou d'un service connectivité à Internet. Des services **VPN** plus avancés peuvent également être livrés sur le réseau Metro **SDH** qui prend en charge l'**EOS**. Avec un service de **VPN**, l'hypothèse est que différents endroits du "même" client existent dans une région métropolitaine, et le client veut être capable de se lier à ces endroits via un réseau virtuel. Ce type de service exige la commutation de paquets. Bien sûr, si tout le besoin du client réside dans un service point à point, aucune commutation n'est requise. La commutation de paquets peut être livrée en utilisant l'une de ces deux méthodes:

- Commutation centralisée.
- Commutation locale.

a. EOS avec commutation centralisée

Avec la commutation centralisée, un circuit **TDM** est fournit à partir de chaque nœud vers le central de l'opérateur (**CO**). Tous les circuits trouvent leurs fins dans le **CO**, où se déroule la commutation de paquets. On note que le fonctionnement du standard **SDH** dans les anneaux à trajet commuté unidirectionnel (**UPSR**[1]) est d'avoir des circuits actifs et des circuits de protection sur l'autre côté de l'anneau pour atteindre le temps de 50 ms d'échec de l'anneau. Ainsi, dans le Metro qui dispose de 50 nœuds, 50 circuits **STM0** actives et 50 circuits **STM0** de protection sont fournis. On note également que dans le cas du brasseur **XC** qui ne supporte pas l'étiquetage des paquets ou leur commutation, 50 interfaces Ethernet ont besoin d'être connecté au commutateur Ethernet au sein du **CO** Dans la figure 1-13, le client A dans les sites 1 et 2 appartient au [**VPN** A], alors que le client B dans les sites 1 et 2 appartient au [**VPN** B].



*** Figure 1-13. **EOS** avec commutation centralisée ***

b. EOS avec commutation locale

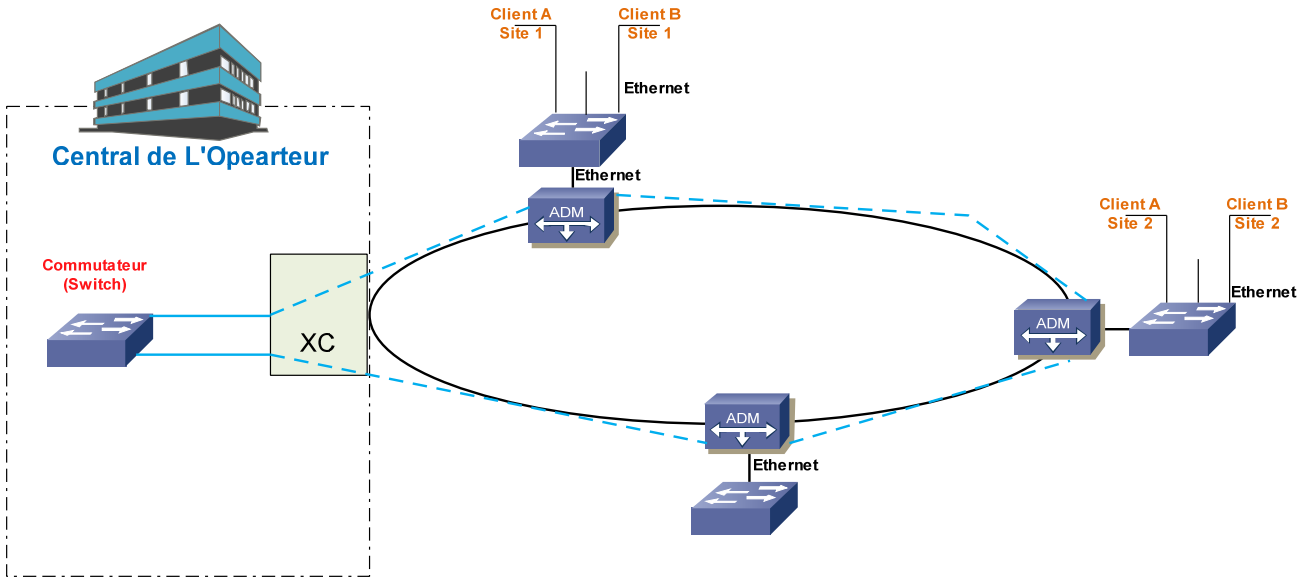
Avec la commutation locale, la commutation de paquets se produit sur chaque nœud de l'anneau. La différence ici est que les circuits **TDM** ne sont plus fournis entre les terminaisons des nœuds et le **CO**, mais resterons toujours fournis autour de l'anneau. Chaque **ADM** dans le nœud termine les circuits pour les deux côtés EST et OUEST, et les paquets sont commuté à la fonction de commutation locale, comme le montre la figure 1-14. Dans ce cas, la protection de l'anneau **SDH** n'est pas utilisée. L'opérateur Metro doit ainsi compter sur la protection de niveau supérieur. Dans le cas d'Ethernet L2, cela signifie la mise en œuvre des mécanismes standards de Spanning Tree, tels que le « Spanning Tree Protocol » (**STP**[2]), ou d'autres mécanismes

[1] UPSR : Unidirectional Path Switching Ring

2 STP : Le Spanning Tree Protocol (aussi appelé STP) est un protocole réseau permettant de déterminer une topologie réseau sans boucle (appelée arbre) dans les LAN avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985.

Mode de fonctionnement

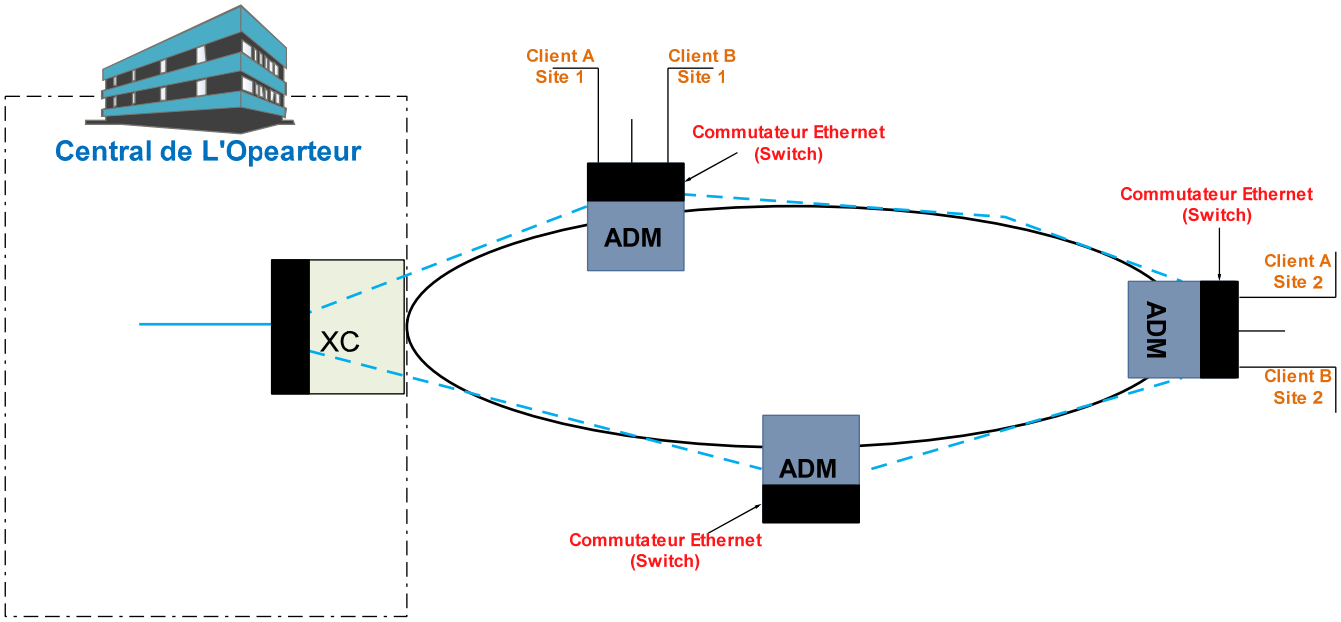
propriétaires qu'offrent les constructeurs des Commutateur Ethernet. A noter également dans la Figure 1-14 que, dans chaque **ADM**, une interface Ethernet distinct est allouée à chaque circuit **TDM** qui se prend fin, à moins que l'**ADM** lui-même a une fonction de commutation de paquets pour agréger le trafic vers le nœud. Si le nœud demande plus de bande passante, le mécanisme du **VCAT** peut être utilisé pour agréger plus de circuits tout en les ressemblant en un seul conduit.



*** Figure 1-14. **EOS** avec la commutation locale. ***

Une variante de la commutation locale est d'intégrer la fonction de commutation Ethernet et la fonction d'**ADM/EOS** dans le même coffre, comme le montre la Figure 1-15.

Les réseaux commutés de type Ethernet doivent avoir un unique chemin entre deux points, cela s'appelle une topologie sans boucle. En effet, la présence de boucle génère des tempêtes de diffusion qui paralysent le réseau. Cependant, un bon réseau doit aussi inclure une redondance pour fournir un chemin alternatif en cas de panne d'une liaison ou d'un commutateur. L'algorithme de « Spanning Tree Minimum » garantit l'unicité du chemin entre deux points du réseau en affectant un port dédié (root port), celui qui a le chemin le plus court vers le root bridge, à chaque segment du LAN (domaine de collision).



*** Figure 1-15. Une variante d'**EOS** avec la commutation locale. ***

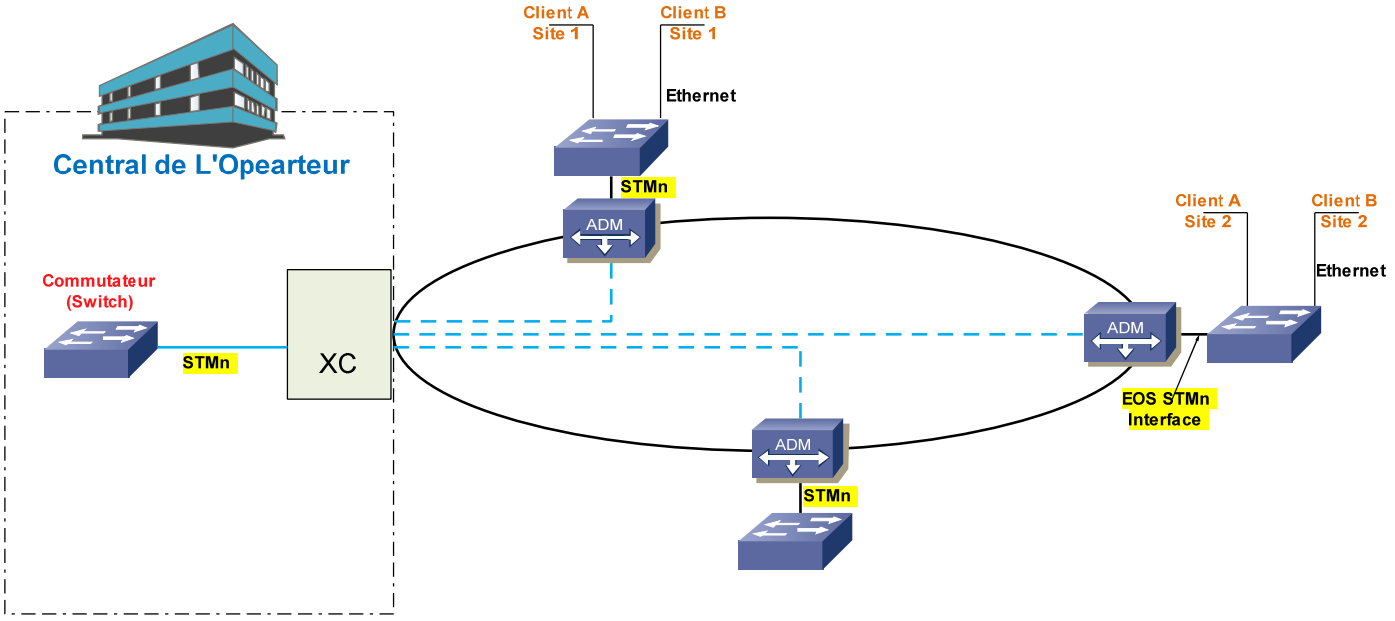
Dans ce cas, les circuits **TDM** sont encore terminés à chaque unité commutateur/**ADM** sur l'anneau. L'avantage de ce modèle est qu'il réduit le nombre d'unités déployées dans le réseau, mais il brouille la ligne entre l'exploitation des données et des réseaux **TDM**.

2.1.6. Les interfaces EOS dans l'équipement de données

Jusqu'à présent, on a discuté les différents scénarios pour avoir une interface **EOS** dans l'équipement de transmission ou de transport. On aborde dans ce qui suit le scénario dans lequel les interfaces **EOS** font partie de l'équipement de données plutôt que l'équipement de transmission. Dans ce modèle, l'équipement de transport n'est pas obligé à assurer le mappage des trames Ethernet transmises dans la charge utile du SDH et le matériel de commutation de données prend cette fonction en charge.

Les interfaces **EOS** à l'intérieur l'équipement de données, comme le montre la Figure 1-16, sont interfaces **SDH** avec une fonction de mappage qui fait correspondre les trames **EOS** effectuées à l'intérieur de la charge utile du **SDH** à une trame Ethernet. La trame Ethernet est à son tour présentée à la logique de commutation à l'intérieur de l'équipement de données. Comme dans le cas de l'équipement de transmission, l'interface **EOS** peut soutenir **VCAT**. L'avantage de ce modèle est que la fonction de commutation, la fonction **EOS**, et les fonctions **VCAT** sont tous dans la même unité et sont découplés de l'unité de **TDM**, qui peut déjà être installé dans le réseau. Cela permet à l'équipement de données d'assurer un meilleur contrôle sur le mappage des différents flux de données sur les circuits **SDH**. Avec ce modèle, les services de commutation Ethernet multipoint à multipoint peuvent être fournis d'une façon efficace tout en tirant parti de

l'infrastructure existante **SDH** héritée. Cela correspond également mieux avec le modèle opérationnel actuel, dans lequel la transmission ou le transport et les données sont gérées séparément.



*** Figure 1-16. **EOS** dans l'équipement de données ***

2.2. Risilient Packet Ring (RPP)

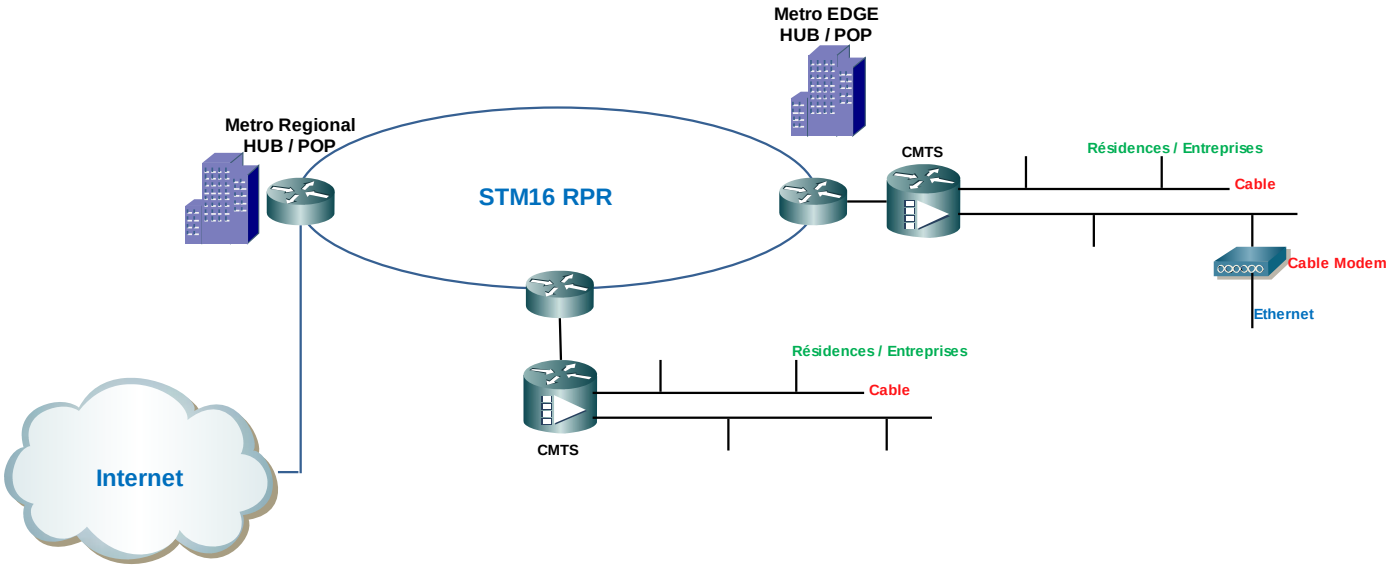
RPR joue également un rôle important dans le développement de services de données dans le Metro. **RPR** est un nouveau protocole Media Access Control (**MAC**) qui est conçu pour optimiser la gestion de la bande passante et de faciliter le déploiement des services de données via un réseau en anneau. Les racines du **RPR** reviennent au point où Cisco Systems a adopté une technologie propriétaire nommée **Data Packet Transport (DPT)** pour optimiser les anneaux de paquets pour la résilience et la gestion de bande passante. Le **DTC** a trouvé son chemin dans le groupe de travail **IEEE 802.17**, qui a conduit à la création de la norme **RPR** qui diffère de l'approche initiale du **DPT**.

RPR a été jusqu'ici une approche très intéressante pour les opérateurs de services multiples (**MSO**[1]), tels que les câblo-opérateurs qui agrègent le trafic à partir de systèmes de terminaison modem câble (**CMTS**[2]) dans le Metro. Jusqu'à présent, les opérateurs historiques de télécommunications ne sont pas largement attirés par le concept **RPR**. La raison principale pour laquelle ces opérateurs n'ont pas intérêt à la technologie du **RPR** est qu'iles considèrent sa déploiement comme des nouveaux déploiements, par rapport au déploiement de l'**EOS**, dont les infrastructures sont existantes et s'avère donc plus évolutif. **RPR** est une nouvelle technologie d'anneaux de paquets qui est déployée sur la fibre noire ou en utilisant le multiplexage par répartition en

[1] MSO: Multiple Service Operators
[2] CMTS: Cable Modem Termination System.

longueur d'onde (**WDM**[1]) au lieu des anneaux traditionnels **SDH**. **RPR** pourrait être déployé en superposition sur l'existante infrastructure SDH, mais la complexité de la superposition des anneaux logiques **RPR** sur les anneaux physiques **SDH** ne sera pas probablement trop attrayant pour nombreux opérateurs. Bien que **RPR** et **EOS** résolvent différents problèmes dans le Metro (l'**EOS** résolve le déploiement de services Ethernet, et le **RPR** résolve l'efficacité de la bande passante sur les anneaux de paquets), les deux technologies seront en compétition pour les parts de l'esprit le fournisseur de Metro.

La figure 1-17 montre un déploiement RPR typique pour un câblo-opérateur. Le **CMTS** agrège le trafic en provenance du câble coaxial des entreprises et des foyers et le fait passer à la portion de données (en supposant que le câble transporte ainsi la voix/vidéo) au routeur **RPR**. Multiples routeurs **RPR** communiquent via un anneau de paquets **STM16**, et le trafic est regroupé dans le Hub de base, où la connectivité à Internet est établie.



*** Figure 1-17. Déploiement du **RPR** ***

Le **RPR** est en quelque sorte plus souvent associées avec des routeurs que des commutateurs (Switchs), alors que l'**EOS** est le plus souvent associés avec des commutateurs (Switchs) que des de routeurs. La raison de ces associations est que le **DTC** a historiquement été déployé en utilisant les routeurs **IP** Cisco pour fournir des services **IP** acheminés sur un anneau de paquets. Alors que les normes **IEEE 802.17** voudraient assurer l'indépendance du **RPR** de la couche 2 (L2) de commutation ou de niveau 3 (L3) de routage, le fait demeure que **RPR** a été adopté jusqu'ici pour les services de L3. En outre, de nombreux routeurs manquent la fonctionnalité correcte de fournir des services de L2, ce qui rend l'**EOS** plus adéquat pour les commutateurs.

[1] WDM: Wavelength division multiplexing.

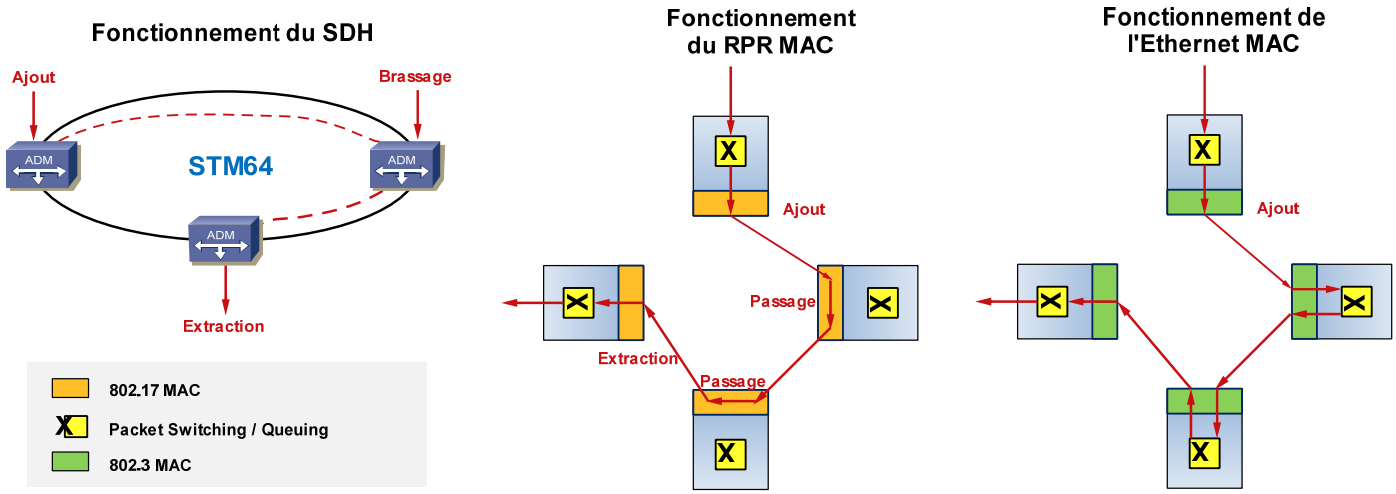
En comparant **RPR** avec les anneaux traditionnels **SDH**, on rend compte que les déploiements **RPR** présentent de nombreux avantages tout simplement parce que le protocole du **RPR** est construit à partir de l'idée de soutenir des anneaux de données.

2.2.1.L'ajout, l'extraction et le passage des paquets RPR

L'exploitation du **RPR** se compose de trois opérations de base: ajouter (Add), extraire (Drop), et en avant ou passage (Forward). Ces opérations imitent les mécanismes d'ajout et l'extraction qui sont utilisés dans les réseaux traditionnels **SDH,** où les circuits sont ajoutés, extraits, et interconnectés ou brassés à l'intérieur d'un anneau.

L'avantage que **RPR** a de plus qu'un anneau de paquet Ethernet commuté traditionnel est que l'exploitation du **MAC 802.3** de l'Ethernet traite les paquets à chaque nœud de l'anneau, indépendamment de savoir si la destination du paquet est derrière ce nœud. En revanche, le **MAC 802.17** du **RPR** fait passer le trafic en avant sur l'anneau sans faire aucune commutation intermédiaire ou de mise en mémoire tampon si le trafic ne fait pas partie du nœud. Cela réduit la quantité de travail que les nœuds individuels ont à faire.

Dans l'exploitation du **RPR** illustré à la figure 1-18, le trafic qui n'appartient pas à un nœud particulier est transité (transmis) sur l'anneau par le **MAC 802.17**. Dans l'exploitation du **MAC 802.3** de l'Ethernet, le trafic est traité et mis en mémoire tampon à chaque nœud pour que la fonction de commutation détermine l'interface de sortie.



*** Figure 1-18. L'ajout, l'extraction et le passage des paquets **RPR** ***

L'avantage du **RPR** par rapport à un anneau **SDH** est que tous les paquets arrivant sur l'anneau partage la totalité de la bande passante de l'anneau, et le mécanisme **RPR** gère l'allocation de bande passante pour éviter la congestion et les points chauds. Dans un anneau **SDH**, les intervalles de temps **TDM** sont attribués à chaque circuit, et la bande passante est retirée de l'anneau même si ces circuits ne portent aucun trafic.

2.2.2. La résilience du RPR

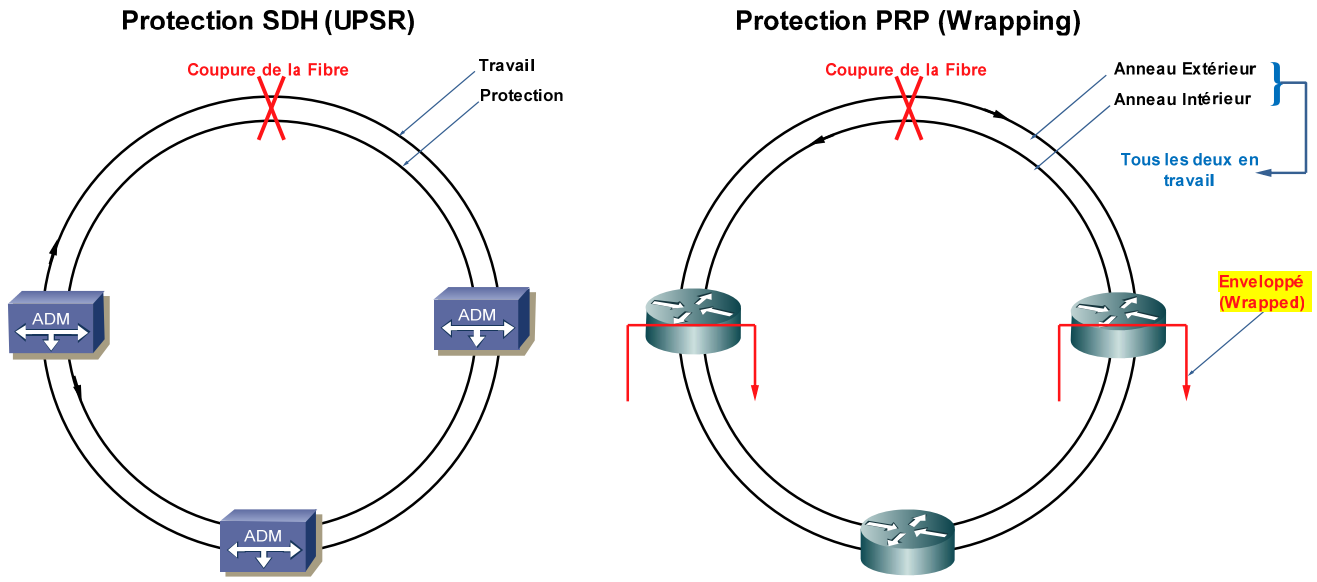
RPR offre une protection de l'anneau en 50 ms, comparable avec la protection traditionnelle du **SDH**. Une protection **RPR** rapide avec utilisation de la totalité de la bande passante de l'anneau est probablement l'un des atouts majeurs que la technologie **RPR** possède par rapport à **SDH** ainsi que d'autres mécanismes de protection de paquets.

La protection RPR est atteinte par deux façons:

- Enveloppement de l'anneau (Ring Wrapping) : l'anneau est réparé à l'endroit de la faute.
- Pilotage de l'anneau (Ring Steering) : En cas de panne, le trafic est redirigé (piloté) à la source vers la partie de fonctionnement de l'anneau.

En général, la couche physique détecte les défauts et signale l'information à la couche **MAC**. Si la panne est déterminée à être critique, chaque nœud **RPR** touché lance une action de « fail-over » pour le flux en service dont il est originaire qu'ils sont touchés par une panne des installations. L'action du « fail-over » est une simple redirection du trafic du chemin corrompu vers le chemin de protection. Les processus de notification d'alarme et la redirection du trafic sont achevés au bout de 50 ms de la panne.

La figure 1-19 compare les anneaux **RPR** et **SDH** et montre les différences. Dans le régime **UPSR** (Unidirectionnal Path Switching Ring), par exemple, une protection de 50 ms est obtenue grâce à l'utilisation d'une fibre de travail et une fibre de protection en veille en même temps. Un nœud d'envoi transmet sur deux fibres (EST et OUEST) dans le même temps, alors qu'un nœud de réception accepte le trafic d'un seul côté. En cas de coupure de fibre, la récupération se fait en moins de 50 ms. En **UPSR**, seulement 50% de la capacité de la fibre est utilisée, parce que l'autre moitié est conservée pour des modes de défaillance. En **RPR**, les deux anneaux de fibres : l'anneau extérieur et l'anneau intérieur, sont employés pour utiliser 100% de la capacité de l'anneau. En cas de panne, l'anneau s'enveloppe, isolant ainsi la partie endommagée. Donc, la bande passante effective d'un anneau **RPR** est deux fois de plus qu'anneau **SDH** en raison de la protection de **SDH**.



*** Figure 1-19. La protection du **RPR** ***

2.2.3.L'équité du RPR

RPR implémente un algorithme de l'équité pour donner à chaque nœud sur l'anneau un partage équitable de l'anneau. **RPR** utilise des mécanismes de contrôle d'accès pour assurer l'équité et pour lier la latence sur l'anneau. Le contrôle d'accès peut être divisé en deux types, qui peuvent être appliquées en même temps:

- Contrôle d'Accès Global : (Global Access Control) Contrôle l'accès de sorte que chaque nœud peut obtenir un partage équitable de la bande passante globale de l'anneau.
- Contrôle d'Accès Local : (Local control Access) Donne au nœud un accès additionnel à l'anneau, (qui est la bande passante au-delà de ce qui a été globalement attribués) pour profiter des segments qui sont moins utilisés.

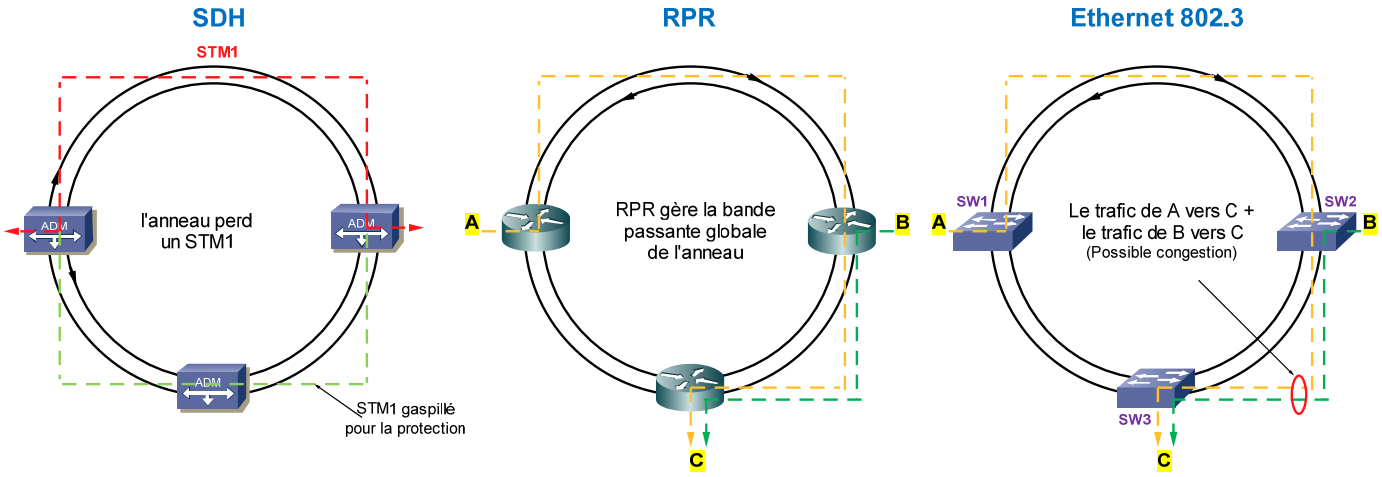
RPR utilise le protocole de réutilisation spéciale (**SRP**[1]), qui est un concept utilisé dans les anneaux pour augmenter de la bande passante totale agrégée. Ceci est possible car plusieurs liaisons de l'anneau peuvent être utilisées simultanément sans que le trafic sur une liaison affecte le trafic sur les autres liaisons. Si un nœud se trouve en état de congestion, il en avise les nœuds en sens mentant sur l'anneau, qui à leurs tours ajustent la vitesse de transmission pour alléger la congestion en sens descendant.

Il contribue de mettre en contraste l'équité de la bande passante de l'anneau entre **RPR** et les anneaux Ethernet L2. Dans le cas d'un anneau Ethernet disposant d'une commutation L2, il manque une chose comparable à l'algorithme de l'équité de l'anneau, parce que les décisions de la **QoS**[2] sont locales au niveau de

[1] SRP : Special Reuse Protocol
[2] QoS : Quality Of Service.

chaque nœud, indépendamment de ce qui est dans l'anneau. On peut utiliser des techniques de limitation de vitesse afin d'éviter qu'une série de clients entrant dans un nœud de surmonter la capacité de l'anneau, mais il serait difficile d'avoir un mécanisme d'équité total sans recourir à des applications logicielles complexes pour la gestion du **QoS** qui seraient chargé de coordonner entre tous les nœuds.

La figure 1-20 montre trois scénarios différents pour le mécanisme **UPSR** (Unidirectionnal Path Switching Ring) de **SDH, RPR**, et les anneaux Ethernet L2. Dans le cas des anneaux **SDH**, si un **STM1** est alloué, l'anneau perd la valeur de bande passante **STM1**, indépendamment du trafic réel. Dans le cas Ethernet, le trafic menant de A vers C et de B vers C peut surmonter la capacité de la liaison en point à point entre les commutateurs SW2 et SW3. Dans le cas **RPR**, l'entité **MAC** dans chaque nœud surveille l'utilisation de ses liens immédiats et crée la disponibilité des informations à tous les nœuds sur l'anneau. Chaque nœud peut ensuite envoyer plus de données ou d'en limiter.



*** Figure 1-20. Bande passante de L'anneau ***

2.3. Le Transport Ethernet

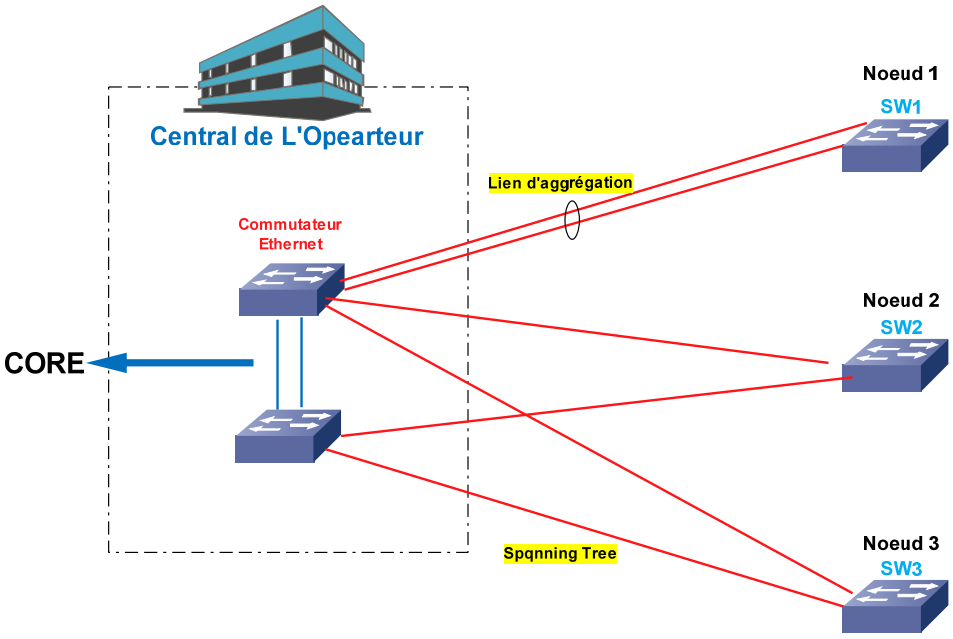
Jusqu'à présent, on a abordé le raisonnement derrière l'adoption d'Ethernet comme interface d'accès plutôt que d'une interface **TDM**. Mais comme on le verra dans ce qui suit, Ethernet n'est pas limité à être une technologie d'accès. Beaucoup d'efforts ont été faits pour étendre l'Ethernet lui-même dans les réseaux métropolitains **MAN**[1] en tant que technologie de transport ou de transmission. Depuis le début des années 2000, les déploiements du Metro Ethernet ont pris de nombreuses formes, certains ont fait leurs preuves, et d'autres n'ont pas. Lorsque la technologie Ethernet est utilisée comme une technologie de transport, le réseau d'accès peut être construit soit en topologie en anneau, soit en topologie en étoile.

2.3.1. Configuration Gigabit Ethernet en étoile

[1] MAN : Metropolitan Area Networks.

Dans une configuration Gigabit Ethernet en étoile, les commutateurs Ethernet déployé dans les nœuds sont à double hébergement (Dual-Homed [1]) dans le plus proche point de présence (**POP**) ou dans le central de l'opérateur (**CO**). Une fibre optique dédiée ou une longueur d'onde dédiée utilisant **WDM**, est utilisée pour assurer la connectivité. Bien que cette approche soit la plus chère pour les déploiements de l'accès en Metro en raison du coût de la fibre, certains opérateurs la considèrent comme la meilleure solution en mesure de la survivance et l'évolutivité par rapport au déploiement d'Ethernet dans une topologie en anneau. Avec le modèle de topologie en étoile, la bande passante dédiée à chaque nœud peut évoluer, parce que la fibre est complètent dédiée au nœud.

Le plan de protection peut être réalisé via des mécanismes tels que l'agrégation de liens selon la norme **802.3ad** ou le concept du double hébergement (Dual-Homed). Avec l'agrégation de liens, deux fibres sont rassemblées dans un grand conduit qui se connecte au **CO**. Le trafic est équilibré entre les deux fibres, et si une fibre est endommagée, l'autre absorbe la pleine charge. Ceci, bien sûr, suppose que les deux fibres prennent deux chemins différents vers le **CO** pour une meilleure protection. Ce scénario est illustré à la figure 1-21 pour la connexion entre le nœud 1 et le **CO**



*** Figure 1-21. Ethernet en étoile ***

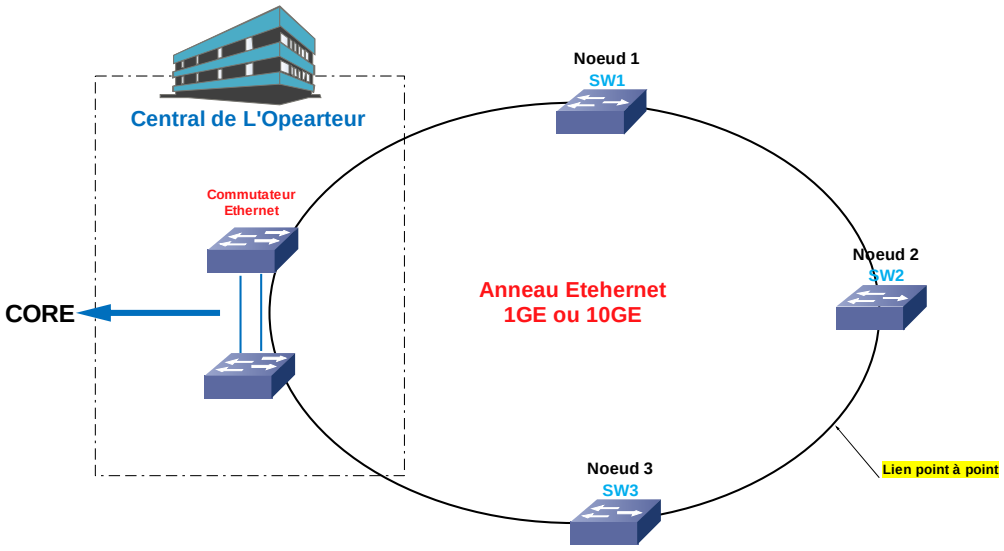
Une autre approche consiste à double héberger chacun des deux fibres dans différents commutateurs au sein du **CO**, comme le montre la Figure 1-21 pour les nœuds 2 et 3. Bien que cela empêche d'avoir un point de défaillance unique sur le côté de commutation, il crée plus de complexité, car l'algorithme du **STP** doit être

[1] Dual-Homed : la connexion d'un terminal de sorte qu'il est desservi par l'un des deux centres de commutation.

exécuté entre les nœuds 2 et 3 et le **CO**, provoquant ainsi le blocage du trafic sur l'un des liens du double hébergement.

2.3.2. Les anneaux Gigabit Ethernet

De nombreux déploiements de fibre dans le Metro sont prévus dans les configurations en anneau. Par conséquent, les topologies en anneau sont les plus simples à implémenter tout en assurant de réaliser des économies. Mais la situation diffère selon le cas. Les déploiements des anneaux pourraient être extrêmement rentables pour un opérateur, mais engendrant de sérieuses problèmes pour un autre. Pour les fibres existantes posées dans une topologie en anneau, les anneaux Gigabit Ethernet sont une série de liaisons point à point entre les commutateurs existants dans les nœuds et le central de l'opérateur (**CO**), comme le montre la Figure 1-22. Aussi simple qu'ils pourraient sembler, les anneaux Gigabit Ethernet peuvent créer de nombreux problèmes pour les opérateurs en raison de la protection et de la limite de la bande passante. Tout d'abord, la capacité anneau pourrait être un problème majeur. Les anneaux Gigabit Ethernet ont seulement 1Go de capacité à partager entre tous les nœuds, et une partie de cette capacité n'est pas disponible parce ce que le protocole de Spanning Tree bloque des portions de l'anneau pour éviter les boucles.



*** Figure 1-22. Les anneaux Gigabit Ethernet ***

Avec l'exploitation l'Ethernet commuté L2, l'anneau lui-même devient une collection de liens point à point. Même sans une coupure de fibre, le protocole de Spanning Tree bloque des portions de l'anneau afin de prévenir les tempêtes de diffusion (Broadcast Storm) causée par les boucles (voir la partie A de la figure 1-23). Les tempêtes de diffusion se produisent, par exemple, quand un paquet avec une destination inconnue atteint un nœud. Le nœud submerge le paquet sur l'anneau selon opération de pontage (bridging) tel que défini dans la norme **802.3d**. S'il existe une boucle dans le réseau (dans ce cas, l'anneau), le paquet pourrait finir par être reçu et transmis par le même nœud à maintes reprises. L'algorithme de Spanning Tree utilise des

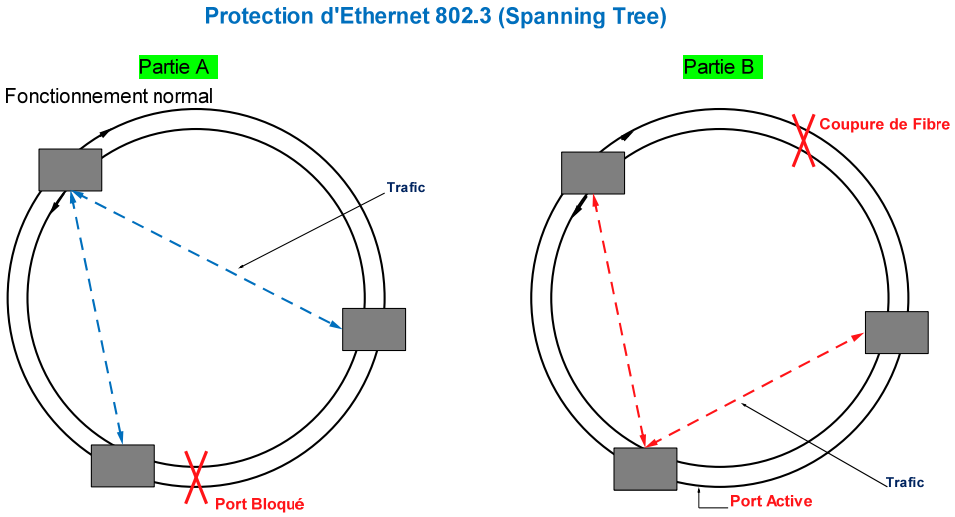
paquets de contrôle appelés (**BPDU** : Bridge Protocol Data Units) pour découvrir les boucles et les bloquer. Spanning tree prend normalement entre 30 et 60 secondes pour converger. La nouvelle norme **IEEE 802.1w** (**RSTP**[1] : Rapid Spanning Tree Protocol) permet une convergence plus rapide, mais ne vient toujours pas près de 50 ms. De nombreux algorithmes propriétaires ont été introduites pour parvenir à une convergence anneau en moins d'une seconde, que plusieurs opérateurs la juge en tant que suffisamment bonne pour que les services de données et même pour la Voix sur **IP** (**VoIP**). Pourtant, à cause de l'incapacité de la commutation L2 de fonctionner dans un environnement en boucle, un grand nombre de ces algorithmes ont encore besoin de bloquer les chemins d'accès redondants dans l'anneau afin de prévenir les tempêtes de diffusion, et ne sont pas considérés comme fiables tels que les mécanismes de protection du **RPR** ou du **SDH** qui appartiennent plus au classe de transmission. Lorsqu'une coupure de la fibre se produit, le Spanning Tree réajuste, et le nouveau chemin d'accès entre les différents nœuds est établi, comme indiqué dans la partie B de la figure 1-23.

[1] En 1998, l'IEEE publie le document 802.1w qui accélère la convergence du protocole STP après un changement de topologie. Il est inclus dans standard IEEE 802.1D-2004. Tandis que le STP classique peut prendre de 30 à 50 secondes pour converger après un changement de topolgie, RSTP est capable de converger en 3 fois la valeur du délai Hello (6 secondes par défaut)[3],[4].
États des ports RSTP

- Root : le port vers le root bridge,
- Designated : le port qui transmet les trames sur un segment,
- Alternate : un port distinct du root port vers le root bridge,
- Backup : un autre port vers un segment connecté au pont.

Le fonctionnement général de RSTP est semblable à celui du STP classique. Les différences sont les suivantes :

- une défaillance du root bridge est détectée en 3 délais hello, c'est-à-dire 6 secondes avec les valeurs par défaut,
- les portes qui ne sont pas connectées à d'autres commutateurs (edge ports) peuvent basculer immédiatement dans l'état forwarding. RSTP continue à observer l'arrivée de BPDU sur ces portes pour s'assurer qu'aucune boucle n'est possible. Si un BPDU est observé, la porte bascule dans le statut non edge.
- contrairement au STP classique, RSTP réagit aux annonces BPDU qui proviennent du root bridge. Un bridge RSTP diffuse son information RSTP sur ses designated ports. Si un bridge reçoit un BPDU indiquant un meilleur root bridge, il place tous les autres ports dans l'état Discarding et informe ce bridge de ce qu'il est le meilleur chemin vers le root. En recevant cette information, celui-ci peut faire transiter le port vers ce bridge immédiatement dans l'état Forwarding sans passer par les états Listening et Learning, puisqu'aucune boucle n'est possible. Ceci constitue une amélioration majeure en termes de vitesse de convergence.
- RSTP conserve des informations au sujet d'un chemin alternatif vers le root bridge, ainsi qu'un chemin de Backup vers les segments, ceci permet une transition rapide en cas de problème sur une liaison.



*** Figure 1-23. Anneaux Gigabit Ethernet - Spanning Tree ***

L'introduction des anneaux 10Gigabit Ethernet voire 40Gigabit Ethernet ou même 100Gigabit Ethernet (le travail de normalisation de ces deux derniers débits ont été finis en juillet 2010 mais jusqu'au jour l'exploitation de cette norme n'est pas répandu en raison du coût élevé des équipements) permettrait d'atténuer d'une façon radicale les problèmes de congestion. Les équipements avec les interfaces plus que 10GE ont été conçus pour les réseaux CORE plutôt que pour l'accès aux nœuds.

3. Les services de Metro Ethernet

3.1. Les bases de commutation L2

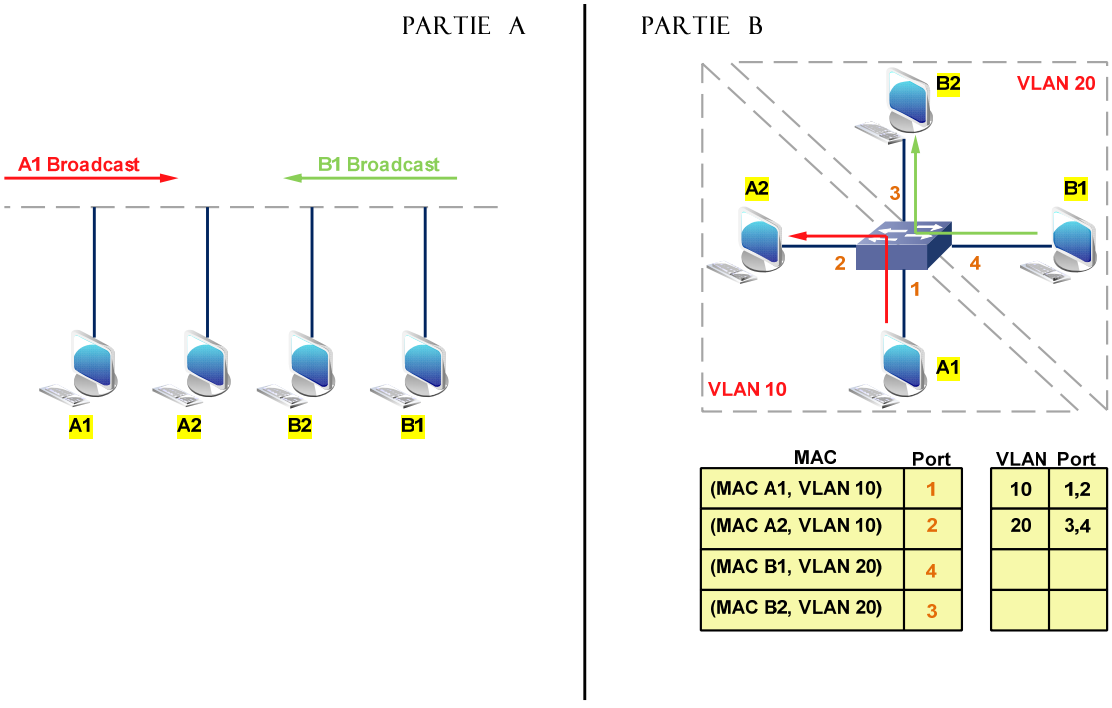
La commutation de la couche L2 permet aux paquets d'être commutés dans le réseau en se basant sur leurs adresses Media Access Control (**MAC**). Quand un paquet arrive au niveau du commutateur, le commutateur contrôle l'adresse **MAC** de destination du paquet et, si elle est connue, envoie le paquet au port de sortie à partir de laquelle il a appris le **MAC** de destination.

Les deux éléments fondamentaux de la commutation Ethernet L2 sont l'adresse **MAC** et les **LAN** virtuels (**VLAN**). De la même manière que le routage IP met en référence les stations sur les réseaux via une adresse **IP** de la couche L3, la commutation Ethernet L2 met en référence les stations terminales via l'adresse **MAC**. Cependant, contrairement à **IP**, dans lequel les adresses **IP** sont attribués par les administrateurs et peuvent être réutilisées dans différents réseaux privés, les adresses **MAC** sont censées être uniques, car ils indiquent le matériel lui-même. Ainsi, les adresses **MAC** ne doivent pas être attribuées par l'administrateur du réseau. (Bien sûr, dans certains cas, les adresses **MAC** peuvent être écrasées ou dupliqués, mais ce n'est pas qu'exige la norme.)

Ethernet est un support de diffusion. Sans la notion de **VLAN**, une émission envoyée par une station sur le réseau local est envoyé à tous les segments physiques du réseau local commuté. Le concept de **VLAN**

permet de segmenter le réseau local en entités logiques, et le trafic est localisé au sein de ces entités logiques. Par exemple, Dans un campus universitaire plusieurs **VLAN** peuvent être attribués, un **VLAN** est dédié pour le corps enseignant, un deuxième **VLAN** est dédié pour les étudiants, et le troisième **VLAN** est dédié pour les visiteurs. Le trafic de diffusion au sein de chacun de ces **VLAN** est isolé à ce **VLAN**.

La figure 1-24 montre le concept d'un réseau local Ethernet utilisant un (Hub) concentrateur (Partie A) et un utilisant un (Switch) commutateur Ethernet (Partie B). Avec un concentrateur Ethernet, toutes les stations sur le réseau **LAN** partagent le même segment physique. Un concentrateur de 10Mbits/s, par exemple, permet le trafic en diffusion (Broadcast) et le trafic d'unicast entre les stations qui partagent la bande passante de 10Mbits/s. Le **LAN** commuté (Partie B) permet à chaque segment une connexion 100Mbits/s (pour cet exemple), et assure la segmentation du réseau local en deux domaines logiques, VLAN10 et VLAN20. La notion de **VLAN** est indépendante des stations elles-mêmes. Le **VLAN** est une allocation par le commutateur. Dans cet exemple, les ports 1 et 2 sont affectés au VLAN10, alors que les ports 3 et 4 sont attribués à VLAN20. Quand les stations A1 et A2 envoient du trafic, le commutateur étiquette le trafic avec le **VLAN** assigné à l'interface et prend la décision de commutation sur la base du nombre de **VLAN**. Le résultat est que le trafic au sein d'un **VLAN** est isolé du trafic des autres **VLAN**.



*** Figure 1-24. **MAC** Ethernet et **VLAN** ***

La commutation Ethernet inclut les concepts de base suivants:

• Apprentissage du **MAC**.

• Inondation.

• Utilisation de la diffusion (Broadcast) et du multicast.

• L'extension du réseau avec des agrégats (trunks).

• Etiquetage **VLAN**.

• La nécessité pour le Protocole Spanning Tree (**STP**)

3.1.1. Apprentissage du MAC

L'apprentissage du **MAC** permet au commutateur Ethernet à apprendre les adresses **MAC** des stations dans le réseau pour déceler le port sur lequel doit envoyer le trafic. Les commutateurs **LAN** gardent normalement une table d'apprentissage **MAC** et une table de VLAN. Le table d'apprentissage **MAC** (Connu aussi par Table de Bridge) associe les **MAC/VLAN** avec un port donné, et le tableau du **VLAN** associe le port avec un **VLAN**. Dans la figure 3-1, la partie B, le commutateur a appris les adresses **MAC** des stations A1, A2, B1 et B2 sur les ports 1, 2, 4 et 3, respectivement. Il montre également que les ports 1 et 2 sont associés à des VLAN10 et les ports 3 et 4 sont associés à des VLAN20.

3.1.2. Inondations

Si le commutateur reçoit un paquet avec une adresse **MAC** de destination qui n'existe pas dans la table d'apprentissage **MAC**, le commutateur envoie ce paquet sur toutes ses interfaces qui appartiennent au même **VLAN** affecté à l'interface d'en provenance du paquet. Le commutateur n'inonde pas la trame vers le port qui a généré la trame d'origine. Ce mécanisme est appelé inondation (Flooding). Il permet la livraison rapide des paquets vers leurs destinations avant même que toutes les adresses **MAC** soient apprises par tous les commutateurs du réseau. L'inconvénient de l'inondation est qu'il consomme les ressources des commutateurs et du réseau, cela n'aurait pas été employé si le commutateur avait déjà appris à quel port pour envoyer le paquet.

Les **VLAN** minimisent les effets de l'inondation parce qu'ils concentrent l'inondation dans un **VLAN** particulier. Le commutateur emploie la table de **VLAN** pour extraire l'identificateur du **VLAN** à partir le numéro du port sur lequel le paquet est arrivé et qui servira par à inonder le paquet à une liste de ports appartenant au même **VLAN**.

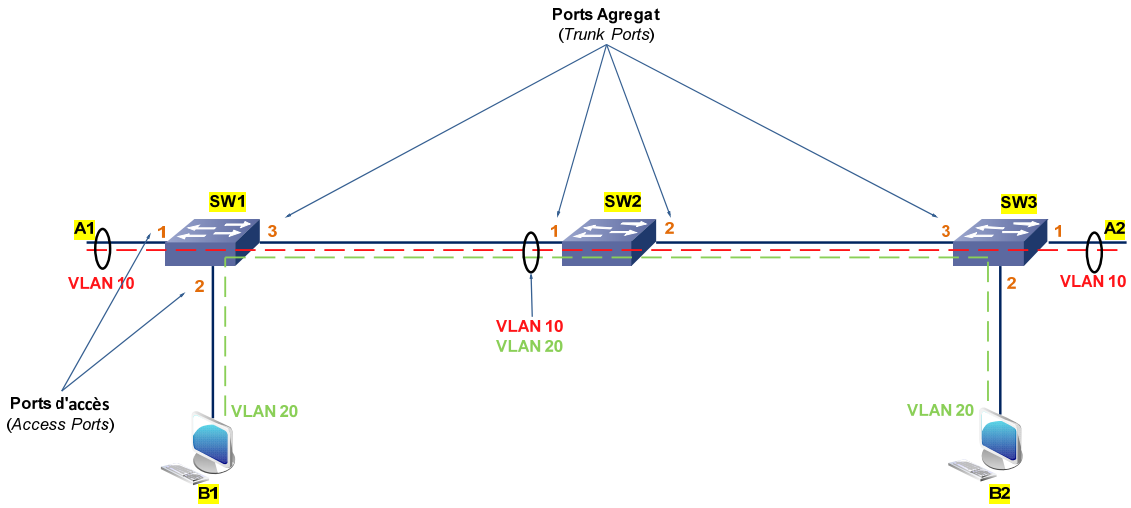
3.1.3. Utilisation de Broadcast et Multicast

Le Broadcast est utilisé pour permettre aux clients de découvrir les ressources qui sont annoncés par les serveurs. Quand un serveur annonce ses services à ses clients, il envoie des messages diffusés à l'adresse **MAC [FF.FF.FF.FF.FF.FF]**, qui signifie «toutes les stations ». Les terminaisons des clients écoutent la diffusion

(Broadcast) et capte seulement les diffusions qui les intéressent, afin de minimiser leur utilisation du processeur. Pour le multicast, qui est une variante de diffusion (Broadcast), une station n'envoie le trafic que vers un groupe de stations, et non à toutes les stations. Les adresses de broadcast et de multicast sont traités comme des destinations inconnues et sont inondées sur tous les ports d'un **VLAN**.

3.1.4. Expansion du réseau avec des agrégats (Trunks)

Jusqu'ici, on vu le cas d'un commutateur L2 unique. Un réseau Ethernet L2 commuté serait composé par plusieurs commutateurs interconnectés avec les ports agrégats (trunks). Les ports agrégats sont similaires aux ports d'accès utilisés pour connecter les terminaisons des stations ; mais ils ont ajouté la tâche de transporter le trafic en provenance de nombreux réseaux locaux virtuels **VLAN** dans le réseau. Ce scénario est illustré à la figure 1-25, où les ports agrégats pourrait connecter les commutateurs Ethernet construit par différents constructeurs, d'où la nécessité d'une normalisation des mécanismes l'étiquetage du **VLAN** (**VLAN** tagging).



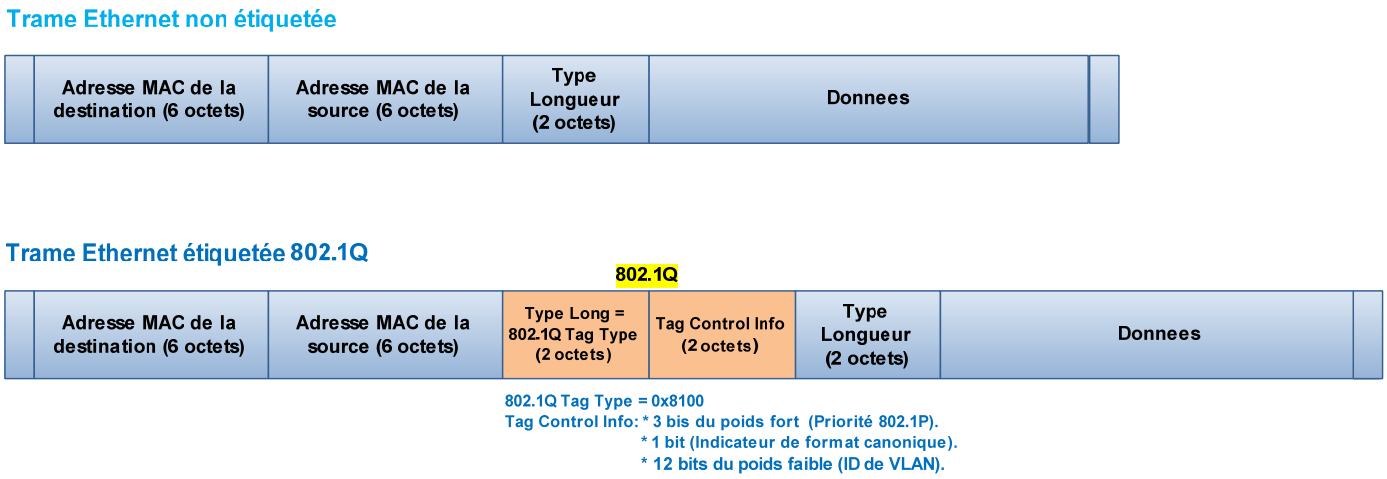
*** Figure 1-25. Les Ports agrégats (Trunks) ***

A la figure 1-25, les commutateurs SW1 et SW3 ont assigné le port d'accès N° :1 avec VLAN10 et le port d'accès N° :2 avec VLAN20. Le port N° :3 est un port de liaison ou port agrégat qui est utilisé pour se connecter à d'autres commutateurs du réseau. Il est à noter que le commutateur SW2 au milieu n'a pas de ports d'accès et est utilisé seulement pour interconnecter les ports agrégats. On peut voir que la simplicité de commutation Ethernet devient extrêmement complexe car les affectations du **VLAN** doivent être suivis à l'intérieur du réseau afin de permettre le juste trafic à être mis sur le juste port. Dans Frame Relay, **ATM** et **MPLS,** des complexités similaires existent, et la signalisation est introduite pour résoudre les problèmes de connectivité du réseau. Ethernet n'a pas défini un protocole de signalisation. Les seuls mécanismes que les réseaux Ethernet ont, sont des applications tierces qui surfent sur le réseau et rendre plus facile à faire certaines allocations de **VLAN**. Bien que ces mécanismes fonctionnent dans les environnements des petites entreprises,

ils ont immédiatement devenu attrayants dans les déploiements des plus grandes entreprises et des réseaux des opérateurs.

3.1.5. Etiquetage VLAN (VLAN Tagging)

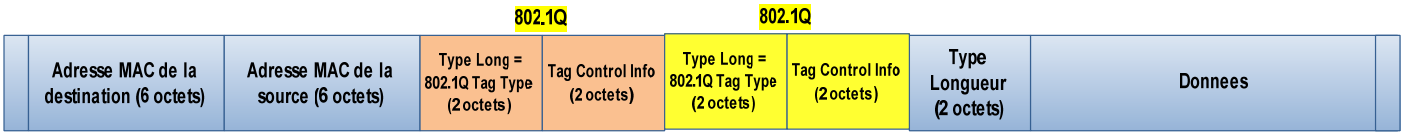
La norme **IEEE 802.1Q** définit la manière dont une trame Ethernet s'étiquète avec un **ID** de **VLAN**. L'**ID** de **VLAN** est attribué par le commutateur et non pas par la station terminale. Le commutateur attribue un numéro de **VLAN** à un port, et chaque paquet reçu sur ce port est alloué à l'**ID** de **VLAN**. Les commutateurs Ethernet commutent les paquets entre les mêmes réseaux locaux virtuels **VLAN**. Le trafic entre les **VLAN** différents est envoyé à une fonction de routage dans le commutateur lui-même (si le commutateur prend en charge la redirection L3) ou un routeur externe. La figure 1-26 montre comment les étiquettes **VLAN** sont insérées à l'intérieur du paquet **VLAN** non étiqueté.



*** Figure 1-26. Paquet **VLAN** Etiqueté ***

Le paquet Ethernet non étiqueté se compose de l'adresse **MAC** de destination et l'adresse **MAC** source, le champ Type, et les données. L'entête de l'étiquette **802.1Q** est inséré entre l'adresse **MAC** source et le champ Type. Il se compose d'un champ Type de 2 octets et d'un autre champ de 2 octets portant les informations du contrôle de l'étiquette (**TCI**: Tag Control Information). Le champ Type sur 2 octets est fixé sur **0x8100** pour indiquer qu'il s'agit d'un paquet **802.1Q** étiqueté. Les 2 octets du champ (Tag Control Information) se composent comme suit : les 3 bits du poids fort indiquent la priorité **802.1P** et les 12 bits du poids faible indiquent l'étiquette intitulée **VLAN ID**. Le champ **802.1P** accorde au paquet Ethernet jusqu'à huit niveaux de priorité différents qui peuvent être utilisés pour offrir différents niveaux de service au sein du réseau. Les 12 bits du **VLAN ID** champ permettent l'attribution d'un maximum de 4096 (2^{12}) numéros de **VLAN** pour distinguer les différents paquets associés aux **VLAN** étiquetés.

Les applications Metro Ethernet exigent des extensions de commutation L2 qui ne sont pas définis dans les normes. Un exemple est la possibilité de faire l'empilage de **VLAN**, qui consiste à faire de multiples étiquetages de **VLAN** au même paquet Ethernet et créer une pile d'**ID** de **VLAN**. Différentes entités peuvent faire la commutation L2 sur les différents niveaux de la pile **VLAN**. Ce concept est appelé Q-en-Q, court pour **802.1Q** en **802.1Q**, comme le montre la Figure 3-4.



*** Figure 1-27. Q-en-Q ***

Comme le montre cette figure, une trame déjà étiquetés peut être de nouveau étiquetée pour créer une hiérarchie. La simplicité de l'Ethernet, le manque de normalisation pour de nombreuses telles extensions, la dépendance à **STP**, et l'explosion des adresses **MAC** contribuent au manque de confiance de nombreux fournisseurs au déploiement des réseaux tout-Ethernet à grande échelle.

3.1.6. La nécessité du Protocole de Spanning Tree (STP)

Les réseaux Ethernet commutés L2 fonctionnent sur la base de l'apprentissage des adresses **MAC** et le mécanisme de l'inondation. Si plusieurs chemins existent pour la même destination, et le paquet possède une destination inconnue, l'inondation du paquet pourrait provoquer renvoie du paquet commutateur d'origine qu'il a mis sur le réseau, provoquant ainsi une tempête de Broadcast. **STP** empêche les boucles dans le réseau en bloquant les chemins redondants et veille à ce qu'un seul chemin actif existe entre chaque deux commutateurs du réseau. **STP** utilise les (**BPDU**), qui sont des paquets de contrôle qui voyagent dans le réseau et d'identifient quel chemin, et par conséquent les ports, qui doivent être bloquées.

3.2. Les concepts des services Metro Ethernet

Le Metro Ethernet Forum **(MEF)** est une organisation à but non lucratif qui a été actif dans la définition des champs d'application, les concepts et la terminologie pour le déploiement de services Ethernet dans le Metro. D'autres organismes de normalisation, tels que l'Internet Engineering Task Force **(IETF)**, ont également défini les moyens de mise à l'échelle des services Ethernet grâce à l'utilisation de la technologie **MPLS**. Bien que les terminologies puissent varier légèrement, les concepts et les orientations prises par ces différentes instances sont convergents.

3.2.1. Définition des services Ethernet

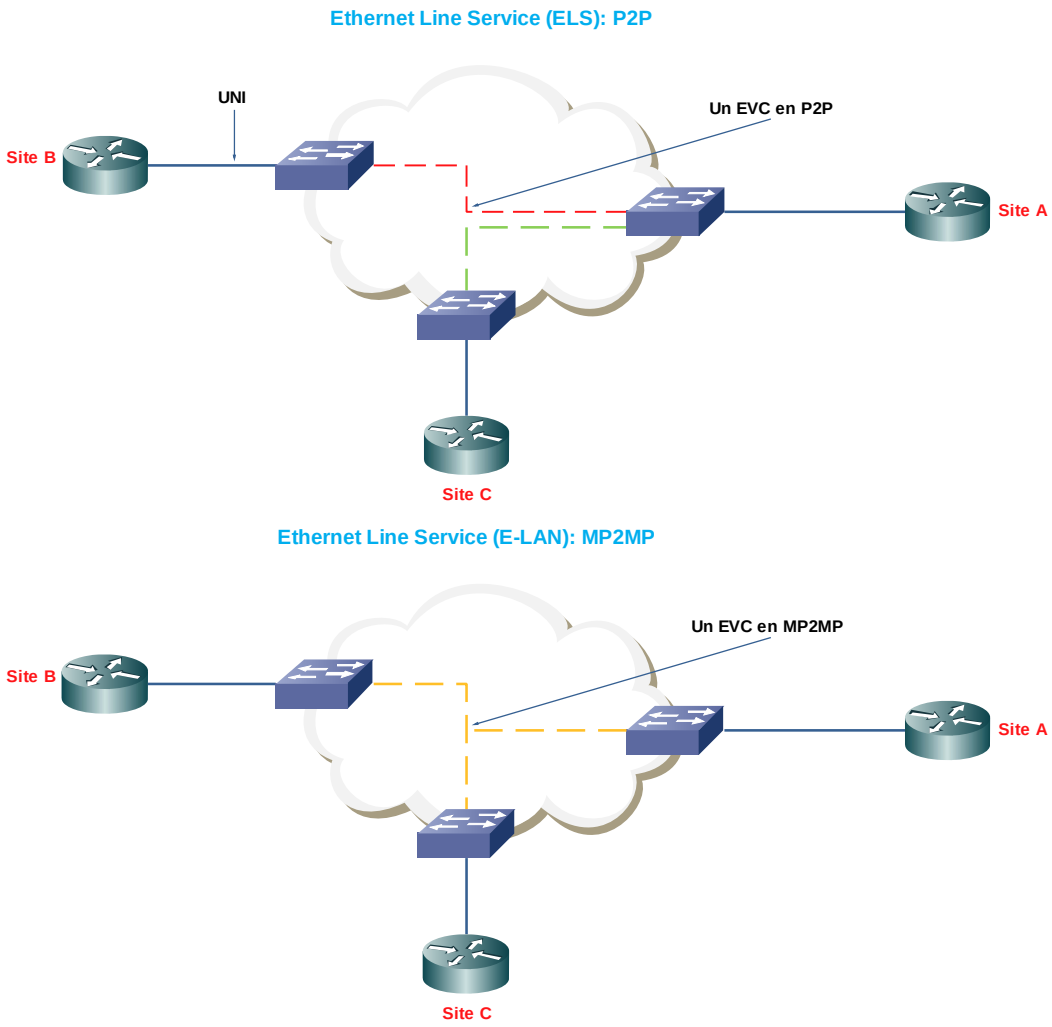
Le **MEF** définit l'interface utilisateur au réseau (**UNI** : User to Network interface) et la connexion virtuelle Ethernet (**EVC** : Ethernet Virtual Connection). L'**UNI** est une interface Ethernet standard qui est le point de démarcation entre les équipements du client et le réseau Metro du fournisseur de services Ethernet.

L'**EVC** est défini par le **MEF** comme «une association de deux ou plusieurs **UNI** ». En d'autres termes, l'**EVC** est un tunnel logique qui relie deux ou plusieurs (Point à Point) ou (Multipoint à Multipoint) sites, permettant le transfert des trames Ethernet entre eux. L'**EVC** agit également comme une séparation entre les différents clients et assure la confidentialité des données et la sécurité d'une façon semblable à Frame Relay ou des circuits virtuels permanents **(PVC :** Permanent Virtual Circuits**)** de la technologie **ATM**.

Le **MEF** a défini deux types de services Ethernet:

- Ethernet Line Service **(ELS)** - Il s'agit essentiellement d'un service Ethernet point à point (P2P).
- Ethernet **LAN** Service (**E-LAN**) - Il s'agit d'un service Ethernet multipoint à multipoint (MP2MP).

L'ELS (Line Ethernet Service) offre une EVC Point à point entre deux abonnés, semblable à un service Frame Relay ou un service de lignes louées (voir Figure 3-5).



*** Figure 1-28. Concepts des services Ethernet***

La figure 1-28 illustre également l'**E-LAN**, qui fournit une connectivité multipoint entre plusieurs abonnés exactement de la même manière qu'un réseau Ethernet commuté. Un service **E-LAN** offre le plus de souplesse dans la fourniture d'un service **VPN** parce qu'un **EVC** touche tous les sites. Si un nouveau site est ajouté au **VPN**, le nouveau site participe à l'**EVC** et dispose d'une connectivité automatique pour tous les autres sites.

3.2.2. Les attributs et les paramètres d'un service Ethernet

a. Attribut de l'interface physique de l'Ethernet

L'attribut de l'interface physique de l'Ethernet a les paramètres suivants:

- ***Le support physique :*** Définit le support physique par la norme **IEEE 802.3**. Des exemples sont les systèmes 10BASE-T, 100BASE-T et 1000Base-X.
- ***La vitesse :*** Définit la vitesse Ethernet: 10Mbps, 100Mbps, 1Gbps ou 10Gbps.
- ***Mode :*** indique la prise en charge du mode **« Full duplex »** ou du mode **«Half duplex »** et de la négociation de la vitesse automatique entre les ports Ethernet.
- ***Couche MAC :*** indique quelle couche **MAC** est prise en charge comme l'a été spécifié par la norme **802.3**.

b. Paramètres de trafic

Le **MEF** a défini un ensemble de profils de bande passante qui peuvent être appliqués à l'**UNI** ou à un **EVC**. Un profil de bande passante est une limite sur la vitesse à laquelle les trames Ethernet peuvent traverser l'**UNI** ou de l'**EVC**. L'administration des profils de bande passante peuvent être une affaire très délicate. Pour les connexions Point à Point où il ya une **EVC** unique entre deux sites, il est facile de calculer un profil de bande passante entrante et sortante du conduit. Toutefois, pour les cas où un service multipoint est livré et il ya la possibilité d'avoir plusieurs **EVC** sur la même interface physique, il devient difficile de déterminer le profil de bande passante d'une **EVC**. Dans de tels cas, la limitation du profil de bande passante par **UNI** pourrait être plus pratique.

Les attributs du service du profil de bande passante sont comme suit :

- Profil de bande passante d'entrée et de sortie par **UNI**.
- Profil de bande passante d'entrée et de sortie par **EVC**.
- Profil de bande passante d'entrée et de sortie par Identificateur **CoS**.
- Profil de bande passante d'entrée par destination **UNI** par **EVC**.

- Profil de la bande passante de sortie par source **UNI** par **EVC**.

Les attributs du service du profil de bande passante consistent en paramètres de trafic suivants :

- **CIR** (Committed Information Rate) : Il s'agit du débit minimum garanti que le réseau doit offrir au service dans des conditions de fonctionnement normales. Un service peut soutenir un **CIR** par **VLAN** sur l'interface **UNI**, mais la somme de tous les **CIR** ne doit pas dépasser la vitesse physique du port. Le **CIR** a un paramètre supplémentaire qui lui est associé appelé (**CBS :** Commited Burst Size). **CBS** est un paramètre du profil de la bande passante. Il limite le nombre maximal d'octets disponibles pour l'éclatement de trames de service émises à la vitesse de l'**UNI** pour en rester conforme au **CIR**. Il définit le taux moyen, mesuré en bits par seconde, des trames de Service d'entrée jusqu'à lequel le réseau fournit des trames de service et répond aux objectifs de performance définis par l'attribut **CoS** (Class Of Service). Les trames qui appartiennent au profil sont ceux qui répondent aux paramètres de **CIR** et **CBS**. Le **CBS** peut être spécifiée en Ko ou Mo. Si, par exemple, un client se voit attribuer un **CIR** de 3Mbps et un **CBS** de 500Kbps, le client garantit un minimum de 3Mbps et peut éclater jusqu'à 500Ko de trafic tout en restant dans les limites du **SLA** (Service Level Agreement). Si les pics de trafic sont supérieurs à 500 Ko, le trafic peut être supprimé ou retardé.

- **PIR** (Peak Information Rate) - Le **PIR** spécifie le taux au-dessus du **CIR** à lequel le trafic est autorisé dans le réseau et qui peut être remis si le réseau n'est pas en état de congestion. Le PIR a un paramètre supplémentaire qui lui est associé appelé (**MBS** : Maximum Burst Size). Le **MBS** est la taille jusqu'à laquelle le trafic est autorisé à éclater sans être rejeté. Le **MBS** peut être spécifié en Ko ou Mo, semblable au **CBS**. Un service d'exemple peut fournir un CIR de 3 Mbps, un CBS de 500Ko, un PIR de 10Mbps, et un MBS de 1Mo. Dans ce cas, le comportement suivant se produit:

- Si le trafic est inférieur ou égal au **CIR** (3Mbps) : Le trafic est contenu dans le profil avec la garantie de livraison. Le trafic est également dans le profil s'il s'éclate ou s'étend à la **CBS** (500 Ko) et peut être diminué ou retardé s'il s'éclate au-delà de 500 Ko.
- Si le trafic est de plus que **CIR** (3 Mbps) et moins que **PIR** (10 Mbps) : Le trafic est hors du profil. Il peut être remis si le réseau n'est en état de congestion et la taille de l'expansion ou de l'éclatement est inférieure au **MBS** (1 Mo).
- Si le trafic est supérieur au **PIR** (10 Mbps) - Le trafic est rejeté.

c. Paramètres de performance

Les paramètres de performance indiquent la qualité de service expérimentée par le client. Ils se composent des éléments suivants:

- Disponibilité

- Retard
- Gigue (Jitter[1])
- Perte

- **Disponibilité**

La disponibilité est spécifiée par les attributs de service suivants:

UNI Service Activation Time (Temps d'activation du service de l'**UNI**) : indique le temps mesuré entre le moment où un ordre de nouveau service ou modification est mis en place, jusqu'à moment où le service est activé et utilisable.

UNI Mean Time To Restore [MTTR] (Temps moyen de rétablissement de l'**UN**I) : Indique le temps nécessaire mesuré à partir du moment où l'**UNI** est indisponible jusqu'à moment où il est restauré ou rétablit. L'indisponibilité peut être causée par une défaillance, comme une coupure de fibre.

EVC Service Activation Time (Temps d'activation de service de l'**EVC**): indique le temps mesuré entre le moment où un ordre de nouveau service ou modification est mis en place, jusqu'à moment où le service est activé et utilisable. Le temps d'activation de service **EVC** commence quand tous **UNI** sont activés. Pour un **EVC** multipoint, par exemple, le service est considéré comme actif quand tous **UNI** sont actifs et opérationnels.

EVC Availability (Disponibilité de l'**EVC**) : indique la fréquence à laquelle le client de l'**EVC** atteint ou dépasse les retards, les pertes, et la performance de la gigue (Jitter) du service sur le même intervalle de mesure. Si un **EVC** ne répond pas aux critères de performance, il est considéré comme indisponible.

EVC [MTTR] (Temps moyen de rétablissement de l'**EVC**) : Indique le temps mesuré entre le moment où l'EVC est indisponible jusqu'à moment où il est disponible de nouveau. De nombreux mécanismes de restauration peuvent être utilisés sur la couche physique (L1), la couche **MAC** (L2), ou de la couche réseau (L3).

- **Retard ou Délai**

Le retard est un paramètre critique qui influe d'une manière significative sur la qualité de service (**QoS**) pour les applications en temps réel. Le retard a toujours été spécifié dans une direction en tant que délai

[1] Dans le domaine des transmissions numériques et plus particulièrement des liaisons en série, la **gigue** (en anglais *jitter*) est le phénomène de fluctuation d'un signal. Cette fluctuation peut être un glissement de phase ou une dispersion temporelle. Elle entraîne des erreurs en sortie lors de la récupération des données. Les normes télécoms, comme la norme SDH, ont spécifié des critères pour qu'un système puisse fonctionner. Ces limites sont basées sur le domaine de fréquences avec les spectres de la gigue. On y définit des spécifications :
- de tolérance de gigue (Jitter Tolerance).
- de transfert de gigue (Jitter Transfer).
- de création de gigue (Jitter Generation).

d'une seule voie ou délai de bout en bout. Le délai entre deux sites dans le Metro est une accumulation de délais, à partir d'un **UNI** à une extrémité, en passant par le réseau de Metro, et en passant par l'**UNI** à l'autre extrémité. Le retard à l'**UNI** est affecté par le débit en ligne à la connexion **UNI** et la taille de la trame Ethernet supportée. Par exemple, une connexion **UNI** de 10Mbps et taille de la trame est de 1518 octets causerait un délai de transmission de 1,2 millisecondes (ms) soit ($1518 * 8 / 10^7$).

Le réseau de Metro lui-même introduit des retards supplémentaires en fonction de la vitesse de réseau du backbone et le niveau de congestion. La performance de retard est définie 95% du délai de des trames de sortie livrées avec succès sur un intervalle de temps. Par exemple, un retard de 15 ms pendant 24 heures signifie que sur une période de 24 heures, 95% des trames livrées avaient un retard d'une seule voie inférieure ou égale à 15 ms.

Le paramètre de retard est utilisé dans les attributs suivants:

- Profil de bande passante entrante et sortante par identifiant **CoS** (attribut de service UNI)
- Classe de service (attribut de service **EVC**)

- **Gigue (Jitter)**

La gigue ou Jitter est un autre paramètre qui affecte la qualité du service (**QoS**). Jitter est également connu comme variation du retard. Jitter a un effet négatif sur les applications en temps réel telles que la téléphonie IP. Le paramètre de gigue est utilisé dans les attributs de service suivants:

- Profil de bande passante entrante et sortante par identifiant **CoS** (attribut de service **UNI**)
- Classe de service (attribut de service **EVC**).

- **Perte**

La perte indique le pourcentage de trames Ethernet qui sont inclus dans le profil et qui ne sont pas livrées d'une manière fiable entre les **UNI** sur un intervalle de temps. Sur une **EVC** en Point à point, par exemple, si 100 trames ont été envoyés à partir d'un UNI vers une seule extrémité et 90 trames qui sont dans le profil ont été reçues à l'autre bout, la perte serait (100-90)/100 = 10%. La perte peut avoir des effets négatifs, selon l'application. Des applications telles que le courrier électronique et les requêtes **HTTP** des navigateurs web peuvent tolérer plus de pertes que l'application du **VoIP**, par exemple. Le paramètre de perte est utilisé dans les attributs suivants:

Profil de bande passante entrante et sortante par identifiant **CoS** (attribut de service **UNI**)

- Classe de service (attribut de service **EVC**)

- **Classe des paramètres de service**

Les paramètres de classe de service (**CoS**) peuvent être définis pour les clients de Metro Ethernet sur la base de divers identificateurs **CoS**, telles que les suivantes:

- **Port physique :** C'est la plus simple forme de **QoS** qui s'applique au port physique de la connexion UNI. Tout le trafic qui entre et sort du port reçoit la même classe de service.
- **Les adresses MAC de destination et de source:** Ce type de classification est utilisé pour accorder différents types de services basés sur des combinaisons des adresses **MAC** de la source et la destination. Bien que ce modèle soit très souple, il est difficile à administrer, en fonction du service lui-même. Si les équipements du client aux extrémités des connexions sont des commutateurs L2 qui font partie d'un service de réseau local à un réseau local (**LAN** to **LAN**), des centaines voire des milliers d'adresses **MAC** devront être surveillées. D'autre part, si les équipements des clients sont des routeurs, les adresses **MAC** qui sont surveillés sont ceux des interfaces du routeur eux-mêmes. Par conséquent, les adresses **MAC** sont beaucoup plus faciles à gérer.
- **VLAN ID :** C'est un moyen très pratique pour l'attribution le **CoS** si l'abonné a différents services sur le port physique où un service est défini par un **ID** de **VLAN** (celles-ci seraient les **VLAN** assignés par l'opérateur).
- **Valeur du 802.1P** : Le champ **802.1P** permet à l'opérateur d'attribuer un maximum de huit différents niveaux de priorités au trafic des clients. Les commutateurs Ethernet utilisent ce champ pour indiquer certaines priorités de base de la transmission, telle que celle des trames avec la priorité N°7 sont transmis devant les trames avec la priorité N°6, et ainsi de suite. C'est une méthode qui peut être utilisée pour différencier entre le trafic **VoIP** et le trafic ordinaire ou par exemple. Dans toutes les pratiques, les fournisseurs de services ne dépassent pas deux ou trois niveaux de priorité, et ce pour rendre la gestion plus facile.
- **Diffserv / IP ToS :** Le champ **IP ToS** est un champ de 3 bits à l'intérieur du paquet **IP** qui est utilisé pour fournir huit différentes classes de service appelé priorité **IP**. Ce champ est semblable au champ **802.1P** s'il est utilisé pour les priorités de transmission de base, mais il est situé à l'intérieur l'en-tête **IP** plutôt que de l'en-tête de l'étiquette Ethernet **802.1Q**. **Diffserv** a défini un schéma plus sophistiqué du **CoS** que le schéma de priorité de transmission simple défini par le **ToS**. **Diffserv** permet d'avoir 64 valeurs de **CoS** différentes, appelées *Diffserv Codepoints* **(DSCP)**. **Diffserv** attribue plus de souplesse pour la configuration des paramètres **CoS**, mais les fournisseurs de services restent encore limités à la question de la gestion.

- **<u>Attribut de Livraison de Trame de Service</u>**

Parce que le réseau de Metro se comporte comme un **LAN** commuté, on doit comprendre quelles trames doivent circuler sur le réseau et qui ne le sont pas. Sur un réseau local typique, les trames transitant sur le réseau pourraient être des trames de données ou des trames de contrôle. Certains services Ethernet prennent en charge la livraison tous les types d'unités de protocole de données Ethernet (**PDU** : Protocol Data Units), d'autres ne peuvent pas. L'attribut de service **EVC** peut définir si une trame particulière est jetée, livré sans réserve, ou livrée sous condition pour chaque paire **UNI** commandée. Les différentes possibilités des trames de données Ethernet sont les suivantes:

- **Les trames Unicast :** Ce sont des trames qui ont une adresse **MAC** de destination spécifiée. Si l'adresse **MAC** de destination est connue par le réseau, la trame est livrée à la destination exacte. Si l'adresse **MAC** est inconnue, le comportement **LAN** est d'inonder le **VLAN** dans le **VLAN** particulier.
- **Les trames de Multicast :** Ce sont des trames qui sont transmises à un groupe restreint de destinations. Ce serait n'importe quelle trame avec le bit le moins significatif (**LSB :** Low significant Bit) de l'adresse de destination définie à 1, sauf pour la diffusion, où tous les bits de l'adresse **MAC** de destination sont mis à 1.
- **Des trames de Bradcast :** La norme **IEEE 802.3** définit l'adresse de diffusion (Broadcast) comme l'adresse **MAC** de destination, **FF.FF.FF.FF.FF.FF**.

Les paquets du contrôle de traitement de la couche 2 sont les différents paquets de contrôle de protocole L2 nécessaires pour des applications spécifiques. Par exemple, les paquets **BPDU** sont nécessaires pour le **STP** (Spanning Tree Protocol). Le fournisseur peut décider de transmettre ou de jeter ces paquets sur l'EVC, selon le service. Ce qui suit est une liste de protocoles L2 normalisés qui peuvent circuler sur une EVC:

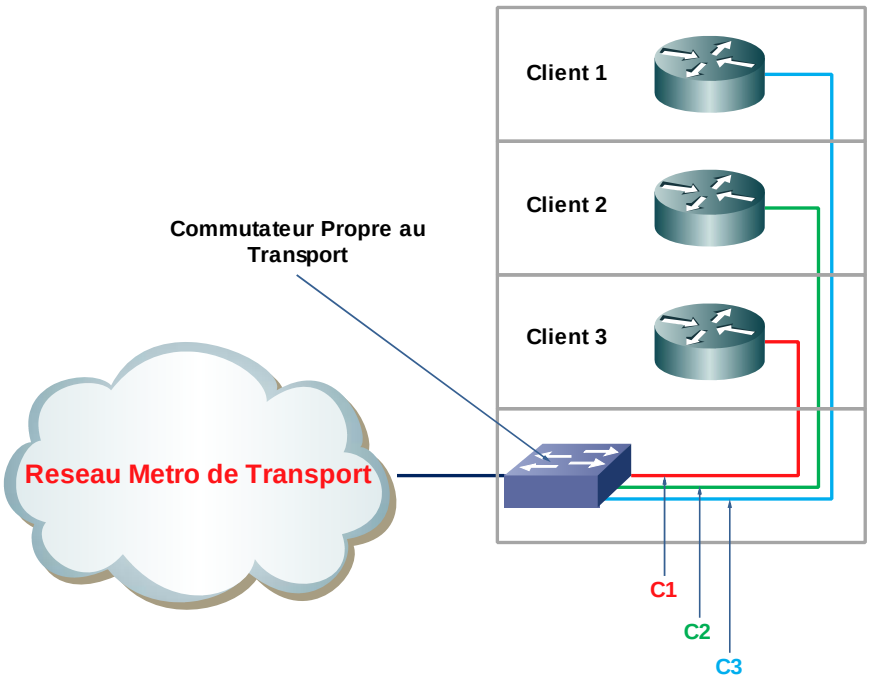
- **IEEE 802.3x MAC Control frames : 802.3x** est un mécanisme de contrôle de flux XON/XOFF qui permet à une interface Ethernet d'envoyer une trame PAUSE en cas de congestion du trafic sur la sortie du commutateur Ethernet. Les trames de contrôle **MAC 802.3x** ont l'adresse de destination ***01.80.C2.00.00.01.***
- **Link Aggregation Control Protocol (LACP)** : Ce protocole permet le regroupement dynamique de plusieurs interfaces Ethernet entre deux commutateurs pour former un conduit plus grand. L'adresse **MAC** de destination pour ces trames de contrôle est de ***01.80.C2.00.00.02***.
- **IEEE 802.1x port authentification** : Ce protocole permet à un utilisateur (un port Ethernet) à être authentifié dans le réseau via un serveur *back-end*. L'adresse **MAC** de destination est de ***01.80.C2.00.00.03***.

- **Generic Attribute Registration Protocol (GARP)** : L'adresse **MAC** de destination est ***01.80.C2.00.00.2X.***
- **STP :** L'adresse **MAC** de destination est de ***01.80.C2.00.00.00.***
- **All Bridge Multicast :** L'adresse MAC de destination est de ***01.80.C2.00.00.10.***

- **<u>Attribut de la prise en charge de l'étiquette VLAN :</u>**

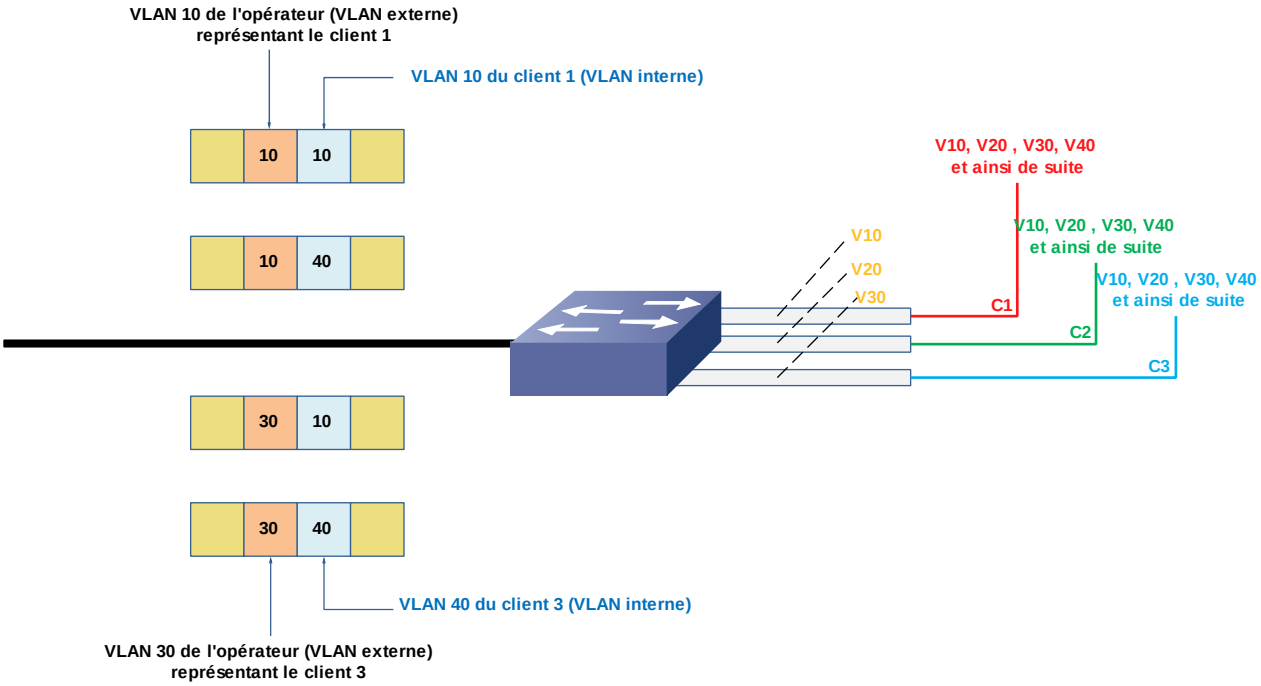
La prise en charge de l'étiquette **VLAN** fournit un autre ensemble de capacités qui sont importantes pour la livraison des trames de services. Les réseaux d'entreprise sont des environnements mono-client, ce qui signifie que les utilisateurs finaux appartiennent à une seule organisation. Les étiquettes de **VLAN** au sein d'une organisation sont indicatifs des différents domaines de diffusion logiques, tels que les différents groupes de travail. Metro Ethernet crée un environnement différent dans lequel le réseau Ethernet prend en charge multiples réseaux d'entreprise qui partagent la même infrastructure, et dans lequel chaque réseau d'entreprise peut encore avoir sa propre segmentation. Les aspects de la prise en charge de différents niveaux de **VLAN** et de la capacité de manipuler les étiquettes des **VLAN** sont devenu très important.

Soit l'exemple d'un site dans lequel le fournisseur de Metro installe un commutateur qui offre des connexions Ethernet multiples à différents petits bureaux dans le bâtiment. Dans ce cas, à partir d'une perspective de l'opérateur, chaque client est identifié par le port physique de l'interface Ethernet que le client utilise pour se connecter. C'est ce que montre la figure 1-29.



*** Figure 1-29. Ethernet dans les environnements multi-client***

Bien que l'identification du client lui-même soit facile, l'isolation du trafic entre les différents clients devient une question intéressante et nécessite une certaine attention de la part du fournisseur. Sans l'attribution d'une attention particulière, le trafic pourrait être échangé entre les différents clients dans le bâtiment au commutateur. On a déjà vu dans que les réseaux locaux virtuels **VLAN** peuvent être utilisés pour séparer les segments physique dans de nombreux segments logiques, mais cela fonctionne dans un environnement mono-client, où le **VLAN** a une signification globale. Dans un environnement multi-client, chaque client peut avoir son propre ensemble de **VLAN** qui se chevauchent avec les **VLAN** des autres clients. Pour assurer le fonctionnement dans ce milieu, les opérateurs ont adopté un modèle très similaire à la façon dont les services Frame Relay et **ATM** ont été déployés. Essentiellement, chaque client est doté par des identificateurs de service similaires aux identificateurs de connexion de liaison de données pour le Frame Relay (**DLCI** : Data-Link Connection Identifier), qui identifient les **EVC** sur lesquelles se déplace le trafic du client. Dans le cas de l'Ethernet, l'**ID** de **VLAN** fournie par un opérateur devient cet identifiant. Ceci est illustré à la figure 1-30.



*** Figure 1-30. Séparation logique du trafic et des Services***

Dans cet exemple, l'opérateur a besoin d'assigner à chaque port physique un ensemble d'**ID** de **VLAN** qui sont représentatifs des services fournis à chaque client. Le client 1, par exemple, est attribué par le VLAN10, client 2 est attribué par le VLAN20, et le client 3 est attribué par le VLAN30. Les VLAN 10, 20, et 30 sont des **VLAN** assignés par l'opérateur qui sont indépendants des affectations internes des **VLAN** par le client. Pour faire cette distinction, le **MEF** a donné le nom **CE-VLAN** pour les **VLAN** internes des clients. Les clients eux-

mêmes peuvent avoir des assignations existantes de **VLAN** (**VLAN-CE**) qui se chevauchent les uns avec les autres et **VLAN** de l'opérateur. Il existe deux types de prise en charge de l'étiquette du VLAN:

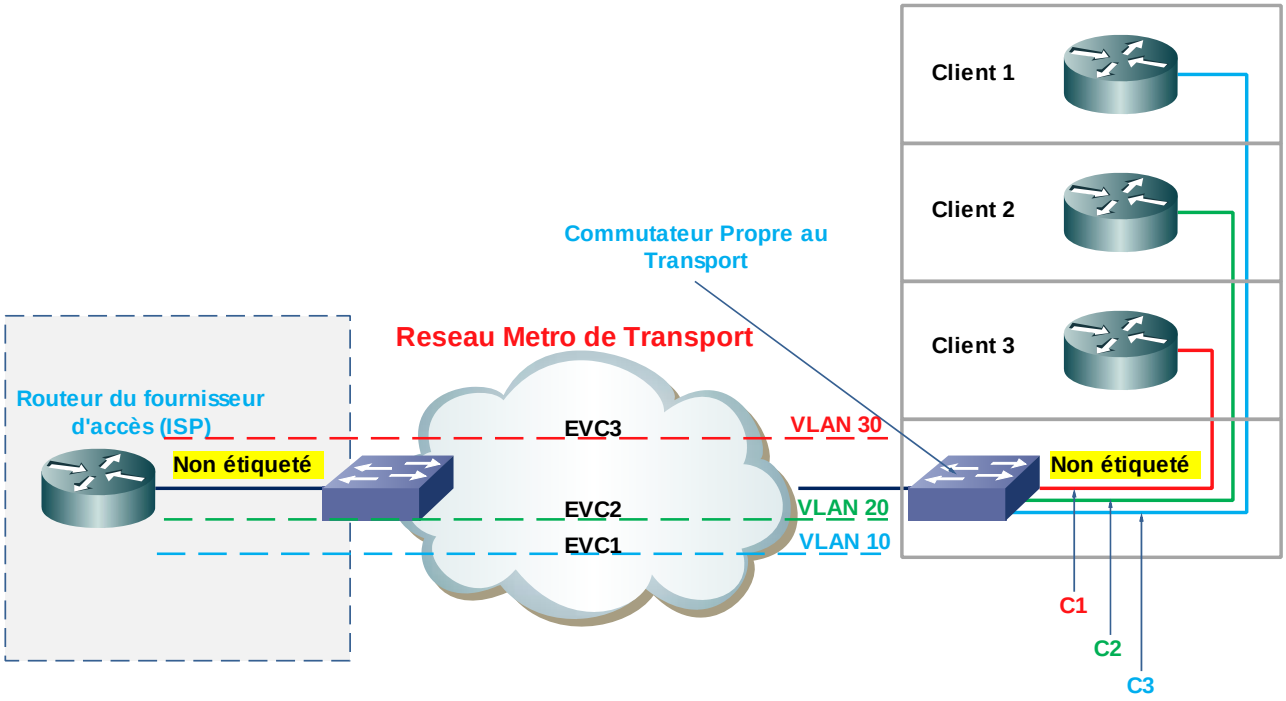
- Préservation de l'étiquette de **VLAN** / Empilement
- Traduction de l'étiquette de **VLAN** / Échange

Préservation de l'étiquette de VLAN / Empilement : Avec la préservation du **VLAN**, toutes les trames Ethernet reçues de client doivent être transmises d'une façon intactes au sein du réseau de l'opérateur à travers l'**EVC**. Cela signifie que l'**ID** de **VLAN** à l'entrée de l'**EVC** est égal à l'**ID** de **VLAN** sur la sortie. Ceci est typique aux services tels que l'extension des **LAN**, où le même réseau local est étendue entre deux endroits différents et les affectations internes des **VLAN** au sein de l'entreprise doivent être préservés. Parce que le commutateur Ethernet de l'opérateur prend en charge plusieurs clients dont leurs **CE-VLAN** se chevauchent, le commutateur de l'opérateur doit être en mesure d'empiler ses propres affectations de **VLAN** sur l'affectation de **VLAN** du client afin de garder la séparation entre le trafic des différents clients. Ce concept est appelé **802.1Q** en **802.1Q** ou empilement Q-en-Q, comme l'a été expliqué précédemment. Avec Q-in-Q, le **VLAN ID** de l'opérateur devient indicative de l'**EVC**, alors que **VLAN ID** du client (**VLAN-CE**) est révélateur de la structure interne du réseau du client et est caché par le réseau de l'opérateur.

Traduction de l'étiquette de VLAN / Échange : La traduction de l'étiquette de **VLAN** ou l'échange se produit lorsque les étiquettes **VLAN** sont locaux à l'**UNI**, ce qui signifie que la valeur de l'étiquette de **VLAN**, si elle existe d'un côté de l'**EVC**, est indépendante de la valeur de l'étiquette de **VLAN** de l'autre côté. Dans le cas où un côté de la **EVC** soutient l'étiquetage de **VLAN** et de l'autre côté n'est pas, l'opérateur supprime l'étiquette de **VLAN** des trames Ethernet avant qu'ils ne soient livrés à destination.

Un autre cas est de deux organisations qui ont fusionné et qui souhaitent lier leurs réseaux locaux ensemble, mais les affectations de **VLAN** interne de chaque organisation ne correspondent pas. L'opérateur peut offrir un service où les **VLAN** sont supprimés d'un côté de l'**EVC** et sont convertis au **VLAN** correcte de l'autre côté de l'**EVC**. Sans ce service, le seul moyen de joindre les deux organisations est par l'intermédiaire de routage **IP**, qui ignore les assignations de **VLAN** et délivre le trafic en fonction des adresses **IP**.

Un autre exemple de la traduction de l'étiquette est un scénario où différents clients sont dotés par la connectivité Internet à un **FAI.** L'opérateur attribue à chaque client une **EVC** distincte. L'opérateur attribue son propre **VLAN ID** pour l'**EVC** puis enlève l'étiquette de **VLAN** avant de faire passer le trafic au **FAI**. Ceci est illustré dans la figure 1-31.



*** Figure 1-31. Traduction VLAN ***

La figure 3-8 représente le support de Metro fournissant une connectivité Internet à trois clients. L'opérateur reçoit les trames non marquées (non étiquetés) à partir des routeurs situés dans chacun des locaux des clients. L'opérateur insert l'étiquette VLAN10 pour l'ensemble du trafic du client 1, VLAN20 pour le trafic du client 2, et VLAN30 pour le trafic du client. L'opérateur utilise les étiquettes **VLAN** pour séparer le trafic des trois clients au sein de son propre réseau. Au point de présence (**POP**), les étiquettes **VLAN** sont retirées de tous les **EVC** et transmis au routeur du **FAI**, qui est chargé d'offrir le service Internet **IP**.

- **Attribut du Service de multiplexage**

Le service de multiplexage est utilisé à l'appui de plusieurs instances d'**EVC** sur la même connexion physique. Ceci permet au même client d'avoir différents services sur la même boucle locale Ethernet.

- **Attribut de Regroupement**

L'attribut de service de Regroupement permet à deux ou plusieurs identifiants **VLAN** d'être mappés à un seul **EVC** à un **UNI**. Avec le regroupement, le prestataire et le client doivent s'entendre sur les identifiants **VLAN** utilisés à l'**UNI** et la correspondance entre chaque **ID** de **VLAN** et un **EVC** spécifique. Un cas particulier de regroupement, est où chaque **ID** de **VLAN** à l'interface **UNI** se mappe en un seul **EVC**. Cet attribut de service est appelé regroupement tout vers un.

- **Filtres attribut de sécurité**

Les filtres de sécurité sont des listes d'accès **MAC** que l'opérateur utilise pour bloquer certaines adresses et les inhiber d'écouler leurs trafic à travers l'**EVC**. Cela pourrait être un service supplémentaire que

l'opérateur peut offrir à la demande du client qui souhaite un niveau de protection contre certaines adresses **MAC**. Les adresses **MAC** qui correspondent à une certaine liste d'accès pourraient être inhibées ou autorisés.

3.3. Les défis avec les réseaux Metro Tout Ethernet

Tous les réseaux Metro tout-Ethernet posent de nombreux défis et l'évolutivité de fiabilité. Ce qui suit sont quelques-unes des questions qui se posent avec un plan de contrôle tout-Ethernet:

- Les restrictions sur le nombre de clients.
- Surveillance du service.
- Evolutivité du Backbone L2.
- Provisionnement de service.
- L'interfonctionnement avec les déploiements existants.

3.3.1. Restrictions sur le nombre de clients

Le plan de contrôle Ethernet restreint le transport à 4096 clients, parce que la norme **802.1Q** définit 12 bits qui peuvent être utilisés comme un **ID** de **VLAN**, ce qui limite le nombre de VLAN à 2^{12} soit 4096. On rappelle que, bien que Q-en-Q permet aux **VLAN** des clients (**VLAN-CE**) à être cachés au réseau de l'opérateur, le transporteur reste toujours limitée à 4096 **ID** de **VLAN** qui sont globales au sein de son réseau. Pour de nombreux opérateurs qui expérimentent avec le service Metro Ethernet, le nombre 4096 semble assez bon pour un réseau expérimental, mais présente à long terme une barrière si le service croît d'une façon radicale.

3.3.2. Surveillance du Service

Ethernet n'a pas un mécanisme intégré qui donne au service de surveillance. Avec **LMI**[1] en Frame Relay, par exemple, la surveillance du service et l'intégrité du service sont facilitées par des messages qui rapportent le statut de la **PVC**. La surveillance des services Ethernet nécessite une intelligence supplémentaire du plan de contrôle. Les nouveaux protocoles (**LMI**) doivent être définis et mis en place entre le réseau du fournisseur de services et les terminaux des clients pour permettre au client de découvrir les différentes **EVC** qui existent sur la connexion **UNI**. Le **LMI** peut apprendre la **CE-VLAN** à la l'**EVC** et peut apprendre les différents paramètres de service tels que les profils de la bande passante. D'autres protocoles doivent être définis pour découvrir l'intégrité de l'**EVC** en cas de défaillance possible. Des protocoles pour l'extraction des informations de l'**UNI** et l'**EVC** sont nécessaires pour rendre ces informations utilisables.

3.3.3. Evolutivité du Backbone L2

[1] LMI : Local Management Interface.

On peut maintenant se doter d'un réseau tout-Ethernet grâce au protocole **STP**. **STP** bloque les ports Ethernet pour éviter les boucles de réseau. L'ingénierie du trafic est normalement une importante exigence pour les opérateurs afin d'avoir un contrôle sur la bande passante réseau et de la trajectoire du trafic. Il semble très étrange pour tout opérateur d'avoir la fluidité du trafic dans son réseau dépendante de la prévention des boucles plutôt que de véritables mesures d'optimisation de la largeur de bande passante.

3.3.4. Provisionnement de service

Le transport d'un **VLAN** à travers le réseau n'est pas une tâche simple. Chaque fois qu'un nouveau **VLAN** de l'opérateur est créé (un nouveau **VPN**), il faut prendre soin de configurer ce **VLAN** sur tous les commutateurs qui doivent participer à ce **VPN**. L'absence de protocoles de signalisation qui permettent aux informations **VPN** d'être échangées, rend la tâche manuelle et fatigante. Même avec l'adoption de nouveaux protocoles tels que **802.1s** («Amendement à **802.1Q** Virtual Bridged Local Area Networks: Multiple Spanning Tree"), la tâche de mise à l'échelle du réseau est presque impossible.

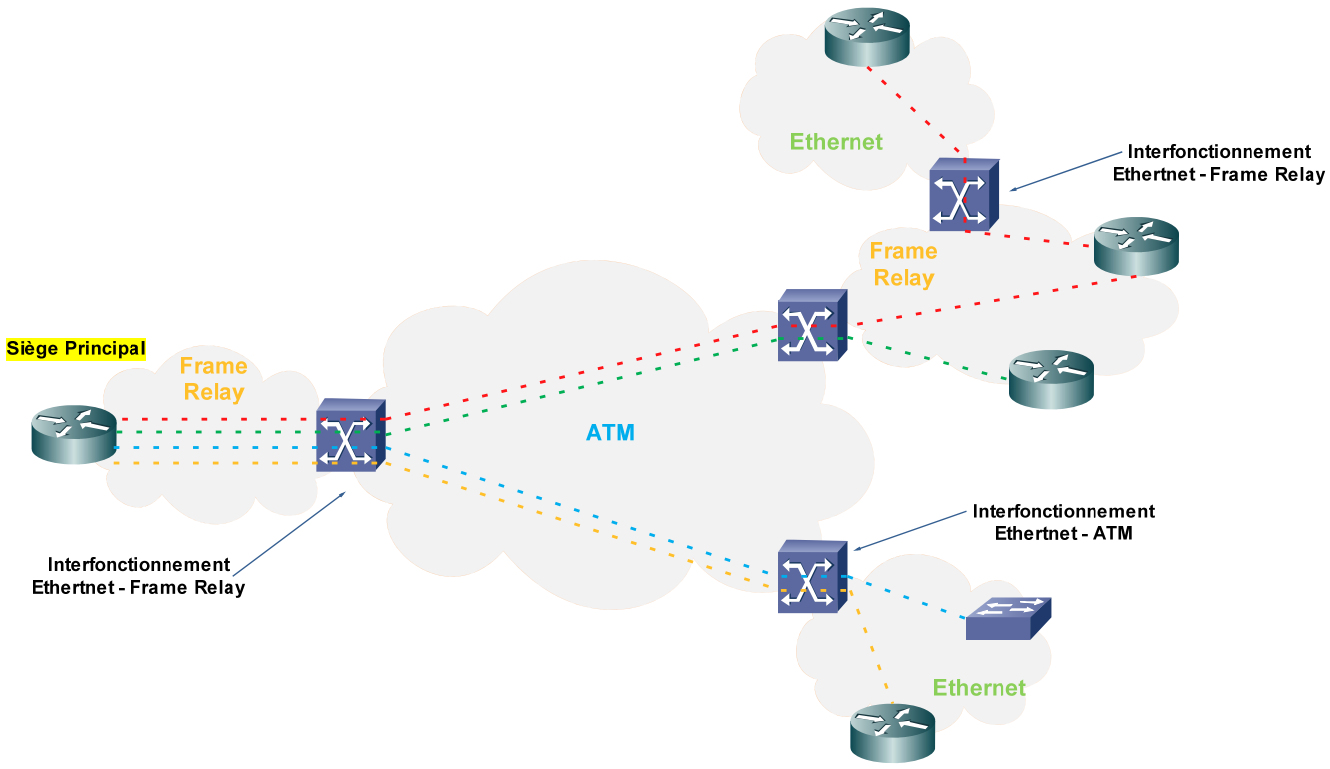
3.3.5. L'interfonctionnement avec les déploiements existants

Un autre défi auquel sont confrontés les déploiements Ethernet est l'interfonctionnement avec les déploiements existants hérités tels que les réseaux Frame Relay et **ATM**. Frame Relay a été largement déployé par de nombreuses entreprises comme un service **WAN**. Les bureaux distants sont connectés au siège via des circuits Point à Point Frame Relay formant une topologie en étoile. Les entreprises qui veulent adopter Ethernet comme technologie d'accès attendent de l'opérateur leurs fournir un moyen pour connecter dotés d'accès Ethernet avec les sites déjà existants rattachés au siège par des accès Frame Relay. Cela signifie qu'une fonction doit exister dans le réseau permettant aux services Frame Relay et Ethernet à travailler ensemble.

L'**IETF** a normalisé dans la **RFC2427**[1] la façon de mener différents protocoles sur Frame Relay, y compris Ethernet. Dans d'autres cas, les réseaux d'accès Frame Relay et Ethernet sont reliés par un réseau cœur **ATM**. Dans ce cas, deux fonctions d'interfonctionnement de service doivent se produisent, l'un entre l'Ethernet et **ATM** et l'autre entre l'**ATM** et Frame Relay. L'interfonctionnement Ethernet vers **ATM** est réalisé en utilisant la **RFC2684**, et l'interfonctionnement de l'**ATM** vers Frame Relay est assuré par la spécification **FRF8.1** du Frame Relay Forum.

La figure 1-32 illustre les fonctions d'interfonctionnement de service.

[1] RFC2427: Multiprotocol Interconnect Over Frame Relay.



*** Figure 1-32. Interfonctionnement de service ***

La figure 1-32 montre un scénario dans lequel un siège d'entreprise est relié à ses sites distants via des connexions Frame Relay transportées à travers un réseau **ATM**. Les différentes fonctions d'interfonctionnement de service sont affichées pour permettre à ces réseaux d'être opérationnels. Pour l'interfonctionnement de service, deux méthodes d'encapsulation sont définis: une est bridgée, et l'autre est routée. Les deux côtés de la connexion sont soit bridgée soit routée. Certains défis peuvent exister si l'une des extrémités de la connexion est connectée à un commutateur **LAN**, et d'où bridgée, tandis que l'autre extrémité est connectée à un routeur. D'autres questions se posent à cause des différents formats du protocole (**ARP**[1]) entre les différentes technologies, telles que l'Ethernet, Frame Relay et **ATM**.

Ce sont tous ces défis qui ont motivé l'apparition d'architectures hybrides comprenant de multiples domaines L2 qui sont connectés par l'intermédiaire d'un cœur **IP/MPLS** fonctionnant en L3. Le réseau peut évoluer parce que la L2 Ethernet serait contraint aux déploiements d'accès plus contrôlés qui limitent les inefficacités des **VLAN** et du **STP**. On peut assurer la rentabilité du réseau par la construction d'un réseau cœur **IP/MPLS** fiable.

[1] ARP: Address Resolution Protocol.

CHAPITRE 2

Les réseaux optiques de routage des longueurs d'onde

Les réseaux optiques de routage des longueurs d'onde ont été introduits avec succès et les organismes de normalisation, tels que l'**IETF**[1], l'**OIF**[2], et l'**ITU-T**[3], sont actuellement actifs pour le développement des normes. Un réseau optique de routage des longueurs d'onde se compose de brasseurs optiques (**OXC**[4]) interconnectés avec des fibres **WDM**[5]. La transmission des données sur ce réseau optique est assurée en utilisant des connexions à commutation de circuit optiques, connues sous le nom de chemins optiques.

Dans ce chapitre, on explore les différents aspects des réseaux optiques de routage des longueurs d'onde. On commence d'abord par la description des principales caractéristiques d'un réseau optique de routage des longueurs et d'introduire le concept le plus important du *chemin optique* et le concept de *groupage de trafic*, ce qui permet à plusieurs utilisateurs de partager le même chemin optique. On présente aussi les régimes de protection et de restauration utilisés.

Les informations sur un chemin optique sont généralement transmises en utilisant le tramage SDH. Les trames Ethernet peuvent également être transmises sur un réseau optique. Dans l'avenir, il est prévu que l'information sera transmise sur le réseau optique en utilisant la nouvelle norme de l'**UIT-T**, c'est la norme **G.709. G.709**, est aussi connue sous le nom de *l'enveloppe numérique* (Digital Wrapper), et permet la transmission des paquets **IP**, des trames Ethernet, des cellules **ATM** et des données synchrones **SDH**.

Le reste du chapitre est consacré au plan de contrôle des réseaux de routage des longueurs d'onde. On présente les différents types d'architectures de plan de contrôle, puis décrire l'architecture de **MPLS**[6] généralisé (**GMPLS**[7]), et l'interface utilisateur réseau (**UNI**[8]) de l'OIF. **GMPLS** est une extension de **MPLS**, et a été conçu pour appliquer les techniques de commutation des étiquettes de **MPLS** aux réseaux à multiplexage temporel (**TDM**[9]) et aux réseaux de routage des longueurs d'onde, en plus des réseaux à commutation de paquets. L'**UNI** de l'**OIF** précise des procédures de signalisation pour les clients afin de créer et supprimer automatiquement une connexion sur un réseau de routage de longueur d'onde.

La signalisation **UNI** a été mis en œuvre par l'extension des protocoles de distribution d'étiquettes, **LDP**[10] et **RSVP**[11].

1. Réseaux de routage des longueurs d'onde

[1] IETF : Internet Engineering Task Force.
[2] OIF : Optical Internetworking Forum.
[3] ITU: International Telecommunication Unit.
[4] OXC: Optical Cross Connect.
[5] WDM: Wavelength Division Multiplexing.
[6] MPLS: Multi-Protocol Label Switch.
[7] GMPLS: Generalized MPLS.
[8] UNI: User Network Interface.
[9] TDM: Time Division Multiplexing.
[10] LDP : Label Distribution Protocol.
[11] RSVP : Ressource Reservation Protocol

Un réseau de routage de longueurs d'onde se compose de des brasseurs optiques (**OXC)** reliés entre eux par des fibres **WDM**. Un brasseur optique (**OXC)** est un commutateur optique N × N, avec N fibres d'entrée et N fibres de sortie. Chaque fibre transmit W longueurs d'onde. Le brasseur optique (**OXC)** peut commuter d'une façon optique toutes les longueurs d'onde arrivants sur ses fibres d'entrée aux longueurs d'onde départant de ses fibres de sortie. Par exemple, il peut commuter le signal optique de longueur d'onde entrant λ_i de la fibre d'entrée ***k*** à la longueur d'onde sortant λ_i de la fibre de sortie ***m***. Si la longueur d'onde λ_i de fibres de sortie ***m*** de est utilisée, et si le brasseur optique (**OXC)** est équipé par des convertisseurs, par la suite le brasseur optique (**OXC)** peut encore commuter le signal optique de longueur d'onde arrivant λ_i de la fibre d'entrée ***k*** à une autre longueur d'onde départant λ_j de la fibre de sortie ***m***.

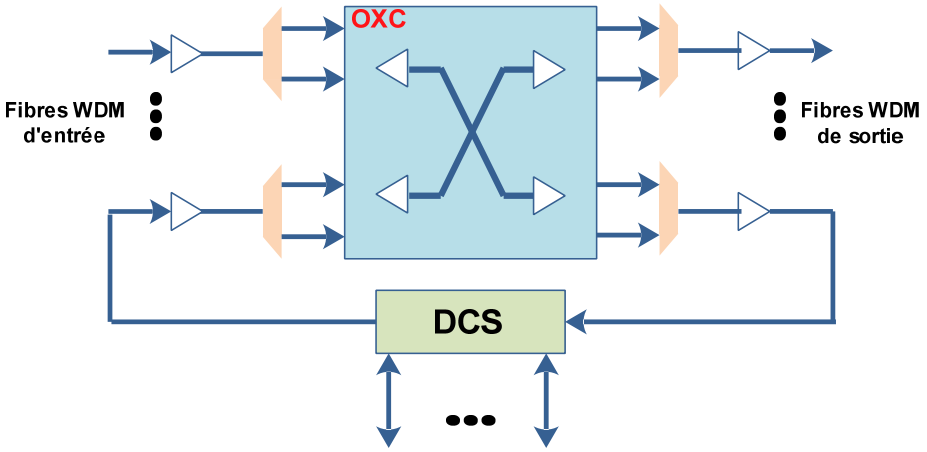
En plus de sa fonction de commuter des longueurs d'onde individuelles, un brasseur optique (**OXC)** peut commuter un ensemble de longueurs d'onde contiguës (connu encore par *Gamme d'ondes*) comme une seule unité. C'est-à-dire, il peut commuter un ensemble de longueurs d'onde contiguës d'une fibre d'entrée à un ensemble de longueurs d'onde contiguës d'une fibre de sortie. Cela peut être une caractéristique souhaitable du brasseur optique (**OXC**), parce qu'elle peut réduire la distorsion des longueurs d'onde individuelles. En outre, un brasseur optique (**OXC)** peut être pas incapable de séparer les longueurs d'onde entrant qui sont étroitement espacés. Dans ce cas, il peut toujours les commuter en utilisant la commutation de gamme d'ondes. Enfin, un brasseur optique (**OXC)** peut également commuter une fibre entière. C'est-à-dire, il peut commuter toutes les longueurs d'onde W d'une fibre d'entrée à une fibre de sortie.

Un **OXC** peut être utilisé comme un multiplexeur à insertion extraction optique (**OADM**[1]). Autrement dit, dit, il peut assurer l'extraction des signaux sur un certain nombre de longueurs d'onde et l'insertion de nouveaux signaux dans ces longueurs d'onde.

Les longueurs d'onde restantes sont commutées par le brasseur optique (**OXC**) d'une façon transparente. Un exemple d'**OADM** est illustré à la figure 2-1. Une de ses fibres de sortie est introduite dans un brasseur numérique (**DCS**[2]) d'un système **SDH**. Typiquement, une trame **SDH** est utilisée pour transmettre des données sur chaque longueur d'onde. Le brasseur numérique (**DCS**) convertit les signaux optiques entrants W dans le domaine électrique, et extrait les trames **SDH** de chaque longueur d'onde. Il peut alors commuter les Intervalles de temps à partir de la trame d'une longueur d'onde sur la trame d'une autre, extraire les affluents virtuels, et en insérer de nouveaux affluents.

Les nouveaux flux W résultant des trames **SDH** sont transmis au brasseur optique (**OXC**), chacun sur une longueur d'onde différente, puis sont permutés à différents fibres de sortie.

[1] OADM : Optical Add/Drop Multiplexer.
[2] DCS: Digital Cross Connect System.

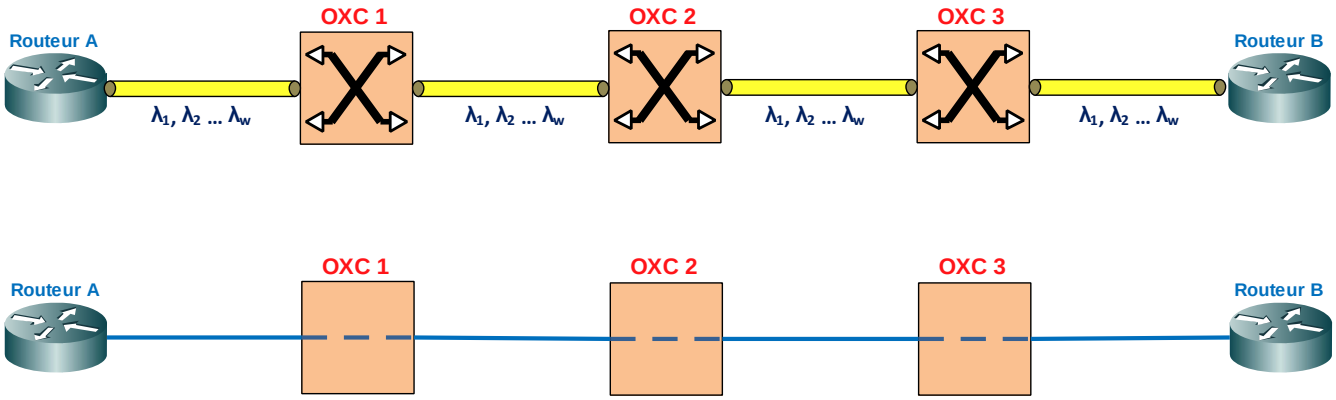


*** Figure 2-1. Un Brasseur optique (**OXC**) avec un Brasseur numérique (**DCS**) ***

1.1. Les chemins optiques

Une caractéristique importante d'un réseau de routage de longueur d'onde, c'est qu'il est un réseau de commutation de circuits. C'est-à-dire, pour qu'un utilisateur puisse transmettre des données à un utilisateur de destination, une connexion doit d'abord être installée. Cette connexion est une connexion de commutation de circuits et qui est établie en utilisant une longueur d'onde sur chaque tronçon tout le long du chemin de la connexion. Par exemple, on considère que deux routeurs **IP** (Routeur A Routeur B) sont connectés via un réseau de longueur d'onde à trois nœuds de routage (voir la figure 2-2). Les liens entre le Routeur A et **OXC1**, entre **OXC1** et **OXC2**, entre **OXC2** et **OXC3**, et enfin entre **OXC3** et le Routeur B, sont supposées être une fibre unique transportant des W longueurs d'onde, qui sont dénommés λ_1, λ_2,… , λ_W. Les données sont transmises d'une façon unidirectionnelle, du Routeur A vers le Routeur B. Pour transmettre des données dans le sens opposé (du Routeur B vers le Routeur A), un autre ensemble de fibres devrait être utilisé.

On suppose que le Routeur **IP** A veut transmettre des données vers le Routeur IP B. par l'utilisation d'un protocole de signalisation, le Routeur A demande l'établissement d'une connexion au Routeur B. La connexion entre les Routeurs A et B est établie par l'attribution de la même longueur d'onde (soit dis-on la longueur d'onde λ_1) sur tous les des liens tout le long du chemin de A vers B. En outre, chaque **OXC** est chargé de passer la longueur d'onde λ_1 à travers sa matrice de commutation d'une façon transparente. En conséquence, un chemin optique est formé entre les Routeurs A et B, sur lequel les données sont transmises optiquement de A vers B. Ce chemin optique connecte les Routeurs A et B dans un seul sens de A vers B. Pour que le routeur B communique avec le Routeur A, un chemin optique distinct doit être établi dans le sens opposé sur un ensemble différent de fibres qui sont mis en place pour transmettre dans la direction opposée.

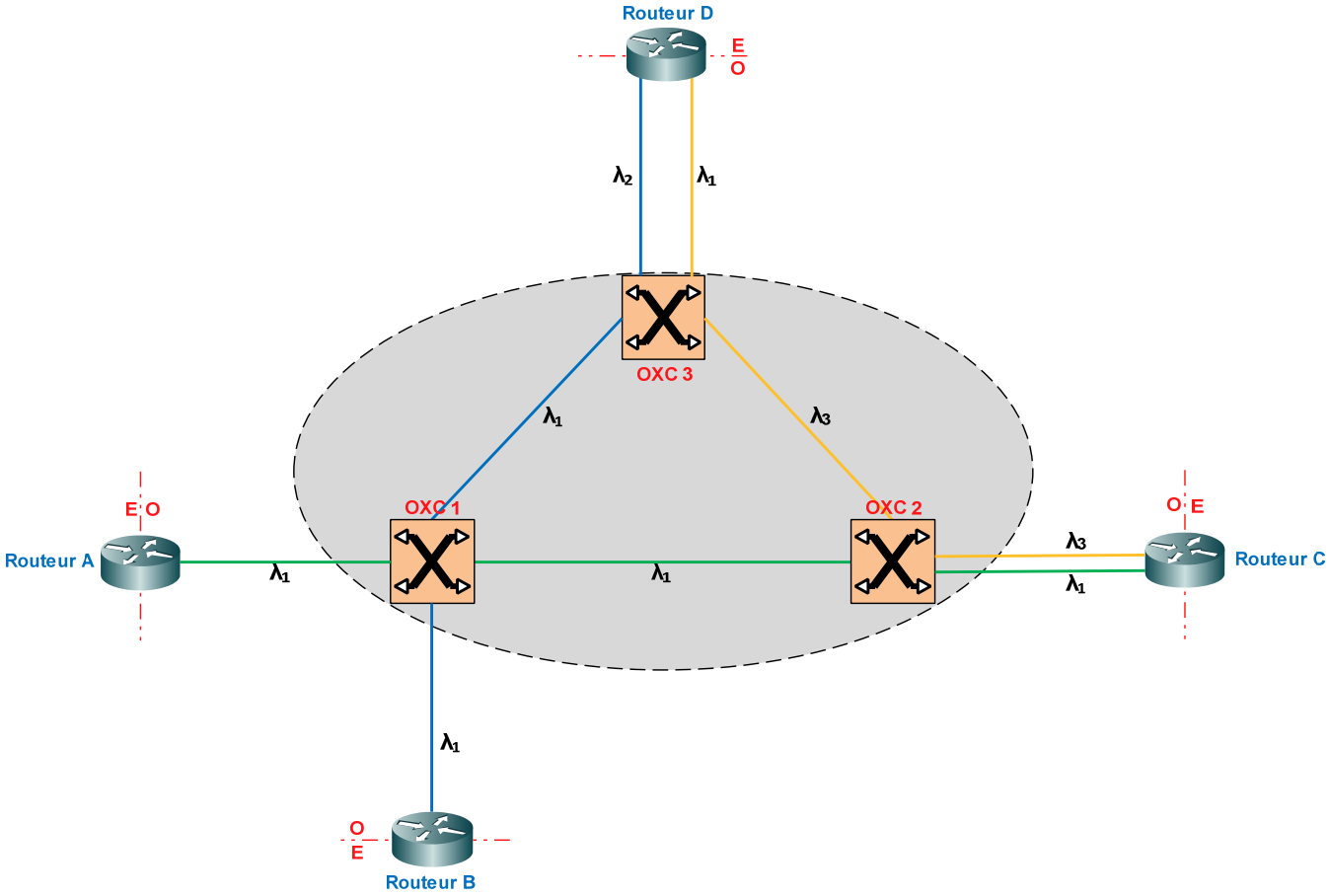


(b) Un Chemin optique entre le Routeur A et le Routeur B.

*** Figure 2-2. Un Chemin Optique ***

Quand on établit un chemin optique sur un réseau de routage de longueur d'onde, la même longueur d'onde doit être utilisée sur chaque tronçon tout le long du chemin. C'est ce qu'on appelle *la contrainte de continuité de longueur d'onde*. La longueur d'onde requise pourrait être indisponible à la fibre de sortie d'un brasseur optique (**OXC**), à travers lequel le chemin optique doit être acheminé. Dans ce cas, l'établissement de la route optique sera bloqué et un message de notification sera envoyé à l'utilisateur demandant le chemin optique. Pour réduire la possibilité qu'un chemin optique soit bloqué, le brasseur optique (**OXC**) peut être équipé par des de convertisseurs. Un convertisseur permet de transformer le signal optique transmis sur une longueur d'onde à une autre longueur d'onde. Dans un brasseur optique (**OXC**), pour chaque fibre de sortie avec un nombre W de longueurs d'onde, il pourrait y avoir des le nombre de ***c*** convertisseurs, où $0 \leq c \leq W$. Lorsque $c = 0$, on dit qu'il n'y a pas de conversion, quand $0<c<W$, on dit qu'il y a une conversion partielle, et quand $c = W$, nous disons qu'il ya une conversion complète. Les convertisseurs sont encore chers, et ils peuvent être déployés dans certains brasseurs optiques (**OXC**) stratégiques dans un réseau de routage de longueurs d'onde. Une hypothèse commune faite dans la littérature est qu'un convertisseur peut transformer un signal sur une longueur d'onde λ à toute autre longueur d'onde. Cependant, actuellement, il ne peut la transformer qu'en une autre longueur d'onde qui lointaine de quelques nm de la longueur d'onde λ.

Un exemple de différents chemins optiques établis sur un réseau de routage de longueur d'onde est représenté sur la figure 2-3. Le réseau optique est constitué par les brasseurs optiques **OXC1**, **OXC2** et **OXC3**. Seul le brasseur optique **OXC3** est supposé être équipé de convertisseurs (au moins deux, pour les raisons de cet exemple). Les Routeurs **IP** A et B sont rattachés à **OXC1** à deux ports d'entrée différents; le Routeur **IP** C est attaché à **OXC2** et le Routeur **IP** D est rattaché à **OXC3**. Les chemins optiques suivants ont été établies: du Routeur A au Routeur C via les brasseurs optiques **OXC1** et **OXC2**; du Routeur B au Routeur D via les brasseurs optiques **OXC1** et **OXC3** et enfin du Routeur C au Routeur D via les brasseurs optiques **OXC2** et **OXC3**. Les longueurs d'onde allouées à chaque chemin optique sont indiquées à la figure 2-3.



*** Figure 2-3. Un exemple de différents chemins optiques***

La longueur d'onde λ_1 est utilisée pour le chemin optique du Routeur A au Routeur C sur tous les tronçons, c'est-à-dire du Routeur A à l'**OXC1**, puis de l'**OXC1** à l'**OXC2**, et enfin de l'**OXC2** au Routeur C. Le chemin optique du Routeur B au Routeur D utilise λ_1 sur le tronçon du Routeur B à l'**OXC1** et de l'**OXC1** à l'**OXC3**, et utilise λ_2 sur le tronçon de l'**OXC3** au Routeur D. Enfin, le chemin optique du Routeur C au Routeur D utilise λ_3 sur le tronçon du Routeur C à l'**OXC2**, puis de l'**OXC2** à l'**OXC3**, et utilise $\lambda_1$sur le tronçon de l'**OXC3** au Routeur D.

Tel que l'on a mentionné ci-dessus, la transmission sur un chemin optique est unidirectionnelle. Dans la figure 2-3, seuls les chemins optiques des routeurs A à C, B à D, et C à D sont présentés. Pour la communication bidirectionnelle entre deux routeurs, un autre chemin optique distinct doit être mis en place dans la direction opposée à travers les mêmes brasseurs optiques (**OXC)**. Par exemple, pour une communication bidirectionnelle entre les routeurs A et C, un autre chemin optique doit être mis en place à partir de C routeur vers le routeur A via l'**OXC2** et l'**OXC1**, en utilisant d'autres liens en fibre. Enfin, on note que la transmission des données au sein du réseau de routage de longueur d'onde se produit entièrement dans le domaine optique. (Dans la figure 2-3, les lignes en pointillés le long des routeurs IP signifient la frontière entre le domaine électrique [E] et l'optique dans le domaine [O].)

Les chemins optiques peuvent être statiques (par exemple dans une connexion **ATM**[1] **PVC**[2]) ou dynamiques (par exemple dans une connexion **ATM SVC**[3]). Les chemins optiques statiques sont établis en utilisant des procédures de gestion de réseau, et restent généralement pour une longue période. Les réseaux privés virtuels (**VPN**[4]) peuvent également être configurés à l'aide de chemins optiques statiques. Les chemins optiques dynamiques sont mis en place en temps réel en utilisant des protocoles de signalisation, comme le **GMPLS** de l'**IETF** et l'interface réseau utilisateur (**UNI**) proposé par l'**OIF**.

1.2. Groupage de trafic

Un chemin optique est utilisé exclusivement par un seul client. Très souvent, la bande passante qu'un client exige est beaucoup inférieure que la bande passante de la longueur d'onde, ce qui signifie qu'une partie de la bande passante du chemin optique reste initialisée. Pour résoudre ce problème, la bande passante d'un chemin optique est divisé en unités à bas débit (ou à basse vitesse), afin qu'il puisse porter les flux de trafic transmis à des débits inférieurs.

Un client peut demander à un ou plusieurs de ces unités à bas débit. Cette technique, connue sous le nom de groupage de trafic, permet le partage de la bande passante d'un chemin optique par plusieurs clients. En comparaison de l'utilisation d'un chemin optique entier, le groupage de trafic améliore l'utilisation de longueurs d'onde et assure des économies de coûts pour les clients.

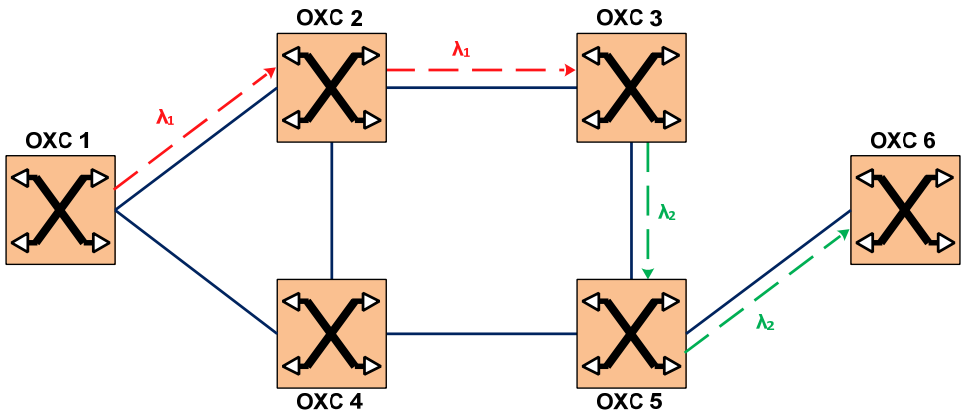
A titre d'exemple, on considère le réseau optique à six nœuds (voir Figure 2-4). L'information est transmise sur le réseau optique utilisant le tramage **SDH** avec un débit de transmission de **STM16** (2,488Gbps). Un chemin optique, indiquée par une ligne pointillée, a été établie à partir de l'**OXC1** à l'**OXC3** à travers l'**OXC2** en utilisant la longueur d'onde λ_1. L'unité à basse vitesse est un **STM1** (155Mbps), ce qui signifie que 16 unités de basse vitesse **STM1** sont disponibles sur le chemin optique. Un utilisateur, attaché à l'**OXC1**, qui veut transmettre des données à un autre utilisateur, attaché à l'**OXC3**, peut demander un nombre entier d'unités basse vitesse **STM1** jusqu'à un total de 16. Si le trafic entre ces deux brasseurs optiques (**OXC**) dépasse 2,488Gbps, d'autres chemins optiques peuvent être établie.

Un chemin optique peut être considéré comme un tunnel entre l'**OXC** de départ et l'**OXC** d'arrivée. Autrement dit, le flux de données transmis sur le chemin optique entre l'**OXC1** et l'**OXC3**, ne peut se provenir que de l'**OXC1** et se terminer à l'**OXC3**. Aucune donnée ne peut être insérée ou extraite du chemin optique au niveau de l'**OXC2**.

[1] ATM : Asynchronous Transfer Mode.
[2] PVC : Permanent Virtual Connection.
[3] SVC : Switched Virtual Connection.
[4] VPN: Virtual Private Network.

Comme l'on a expliqué précédemment, si aucune conversion n'est disponible, alors la même longueur d'onde doit être affectée à un chemin optique sur l'ensemble du ses tronçons. Cependant, la contrainte de continuité de longueur d'onde n'est pas nécessaire si la conversion est disponible. Par exemple, le chemin optique entre l'**OXC1** et l'**OXC3** utilise la même longueur d'onde, car il a été supposé que l'**OXC2** n'est pas équipé de convertisseurs. Toutefois, si l'**OXC2** est équipé de convertisseurs, par la suite le chemin optique peut être établi en utilisant n'importe quelle longueur d'onde sur les liens entre **OXC1** à **OXC2**, et entre **OXC2** à **OXC3**.

Enfin, un flux de données peut parcourir plus qu'un chemin optique en vue d'atteindre sa destination. Par exemple, on suppose qu'un utilisateur attaché à l'**OXC1** une demande quatre unités basse vitesse **STM1** pour transmettre un flux de données en **STM4** (622Mbps) à un utilisateur attaché à l'**OXC4**. Dans ce cas, un nouveau chemin optique doit être établi entre l'**OXC1** et l'**OXC4**, peut-être à travers l'**OXC6** et l'**OXC5**. On suppose qu'un chemin optique entre l'**OXC3** et l'**OXC4** existe déjà. Ce chemin optique (représenté sur la figure 2-4 par une ligne pointillée) est acheminé à travers l'**OXC5** et utilise la longueur d'onde λ_2. Dans ce cas, le flux de données **STM4** seront acheminés vers l'**OXC3** sur le chemin optique de l'**OXC1** à l'**OXC3**, puis vers l'**OXC4** sur le chemin optique de l'**OXC3** à l'**OXC4**. Cette solution suppose qu'il existe une capacité disponible sur les deux chemins optiques pour transporter le flux de 622Mbps. En outre, il suppose que l'**OXC3** possède un brasseur numérique (**DCS**) SDH qui permet à l'**OXC3** d'extraire le flux de données entrants de la trame **SDH** sur le premier chemin optique et de le déplacer dans les trames SDH du deuxième chemin optique.



*** Figure 2-4. Un exemple de groupage de trafic***

2. Les plans de protection

Dans les paragraphes qui suivent on aborde les plans de protection contre les défaillances des composants matériels dans un réseau optique. Les pannes de lien sont les plus fréquentes et surviennent quand un câble de fibre est coupé accidentellement en creusant dans une zone par laquelle passent les câbles de fibres. Un lien peut également échouer si un amplificateur qui amplifie le signal multiplexé de toutes les

longueurs d'onde sur une fibre tombe en panne. Une longueur d'onde individuelle au sein d'une fibre peut également échouer si son émetteur ou son récepteur échoue. Enfin, un brasseur optique (**OXC**) peut échouer.

La protection peut être effectuée au niveau d'un chemin optique individuel ou au niveau d'une seule fibre. La protection du chemin désigne les plans pour la restauration d'un chemin optique, et la protection du lien désigne les plans pour la restauration d'une seule fibre, par laquelle toutes les longueurs d'onde sont restaurées en même temps.

Ci-dessous, on examine les plans de protection de chemin et de lien pour les liaisons point à point, les anneaux optiques WDM, et les réseaux optiques maillés de routage de longueurs d'onde.

2.1. Liens Point à point

Le réseau optique le plus simple est un lien WDM point à point qui relie deux nœuds. La protection du lien peut être faite par une manière dédiée 1+1 ou d'une manière non-dédié 1:1 ou 1:N. Dans le plan 1+1, le signal est transmis simultanément sur deux fibres distinctes, qui sont de préférence diversement acheminées (c'est-à-dire, qu'ils suivent des chemins différents géographiquement). Le récepteur surveille la qualité des deux signaux et sélectionne le meilleur des deux. Si une fibre échoue, le récepteur continue à recevoir des données sur l'autre fibre. Dans le plan 1:1, il y a encore deux fibres diversement acheminées, une fibre de travail et une fibre de protection. Le signal est transmis sur la fibre de travail. Si elle échoue, alors la source et la destination basculent à la fois à la fibre de protection. Le plan 1:N est une généralisation du régime de 1:1, où N fibres de travail sont protégés par une fibre unique de protection. Comme il y a une seule fibre de protection, une seule fibre de travail peut être protégée à tout moment.

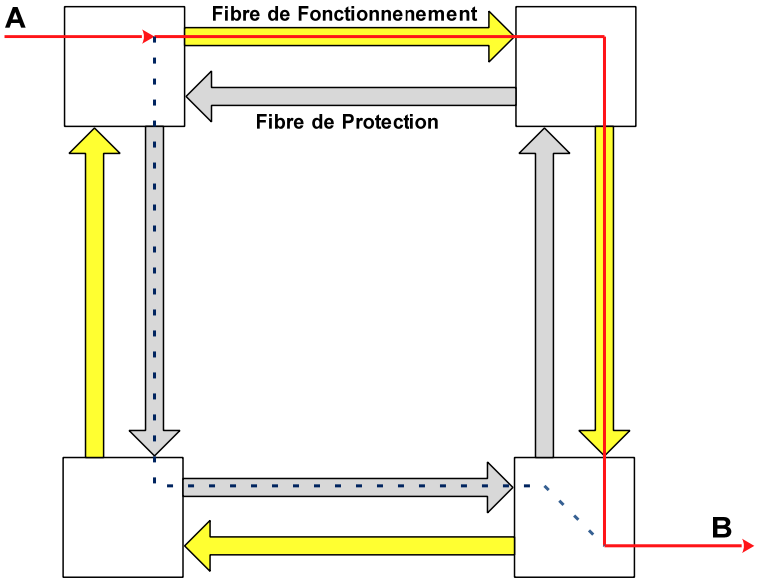
2.2. Les anneaux optiques WDM

Les anneaux optiques **WDM** peuvent être vus comme une extension des anneaux **SDH** dans le domaine **WDM**. Plusieurs différentes architectures d'anneaux **WDM** ont été proposées, qui varient des anneaux statiques simples aux anneaux dynamiques les plus avancés. Ci-dessous, on examinera les plans de protection de trois types d'anneaux **WDM**: les anneaux optiques à partage de chemin unidirectionnel (**OUPSR**[1]), les anneaux optiques à partage de lien bidirectionnel sur deux fibres (**2F-OBLSR**[2]), et les anneaux optiques à partage de lien bidirectionnel sur quatre fibres (**4F- OBLSR**[3]).

L'**OUPSR** est unidirectionnel. Il s'agit d'un anneau de travail et un anneau de protection qui transmettent dans des directions opposées (voir la figure 2-5). Le plan de protection 1+1 est utilisé pour mettre en œuvre plan simple pour la protection du chemin. C'est-à-dire, le chemin optique est divisé au niveau du nœud source

[1] OUPSR :Optical Unidirectionnal Path Sharing Ring.
[2] 2F-OBLSR : Two Fibers - Optical Bidirectionnal Link Sharing Ring.
[3] 4F-OBLSR : Four Fibers - Optical Bidirectionnal Link Sharing Ring.

et il est transmis à travers l'anneau de travail et l'anneau de protection (voir la figure 2-5 de A à B). La destination choisit le meilleur signal. Quand un lien en fibre est brisé, le récepteur continue à recevoir le signal sur l'autre voie. L'**OUPSR** fournit une architecture simple et robuste, sans avoir besoin de protocoles complexes pour la signalisation de la protection. Ce type d'anneaux est généralement utilisé comme un anneau *Metro Edge*, et il connecte un petit nombre de nœuds (par exemple, les réseaux d'accès et les sites des clients) à un nœud concentrateur, qui est attaché à un anneau *Metro Core*. Le trafic transmis sur l'anneau est statique et il présente le comportement du concentrateur (hub). C'est-à-dire, il est dirigé à partir des nœuds vers le concentrateur et à partir du concentrateur vers les nœuds. Les chemins optiques statiques sont utilisés.



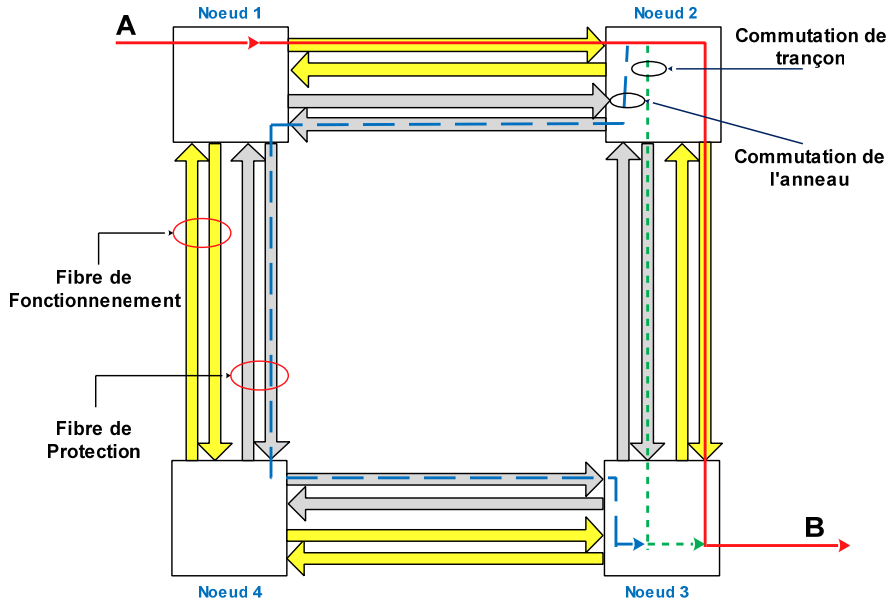
*** Figure 2-5. Un Anneau optique à partage de chemin unidirectionnel (**OUPSR**)***

Les anneaux optiques à partage de chemin bidirectionnel sur deux fibres ou sur quatre fibres sont utilisés dans le *Metro Core* où les modèles de trafic changent dynamiquement. Un protocole de signalisation est utilisé pour établir et mettre fin aux chemins optiques et les plans de protection sont accomplis en utilisant un protocole de signalisation de la protection distribué en temps réel connue sous le nom de commutation de protection automatique optique (Optical **APS**[1]).

Les anneaux optiques à partage de lien bidirectionnel sur deux fibres (**2F-OBLSR**) utilisent deux anneaux, qui transmettent dans des directions opposées (comme dans le cas de l'**OUPSR**). Chaque fibre est partitionnée en deux ensembles de longueurs d'onde; un ensemble de longueurs d'onde de travail et un ensemble de longueurs d'onde de protection. Si une fibre échoue, le trafic sera réacheminé sur les longueurs d'onde de protection de l'autre fibre.

[1] APS : Automatic Protection Switching.

Les anneaux optiques à partage de lien bidirectionnel sur quatre fibres (**4F-OBLSR**) utilisent deux fibres de travail et deux fibres de protection (voir la figure 2-6). La protection peut être faite à la fois au niveau de la fibre ou au niveau du chemin optique. La commutation de protection en fibres est utilisée pour restaurer une défaillance du réseau causé par une coupure de fibre ou par une défaillance d'un amplificateur optique. La commutation de protection en chemins optiques est utilisée pour restaurer un chemin optique qui a échoué en raison d'une panne de l'émetteur ou du récepteur.



*** Figure 2-6. Anneau optique à partage de lien bidirectionnel sur quatre fibres (**4F-OBLSR**) ***

On prend un chemin optique de l'utilisateur A à l'utilisateur B (voir la ligne continue de la figure 2-6). Ce chemin optique est acheminé à travers les nœuds : 1, 2 et 3. On suppose que le chemin optique échoue sur le lien entre les nœuds 2 et 3. Dans ce cas, le mécanisme de protection déviera le chemin optique à la fibre de protection du nœud 2 au nœud 3 (voir la ligne pointillée étiquetés «commutation de tronçon » à la figure 2-6). Si la fibre de travail du nœud 2 au nœud 3 échoue aussi, alors tous les chemins optiques seront déviés vers la fibre de protection du nœud 2 au nœud 3, comme dans le cas du chemin optique susmentionné. Ceci est connu sous le nom de « commutation de tronçon ». Lorsque les quatre fibres sont coupées entre les nœuds 2 et 3, le trafic sera dévié sur les fibres de travail dans la direction opposée. Ceci est connu sous le nom de « commutation de l'anneau ». Dans ce cas, le chemin optique de A à B sera détourné, c'est-à-dire, il sera réacheminé de retour vers le nœud 1, puis vers le nœud 4 et enfin vers le nœud 3. (Voir la ligne en pointillé portant la mention «Commutation de l'anneau » à la figure 2-6.)

2.3. Réseaux optiques maillés

Un réseau maillé peut employer à la fois la protection du chemin optique et la protection du lien. La protection du lien peut être réalisée en utilisant les plans de protection point-à-point 1+1, 1:1 et 1:N. La

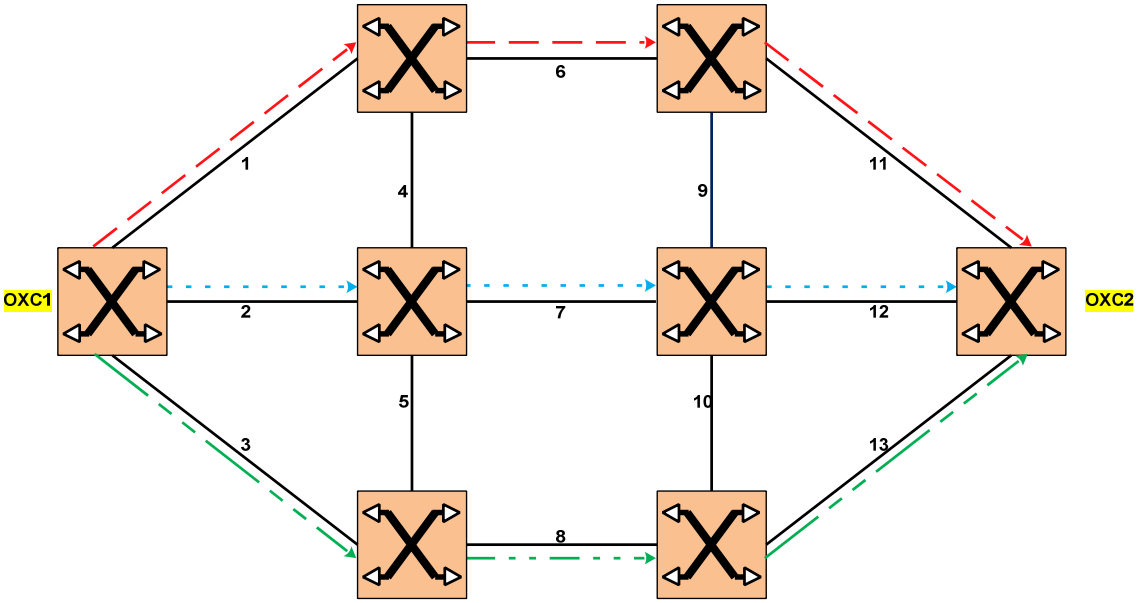
protection du chemin utilise des chemins de sauvegarde dédiés ou partagé. Par ailleurs, une topologie maillée arbitraire peut être organisée dans un ensemble d'anneaux optiques **WDM**, qui permet des plans de protection en anneau.

Le plan de protection du chemin 1+1 est la forme la plus simple de protection. Il est aussi la solution la plus coûteuse et qui engendre un faible rendement de la bande passante. Le signal de l'utilisateur est divisé en deux exemplaires, et chaque copie est transmise simultanément sur deux chemins optiques distincts. Les chemins optiques peuvent être diversement acheminés (c'est à dire qu'ils suivent des chemins différents géographiquement) ou ils peuvent passer par les mêmes brasseurs optiques (**OXC**) avec l'utilisation de différentes fibres. Le récepteur surveille la qualité des deux signaux et sélectionne le meilleur des deux. Si un chemin optique échoue, le récepteur continue à recevoir des données sur l'autre chemin optique.

Dans le cas de la protection du chemin 1:1, le signal de l'utilisateur est transmis à travers un chemin optique de travail. Le chemin optique de protection ou de sécurisation est également établi, mais il n'est pas utilisé. Si le chemin optique de travail échoue, La source et la destination basculent vers le chemin optique de protection. Comme la bande passante allouée au chemin optique de protection n'est pas utilisée pendant le fonctionnement normal, elle peut être partagée par plusieurs chemins optiques de travail. C'est le plan de protection du chemin 1:N.

Un concept important dans ces plans de protection est le concept du groupe de liens à risque partagé (**SRLG**[1]). Un **SRLG** est un groupe de liens qui partagent les mêmes ressources physiques, comme un câble, un conduit, et un brasseur optique (**OXC**). La défaillance de ces ressources physiques provoque une défaillance de tous les liens. Chaque ressource physique commune est associée à un identificateur appelé le **SRLG**. Lors de la configuration des chemins optiques de travail et de protection, on prend soin pour que les deux chemins optiques ne soient pas acheminés à travers le même **SRLG**. Par exemple, on considère le réseau optique représenté sur la figure 2-7. Le chemin optique de travail de l'**OXC1** à l'**OXC2** qui utilise les liens {1, 6, 11} et de son chemin optique de protection qui utilise les liens {3, 8, 13} n'utilisent pas le même **SRLG**. Autrement dit, ils sont à **SRLG** disjoints.

[1] SRLG : Shared Risk Link Group.



*** Figure 2-7. Protection du chemin***

Le concept de **SRLG** peut également être utilisé dans le plan de protection partagée 1:N. Par exemple, dans la figure 2-7, les deux chemins optiques de travail {1, 6, 11} et {2, 7, 12} de l'**OXC1** à l'**OXC2** sont à **SRLG** disjoints. Par conséquent, il est logique qu'ils utilisent tous les deux le même chemin optique de protection à **SRLG** disjoints {3, 8, 13}. C'est parce qu'une défaillance unique d'une ressource physique le long du trajet de l'une des chemins optiques de travail (à l'exclusion des **OXC** de départ et d'arrivée) ne causera pas la défaillance des deux chemins optiques de travail en même temps. Alors, dans ce cas, le chemin optique de la protection ne sera utilisé que par l'un des deux chemins optiques de travail.

Dans les plans de protection, les routes de protection de secours sont pré-planifiées et les ressources nécessaires (par exemple : longueurs d'onde, des fibres, et la bande passante au sein d'un brasseur optique **OXC**) sont attribués à l'avance. Pendant le fonctionnement normal du réseau, ces ressources sont soit maintenus en veille, soit sont utilisés pour transmettre le trafic de faible priorité qui peut être interrompu lorsqu'une défaillance se produit. Une autre stratégie, connue sous le nom de *restauration dynamique*, consiste à calculer un chemin de protection et d'allouer des ressources pour la récupération au moment où se produit une défaillance du réseau. Cette approche a une utilisation plus efficace des ressources, mais le temps de récupération est plus long que dans le cas d'un plan de protection préalable.

3. Le Standard UIT-T G.709 – L'Enveloppe Numérique

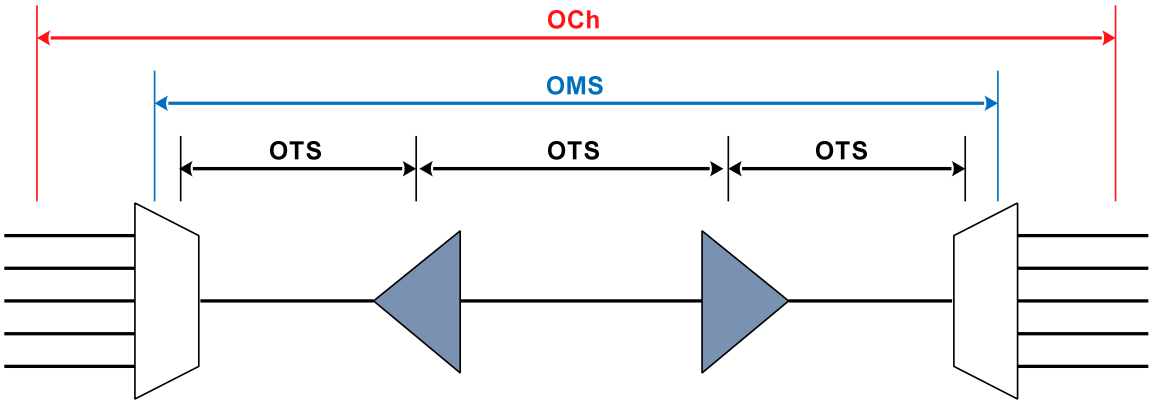
L'information sur un chemin optique est généralement transmise à l'aide de tramage **SDH**. En outre, les trames Ethernet peuvent être transmises sur un réseau optique. Il est prévu que l'information sera transmise sur le réseau optique en utilisant la nouvelle norme de l'**UIT-T G.709**, autrement connu sous le nom de *l'enveloppe numérique*. Cette norme définit les interfaces nœud de réseau entre deux opérateurs de réseaux optiques, ou entre sous-réseaux de fournisseurs dans le même réseau d'un opérateur. Voici quelques-unes des caractéristiques de la norme **G.709**:

- *Types de trafic*: La norme permet la transmission de différents types de trafic, comme des paquets **IP** et des trames Gigabit Ethernet en utilisant la procédure (**GFP**[1]), des cellules **ATM** et des données synchrone **SDH**.
- *Granularité du débit binaire*: la norme **G.709** prévoit trois granularités de débit: 2,488Gbps, 9.95Gbps et 39,81Gbps. Cette granularité est plus grosse que celle de **SDH**, mais convient pour les réseaux térabit, car elle évite le grand nombre de voies à faible débit binaire qui devrait être utilisées avec **SDH**.
- *Surveillance des connexions*: **G.709** fournit également des capacités de surveillance des connexions qui vont au-delà de celles de **SDH**.
- *Correction d'erreur (***FEC**[2]*)*: Comme les débits de transmission augmentent à 10Gbps et la dépassent, les paramètres physiques de la fibre optique jouent un rôle important dans la dégradation du signal optique transmis. Le **FEC** peut être utilisé pour détecter et corriger les erreurs sur les bits causée par des déficiences physiques sur les liens de transmission. Le **FEC** permet la transmission à des débits plus élevés, sans dégradation des performances.

Dans l'**UIT-T**, un réseau optique est appelé le *réseau de transport optique* (**OTN**[3]). Il se compose de trois couches: le *canal optique* (**Och**[4]), la *section de multiplexage optique* (**OMS**[5]), et la *section de transmission optique* (**OTS**[6]). (Voir la figure 2-8.) Le canal optique est une connexion optique entre deux utilisateurs, et il prend un chemin optique entier. Les canaux optiques sont multiplexés et transmis comme un seul signal sur une fibre. La section située entre un multiplexeur et un démultiplexeur sur laquelle le signal multiplexé est transporté est appelée section de multiplexage optique. Enfin, le transport entre deux points d'accès sur lesquels le signal multiplexé est transmis est appelé la section de transmission optique.

Chacune des couches OTN est associée à une structure de trame et des entêtes appropriés.

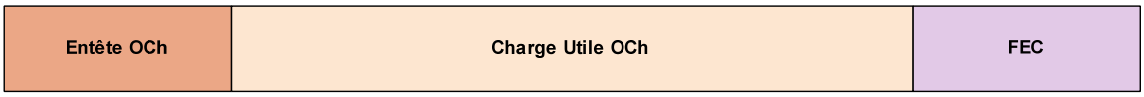
[1] GFP : Generic Framing Procedure.
[2] FEC : Forward Error Correction.
[3] OTN: Optical Transport Network.
[4] Och: Optical Channel.
[5] OMS: Optical Multiplex Section.
[6] OTS: Optical Transmission Section.



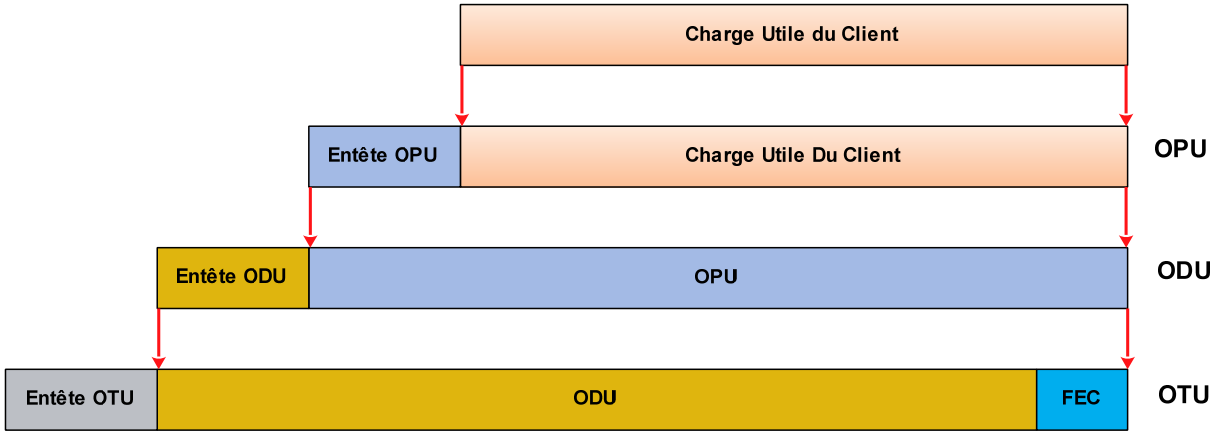
*** Figure 2-8. Structure des couches d'un réseau de transport optique (**OTN**) ***

3.1. Trame du canal optique (Och)

Les données de l'utilisateur sont transmises dans des trames qui contiennent plusieurs types d'entêtes, le champ de la charge utile, et le champ de la correction d'erreurs (**FEC**[1]), comme le montre la figure 2-9. Les entêtes de canaux optiques sont présentés dans la figure 2-10. La charge utile du client est encapsulée avec l'entête (**OPU**[2]) qui comprend des informations relatives au type de trafic fournies par l'utilisateur. L'**OPU** qui en résulte est ensuite encapsulé avec l'entête (**ODU**[3]), qui fournit des informations pour le suivi connexion en tandem, et la supervision chemin de bout en bout. Enfin, l'**ODU** résultant est encapsulé avec l'entête (**OTU**[4]), qui comprend des informations pour le suivi du signal sur une section. L'**ODU** est également encapsulé avec la **FEC**.



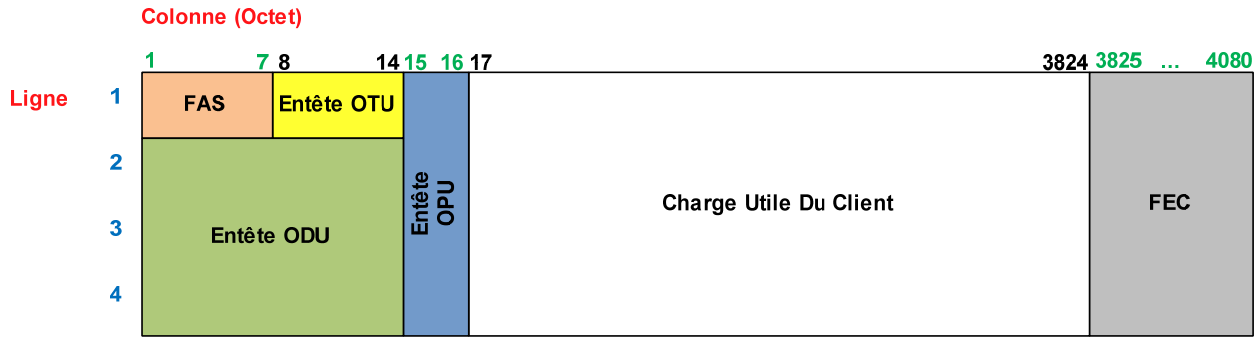
*** Figure 2-9. Trame du canal optique **Och** ***



[1] FEC: Forward Error Correction.
[2] OPU: Och Payload Unit.
[3] ODU: Och Data Unit.
[4] OTU: Och Transmission Unit.

*** Figure 2-10. Les entêtes du canal optique **Och** ***

Comme dans la trame de **SDH**, la trame de l'**OTU** est arrangée dans une matrice constituée de quatre lignes de 4080 octets chacun (voir Figure 2-11). Les données sont transmises en série, ligne par ligne à partir de la gauche de la première rangée. On rappelle qu'une trame **SDH** est transmise tous les 125µs. Les débits de transmission les plus élevés en **SDH** sont atteints en augmentant la taille de la trame **SDH**. Contrairement à **SDH**, la taille de la trame de l'**OTU** ne change pas avec l'augmentation de la vitesse de transmission. Les débits de transmission les plus élevés sont atteints tout simplement par l'augmentation du débit de transmission de la trame de l'**OTU**. Il s'agit d'un départ principal du concept traditionnel de 125µs, qui a été utilisé dans les réseaux de communication. Trois débits de transmission ont été définis pour la transmission des trames **OTU**: 2,488Gbps, 9.95Gbps et 39,81Gbps. Le temps pour transmettre une trame de l'**OTU** est 48.971µs lorsque le débit de transmission est de 2,488Gbps, 12.191µs lorsque le débit de transmission est de 9.95Gbps, et 3.035µs lorsque le taux de transmission est 39,81Gbps.



*** Figure 2-11. Format de la trame **OTU*****

3.2. Les types d'entêtes

a. Les entêtes OPU

Les champs d'entêtes **OPU** sont situés dans les rangées (lignes) de 1 à 4 et les colonnes 15 et 16. Ils fournissent des informations relatives au signal du client, c'est-à-dire les données transmises par l'utilisateur. Cet entête est créé au point où le signal du client est provenu, et il est utilisé au point où le signal du client est terminé. Tous les octets sont réservés à l'exception de l'octet de l'identifiant de la structure de la charge utile (**PSI**[1]), situé sur la ligne N°:4 et la colonne N°:15. Ce champ est utilisé pour transporter un message de 256

[1] PSI: Payload Structure Identifier.

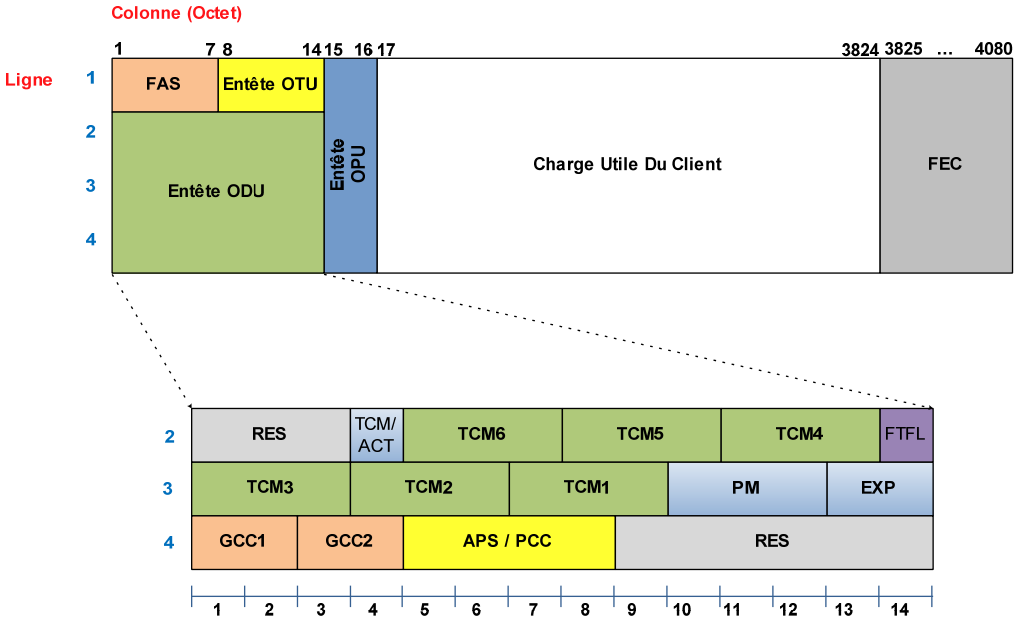
octets sur une multi-trame. Le premier octet de ce message contient le type de la charge utile (**PT**[1]) qui est utilisé pour identifier le type de la charge utile transportée dans l'**OPUU**.

b. Les entêtes ODU

Les champs d'entêtes **ODU** sont situés sur les lignes de 2 à 4 et les colonnes de 1 à 14. Il fournit de deux entêtes importants: l'entête de la surveillance du chemin (**PM**[2]), et l'entête de la surveillance de la connexion en tandem (**TCM**[3]). L'entête **ODU** de la surveillance du chemin permet la surveillance de sections particulières au sein du réseau ainsi que la localisation du défaut dans le réseau. La surveillance des connexions en tandem permet la gestion des signaux sur multiples réseaux. Comme le montre la Figure 2-12, les champs suivants ont été définis:

- **RES:** Réservé
- **TCM/ACT**: Activation/Désactivation des champs **TCM**.
- **TCM**i: Surveillance de connexion en tandem de la i^{ème} connexion.
- **FTFL**[4]: Canal de reportage du type de défaut et de localisation du défaut.
- **PM**: Surveillance du chemin.
- **EXP**: Réservés à des fins expérimentales
- **GCC**[5]: Canal de communication générale
- **APS**[6]**/PCC**[7]: La commutation de la protection automatique et canal de communication de la protection.

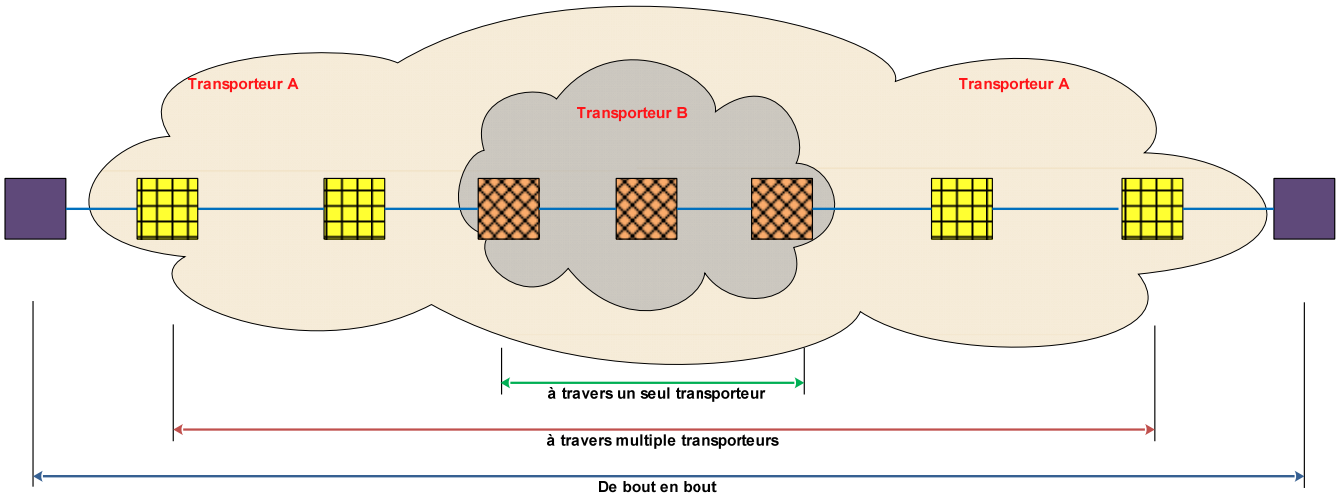
[1] PT: Payload Type.
[2] PM: Path Monitoring.
[3] TCM: Tandem Connection Monitoring.
[4] FTFL: Fault Type and Fault Location.
[5] GCC: General Communication Channel.
[6] APS: Automatic Protection Switching.
[7] PCC: Protection Communication Channel.



*** Figure 2-12. Le champ de l'entête **ODU** ***

L'entête de la surveillance du chemin (**PM**) occupe les colonnes 10, 11 et 12 de la troisième rangée (ligne). L'octet N°:10 porte l'identificateur de la trace de la piste, qui est utilisé pour identifier le signal de la source à la destination. L'octet N°:11 porte le résultat du **BIP**[1]-8, calculé sur l'ensemble de l'**OPU** et inséré deux trames plus tard.

L'entête de la surveillance de connexion en tandem (**TCM**) occupe colonnes de 5 à 13 de la deuxième rangée (ligne), et les colonnes de 1 à 9 de la troisième rangée (ligne). La fonctionnalité **TCM** permet à un opérateur de réseau de surveiller les performances d'erreur d'une connexion qui commence et se termine au sein de son propre réseau, mais qui traverse d'autres différents opérateurs. Un exemple d'un tel lien est illustré à la figure 2-13.

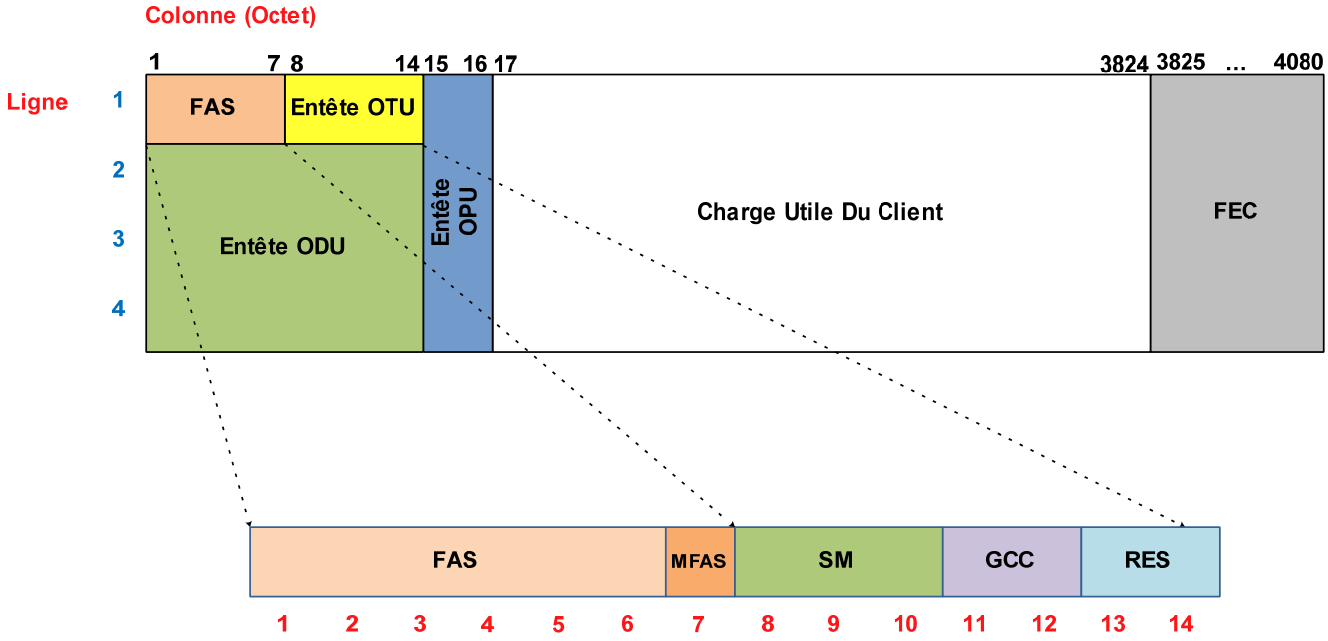


[1] BIP: Bit Interleaved Parity.

*** Figure 2-13. Un exemple de surveillance de réseau***

c. Les entêtes FAS et OTU

Le champ du signal d'alignement de trame (**FAS**[1]) est situé dans les colonnes de 1 à 7 de la première ligne, comme le montre la Figure 2-14. Le **FAS** est effectué dans les six premiers octets et est utilisé par l'équipement de réception pour indiquer le début de la trame de l'**OTU**. La valeur du **FAS** est la même que pour **SDH** (c'est-à-dire : $[F6F6F6282828]_{HEX}$), et elle est transmise sans cryptage. Certains entêtes sont transmis sur des trames **OTU** successives. Par exemple, comme nous l'avons vu ci-dessus, l'octet de l'identificateur de la structure de la charge utile (**PSI**) appartenant à l'entête **OPU** (situé sur la ligne 4 et la colonne 15) est utilisé pour transporter un message de 256 octets. Dans cette perspective, des groupes de trames **ODU** successives sont organisés logiquement en multi-trames. La position d'une trame **ODU** dans une multi-trame est indiquée par l'octet du signal d'alignement de multi-trames (**MFAS**[2]) situé à la ligne N°:1, colonne N°:7. La valeur de l'octet **MFAS** est incrémenté chaque trame, offrant ainsi une multi-trame composée de 256 trames. Il est transmis cryptés avec le reste de la trame **OTU**.



*** Figure 2-14 Les entêtes **FAS** et **OTU** ***

Dans la figure 2-14, les champs des entêtes **OTU** sont situés dans les colonnes de 8 à 14 de la première rangée. Ces champs offrent les fonctions de supervision pour la surveillance de la section et conditionnent le signal pour le transport entre les points de recalage, le remodelage et la régénération (3R) dans le réseau

[1] FAS: Frame Alignment Signal.
[2] MFAS: Multi-Frame Alignment Signal.

optique. Les champs suivants ont été définis: Section de la surveillance (**SM**[1]) et le canal de communication générale (**GCC**[2]).

Enfin, la correction d'erreurs (**FEC**) est effectuée dans les colonnes de 3825 à 4080 de tous les quatre rangs. Le code Reed-Solomon **RS** (255/239) est utilisé.

d. Les Signaux du client

Comme l'a été mentionné plus tôt, les types de trafic suivants peuvent être mappés sur la charge utile **OPU**:

• **SDH**: les flux de données **STM16**, **STM64**, et **STM256** sont mappés sur une charge utile **OPU** en utilisant une horloge générés localement ou une horloge provenant du signal **SDH**.

• les trames **IP** et les trames Ethernet: Ceci est fait en utilisant la procédure de trame générique (**GFP**[3]).

• Les cellules **ATM**: Un flux de cellules **ATM** à débit binaire constant avec une capacité identique à la charge utile de l'**OPU** est mappé en alignant les octets des cellules **ATM** aux octets de l'**OPU**. Une cellule peut chevaucher deux charges utiles OPU successives.

• Les signaux de test.

4. Architecture du plan de contrôle

Le plan de contrôle comprend des protocoles qui sont utilisés pour soutenir le plan de données, qui s'intéresse à la transmission de données. Les protocoles du plan de contrôle sont concernés par la signalisation, le routage et la gestion de réseau. La signalisation est utilisée pour configurer, maintenir et résilier les connexions. Les protocoles **ATM : Q.2931**[4] et **PNNI**[5], et les protocoles de distribution des étiquettes pour la mise en place des **LSP**[6] sont des exemples de protocoles de signalisation. Le routage est une partie importante du fonctionnement du réseau. Il est utilisé pour construire et maintenir des routes que les données devront les suivre afin d'atteindre une destination.

[1] SM: Section Monitoring.
[2] GCC : General Communication Channel.
[3] GFP: Generic Frame Procedure.
[4] Q.2931 : Protocole de signalisation utilisé pour configurer une **SVC** (Switched Virtual Connection).
[5] PNNI: (Private Network Node Interface Or Private Network-Network Interface) Protocole qui se consiste en deux composants : le protocole de signalisation **PNNI** et le protocole de routage **PNNI**. Le protocole de signalisation **PNNI** permet d'établir, de maintenir et de résilier dynamiquement les connexions **ATM** des interfaces des réseaux ou des interfaces des nœuds des réseaux privés. Le Protocole de routage **PNNI** est utilisé pour distribuer la topologie du réseau et les informations d'accessibilité entre les commutateurs (Switch) ou les groupes de commutateurs.
[6] LSP : Label Switched Path.

Enfin, la gestion du réseau s'intéresse par le contrôle du réseau afin de maximiser son efficacité et sa productivité. Modèle de l'**ISO**[1] divise la gestion du réseau en cinq catégories: gestion des pannes, la gestion de comptage, gestion de la configuration, gestion de la sécurité et la gestion de la performance.

Il existe essentiellement deux différentes architectures du plan de contrôle. Dans la première, l'utilisateur est isolé du réseau via une interface réseau utilisateur (**UNI**[2]). L'utilisateur n'a pas de connaissance sur la topologie du réseau, son plan de contrôle et de son plan de données. Les nœuds dans le réseau s'interagissent les uns avec les autres via une interface réseau-nœud (**NNI**[3]). Un bon exemple de cette architecture de plan de contrôle est le réseau **ATM**. Un utilisateur ne peut accéder au réseau **ATM** qu'au travers un **UNI ATM**, et les commutateurs **ATM** à l'intérieur d'un réseau **ATM** s'interagissent les uns avec les autres via un **NNI**, tel que **PNNI** dans le cas d'un réseau privé.

Dans la deuxième architecture du plan de contrôle, l'utilisateur n'est pas isolé du réseau par un **UNI**, et les nœuds à l'intérieur du réseau ne permettent pas de s'interagir les uns avec les autres via une **NNI** séparée. Plutôt, tous les utilisateurs et les nœuds exécutent le même ensemble de protocoles. Un bon exemple de cette architecture est le réseau **IP**.

Tous les deux architectures du plan de contrôle ont été utilisées pour élaborer différents des plans de contrôle pour les réseaux de routage des longueurs d'onde des. L'**OIF**, en suivant la première architecture du plan de contrôle, a proposé une interface réseau utilisateur **UNI**. Il fonctionne également sur une interface réseau-nœud **NNI**. L'**IETF** a proposé trois différents modèles de plan de contrôle pour la transmission du trafic **IP** sur un réseau optique, qui sont fondées sur les deux architectures de plan de contrôle précédemment décrites.

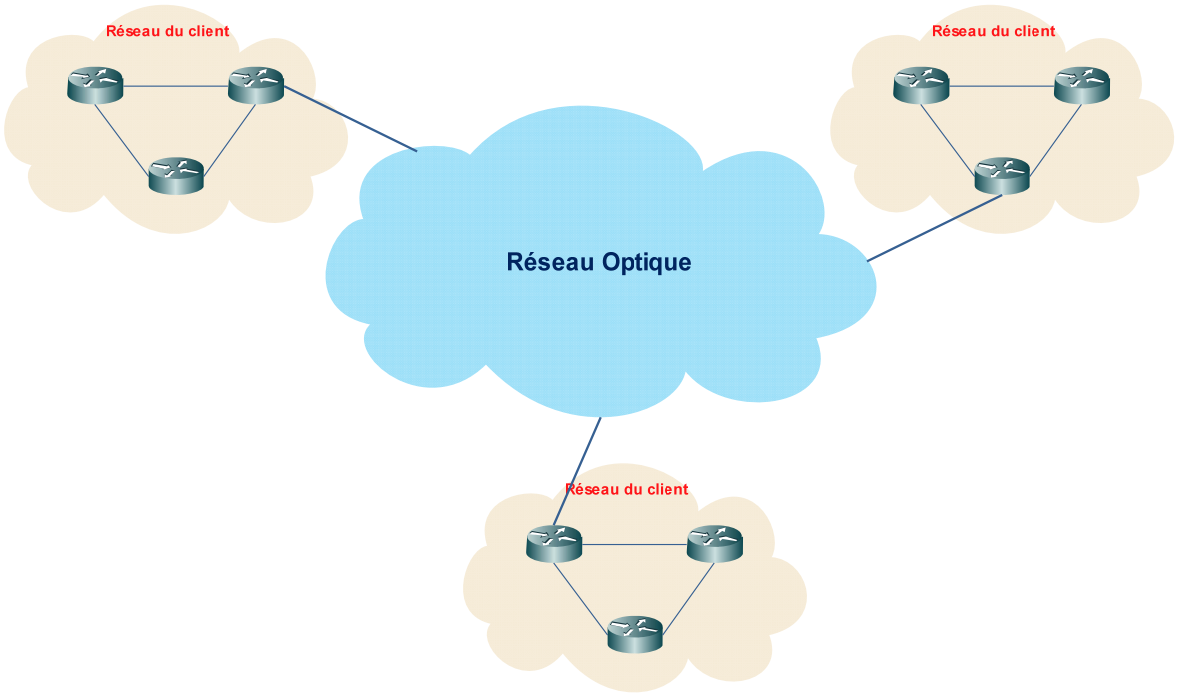
Un réseau optique permet l'interconnectivité aux réseaux de clients (voir la figure 2-15). Ces réseaux de clients pourraient être des réseaux de commutation de paquets, tels que **IP**, **ATM**, et le réseau Frame Relay ou des réseaux de commutation de circuits, tels que **SDH**.

Un vaste réseau optique sera typiquement constitué de petits sous-réseaux optiques interconnectés, chacun représentant un *domaine de contrôle* séparé. Chacun de ces petits réseaux pourrait être un système administratif différent.

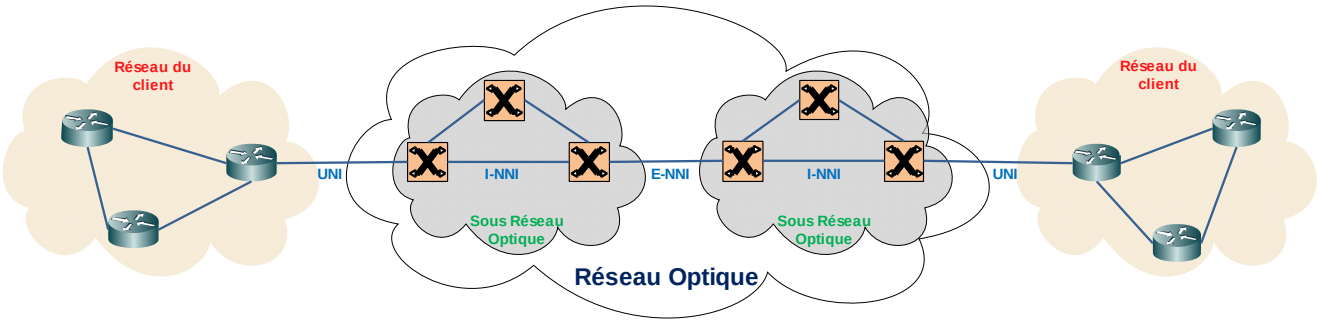
[1] ISO : International Organization of Standards.
[2] UNI: User Network Interface.
[3] NNI: Network-Node Interface.

Dans la première l'architecture du plan de contrôle, les trois interfaces suivantes ont été définies: l'interface réseau-utilisateur (**UNI**), interface réseau interne-nœud (**I-NNI**[1]), et l'interface réseau externe-nœud (**E-NNI**[2]). (Voir Figure 2-16.)

Comme mentionné ci-dessus, l'**OIF** a précisé un **UNI** qui prévoit des procédures de signalisation pour les clients afin de créer automatiquement une connexion, supprimer une connexion, et d'interroger l'état d'une connexion sur un réseau de routage de longueur d'onde optique. L'UNI est basé sur les protocoles de distribution d'étiquettes **LDP**[3] et **RSVP-TE**[4].



*** Figure 2-15. Réseaux de clients interconnectés à travers un réseau optique***



[1] I-NNI: Internal Network-Node Interface.
[2] E-NNI: External Network-Node Interface.
[3] LDP: Label Distribution Protocol.
[4] RSVP-TE: Resource Reservation Protocol – Traffic Engineering.

*** Figure 2-16. Les interfaces UNI, I-NNI et E-NNI ***

L'**IETF** a défini trois différents modèles de plan de contrôle: le modèle de l'égal (*The peer model*), le modèle de recouvrement (*The Overlay model*), et le modèle augmenté (*The augmented model*). Dans la discussion ci-dessous et dans la figure 2-15, on suppose que les réseaux des clients sont des réseaux **IP**. Le plan de données pour les réseaux est présenté comme un mélange de commutation de paquets et commutation de circuits. La commutation par paquets est utilisée dans les réseaux **IP**; la commutation de circuits est utilisée au sein du réseau optique, où un circuit est un chemin optique ou un canal à bas débit si groupage de trafic est utilisé.

Le modèle de l'égal utilise la deuxième architecture du plan de contrôle décrite ci-dessus. Autrement dit, les réseaux de clients et le réseau optique sont traités comme un réseau unique du point de vue du plan de contrôle. L'architecture du **MPLS** généralisé (**GMPLS**) est utilisée dans le plan de contrôle. Le **GMPLS** est une extension du **MPLS**. Les réseaux **IP** et les réseaux optiques exécutent le même protocole de routage **IP** : l'**OSPF**[1] avec extensions optiques appropriées. Par conséquent, tous les nœuds optiques et les routeurs **IP** maintiennent la même topologie et les informations d'état des liens. Un routeur **IP** calcule un **LSP** de bout en bout, qui est ensuite mis en place en utilisant les protocoles de distribution d'étiquettes CR-**LDP**[2] ou **RSVP-TE**, étendus convenablement pour le **GMPLS**.

Dans le modèle de recouvrement, le réseau optique utilise la première architecture du plan de contrôle décrit ci-dessus (voir aussi la figure 2-16). Un réseau **IP** du client est connecté au réseau optique à travers un routeur **IP** de périphérie qui a une interface optique à son nœud optique d'entrée, par exemple le nœud optique à lequel il est directement rattaché. Avant qu'un routeur **IP** de périphérie puisse transmettre sur le réseau optique, il doit demander une connexion à partir de son nœud optique d'entrée. Ceci est fait en utilisant un protocole de signalisation défini sur une **UNI**. Une connexion sur le réseau optique peut être un chemin optique (permanent ou commuté) ou un sous-canal. Le routeur de périphérique ne connait pas la topologie du réseau optique, ni de son contrôle et son plan de données. Le plan de contrôle du réseau optique peut être basé sur **GMPLS**. Cependant, l'**UNI** maintient une séparation stricte des réseaux de clients et le réseau optique.

Enfin, dans le modèle augmenté, les réseaux **IP** du client et le réseau optique utilisent des plans de contrôle séparés. Toutefois, les informations de routage d'un réseau passent à l'autre. Par exemple, les adresses **IP** d'un réseau **IP** du client peuvent être transportées par le réseau optique à un autre réseau **IP** du client pour permettre l'accessibilité. Le routage dans le réseau **IP** et le réseau optique est séparé, mais les deux

[1] OSPF: Open Short Path First.
[2] CR-LDP: Constraint Routing – Label Distribution Protocol.

réseaux utilisent le même protocole de routage. Le protocole routage d'interdomaine **IP**, le protocole **BGP**[1] peut être adapté pour l'échange d'informations entre domaines **IP** et optique.

5. MPLS Généralisé (GMPLS)

L'architecture du **MPLS** généralisé (**GMPLS**), est une extension du **MPLS**. **MPLS** a été conçu à l'origine d'introduire les chemins à commutation des étiquette dans le réseau **IP**, il est également applicable à l'**ATM**, Frame Relay et les réseaux basés sur Ethernet. L'architecture **GMPLS** a été conçue en vue de l'application des *techniques de commutation d'étiquettes* aux réseaux à *multiplexage temporel* (**TDM)** et les réseaux de routage de longueurs d'onde en plus des réseaux à commutation de paquets.

Un réseau **TDM** est un réseau de liens **SDH** interconnectés entre eux par des systèmes de brasseurs numériques (**DCS**). Un **DCS** termine le signal **SDH** sur chaque lien entrant, le convertit dans le domaine électrique, et commute ensuite le contenu de certains affluents virtuels aux différentes trames sortantes **SDH**. Il extrait aussi certains affluents virtuels, et en ajoute de nouveaux aux trames sortantes. Les trames sortantes sont ensuite transmises à travers des liaisons de sortie **SDH** de sortie de du commutateur. L'agrégation des charges utiles **SDH** à un plus haut niveau de **SDH** peut aussi être faite aux les liens de sortie. Une connexion de commutation de circuits à travers un tel réseau **SDH** peut être mise en place par l'attribution d'un ou plusieurs intervalles d'une trame **SDH** sur les liaisons qui forment le chemin d'accès. **GMPLS** peut être utilisé pour configurer les brasseurs numériques (**DCS**) de **SDH**, de manière à établir une connexion de commutation de circuits.

GMPLS peut également être utilisé pour configurer un chemin optique dans un réseau optique de routage de longueurs d'onde. En outre, il peut être utilisé pour configurer un brasseur optique (**OXC**) afin de commuter l'intégralité d'un signal optique d'une fibre d'entrée à une fibre de sortie.

En **GMPLS**, les routeurs **IP**, les commutateurs **ATM**, les commutateurs de Frame Relay, les commutateurs Ethernet, les brasseurs numériques (**DCS)** et les brasseurs optiques (**OXC)** sont tous traités comme un seul réseau **IP** du point de vue du contrôle. Il n'existe plus d'**UNI** et de **NNI**, puisque **GMPLS** est un protocole « peer-to-peer ».

GMPLS est une architecture et son implémentation nécessite un protocole de signalisation. Tous les deux protocoles **RSVP-TE** et **CR-LDP** ont été étendus la prise en charge de **GMPLS**.

Dans ce qui suit, on décrit les caractéristiques de base de l'architecture **GMPLS** et les extensions proposées pour **CR-LDP** et **RSVP-TE**.

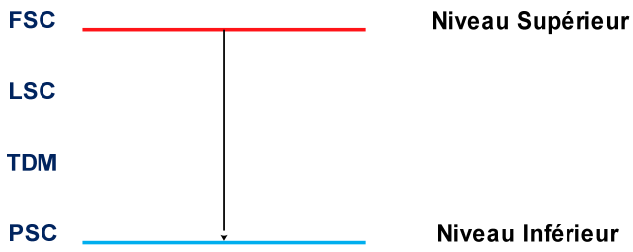
5.1. Caractéristiques de base de GMPLS

[1] BGP: Border Gateway Protocol.

Un **LSR**[1] à capacité **GMPLS** peut prendre en charge un ou plusieurs des interfaces suivantes:

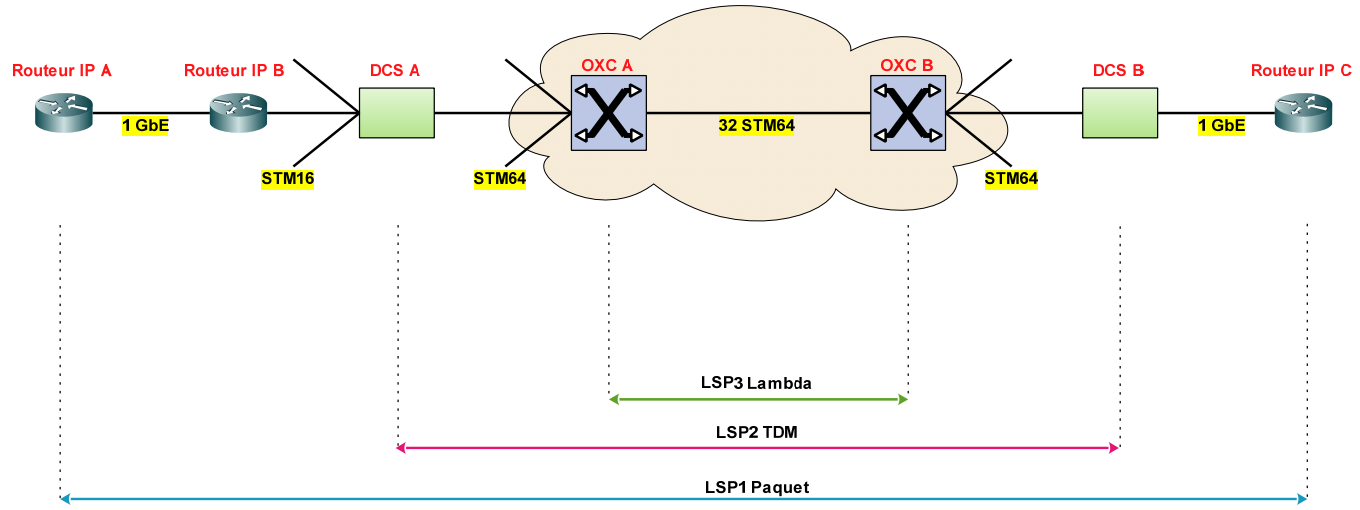
1. Les interfaces à capacité de commutation de paquets (**PSC**[2]): Ce sont les différentes interfaces utilisées pour recevoir et transmettre les paquets, comme les paquets **IP**, des cellules **ATM**, les trames Frame Relay, et des trames Ethernet. La transmission de ces paquets est basée sur: une étiquette encapsulée, le champ **VPI**[3]**/VCI**[4] de l'entête de la cellule **ATM**, ou le champ **DLCI**[5] de la trame du Frame Relay.
2. Les interfaces à capacité de multiplexage temporel (**TDM**): Ils transmettent les données fondées sur le(s) intervalles de temps des données dans une trame. Cette interface est utilisée dans un brasseur numérique (**DCS**) de **SDH**.
3. Les interfaces à capacité de commutation de longueurs d'onde «Lambde » (**LSC**[6]): ils transmettent les données d'une longueur d'onde entrante à une longueur d'onde sortante. Cette interface est utilisée dans les brasseurs optiques (**OXC**).
4. Les interfaces à capacité de commutation de fibres (**FSC**[7]): Ils transmettent les données d'un (ou plusieurs) fibres entrants à un (ou plusieurs) fibres de sortie. Ils sont utilisés dans un brasseur optique (**OXC**) qui peut fonctionner au niveau d'un (ou plusieurs) fibres.

Ces quatre interfaces sont ordonnées d'une façon hiérarchique (voir la figure 2-17). Au sommet de la hiérarchie est le **FSC**, suivie par le **LSC**, puis **TDM**, et enfin on trouve le **PSC**. Cet ordre des interfaces est utilisé par **GMPLS** pour soutenir les **LSP**[8] hiérarchiques. On considère un **LSP** qui commence et se termine à une interface de commutation de paquets. Ce **LSP** peut passer par plusieurs types de réseaux, où il peut être imbriqué avec d'autres **LSP** dans un **LSP** d'ordre supérieur. Ce dernier peut commencer et finir à une interface de commutation de paquets, une interface à division de temps, une interface de commutation de lambdas (longueurs d'onde), ou d'une interface de commutations de fibres. En général, l'imbrication des **LSP** dans un **LSP** d'ordre supérieur se fait suivant la hiérarchie de ces quatre interfaces (voir la figure 2-17).



*** Figure 2-17. Hiérarchie des quatre types d'interface ***

[1] LSR: Label Switching Router.
[2] PSC: Packet-Switching Capable.
[3] VPI: Virtual Path Identifier.
[4] VCI: Virtual Channel Identifier.
[5] DLCI: Data Link Connection Identifier.
[6] LSC: Lambda Switch Capable.
[7] FSC: Fiber Switch Capable.
[8] LSP: Label Switched Path.



*** Figure 2-18. Un exemple d'un **LSP** à structure hiérarchique ***

Un exemple d'un **LSP** à structure hiérarchique est illustré à la figure 2-18. On suppose qu'un certain nombre de routeurs **IP** sont connectés à un réseau **SDH**, qui à son tour est relié à un réseau Backbone de routage de longueurs d'onde. Le **LSP** commence au routeur **IP** A et se termine au routeur **IP** C. Comme on le voit, le routeur **IP** A est connecté au routeur **IP** B par une liaison de 1-GbE et routeur **IP** B est connecté à son tour à un brasseur numérique (**DCS**) à travers lien **SDH** de **STM16**. Le (**DCS**) A est connecté au brasseur optique (**OXC**) A par un lien **SDH** de **STM64**. Les deux brasseurs optiques (**OXC**) A et B font partie d'un réseau de routage de longueur d'onde, et sont reliés par une fibre unique qui possède 32 longueurs d'onde, chaque longueur d'onde portant un flux **SDH** dont le débit est de **STM64**. A l'autre côté du réseau optique de routage des longueurs d'onde, le brasseur optique (**OXC**) B est connecté au brasseur numérique (**DCS**) B via un lien **SDH** de **STM16**, et le (**DCS**) B est connecté au routeur **IP** C via une liaison 1-GbE.

Les interfaces sur le chemin du **LSP** à partir du routeur **IP** A jusqu'au routeur **IP** C peuvent être facilement déduites. Les liens 1-GbE entre les routeurs **IP** A et B, et entre le brasseur numérique (**DCS**) B et le routeur **IP** C ont des interfaces du niveau **PSC**. Les liens **SDH** entre le routeur **IP** B et le brasseur numérique (**DCS**) A, entre le (**DCS**) A et l'(**OXC**) A, et enfin entre l'(**OXC**) B et le (**DCS**) B ont des interfaces du niveau **TDM**. Finalement, le lien entre les deux brasseurs optiques (**OXC**) A et B a une interface **LSC**.

Lorsqu'on se dirige vers le réseau optique de routage des longueurs d'onde, la capacité de des liens augmente. (Ceci est indiqué dans la figure 2-18 en utilisant des lignes plus épaisses). A l'autre côté du réseau optique de routage des longueurs d'onde, les capacités des liens diminuent à mesure qu'on se dirige vers le bord. L'augmentation de la capacité du lien aussi qu'on se rapproche du réseau Backbone est normal, puisque les liens transportent plus de trafic que ceux à la périphérie du réseau.

Dans la figure 2-18, le **LSP** entre les routeurs **IP** A et C est étiqueté comme *LSP1 paquet*. Comme on le voit, ce **LSP** est imbriquée avec d'autres **LSP** dans le *LSP2 TDM*, qui à son tour est imbriqué dans le *LSP3 Lambda*. Lorsque le LSP1 est établi, le brasseur numérique (**DCS**) A essayera d'allouer la bande passante au sein de son *LSP2 TDM*. Si cela n'est pas possible, le (**DCS**) A mettra en place un nouveau *LSP2 TDM* vers le (**DCS**) B. Le nouveau *LSP2 TDM* sera imbriqué dans le chemin optique *LSP3 Lambda*, si la bande passante est disponible. Sinon, le brasseur optique (**OXC**) A essayera d'établir un chemin nouveau optique vers l'(**OXC**) B. Si le *LSP2* et le *LSP3* n'existent pas au moment où un routeur **IP** A tente d'établir le LSP1, alors la création du *LSP1* déclenchera le (**DCS**) A afin d'établir le *LSP2 TDM*, ensuite l'(**OXC**) A mettre en place *LSP3 Lambda*.

a. La demande de l'étiquette généralisée

La demande de l'étiquette généralisée est utilisée pour communiquer les caractéristiques requises pour soutenir la création d'un **LSP**. L'information exigée dans une demande de l'étiquette généralisée est illustré à la figure 2-19. Les champs suivants ont été définis:

*** Figure 2-19. L'information transportée dans une demande d'étiquette généralisée ***

- Type d'encodage du **LSP**: Ce champ de 8 bits indique comment les données à transmettre à travers le LSP devront être encodées. Les valeurs suivantes ont été définies:

Valeur	Type
1	Packet
2	Ethernet V2/DIX
3	ANSI PDH
4	ETSI PDH
5	SDH ITU-T G.707
6	SONET ANSI T1.105
7	Digital Wrapper
8	Lambda (Photonic)
9	Fiber
10	Ethernet 802.3
11	Fiber Channel

- Type de commutation: Un champ de 8 bits utilisé pour indiquer le type de la commutation qui doit être effectuée sur un lien particulier. Ce champ est utilisé sur les liens qui annoncent plus qu'un type de capacité de commutation.

• Identifiant de la charge utile généralisé (**G-PID**[1]): Un champ de 16 bits utilisé pour identifier la charge utile transportée par un **LSP**. Il est utilisé par les extrémités du **LSP**. Ce qui suit sont quelques-unes des valeurs spécifiées:

[1] G-PID: Generalized Payload Identifier.

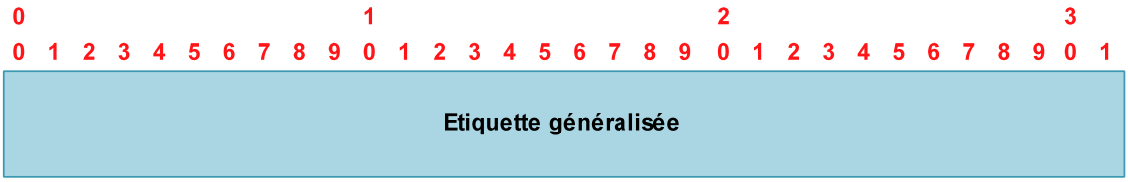
Valeur	Type	Technologie
0	Inconnu	Tous
14	Byte synchronous mapping of E1	SONET / SDH
17	Bit synchronous mapping of DS1 / T1	SONET / SDH
28	PoS – No Scrambling, 16 bit CRC	SONET / SDH
32	ATM mapping	SONET / SDH
33	Ethernet	Lambda, Fibre
34	SDH	Lambda, Fibre
35	SONET	Lambda, Fibre
36	Digital Wrapper	Lambda, Fibre
37	Lambda	Fibre

b. L'étiquette généralisée

Depuis que le champ d'application de **MPLS** a été élargi dans le domaine optique et le domaine **TDM**, plusieurs nouvelles formes d'étiquettes sont exigées. L'étiquette généralisée ne tient pas compte seulement de l'étiquette du type **MPLS** qui se déplace dans la bande avec le paquet associé, mais permet aussi des étiquettes qui identifient les intervalles de temps, des longueurs d'onde, ou une fibre. Ces nouvelles formes d'étiquettes, qui sont collectivement connues sous le nom de l'étiquette généralisée, peuvent porter une étiquette qui représente:

- Etiquette **MPLS** générique, étiquette Frame Relay, étiquette **ATM**.
- Un ensemble d'intervalles de temps dans une trame **SDH**.
- Une seule longueur d'onde dans une bande de fréquence ou dans une fibre.
- Une seule bande de fréquence dans une fibre.
- Une seule fibre dans un faisceau.

Puisque le nœud, à l'aide de **GMPLS,** connaît le type de lien utilisé, l'étiquette généralisée ne contient pas un champ de type. L'étiquette généralisée n'est pas hiérarchique. Lorsque multiples niveaux d'étiquettes sont requis, chaque **LSP** doit être établi séparément. L'information portée sur l'étiquette généralisée est illustré à la figure 2-20. L'interprétation du champ d'étiquettes dépend du type du lien sur lequel l'étiquette est utilisée.



*** Figure 2-20. L'information transmise dans l'étiquette généralisée. ***

c. L'étiquette suggérée

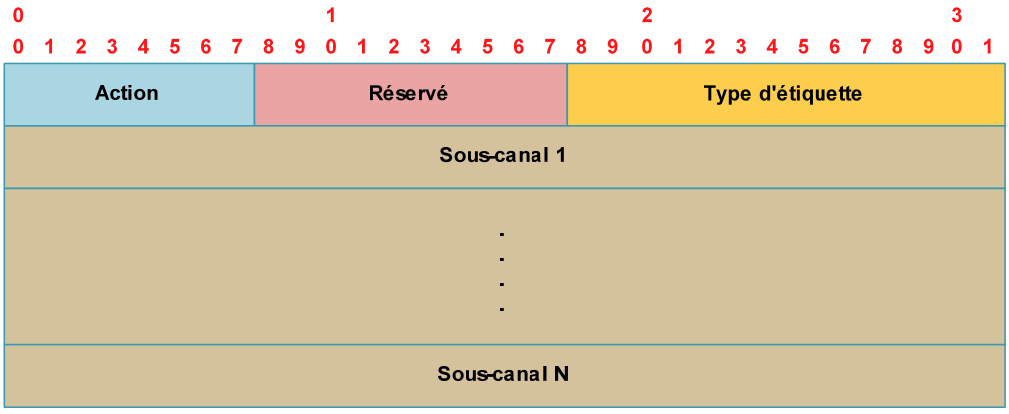
GMPLS permet l'utilisation d'une étiquette suggérée. Cette étiquette est utilisée pour fournir un nœud en sens descendant avec une préférence de l'étiquette du nœud en sens montant. Ceci permet au nœud en sens montant de commencer à configurer son matériel avec l'étiquette suggérée (proposée) avant que l'étiquette est communiquée par le nœud en sens descendant. C'est une option utile, si le temps de configuration n'est pas sans importance. Une étiquette suggérée peut être sur-infestée par le nœud en sens descendant. Le format d'étiquette suggérée est le même que le format d'étiquette généralisée.

d. L'ensemble d'étiquettes

L'ensemble d'étiquettes est utilisé pour limiter le choix d'étiquettes d'un nœud en sens descendant à un ensemble d'étiquettes acceptables. Le récepteur de l'ensemble d'étiquettes doit restreindre son choix d'étiquettes en fonction de l'ensemble d'étiquettes. Un ensemble d'étiquettes pourraient être présents sur de nombreux sauts, dans ce cas, chaque nœud génère son propre ensemble d'étiquettes peut-être sur la base de l'ensemble entrant d'étiquette et les capacités matérielles du nœud.

Un ensemble d'étiquettes est utile dans le domaine optique dans les quatre cas suivants:

- 1er Cas: L'équipement d'extrémité est seulement capable de transmettre ou de recevoir sur un petit ensemble de longueurs d'onde spécifiques.
- 2ème Cas: Il ya une séquence d'interfaces qui ne peuvent pas supporter la conversion de longueur d'onde, et exigent la même longueur d'onde à utiliser sur une séquence de sauts ou même sur l'intégralité du chemin.
- 3ème Cas: Limiter le nombre de conversions de longueur d'onde le long du chemin.
- 4ème Cas: Les deux extrémités d'un lien supportent différents ensemble de longueurs d'onde.



*** Figure 2-21. L'information véhiculée dans un ensemble d'étiquettes ***

L'information véhiculée dans un ensemble d'étiquettes est illustré à la figure 2-21. Un ensemble d'étiquettes se compose d'un ou plusieurs éléments de l'ensemble d'étiquettes. Chaque élément est appelé

un « sous-canal », et a le même format que l'étiquette généralisée. Les champs suivants ont été définis outre que le sous-canal:

- Action: C'est un champ de 8 bits qui indique la façon dont l'ensemble d'étiquettes doit être interprété. Les valeurs suivantes ont été définies:
  - *Liste incluse* (valeur fixée à 0): Indique que l'ensemble d'étiquettes contient un ou plusieurs éléments « sous-canal », qui devraient être inclus dans l'ensemble d'étiquettes.
  - *Liste exclusive* (valeur fixée à 1): Indique que l'ensemble d'étiquettes contient un ou plusieurs éléments « sous-canal », qui devraient être exclus de l'ensemble d'étiquettes.
  - *Gamme incluse* (valeur fixée à 2): Indique que l'ensemble d'étiquettes contient une gamme d'étiquettes. L'objet/**TLV** contient deux éléments « sous-canal »: le premier indique le début de la gamme, et le second indique la fin de la gamme. Une valeur de 0 indique qu'il n'y a pas de limite sur la partie correspondante de la gamme.
  - *Gamme Exclusive* (valeur fixée à 3): Indique que l'ensemble d'étiquettes contient une gamme d'étiquettes qui devrait être exclue de l'ensemble d'étiquettes. Comme ci-dessus, l'objet/**TLV**[1] contient deux éléments « sous-canal »: le premier indique le début de la gamme, et le second indique la fin de la gamme. Une valeur de 0 indique qu'il n'y a pas de limite sur la partie correspondante de la gamme.
- Type de l'étiquette: Un champ de 14 bits qui est utilisé pour indiquer le type et le format des étiquettes qui sont effectuées dans l'objet/**TLV**.

e. Les LSP bidirectionnels

En **MPLS**, un **LSP** bidirectionnel est établie par la configuration de deux **LSP** unidirectionnel séparément. **GMPLS**, contrairement à **MPLS**, supporte la création d'un **LSP** bidirectionnel. C'est-à-dire, les deux directions du **LSP** sont établies en utilisant un seul ensemble de messages de signalisation.

Pour un LSP bidirectionnel, deux étiquettes doivent être allouées sur le même saut. La configuration bidirectionnelle est indiquée par la présence d'une étiquette d'objet/**TLV** en sens montant dans le message de signalisation approprié. Une étiquette en sens montant a le même format que l'étiquette généralisée précédemment.

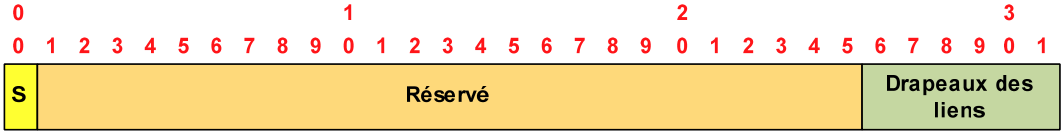
f. L'information de la protection

L'information de la protection est utilisée pour indiquer le type de protection souhaitée: [Protection dédiée 1+1, Protection dédiée 1:1, Protection commune 1:N, ou non protégé] par le **LSP** requis sur un lien.

[1] TLV: Type Length Value.

L'information de la protection indique également si le **LSP** est un **LSP** primaire ou un **LSP** secondaire. Il est supposé que les capacités de protection de chaque lien sont connues parmi les notifications de routage.

L'information requise dans l'information de protection est représenté sur la Figure 2-22. Les champs suivants ont été définis:



*** Figure 2-22. L'information Requise dans l'information de la protection***

- Secondaire (S): Un champ de 1 bit qui est utilisé pour indiquer que le **LSP** requis est un **LSP** secondaire.
- Réservés: Un champ de 25 bits réservés, mis tous à 0.
- Drapeaux des liens: Ce champ de 6 bits indique le type de protection souhaitée sur un lien. Les drapeaux suivants ont été définis:
  - *Protection améliorée:* Indique qu'un régime de protection plus fiable que la protection dédié 1+1 doit être utilisé (à savoir, **4F-BLSR**).
  - *Protection dédiée 1+1:* Indique qu'un régime de protection 1+1 doit être utilisé.
  - *Protection dédiée 1:1:* Indique qu'un régime de protection 1:1 doit être utilisé.
  - Protection partagée: Il indique que le régime de protection commune 1:N doit être utilisé.
  - *Non protégé*: Aucune protection n'est nécessaire.
  - *Trafic supplémentaire*: Indique que le **LSP** requis devrait utiliser les liens qui protègent d'autres **LSP** primaire. Le **LSP** requis peut être préempté si les liens portants le **LSP** primaire échouent.

g. Les extensions CR-LDP et RSVP-TE pour GMPLS

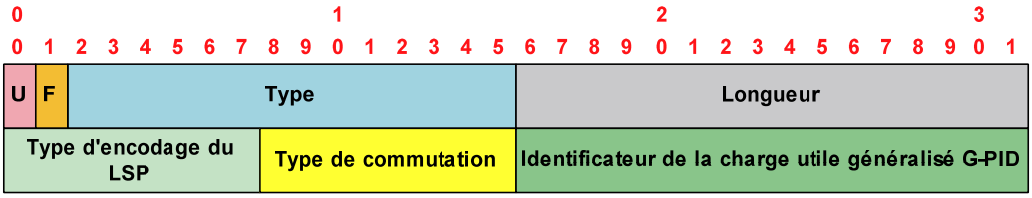
GMPLS est une architecture, et comme dans le cas de la technologie **MPLS**, elle nécessite un protocole de signalisation pour la distribution fiable des agglutinations d'étiquettes. Tous les deux protocoles **CR-LDP**[1] et **RSVP-TE**[2] ont été étendues pour supporter le **GMPLS**. **IS-IS**[3] et **OSPF**[4] ont également été étendus pour supporter **GMPLS**.

5.2. Extensions CR-LDP pour GMPLS

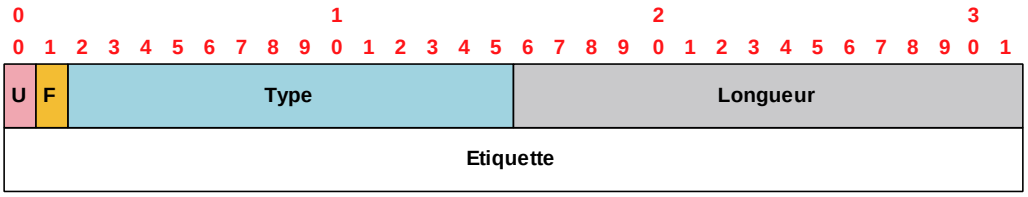
De nouveaux **TLV** ont été introduites dans **CR-LDP** pour soutenir l'opération d'étiquetage généralisé. Plus précisément, la demande d'étiquette généralisée **TLV** est illustré à la figure 2-23, l'étiquette généralisée

[1] CR-LDP : Constraint Routing - Label Distribution Protocol.
[2] RSVP-TE : Ressource Reservation Protocol – Traffic Engineering.
[3] IS-IS :
[4] OSPF : Open Shortest Path First.

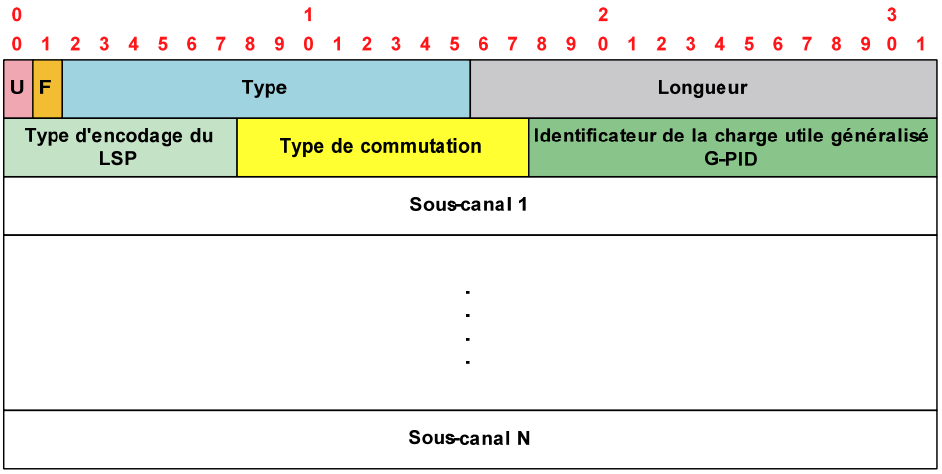
TLV est illustré à la figure 2-24, l'étiquette suggérée **TLV** est la même que l'étiquette généralisée **TLV**, et l'ensemble d'étiquettes **TLV** est illustré à la figure 2-25.



*** Figure 2-23. Demande de l'étiquette généralisée **TLV** en **CR-LDP***



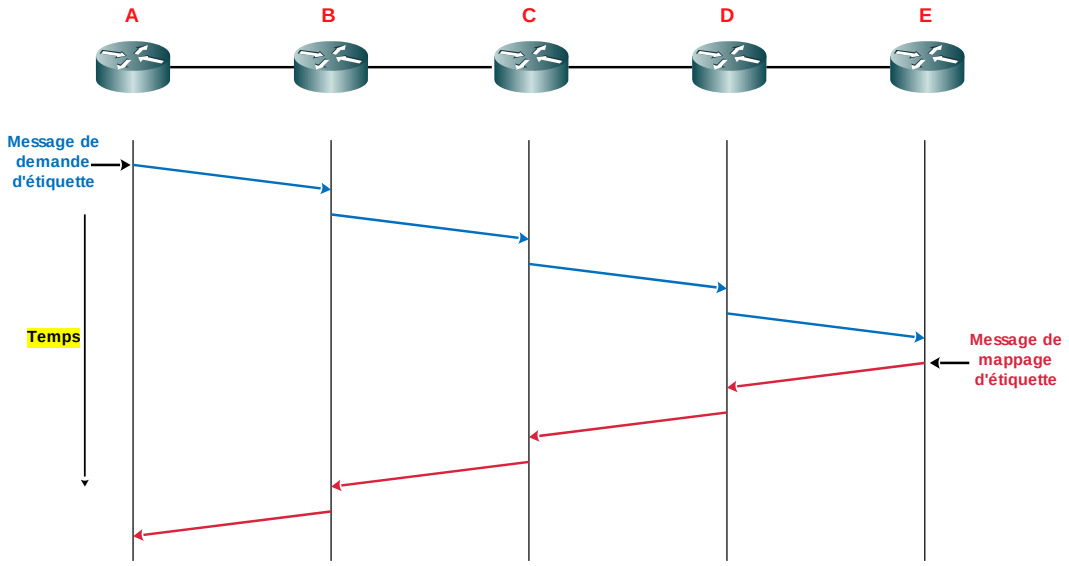
*** Figure 2-24. L'étiquette généralisée **TLV** en **CR-LDP***



*** Figure 2-25. L'ensemble d'étiquettes en **CR-LDP***

Le processus d'établissement d'un **LSP** bidirectionnel est le même que celui utilisé pour établir un **LSP** unidirectionnel avec quelques ajouts. Un **LSP** unidirectionnel, à partir du **LSR**[1] A jusqu'au **LSR** E, est configuré. Ceci est fait en utilisant un message de demande d'étiquette dans le sens descendant (en aval) (du **LSR** A au **LSR** E), et un message de mappage d'étiquette dans le sens montant (du **LSR** E au **LSR** A). Les étiquettes pour le **LSP** unidirectionnel du **LSR** A au **LSR** E sont mis en place aussi que le message de mappage d'étiquette voyage en sens montant (en amont). C'est parce que, un **CR-LSP**[2] est mis en place en utilisant le sens descendant à la demande avec le contrôle commandé. Pour supporter un **LSP** bidirectionnel une étiquette en sens montant est ajoutée au message de demande d'étiquette.

[1] LSR: Label Switching Router.
[2] CR-LSP: Constraint Routing- Label Switched Path.

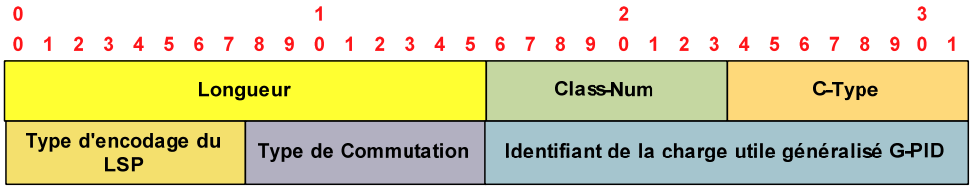


*** Figure 2-26. L'établissement d'un **CR-LDP** ***

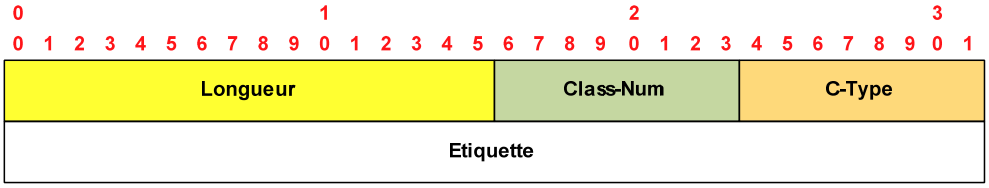
Un nœud de réception fournit une nouvelle étiquette en sens montant (en amont) et en transmet ensuite le message de demande au nœud suivant en sens descendant (en aval). De cette manière, lorsque le message de demande se propage vers la destination **LSR** E, des étiquettes pour le chemin [**LSR** E - **LSR** A] sont mises en place. Les étiquettes pour le chemin [**LSR** A - **LSR** E] sont mis en place aussi que le message de mappage se propage vers le **LSR** A.

5.3. Extensions RSVP-TE Pour GMPLS

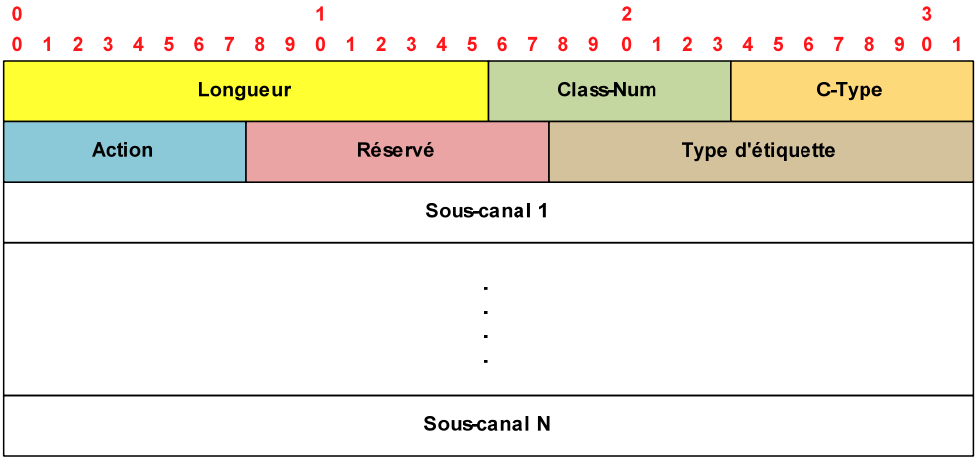
Comme dans le cas de **CR-LDP**, de nouveaux objets ont été introduits dans le **RSVP-TE** pour soutenir l'opération d'étiquetage généralisé. L'objet de la demande de l'étiquette généralisée et l'objet d'étiquette suggérée ou proposée (qui sont les mêmes) sont présentés dans la figure 2-27; l'objet d'étiquette généralisée est illustré à la figure 2-28, et l'objet de l'ensemble d'étiquette est illustré à la figure 2-29.



*** Figure 2-27. L'objet de la demande de l'étiquette généralisée en **RSVP-TE** ***



*** Figure 2-28. L'objet de l'étiquette généralisée en **RSVP-TE** ***



*** Figure 2-29. L'objet de l'ensemble d'étiquettes en **RSVP-TE** ***

Les **LSP** bidirectionnels sont installés en utilisant le même processus de l'établissement d'un **LSP** unidirectionnel avec quelques ajouts. Une étiquette en sens descendant (en amont) est ajoutée au message du chemin (*Path message*), qui permet l'attribution d'étiquettes le long du chemin à partir du **LSR** destination vers le **LSR** source. Les étiquettes le long du chemin à partir du **LSR** destination vers le **LSR** source sont attribuées comme dans le **LSP** unidirectionnelle en utilisant le message Resv (*Resv message*).

6. L'interface UNI proposée par l'OIF

L'interface **UNI** proposée ou définit par l'**OIF** précise des procédures de signalisation pour les clients afin d'assurer d'une façon automatique la création d'une connexion, la suppression d'une connexion, et d'interroger le statut d'une connexion sur un réseau de routage de longueur d'onde. La signalisation **UNI** a été implémentée par l'extension des protocoles de distribution d'étiquettes **LDP** et **RSVP**. Elle utilise également des extensions du protocole **LMP**[1]. Le client est un équipement de commutation de paquets, tel qu'un routeur **IP** et un commutateur **ATM**, ou brasseur numérique **SDH** qui est connecté au réseau optique. Le côté client de l'interface **UNI** de l'**OIF** est connu sous le nom d'**UNI-C** et le côté réseau optique est connu sous le nom d'**UNI-N**.

Un lien **SDH** est utilisé pour la transmission de données entre un client et son nœud optique d'entrée, connu sous le nom de l'élément terminal de réseau (**TNE**[2]). Le taux de transmission du lien **SDH** lien peut être jusqu'à STM256.

Les messages de signalisation de l'**UNI** entre l'**UNI-C** et l'**UNI-N** sont transportés dans des paquets **IP**, sur le canal de contrôle **IP** (**IPCC**[3]). Cette chaîne peut être dans la fibre ou en dehors de la fibre. L'**IPCC** dans la fibre est transmise sur un canal qui est intégré dans le lien SDH utilisé pour la transmission de données. Ce canal est

[1] LMP: Link Management Protocol.
[2] TNE: Terminal Network Element.
[3] IPCC: IP Control Channel.

formé des octets de D1 à D12 de la section d'entête de la trame **SDH**. L'**IPCC** en dehors de la fibre est séparée du lien de données **SDH**, et peut être une liaison Ethernet entre le **UNI-C** et **UNI-N** ou sur un réseau **IP** (voir la figure 2-30).

*** Figure 2-30. L'**IPCC** en dehors de la fibre ***

Comme mentionné ci-dessus, l'**UNI** isole les clients du réseau optique. Dans cette perspective, la topologie, les ressources et l'adressage du réseau optique ne sont pas révélés aux clients. Le réseau optique peut utiliser des adresses internes pour le routage interne, le provisionnement et la gestion du réseau. En outre, les clients peuvent utiliser leurs propres adresses. Compte tenu de ces deux ensembles d'adresses, une adresse du réseau de transport administratif (**TNA**[1]) est utilisée par l'**UNI** pour identifier l'adresse d'un client. L'adresse **TNA** est une adresse unique définie au niveau mondial, elle est distincte de l'espace d'adressage natif à la fois des clients et du réseau. Pour maintenir la compatibilité avec les périphériques réseau qui utilisent différents types d'adressage, la **TNA** peut être sous la forme d'**IPv4**, **IPv6**, et **NSAP**[2]. L'**UNI** permet une connexion entre deux adresses de type **TNA**.

Les principaux services offerts à un client par l'**UNI** sont la possibilité de créer et supprimer des connexions sur le réseau optique à la demande. En outre, la découverte du voisinage réseau et la découverte du service peuvent être offerts en option. Les procédures de découverte de voisinage permettent à un **TNE** et un dispositif client y directement attaché de déterminer et d'identifier l'un l'autre, sans passer par la configuration manuelle nécessaire des **UNI-C** et **UNI-N** correspondants. La découverte de service est un processus par lequel un dispositif client obtient des informations sur les services disponibles sur le réseau optique.

6.1. Les messages abstraits de l'UNI

L'**OIF** a défini un certain nombre de messages abstraits pour être utilisé sur l'**UNI**. L'implémentation effective de ces messages dépend de quel protocole est utilisée **LDP** ou **RSVP**. Ces messages sont utilisés pour

[1] TNA: Transport Network Administrative.
[2] NSAP: Network Service Access Point.

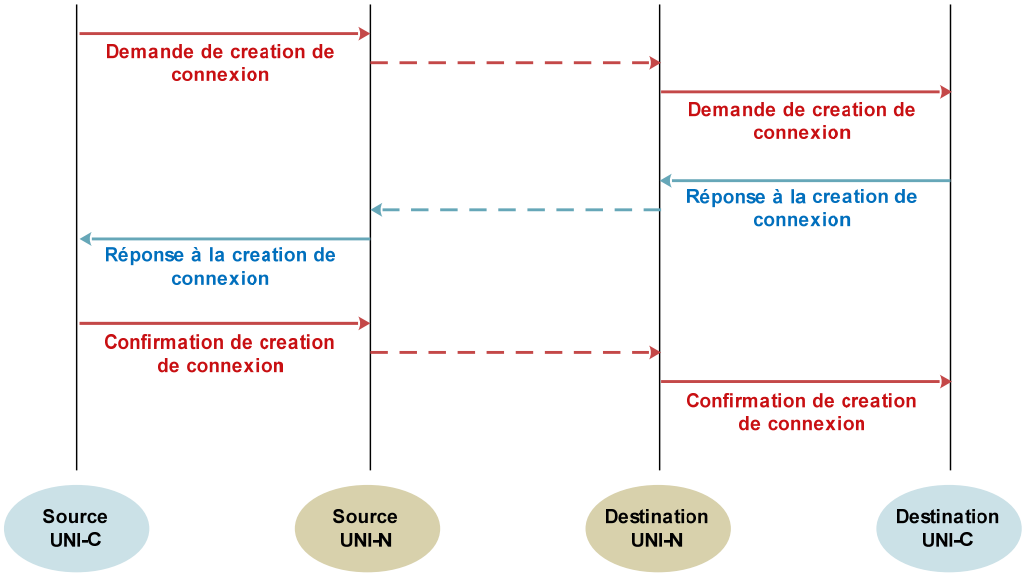
créer une connexion, supprimer une connexion, et interroger le statut d'une connexion établie sur l'**UNI**. On rappelle que la connexion est une route optique ou un canal de basse vitesse d'un chemin optique. Du point de vue de l'**UNI**, une connexion est un circuit dont la largeur de bande a une taille fixe entre un nœud optique d'entrée et un nœud optique de sortie avec une trame spécifiée. En ce moment, seul le tramage **SDH** est utilisé. Une connexion peut être unidirectionnelle ou bidirectionnelle.

Les messages abstraits suivants ont été définis:

- Demande de création d'une connexion (*Connection create request*): envoyé par la source **UNI-C** à son nœud d'entrée **UNI-N** afin de demander l'établissement d'une connexion. Il est également envoyé nœud de sortie **UNI-N** vers la destination **UNI-C** pour indiquer une demande de connexion entrante.
- Réponse de création d'une connexion (*Connection create response*): Sert à informer la source **UNI-C** (c'est-à-dire qui a initié la demande de connexion) de l'établissement de la connexion. Il est envoyé à partir de la destination **UNI-C** à la destination **UNI-N**, et de la source **UNI-N** à la source **UNI-C**, ensuite ils peuvent débuter la transmission des données à la réception de ce message.
- Confirmation de création d'une connexion (*Connection create confirmation*): Employée par la source **UNI-C** à la source **UNI-N** afin de confirmer l'exécution de l'établissement de la connexion. Il est également utilisé par la destination **UNI-N** vers la destination **UNI-C** pour indiquer que la connexion a été établie avec succès.
- Demande de suppression d'une connexion (*Connection delete request*): est utilisée pour initialiser la suppression d'un lien, il peut être envoyé par à n'importe quel **UNI-C**. Il peut également être envoyé par le réseau en cas de défaillance interne.
- Réponse de suppression d'une connexion (*Connection delete response*): est utilisé pour signaler l'achèvement de la suppression d'une procédure de connexion.
- Demande de l'état d'une connexion (*Connection Status enquery*): Ce message est utilisé pour en savoir davantage sur l'état et les attributs d'une connexion.
- Réponse de l'état d'une connexion (Connection Status response): Permet de retourner l'état de la connexion spécifiée et ses attributs.
- Notification: Utilisé par un **UNI-N** à n'importe quel **UNI-C** pour indiquer un changement de statut de la connexion.

La figure 2-31 montre les messages impliqués durant l'établissement d'une connexion. Comme on le voit, la source **UNI-C** envoie une demande d'établissement d'une connexion à son **UNI-N** d'entrée. Cette demande est propagée à la destination **UNI-N** de sortie, qui l'envoie à son tour à la destination **UNI-C**. Une réponse d'acceptation de création de la connexion est envoyée par la destination **UNI-C** à son correspondant

UNI-N. Ce message se propage ensuite vers la source **UNI-N**, qui l'envoie à la source **UNI-C**. La confirmation de la connexion vient par la suite (voir la figure 2-31).



*** Figure 2-31. Etablissement d'une connexion avec succès***

Chaque message a un certain nombre d'attributs obligatoires et facultatifs. Ces attributs sont organisés dans les catégories logiques suivantes:

- Les attributs liés à l'identification: il s'agit notamment: les adresses **TNA** de la source et de la destination, le client ou le numéro de port **TNA** utilisé pour la connexion, une étiquette généralisée et un **ID** de connexion locale, ces attributs sont utilisés dans tous les messages afin d'identifier à quel connexion ils s'appliquent. L'**ID** de connexion locale est attribué par la source **UNI-C** et, comme son nom l'indique, a une signification locale. C'est-à-dire, il est uniquement valable entre l'**UNI-C** et l'**UNI-N** d'entrée. Un identifiant de connexion similaire est utilisé entre l'**UNI-N** et l'**UNI-C** de sortie.
- Les attributs liés au service: Ce sont: le type de l'encodage; les paramètres de trafic **SONET/SDH**; la directionnalité; un identifiant de la charge utile généralisé et le niveau de service. Le type de l'encodage indique si le format est **SONET** ou **SDH**. Les paramètres de trafic **SONET/SDH** fournissent des informations concernant le type du signal et la manière dont les données ont été concaténées. L'attribut directionnalité indique si la connexion est unidirectionnelle ou bidirectionnelle. L'identificateur de la charge utile généralisé indique la charge utile transportée dans la connexion établie. Enfin, l'attribut de niveau de service indique une classe de service **CoS**. Un opérateur peut préciser une gamme de différentes classes de service, tels que l'or, de bronze et d'argent. Puisque le réseau optique est un réseau de commutation de circuits, ces classes de service **CoS** ne sont pas liées aux paramètres **QoS** familiers dans les réseaux de commutation de paquets, tels que la perte de paquets et le retard de bout

en bout. Plutôt, ils se reportent à des questions telles que le régime de restauration nécessaires (par exemple : pas de restauration, protection 1+1, etc.) et la configuration de la connexion.

- Les attributs liés au routage: Le seul attribut défini, c'est la diversité. Cet attribut peut être utilisé quand une nouvelle connexion est en cours de création, afin d'indiquer la diversité d'une nouvelle connexion avec une liste de n connexions existantes qui commencent au même **UNI-C**. L'attribut contient n éléments sous la forme {Type de diversité, **ID** connexion locale}, où l'**ID** de connexion locale indique l'un des n connexions existantes qui commencent au même **UNI-C**. Les types de diversité suivants sont possibles:
    - Diversité du nœud: La nouvelle connexion ne doit pas utiliser tous les nœuds du réseau qui sont dans le chemin de la connexion désigné par l'**ID** de connexion locale.
    - Diversité de lien: La nouvelle connexion ne doit pas utiliser tous les liens du réseau qui sont dans le chemin de la connexion désigné par l'**ID** de connexion locale.
    - Diversité de **SRLG**[1]: La nouvelle connexion ne doit pas utiliser tous les liens de réseau qui ont le même **SRLG** que ceux du chemin de la connexion désigné par l'**ID** de connexion locale.
    - Chemin partagé: La nouvelle connexion doit utiliser les mêmes liens du réseau que ceux utilisés par la connexion désigné par l'**ID** de connexion locale.
- Les attributs liés à la politique: Le seul attribut défini est l'identificateur de contrat (*contract ID*), qui est attribué par le prestataire de services et configuré dans les clients.

A titre d'exemple, les attributs suivant obligatoire et en option sont utilisés pour la demande de création d'une connexion:

- Source TNA (Obligatoire)
- Identifiant du port logique à la source (Obligatoire)
- Etiquette généralisée à la source (Option)
- Adresse TNA à la destination (Obligatoire)
- Identifiant du port logique à la destination (Option)
- Etiquette généralisée à la destination (Option)
- **ID** de connexion locale (Obligatoire)
- **ID** de Contrat (Option)
- Type de l'encodage (Obligatoire)
- Paramètres de trafic **SONET / SDH** (Obligatoire)
- Directionalité (Option)
- Identifiant de la charge utile généralisée (Option)

[1] SRLG: Shared Risk Link Group.

- Niveau de service (Option)
- La diversité (Option)

La signalisation **UNI** a été mis en œuvre par l'extension des protocoles de distribution d'étiquettes **LDP**[1] et **RSVP**[2]. Ci-dessous, nous décrivons les extensions **LDP** et **RSVP**.

6.2. Extensions LDP pour la signalisation UNI

Deux principes directeurs ont été utilisés lors de l'extension du **LDP**; limiter l'introduction de nouveaux messages **LDP** et les extensions **LDP** devraient être facilement implémentées en tant que des ajouts (additions) simples sur les implémentations **LDP** existantes sans violer la sémantique **LDP**. En conséquence, seuls deux nouveaux messages (un message de demande à l'état et un message de réponse d'état) ont été introduits. Les codages des **TLV** généraux pour **LDP** et **CR-LDP** sont également utilisés dans la signalisation de l'**UNI** proposé par l'**OIF**. En outre, les nouveaux **TLV** ont été introduits pour porter les attributs définis dans la norme **UNI**.

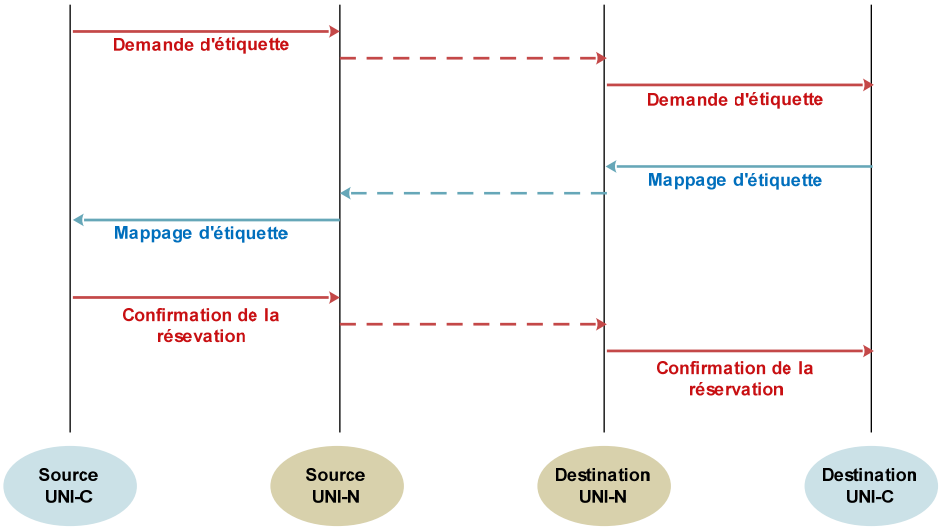
- **Initialisation de la session LDP**

Une seule session **LDP** est établie entre l'**UNI-C** et l'**UNI-N**, quel que soit le nombre de liaisons de données entre le client et le **TNE**.

- **Etablissement de connexion**

La demande de création de connexion est mise en œuvre en utilisant le message de demande d'étiquette. Ce message est envoyé à partir de la source d'**UNI-C** à la source d'**UNI-N**. À l'autre extrémité, le message de demande de label est envoyé par la destination **UNI-N** vers la destination **UNI-C**. La destination **UNI-C** répond à la destination **UNI-N** avec un message de mappage d'étiquette, qui, à l'autre extrémité, il est envoyé à partir de la source d'**UNI-N** à la source **UNI-C**. La destination **UNI-C** peut indiquer dans son message de mappage d'étiquette qu'une confirmation de réservation est nécessaire. Dans ce cas, une confirmation de réservation est envoyée par la source **UNI-C** à la source d'**UNI-N**, et de la destination **UNI-N** vers la destination **UNI-C**, comme l'indique la Figure 2-32. Le message de confirmation de réservation est implémenté en utilisant le message **LDP** de notification avec le code de statut défini sur «confirmation de réservation".

[1] LDP : Label Distribution Protocol.
[2] RSVP : Resource Reservation Protocol.



*** Figure 2-32. Etablissement d'une connexion avec succès en utilisant **LDP** ***

Une demande de création de connexion spécifie habituellement une connexion bidirectionnelle. La réception du message de demande d'étiquette par la destination **UNI-C** signifie que les ressources nécessaires pour établir la connexion avec les attributs spécifiés sont disponibles dans le réseau. Cependant, ceci n'implique pas que la connexion est disponible pour la transmission de données. Plus précisément, la configuration des brasseurs intermédiaires peut-être pas encore faite. Ce processus commence lorsque la destination **UNI-C** envoie un message de mappage d'étiquette en réponse au message de demande étiquette.

Le message de création de connexion peut échouer pour un certain nombre de raisons, comme l'absence de bande passante disponible, la violation de **SLA**[1], et le rejet de la connexion par destination **UNI-C**. Dans ces cas, la défaillance est indiquée à la source **UNI-C** en utilisant le message de notification **LDP**, avec le code d'état mis à la raison de la défaillance.

- **Suppression de connexion**

Pour informer son égal de cesser à utiliser une étiquette particulière, un routeur **LSR** en **LDP** peut employer l'un des deux messages différents: *Le message de retrait d'étiquette* ou *Le message de libération d'étiquette*. Un **LSR** A envoie un *message de retrait d'étiquette* à un égal **LSR** B pour indiquer que B doit cesser l'utilisation d'une étiquette spécifique que A avait précédemment annoncé. Par ailleurs, le **LSR** A envoie *un message de libération d'étiquette* à un égal **LSR** B pour indiquer qu'il n'a plus besoin d'une étiquette spécifique que B avait précédemment annoncé.

Dans les extensions **LDP** de l'**UNI**, tous les deux messages de retrait d'étiquette et de libération d'étiquette sont utilisés. Le choix du message à utiliser dépend de l'entité qui initie la suppression. Le message de retrait d'étiquette est utilisé lorsque la suppression de la connexion est, dans le sens montant

[1] SLA: Service Level Agreement.

(Upstream), c'est à dire, de la destination **UNI-C** vers la source **UNI-C**. Le message de libération d'étiquette est utilisé dans le sens descendant (Downstream), c'est à dire, de la source **UNI-C** à la destination **UNI-C**.

- **La détection des pannes et la récupération**

Le message **LDP** « *keepAlive »* est utilisé pour détecter la signalisation des échecs de communication entre un **UNI-C** et un **UNI-N**, à moins qu'un autre mécanisme soit en place pour détecter la signalisation des pannes d'une façon plus efficace. Lors de la signalisation d'une panne de communication, toutes les connexions actives seront maintenues alors que toutes les connexions qui sont en train d'être mis en place seront effacées.

6.3. Extensions RSVP pour la signalisation UNI

Les définitions de protocole **RSVP** s'appliquent uniquement à la signalisation **UNI** - qui est, entre la source **UNI-C** et la source **UNI-N** et la destination **UNI-N** et la destination **UNI-C**. Le réseau est supposé fournir la coordination des messages de signalisation entre les côtés de la source et de la destination de la connexion.

La plupart des messages **UNI** abstraits sont directement pris en charge par la réutilisation des procédures, messages et objets existants définis dans le protocole **RSVP-TE** et extensions **GMPLS** du protocole **RSVP-TE**. Le tableau suivant donne la correspondance entre les messages **UNI** abstraits définis par l'**OIF** et les messages **RSVP**.

Message abstrait	Message **RSVP**
Connection create request	Path
Connection create response	Path, PathErr
Connection create confirmation	ResvConf
Connection delete request	Path or Resv
Connection delete response	PathErr or PathTear
Connection status enquiry	Implicit
Connection status response	Implicit
Notification	PathErr , ResvErr

*** Table 2-1. Mappage entre les messages abstraits et les messages RSVP ***

CHAPITRE 3

Mise à niveau du réseau de transport de TUNISIE TELECOM

Les réseaux traditionnels de téléphonie fixe des opérateurs historiques dans le monde sont basés sur la commutation de circuits (aussi nommée transmission **TDM**) entre les lignes d'abonnés, et sur une organisation hiérarchique des commutateurs selon différentes zones d'appels. De plus, ce réseau de téléphonie cohabite avec un ou plusieurs réseaux dédiés au transport de données (dont le réseau utilisé pour la fourniture de services haut-débit **DSL**).

La problématique de passage à une architecture **NGN** (Next Generation Network) du cœur de réseau fixe des opérateurs historiques s'inscrit avant tout dans une logique de diminution des coûts, avec le passage à une infrastructure unique basée sur **IP** pour le transport de tout type de flux, voix ou données, et pour toute technologie d'accès (**DSL, FTTH, RTC, WiFi**, etc.). Ainsi que les réseaux mobiles de nouvelles générations (3G+, 4G et voire 4G+) ont devenues des réseaux orientés vers le transport des données, et la voix n'est devenue qu'un simple service parmi plusieurs autres.

Comme l'on a vu dans les deux chapitres qui précèdent, les réseaux de transport des données ont changé d'aspect, et ce changement a entrainé les operateurs historiques à assurer des changements et des mises à niveau radicaux dans leurs infrastructures de transport pour supporter le besoin des services récents ou pour augmenter la bande passante d'autres anciens. Ainsi les réseaux à base d'Ethernet et les réseaux de routage des longueurs d'onde seront largement déployés afin de gagner le défi technico-économique face à une concurrence féroce.

Nous verrons par la suite l'impact l'expérience de Tunisie Telecom en tant qu'opérateur historique dans la modernisation et la mise à niveau de son réseau de transmission/transport.

1. Evolution des services véhiculés par le réseau de transmission

Le réseau de transport est simulable à une locomotive qui traine derrière elle tous les autres services, c'est pour cela qu'il doit être conçu avec précision afin qu'il soit capable d'assurer le transport adéquat des services existants et prospects ainsi qu'une souplesse et dynamisme en son extension ou son accommodation avec de nouvelles services.

Lorsqu'on met le réseau de Transmission de Tunisie Telecom sous études, on trouve que ce réseau est basé sur la transmission sur les fibres optiques, et comme le dépôt des câbles en fibres a débuté dès les années 90, elles sont pourvues d'un nombre de fibre faible (8, 10, 12, 16 et au plus 24). Le changement de ces câbles demande des investissements très forts pour le génie civil et pour le coût des nouveaux câbles (144 **FO** par exemple). Avec un nombre important de faisceaux hertziens qui sont utilisés généralement pour raccorder les **BTS** distantes et extérieures.

Tunisie Telecom, afin d'implanter son réseau mobile **3G+**, a choisi de faire le « backhauling » de ces nouveaux **Node B**[1] vers les **RNC**[2] au biais des liaisons Ethernet en fibres optiques soit en Fibre noire, soit via un système de transmission, engendrant le dépose de centaines d'équipements de faisceaux hertziens et l'augmentation de la bande passante et de la qualité du signal véhiculé entre le **Node B** et le **RNC**. Par la suite l'entreprise peut être prête à la migration vers de nouveaux réseaux mobile plus gourmande en termes de débit tel que **LTE**[3] ainsi qu'elle peut intensifier l'exploitation des câbles en fibres mises en œuvre pour servir les **Node B** par l'utilisation des autres paires de fibres optiques pour ces réseaux d'accès **FTTx**[4] ou **MSAN** et ainsi mieux exploiter le gigantesque réseau en cuivre en augmentant le débit provenant jusqu'aux clients et de lancer d'autres services tel que : **IPTV**[5] ou **VoD**[6]…

1.1 Evolution des réseaux mobiles

Les réseaux mobiles de deuxième génération (**2G**) connus encore sous le nom de **GSM** utilisent des liens **E1** (2.048 Mbps) pour les liaisons Abis (liaison entre le **BTS** et le **BSC**) et Ater (Liaison entre le **BSC** et le **MSC**), ces liens électriques prennent plusieurs supports de transmission tel que les fibres optiques, les faisceaux hertziens et les modems HDSL sur paires torsadées en cuivre.

Le tableau suivant montre la nature du support sur l'interface Abis du réseau cellulaire de Tunisie Telecom :

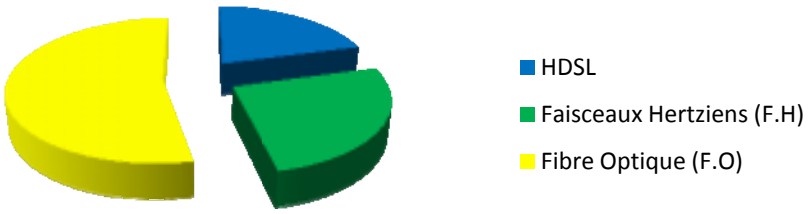
Interface Abis (2.048 Mbps)	Nombre	Pourcentage
HDSL	508	20,68 %
Faisceaux Hertziens (F.H)	637	25,94 %
Fibre Optique (F.O)	1311	53,38 %

[1] **Node B**: C'est un élément du réseau d'accès Radio gère la couche physique de l'interface air, c'est à dire le codage du canal, l'entrelacement, l'adaptation de débit et l'étalement. Il gère aussi le contrôle de puissance en boucle fermée. C'est l'équivalent de la station de base (**BTS**) ou analogiques.
[2] **RNC**: Radio Netwok Controller, c'est un élément du réseau d'accès Radio, équivalent au (**BSC**) des réseaux **GSM**.
[3] **LTE**: Long-Term Evolution, c'est une progression des réseaux proposée mobiles par le **3GPP** (Third Generation Partnership Project) et qui est projeté d'être un système de communications mobiles qui peut prendre l'industrie des télécoms dans les 2020s, connue parfois sous le nom de (**4G**).
[4] FTTx: Fiber To The x: {C = Curb, H = Home, B = Building, N = Node, P = Premises}, technologie dont le but est d'assurer des liens optiques pour les clients afin d'augmenter le débit, la sécurité et la qualité.
[5] **IPTV**: Technologie utilisant l'infrastructure des réseaux d'accès **FTTx** ou **MSAN** pour la diffusion des chaines télévisées numériques.
[6] **VoD**: Video on demand.

2456

*** Tableau 3.1 – Nombre d'interfaces **Abis** par type de support de Transmission ***

A partir de ce tableau, on dégage la Figure 3.1 qui montre le part de chaque support de transmission dans le réseau **GSM** de Tunisie Telecom,

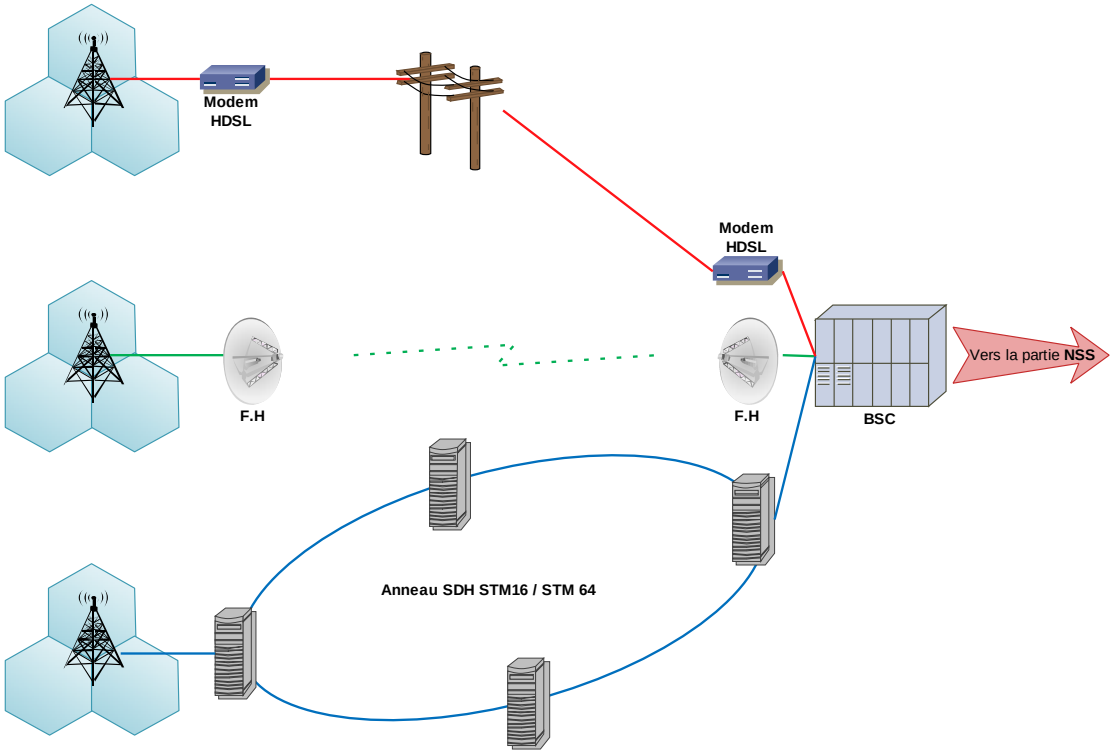


*** Figure 3.1 – Part de chaque support de transmission sur l'interface **Abis** du réseau **GSM** de TT***

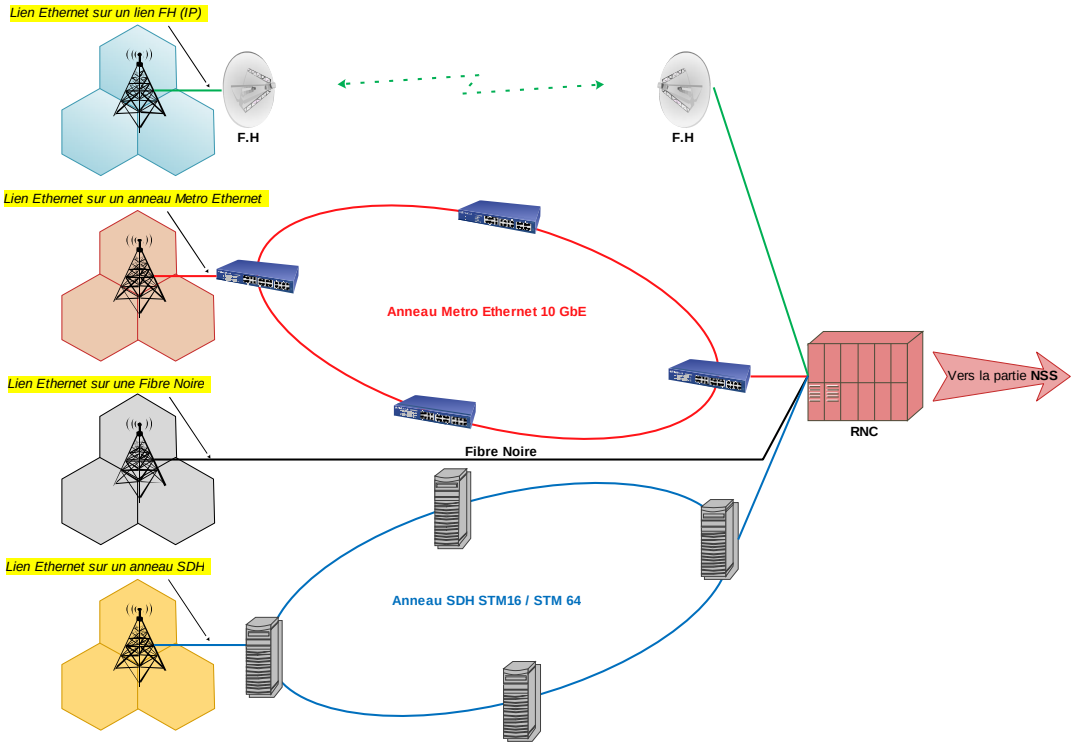
Les réseaux **TDM** traditionnelles **PDH** et **SDH** suffisent pour la satisfaction des besoins du réseau **GSM**, mais avec l'arrivée des réseaux **UMTS**, la nature des liens reliant le **Node B** au **RNC** (de Backhauling) connait un changement radical, ainsi la quasi-majorité de ces liens sera en fibres optiques afin d'offrir des débits de plus en plus importants pouvant satisfaire le besoin des clients du réseau mobile (**3G**) et assurer une très bonne qualité des services. Ce besoin a entrainer Tunisie Telecom à déployer des réseaux de transport à base d'Ethernet, soit en technologie **EOS** (Ethernet Over **SDH**) afin de bien exploiter les réseaux **SDH** dont l'infrastructure existe depuis un certain temps et son changement causera des dépenses lourdes pour l'opérateur, soit en utilisant le réseau Metro Ethernet récemment déployé en superposition partielle avec l'ancien réseau **SDH**.

La figure 3.2 schématise les différents supports de transmission utilisés pour l'interface Abis entre la **BTS** et le **BSC**, la figure 3.3 montre le progrès des liens de transmission servant pour l'opération du backhauling dans le sous système Radio (**BSS**[1]) du réseau **UMTS** (3G).

[11] BSS: Base Station Sub-System.



*** Figure 3.2 – L'interface Abis sur différents supports de Transmission ***



*** Figure 3.3 – L'interface **Iub** du réseau **UMTS** (3G) de Tunisie Telecom ***

Comme l'on peut voir sur la figure précédente, Tunisie Telecom assure le backhauling des **Node B** vers les **RNC** en utilisant quatre méthodes différentes dont les plus adoptes sont les trois dernières méthodes

basées sur une transmission optique directe (Fibre Noir) ou en utilisant des anneaux **SDH** qui adoptent la technologie **EOS** ou par l'exploitation des anneaux Metro Ethernet. Tunisie Telecom veut limiter l'utilisation des faisceaux hertziens pour le backhauling des **Node B** à moins de 1% du nombre total de liens assurant la transmission sur la partie **BSS**.

1.2 Evolution des réseaux d'accès

A. Le cas de FTTH

Malgré ses avantages, la fibre optique n'a pas été largement utilisée dans le « dernier mille » (par exemple, le segment du réseau qui s'étend directement du Central de l'opérateur au client). À cause du coût élevé et la disponibilité limitée des services d'accès optiques, ce segment est typiquement basé sur le cuivre.

Les services à très haut débit disponibles aux clients résidentiels et les petites entreprises sont pour le moment limités à la technologie (**xDSL**), mais cette technologie reste limitée en termes de distance et de débit, le tableau suivant montre cette limitation :

Transport	**ADSL[1]**				**VDSL[2]**				
	De base	**+**	**2**	**+2**	**De base**			**2**	
Bande Passante en sens descendant (Mb/s)	3	8	15	20	13	26	52	30	100
Distance maximale (km)	3	3	6	1.5	1.5	1	0.3	1	0.3

*** Tableau 3.2 - Développement de la bande passante de la technologie d'accès **xDSL** ***

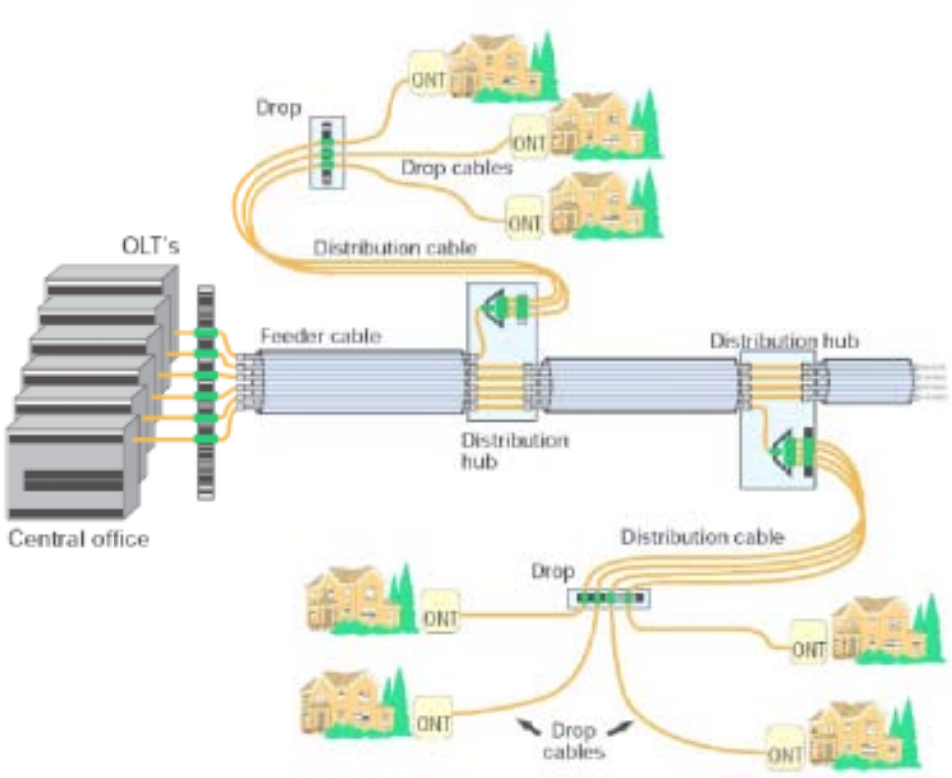
Bien que les fibres optiques vainquent la plupart de ces limitations, un des obstacles face à la fourniture des services en fibres optiques d'une façon directe aux résidences et aux petites entreprises, a été le coût élevé de la connexion de chaque client au central de l'opérateur (Par exemple, le coût de déploiement du câble en fibres optiques). Un nombre important de connexions point à point (**P2P**) exigerait beaucoup de composants actifs et un investissement élevé pour les câbles en fibres optiques, donc mener à des installations prohibitives et des coûts importantes pour l'entretien, comparé à un réseau de distribution traditionnel en cuivre (lequel devient très vieux et exige l'entretien lui aussi).

Bien qu'elle supporte les connexions en point à point (**P2P**), la technologie **FTTx** supporte aussi les connexions en point à multipoints (**P2MP**) qui offre une solution attrayante pour l'ensemble des problèmes susmentionnés. Avec la solution **FTTx** basée sur les normes **PON** (Passive Optical Network), aucun composant

[1] **ADSL**: Asymmetric Digital Subscriber Line.
[2] **VDSL**: Very-high-speed Digital Subscriber Line.

actif n'est utilisé entre le client et le central de l'opérateur, permettant à plusieurs clients de partager la même connexion. Ceci peut être accompli par l'utilisation d'un ou plusieurs filtres passifs permettant la connexion de plus que 32 clients sur la même fibre d'alimentation.

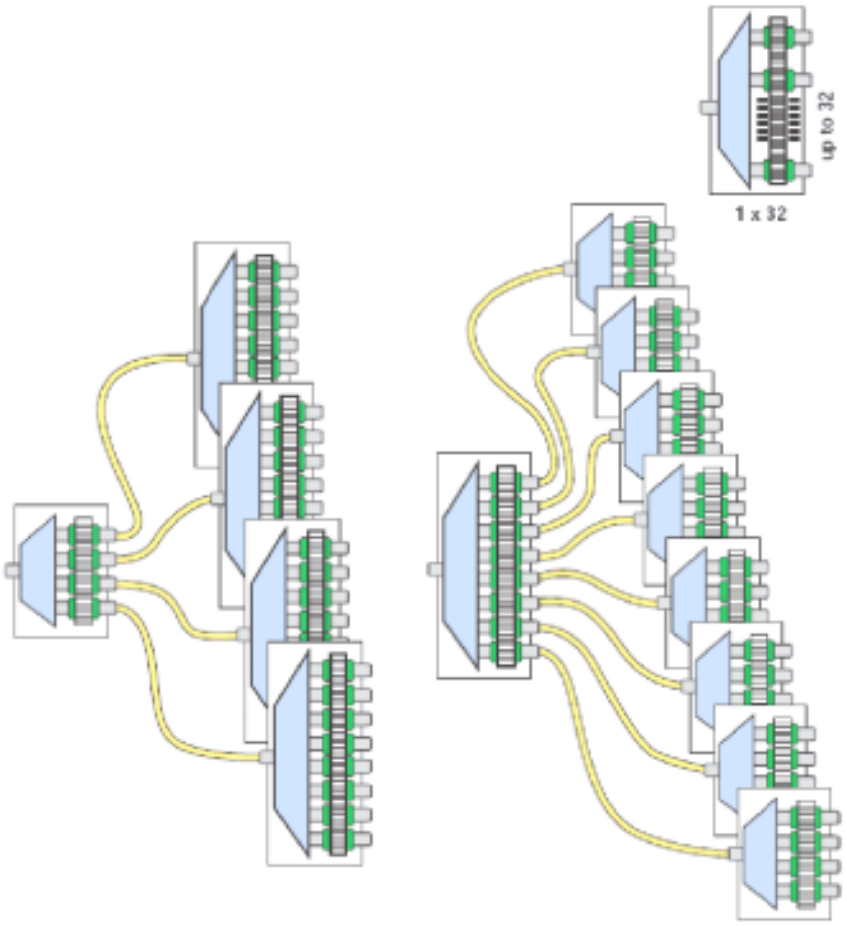
Tunisie Telecom a choisi la solution de **FTTH** pour alimenter les zones industrielles dont les entreprises ont un besoin croissant de la bande passante, et leurs assurer la livraison d'un service à très haut débit dont la qualité est meilleure et pouvant parcourir une distance allant jusqu'à 20 km. Avec cette solution, Tunisie Telecom peut offrir à ces clients, outre la transmission de données à tres haut débit, les services de téléphonie (**POTS** ou **VoIP**) et de vidéo.



*** Figure 3.4 - Topologie **PON** d'un réseau **FTTH** ***

La figure 3-4 montre la manière de connexion en (**P2MP**) d'un **ONT**[1] chez le client à un **OLT**[2] au niveau du central de l'opérateur.

[1] **ONT**: Optical network Termination.
[2] **OLT**: Optical Line Termination.



*** Figure 3.5 - Scénarios de partage d'une fibre d'alimentation entre 32 clients ***

La figure 3-5 montre les scénarios de partage d'une fibre d'alimentation entre 32 clients en utilisant les filtres.

Il est a noté que les architectures **PON** sont définies par les recommandations de **UIT-T**[1] et les standards de l'**IEEE**[2] ; l'**UIT-T** a standardisée **BPON** et **GPON**, alors que l'**IEEE** a standardisé **EPON**, un des différences majeures entre ces architectures sont les protocoles qui l'utilisent pour la transmission:

- **BPON** (Broadband **PON**), a été défini par la série de recommandation **G.983.x** de l'**UIT-T**, transporte n'importe quel type de données (voix, video, données **IP**…) en utilisant le protocole **ATM**[3] indifféremment du type du trame du lien de données.
- **GPON** (Gigabit **PON**), a été défini par la série de recommandation **G.984.x** de l'**UIT-T**, transporte n'importe quel type de données en utilisant le protocole **ATM** et la méthode **GEM**[4]. La méthode **GEM** encapsule les données sur le **GPON** et fournit une communication orientée connexion. **GPON**

[1] **UIT-T**: Union International de Télécommunications – Secteur de Standardisation de Télécommunications. www.itu.int
[2] **IEEE**: Institute of Electrical and Electronic Engineering. www.ieee.org
[3] **ATM:** Asynchronous Transfer Mode.
[4] **GEM**: GPON Encapsulation Method.

est optimisé sur la couche physique afin de supporter des débits plus élevées et des distances trop longues que les autres technologies du **PON**.

- **EPON** (Ethernet **PON**), a été défini par le standard IEEE 802.3ah-2004, utilise le protocole **MPCP** (Multipoint [*Media Access*] Control Protocol).

Le tableau suivant montre la bande passante et la distance maximale pour chacune des technologies décrites ci-haut :

Transport			**PON**		
			BPON	**GPON**	**EPON**
Bande Passante en sens descendant (Mb/s)	Maximale		155.52 622.08 1244.16	1244.16 2488.32	1000 nominal
	Partagée	1 × 16			~ 80
		1 × 32	~ 20 à 622.08 ~ 40 à 1244.16	~ 40 à 1244.16 ~ 80 à 2488.32	~ 40
Distance maximale (km)			20	20	10 20 (en utilisant le **FEC**[1]) **FEC**[1])

*** Tableau 3.3 – Comparaison entre les différentes variantes de la technologie **PON*****

B. Le cas du MSAN

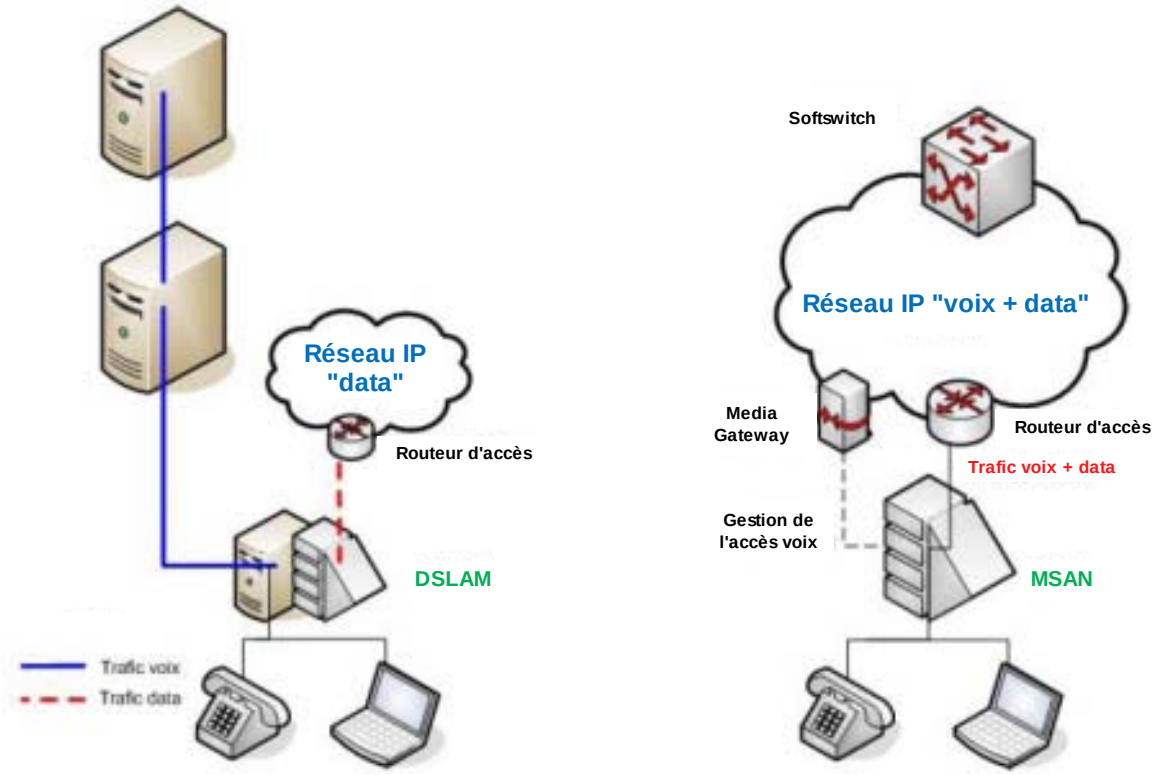
Un réseau **NGN** utilise un ensemble d'équipements qui jouent le même rôle qu'un commutateur traditionnel, mais qui sont désormais séparés en composants distincts :

- Le « Softswitch » est la solution qui gère dans un réseau **NGN** l'intelligence du service de commutation (gestion de tables d'appels, gestion des plans de numérotation). Toutefois, ce Softswitch n'est plus associé à un point physique du réseau, et ne gère plus les liens physiques du réseau, comme c'était le cas dans un réseau **TDM**.
- Le « Media Gateway », dont le rôle est d'assurer la gestion (disponibilité, détection de fautes) de la couche physique du réseau. Cette couche physique peut être le réseau de transmission, ou le réseau d'accès. Dans le cas où il s'agit du réseau d'accès, la fonction de Media Gateway peut être embarquée dans l'équipement d'accès lui-même, comme c'est le cas pour un **MSAN**.

[1] **FEC**: Forward Error Correction. C'est un champs utilisé par la couche Transport dans les systèmes de communication, il est basé sur la transmission des données sous un format codé (code à base de blocs). Le plus répandu est le format Reed-Solomon qui a une longueur de 255 octets, qui introduit une redondance (l'addition d'un entête redondant formé de 16 octets à un bloc constant de 239 octets de données), permettant au décodeur de détecter et de corriger les erreurs de transmission.

Dans la plupart des réseaux **NGN** déployés après 2004, la coexistence d'offres d'accès data et d'offres d'accès voix dans le portefeuille des opérateurs amène le déploiement de solutions « tout en un », permettant le contrôle d'accès pour les services voix et les services data. Ces solutions tout en un sont des **MSAN**.

La figure 3.6 représente les topologies comparées d'un réseau **NGN** et d'un réseau **TDM**, dans le cas de Tunisie Telecom.



*** Figure 3.6 – Comparaison d'un réseau d'accès **NGN** (droite) et d'un réseau traditionnel **TDM** (gauche)***

Les **MSAN** constituent une évolution naturelle des **DSLAM**s. Un **MSAN** est un équipement qui constitue, dans la plupart des architectures de type **NGN**, un point d'entrée unique vers les réseaux d'accès des opérateurs. A la différence d'un **DSLAM**, dont le châssis ne peut supporter que des cartes permettant de proposer des services de type **xDSL**, un **MSAN** peut supporter des cartes **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.

La volonté de passage à une architecture **NGN** (Next Generation Network) au niveau du cœur de réseau fixe de Tunisie Telecom, comme la plupart des opérateurs historiques, s'inscrit avant tout dans une logique de diminution des coûts, avec le passage à une infrastructure unique basée sur l'**IP** pour le transport de tout type de flux, voix ou données, et pour toute technologie d'accès (**DSL, FTTH, RTC, WiFi**, etc.). Avec le développement de l'internet et des nouveaux services comme la téléphonie mobile, les opérateurs historiques doivent en effet faire face à la chute des revenus traditionnels basés sur la voix commutée. Il leur faut

proposer des offres plus riches combinant la voix à d'autres services, préparer la convergence fixe-mobile et déployer ces nouveaux services plus facilement et surtout plus rapidement. Par ailleurs, beaucoup de réseaux fixes numériques ont des plates-formes de commutation qui arrivent en fin de vie et deviennent délicates à faire évoluer et à entretenir, à cause principalement de l'accroissement de leurs coûts de maintenance. La solution de la migration vers le **NGN** est perçue par beaucoup d'acteurs comme une réponse aux questions que se posent l'industrie des télécoms en termes de relais de croissance, tant pour les opérateurs à la recherche de revenus additionnels générés par de nouveaux services, que pour les équipementiers qui espèrent l'ouverture d'un marché large et dynamique. La nouvelle génération d'équipements **NGN** qui est largement orientée autour de l'**IP** présente en effet des capacités de commutation très nettement supérieures à celles des équipements traditionnels, ainsi que des avantages significatifs en matière de coûts. Ainsi, le nombre de nœuds physiques nécessaires est moins important que pour un réseau **RTC**, permettant de réaliser d'importantes économies au niveau immobilier, grâce à une baisse significative des dépenses liées à la location ou la propriété et l'entretien d'immeubles ou d'espaces dédiés aux équipements du réseau traditionnel. Le nombre d'équipements nécessaires est plus faible, permettant des économies directes en termes de coûts en capital, car même si le prix d'un Softswitch est supérieur à celui d'un commutateur traditionnel, son gain en efficacité compense largement cette différence. En termes de coûts opérationnels, le retour sur investissement est aussi immédiat. Moins d'équipements signifie moins de maintenance, moins de personnel, moins de véhicules, moins de dépenses d'électricité. Les économies liées à la réduction du personnel technique peuvent être significatives pour les opérateurs historiques qui disposent de très importants effectifs techniques. En outre, le déploiement de nouvelles technologies peut impliquer la formation des équipes existantes ou le recrutement de nouvelles compétences.

2. Changement du réseau de transmission

Comme l'on a vu précédemment, les applications et les services implantés ont forcé Tunisie Telecom à faire des changements radicaux sur l'architecture de son réseau de transmission afin de satisfaire le besoins de plus en plus croissants et à moindre coût.

Un réseau **OTN**[1] de routage de longueurs d'ondes basée sur la technologie **DWDM**[2] aurait être mis en place pour limiter les dépenses très couteuses pour les travaux de génie civil afin de changer des anciens câbles de fibres optiques qui sont pauvres en nombre de fibres (la plupart des câbles existant possèdent moins de 24 **FO**, vu l'ancienneté de leurs poses).

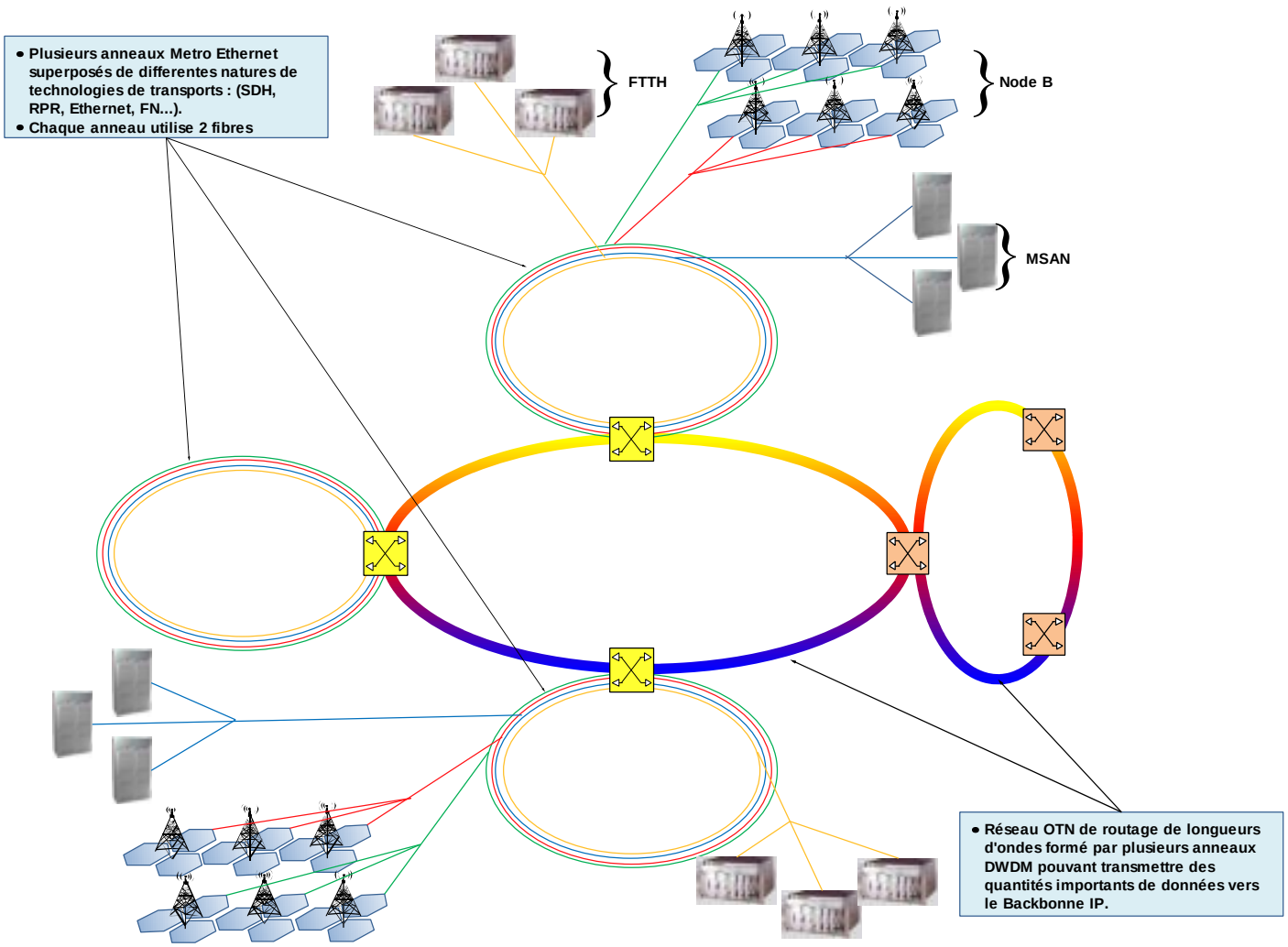
[1] **OTN**: Optical Transport Network.
[2] **DWDM**: Dense Wivelength Division Multiplexing.

Le réseau **OTN** assure le transport et le routage d'une très grande quantité d'informations entre les nœuds du réseau (ce type de réseau sera principalement utilisé en Backbone) et supporte tout type de données (**TDM, IP, ATM** …).

Le réseau de transport optique **OTN** de Tunisie Telecom est formé par plusieurs anneaux reliés entre eux au niveau de plusieurs nœuds (11 nœuds pour le moment), ceci permet d'avoir un aspect maillé au réseau permettant de créer des itinéraires optiques (des chemins optiques) entre les nœuds existants d'une façon souple et rapide.

En termes de sécurité des liaisons sur le réseau optique **OTN**, on peut utiliser des protocoles de protection sur deux fibres ou même on peut améliorer la protection en utilisant quartes fibres dont le fonctionnement a été décrit précédemment dans le deuxième chapitre.

La figure suivante montre l'agrégation des données de plusieurs nœuds, ensuite la concentration de ce trafic afin de le véhiculer vers le réseau cœur de l'operateur et le routage du trafic vers la destination souhaitée selon le son origine (le trafic en provenance des Node B par exemple sera transmis vers les **RNC** puis vers les **MSC** pour la voix et les **SGSN** pour les données).



*** Figure 3.7 – Vue globale du réseau Optique de Tunisie Telecom ***

- CONCLUSION -

Le but de Tunisie Telecom étant l'augmentation de ces recettes dans un monde caractérisé par concurrence impitoyable et ce par l'introduction de nouveaux services et ainsi la compensation de la diminution des recettes des services vocaux (sur la branche de la téléphonie fixe), cette augmentation désirée des recettes sera appuyée sur l'augmentation des activités commerciales dans le domaine du large bande et la réduction des coûts grâce au partage de l'infrastructure et des systèmes de réseau ce qui crée des énormes économies en fonction du type de réseau choisi, du niveau de modernisation des équipements et de l'augmentation du nombre de clients et finalement par la simplification de l'exploitation et de la maintenance, d'où une diminution des dépenses d'exploitation.

Les réseaux de transports de l'operateur historique sont pour le moment dans la phase de leurs mise à niveau afin de relever les défis et d'assurer la hausse des bénéfices et la satisfaction de la clientèle.

- REFERENCES -

[01] – **Metro Ethernet**
Sam HALABI, Cisco Press, 2004.

[02] – **Connection Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks**
Harry G. Perros, John Wiley & Sons Ltd, 2006.

[03] – **DWDM Network Design and Engineering Solutions**.
Ashwin GUMASTE, Cisco Press, 2003.

[04] – **Network Recovery : Protection and Restoration of Optical, SONET/SDH, IP and MPLS**
Jean Philippe VASSEUR & Mario PICKAVET & Piet DEMEESTER, Elsevier, 2004.

[05] – **DWDM Basic Principle**
ZTE University, 2007.

[06] – **40 Gb/s and 100 Gb/s Ethernet**
Paul KISH, CNS Magazine (www.cnsmagazine.com), January/February 2009.

[07] – **Carrier Ethernet: The Challenges of Ethernet Access – Reference Guide.**
RAD Data Communications (www.rad.com), 2008.

[08] - **IEEE 802.3ba 40 and100 Gigabit Ethernet Architecture**
Ilango GANGA, IEEE802.3ba Task Force, 2010.

[09] – **Optical Fibers, Cables and Systems**
ITU, 2010.

[10] – **FTTx Technology and Testing.**
André GERARD, EXFO, 2005.

[11] – **SONET/SDH explained in functional models**
Huub VAN HELVOORT, John WILEY & Sons, 2005.

[12] – **The Cable and Telecommunications Professional's Reference.**
Edited By: Goff HILL, Elsevier & Focal Press, 2008.

[13] – **The Key Benefits of OTN Networks – White Paper**
Fujitsu (us.fujitsu.com/telecom), 2007.

[14] – **Overview of RPR**
Huawei University, 2008.