Université du Québec à Montréal
Département d'Informatique

ꕥ🕮ꕥ

DOCTORAT EN INFORMATIQUE COGNITIVE

DIC9410 – Présentation du projet

Sujet du projet

Intégration de la technologie des systèmes multiagents dans l'architecture OVPN

Étudiant : VO, Viet Minh Nhat (VOXV29077401)
Sous la supervision de : Professeur Abdel Obaid
Professeur Pierre Poirrier

Hiver 2004

Table des matières

1. Revue de littérature et problématique

Le réseau privé virtuel VPN (*Virtual Private Network*) est bien connu comme une solution efficace dans l'interconnexion des réseaux (sites) de clients (ex. réseaux d'entreprises) se basant sur un réseau d'infrastructure publique (comme Internet). Une tendance actuelle est le remplacement des réseaux d'infrastructures non optiques par des réseaux optiques pour profiter de la capacité de bande passante des fibres optiques. À cause des différences importantes dans la technologie de transport (optique versus non optique) et dans le type de porteur de données (trame optique versus paquet électronique), l'architecture VPN traditionnelle doit être changée pour s'adapter à l 'environnement de transport optique. Le nouveau type de réseaux VPN s'appelle alors réseau VPN optique OVPN (*Optical VPN*).

Ce chapitre présentera une revue des types de réseaux VPN non optiques et des problèmes actuels pour les transformer en réseaux VPN optiques. Nous commençons par un résumé de l'architecture VPN non optique et des différents types de réseaux VPN. Ensuite, les différentes approches du réseau VPN pour l'infrastructure optique (réseaux OVPN) seront discutées. Une technique typique de la tunnellisation optique (i.e. protocole GMPLS - Generalized MultiProtocol Label Switching [18]) est aussi décrite. Enfin, en nous basant sur le besoin d'utilisation des services OVPN et les problèmes du transport optique actuel, nous définirons notre sujet de recherche.

1.1. Brève revue du réseau VPN non optique

Traditionnellement, la façon la plus commune pour interconnecter des réseaux (sites) séparés de clients consiste à utiliser des lignes louées (*leased-lines*) de type FR (*Frame Relay*) ou ATM (*Asynchronous Transfer Mode*). Cette méthode est simple mais inefficace parce que :

- Les lignes louées sont généralement chères;
- Les lignes louées ne sont pas flexibles en ce qui concerne la quantité de bande passante disponible. Le client peut devoir choisir entre une ligne louée moins chère avec peu de bande passante et une autre beaucoup plus chère avec plus de bande passante que nécessaire.
- Les clients doivent être responsables de la planification du réseau des lignes louées et du contrôle du routage des données sur ces lignes.
- Les lignes louées utilisent traditionnellement le protocole FR ou ATM, tandis que la plupart des services actuels de réseaux emploient le protocole IP (*Internet Protocol*). Le fournisseur de service de réseau devra alors gérer en même temps les lignes louées FR ou ATM aussi bien que les connexions IP, ce qui est plus difficile et augmente donc le coût des lignes louées pour le client.

Les réseaux privés virtuels VPN [1]-[12] ont été proposés comme méthode pour relier des sites de clients sur la base d'un réseau d'infrastructure (*backbone*) publique (comme Internet), au lieu des lignes louées. Avec une approche VPN, le fournisseur de services de réseaux peut offrir des connexions plus économiques que les lignes louées parce que les ressources disponibles temporairement (telles que les fibres, la bande passante…) du réseau public peuvent être partagées par différents clients. En outre, le client est aussi libéré des tâches complexes comme la planification du réseau, le contrôle du routage, etc.

1.1.1. L'architecture VPN générale

Pour soutenir des services VPN, des fonctions VPN sont assignées aux nœuds d'un réseau d'infrastructure. Par exemple, pour accéder au réseau du fournisseur, les sites de clients utilisent des dispositifs (tels que des commutateurs ou des routeurs) qu'on appelle « dispositifs de périphérie du client » CE (*Customer Edge*). Bien que ces dispositifs fassent en fait partie du réseau de clients plutôt que celui du fournisseur, ils sont dans la plupart des cas contrôlés (voire même possédés) par le fournisseur de services.

Dans le réseau de fournisseur, les dispositifs tels que les routeurs dédiés pour relier les sites de clients portent le nom de « dispositif de périphérie du fournisseur » PE (*Provider Edge*). Il existe aussi des dispositifs qui acheminent (*forward*) seulement des trafics VPN, mais qui ne possèdent aucune fonction VPN : Ils s'appellent les dispositifs du fournisseur P (*Provider*). La Figure 1-1 illustre l'architecture VPN.

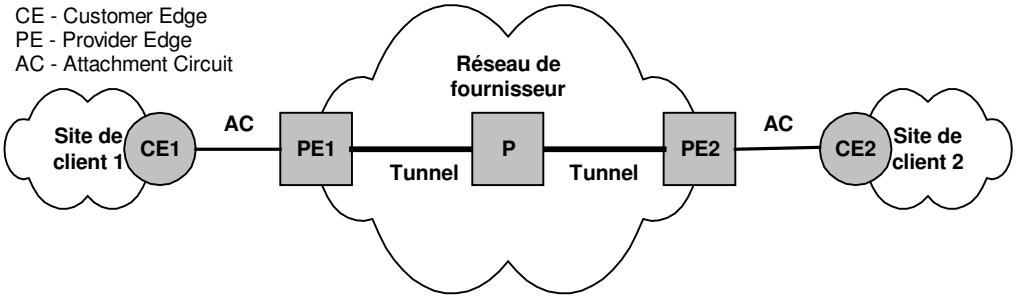

Figure 1-1 : Une architecture VPN non-optique générale

Tel qu'illustré dans Figure 1-1, on nomme « circuit d'attachement » (AC, *Attachment Circuit*) le lien établi entre le périphérique du client (CE) et celui du fournisseur (un routeur PE). Un circuit d'attachement AC peut être un lien physique (comme une ligne FR ou ATM) ou logique (comme une connexion IP). Il peut être un service de transport sur la couche 2 (comme un service FR ou ATM) ou sur la couche 3 (comme un service IP). Pour le transport des données entre deux routeurs PE, les tunnels sont établis à travers le réseau de fournisseur. La concaténation « AC, Tunnel, AC » forme alors un lien de bout-en-bout (end-to-end) entre deux périphériques CE, qu'on appelle « circuit virtuel » VC (*Virtual Circuit*).

1.1.2. La technique de tunnellisation

Le transport des données entre des routeurs PE dans un réseau VPN est réalisé par des tunnels. La technique de tunnellisation est une méthode d'encapsulation des données dans laquelle un en-tête supplémentaire (appelé *étiquette*) est ajouté aux paquets de données par les terminaux (routeurs PE) (Figure 1-2). Les paquets étiquetés seront alors acheminés par des nœuds intermédiaires sur la base de cette étiquette sans voir le contenu du paquet original. Les paquets qui ont la même étiquette sont transférés de la même manière en passant un nœud. De cette façon, un tunnel est établi entre les terminaux à travers le réseau du fournisseur. Les protocoles typiques supportant la technique de tunnellisation sont IPsec [14], GRE [15], L2TP [17] et MPLS [13].

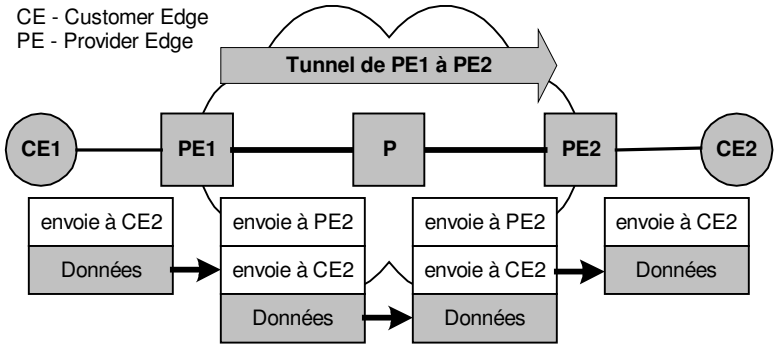

Figure 1-2 : Un exemple de la tunnellisation

Par l'utilisation de la technique de tunnellisation, les équipements du réseau du fournisseur (commutateurs P) n'ont pas besoin de reconnaître des trafics VPN, mais simplement de pouvoir acheminer des données étiquetées. Cette technique réduit considérablement les ressources consommées et la quantité de configuration exigée pour établir des connexions. En outre, par la transmission des données entre les sites de clients via des tunnels, il est possible de maintenir la séparation des trafics entre les différents services VPN et d'empêcher la fuite de données d'un trafic VPN dans le réseau de fournisseur ou dans le reste de l'Internet.

1.1.3. Les réseaux VPN non optiques

Plusieurs types de réseaux VPN non optiques ont été proposés [1]-[12]. La classification des types de réseaux dépend des critères de catégorisation. Normalement, on se base sur la couche où les paquets de données sont traités (comme sur la couche 2 (L2VPN) ou sur la couche 3 (L3VPN)) ou sur les nœuds où les fonctions VPN sont situées (comme sur CE (*CE-based VPN*) ou sur PE (*PE-based VPN*)).

A. Les réseaux VPN basés sur le périphérique du client

Les réseaux VPN basés sur le périphérique du client CE (*CE-based VPNs*) [1][2] sont semblables aux lignes louées FR ou ATM, avec des tunnels basés sur protocole IP établis entre les périphériques CE (Figure 1-3). Les routeurs PE et les commutateurs P sont transparents par rapport au VPN. Les tunnels entre les périphériques CE

sont établis par des protocoles tels que IPsec [14] ou L2TP [17] qui fournissent une transmission sécurisée du trafic IP au niveau de la couche 3 (L3VPN), ou au niveau de la couche 2 (L2VPN).

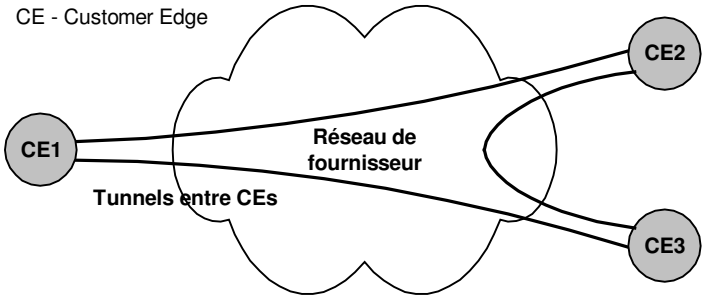

Figure 1-3 : Un exemple du réseau VPN basé sur CE

Les réseaux VPN basés sur le périphérique du client (CE) sont les plus simples parce que le réseau de fournisseur ne participe à aucun contrôle ni routage du trafic. Les périphériques du fournisseur (PE) peuvent alors être de simples routeurs IP standards. Ce qui constitue des avantages pour le fournisseur. De plus, dans les réseaux VPN basés sur le périphérique du client (CE), les routeurs PE n'ont pas besoin de mémoriser les états ou les adresses des éléments participant à un VPN. Ils n'ont plus besoin de participer dans le routage interne du réseau VPN. Ceci signifie que ce modèle est bien extensible par rapport au réseau de fournisseur. Cependant, un des problèmes des réseaux VPN basés sur le périphérique du client (CE) est la quantité de travail exigée pour gérer et configurer les périphériques CE. La gestion et la configuration peuvent alors devenir extrêmement complexes, en particulier si le réseau VPN se compose d'un grand nombre de sites de clients. En outre, l'utilisateur peut devoir acheter de nouveaux équipements pour supporter des fonctions VPN. Une manière de réduire la complexité de la gestion et du contrôle pour l'utilisateur est de laisser le fournisseur contrôler et gérer ses périphériques CE.

B. Les réseaux VPN basés sur le périphérique du fournisseur

Il existe plusieurs types de réseaux VPN basés sur le périphérique du fournisseur PE [11][12] et qui se distinguent par la technique de tunnellisation des données ou par la manière de gérer les connexions qu'ils utilisent. Cependant, la méthode la plus populaire pour les distinguer se base sur la couche (2 ou 3) dans laquelle les paquets de données sont traités.

Dans les réseaux VPN basés sur les périphériques du fournisseur (PE) de la couche 3, il est nécessaire que le routeur PE achemine des paquets IP entre des sites qui appartiennent à différents clients et à des membres de plusieurs réseaux VPN. Le routeur PE peut devoir conduire des paquets entre sites client locaux à travers le VPN. Ceci est complexifié par le fait que les réseaux VPN sont des réseaux privés et ainsi on peut légitimement employer les mêmes espaces d'adresses pour identifier des éléments (telles que les connexions ou les nœuds). La même adresse IP peut être également employée dans l'Internet ou dans le réseau du fournisseur. Par

conséquent, chaque routeur PE requiert plusieurs tables de routage séparées. En particulier, ils exigent une table virtuelle de routage et d'acheminement VRF (*Virtual Routing and Forwarding*) pour chaque réseau VPN.

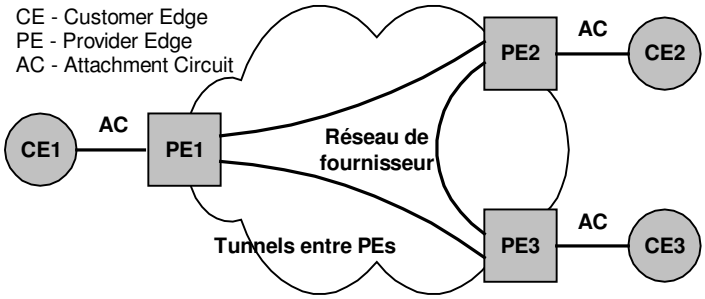

Figure 1-4 : Un exemple du réseau VPN basé sur PE

Le même problème existe pour les réseaux VPN basés sur le périphérique du fournisseur (PE) de la couche 2. Bien que les données soient acheminées par un routeur PE sur la base d'informations de la couche 2 plutôt que l'adresse IP de la destination, les tables d'acheminement de la couche 2 sont toujours stockées selon la base d'un par réseau VPN (One per VPN).

Pour les réseaux VPN basés sur les périphériques du fournisseur (PE), les routeurs PE exécutent la plupart des fonctions VPN spécifiées. Les périphériques CE sur les sites de clients peuvent alors être des commutateurs ou des routeurs standards et il n'est pas nécessaire de les renouveler. En outre, puisque le fournisseur de service de réseau est responsable de la gestion des réseaux VPN, peu de travail est exigé du client. Cependant, cette caractéristique entraîne qu'il y aura beaucoup de travail exigé du fournisseur et il est probable que celui-ci devra remplacer ses équipements pour supporter des réseaux VPN.

1.2. Différentes approches du réseau VPN optique

L'avancement et l'évolution rapides des technologies optiques ont permis aux systèmes de transmission optique point à point d'aller vers des réseaux d'infrastructures entièrement optiques. Ce changement permettra de profiter pleinement de la bande passante optique disponible en éliminant le besoin de conversion optoélectronique, et vice-versa, des paquets de données à chaque nœud. L'utilisation de l'infrastructure optique pour supporter des réseaux VPN devient dès lors une tendance actuelle, laquelle créera un bon moyen pour la communication de haute bande passante et un partage élevé des ressources. Le problème posé est de voir comment il est possible de transformer les réseaux VPN non optiques actuels en réseaux capables de s'adapter à l'infrastructure optique. En outre, puisque le réseau public comme l'Internet est une ressource ouverte pour toutes les applications, les services VPN doivent co-exister avec des trafics réguliers, tolérer des pannes de réseaux, protéger contre la fuite de données, etc.

1.2.1. Approche héritée des réseaux VPN non-optiques

L'approche présentée dans [26] est héritée des réseaux VPN de type non optique. Une architecture VPN optique OVPN (*Optical VPN*) est construite des éléments du réseau optique ONE (Optical Network Element) comme dans la Figure 1-5. On distingue deux types de dispositifs ONE : les dispositifs ONE appartenant aux réseaux de fournisseur, nommés P-ONE (*provider ONE*), sont les dispositifs ONE qui ne se connectent qu'à d'autres dispositifs ONE, tandis que les dispositifs ONE de périphérie du fournisseur, nommés PE-ONE (*provider edge ONE*), sont les dispositifs ONE qui connectent à des autres dispositifs ONE mais aussi aux dispositifs de périphérie du client CD (*Customer Device*). Les périphériques CD peuvent être des équipements non optiques (comme des routeurs ou des commutateurs IP standards) ou des équipements optiques (comme des commutateurs SONET/SDH.)

Les périphériques du client (CD) se connectent aux routeurs PE-ONE à travers des « ports ». Chaque port peut supporter un ou plusieurs canaux optiques, dont chacun peut correspondre à une longueur d'onde ou un groupe d'intervalles de temps (*time-slots*) sur une longueur d'onde. Une périphérique CD peut se connecter à plusieurs routeurs PE-ONE et, à l'inverse, un routeur PE peut se connecter à plus d'une périphérique CD par des ports différents.

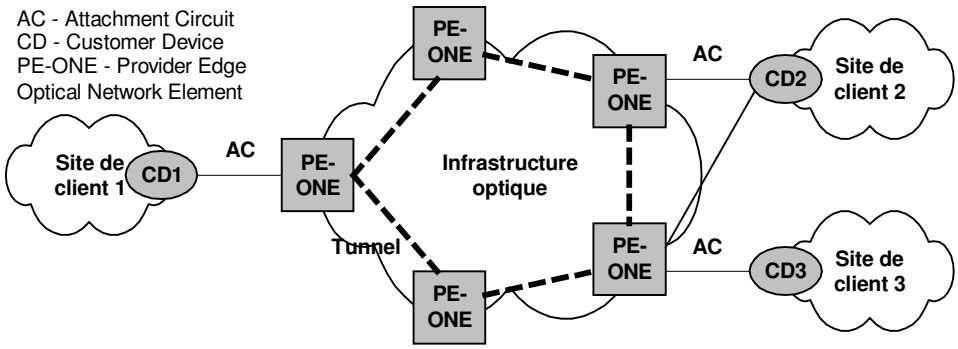

Figure 1-5 : Architecture OVPN de référence

Les portes de la périphérique CD et du routeur PE-ONE sont identifiés par la paire formée de l'adresse IP de l'équipement et de l'index d'interface de port (*IP address*, *interface index*). L'interface de port dans un réseau OVPN doit être indexée différemment, alors qu'elles peuvent être identiques pour des réseaux OVPN différents. L'identificateur de chaque port est alors unique dans chaque réseau OVPN. On distingue deux types d'identificateurs de port : l'identificateur de port du client CPI (*Customer Port Identifier*) et l'identificateur de port du fournisseur PPI (*Provider Port Identifier*)

Pour séparer la gestion des réseaux OVPN et éviter l'effet de l'ajout ou du retrait d'un port, un routeur PE-ONE maintient une table d'informations sur ports (PIT, *Port Information Table*) pour chaque réseau OVPN. Une table PIT enregistre une liste de paires « CPI, PPI » et « PPI, PPI » pour toutes les connexions dans son réseau

OVPN (Figure 1-6). Une table PIT est essentiellement identique à une table VRF dans un réseau VPN non optique basé sur le périphérique du fournisseur (PE) de la couche 3.

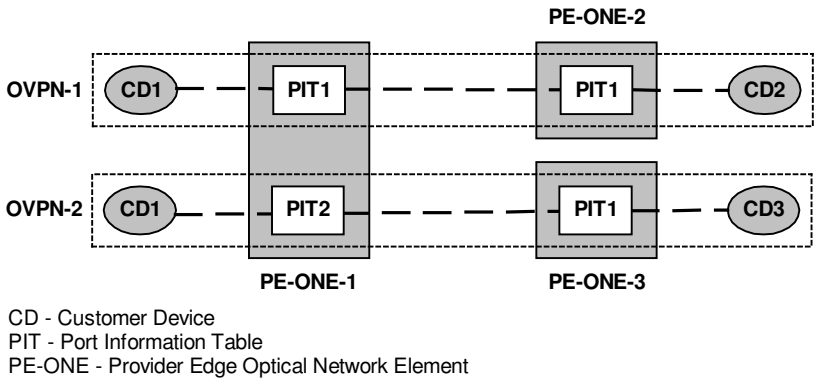

Figure 1-6 : Séparation de gestion des routeurs PE-ONE pour les différents réseaux OVPN

Il est clair que cette approche se base sur le périphérique du fournisseur (PE) : les fonctions VPN sont situées sur les routeurs PE-ONE et le client est alors transparent par rapport au réseau OVPN. Le désavantage de cette approche est qu'elle n'est pas complète; elle ne touche que la structure et les interactions entre dispositifs CD et routeurs PE-ONE. L'établissement des connexions entre routeurs PE-ONE n'est pas décrit et la manière de gérer et de contrôler la signalisation et l'établissement des services OVPN n'est pas présentée.

1.2.2. Approche basée la topologie virtuelle

Contrairement à l'approche précédente, les propositions dans [27], [28] cherchent à établir une topologie virtuelle pour un réseau OVPN dans le réseau de fournisseur. Une topologie virtuelle est un ensemble de chemins optiques (*lightpaths*) fournis pour interconnecter des sites de clients participants à un réseau OVPN. Le concept de topologie virtuel a été introduit dans [30].

Dans [27], on établit un réseau OVPN en considérant les caractéristiques demandées de la topologie logique et des différents types de chemins optiques disponibles. L'objectif est de répondre aux demandes concernant la qualité de service QoS (*Quality of Service*) d'un réseau OVPN et d'utiliser de manière optimale la capacité du réseau d'infrastructure. On distingue les réseaux OVPN différents dans les différents domaines en fournissant des chemins optiques avec différentes qualités de service (QoS). On distingue trois types de chemins optiques sur lequel le trafic OVPN est transporté: (1) les chemins optiques spécialisés (DLP, *Dedicated LightPath*): Le lien tout-optique traversant des commutateurs optiques OXC (*Optical Cross-Connect*) et dédié à un seul réseau OVPN; (2) les chemins optiques partagés (SLP, *Shared LightPath*): Le lien tout-optique partagé par de multiples réseaux OVPN; et (3) le chemin optique multi-bonds (MHP, *Multi-Hops Path*): Le lien hybride construit de chemins optiques de longueurs d'onde différentes (les conversions optoélectroniques et vice-versa sont alors permises) pour chaque bond optique (l'intervalle entre deux nœuds successifs).

Selon les demandes de qualité de service (QoS) pour un réseau OVPN, un ou plusieurs types de chemins optiques seront utilisés pour transporter le trafic OVPN. En donnant un ensemble de réseaux OVPN et leurs spécifications, le réseau va tenter de satisfaire les demandes de service de type 1 en utilisant des chemins optiques DLP (*lightpaths DLPs*), les demandes de service de type 2 en utilisant des chemins optiques SLP (*lightpaths SLPs*), et les demandes de service de type 3 en utilisant des chemins optiques MHP (lightpaths MHPs). Quand des chemins optiques DLP ne sont plus disponibles, il établit des chemins optiques SLP où le nombre de réseaux OVPN partagés sur un chemin optique est limité en se basant sur des spécifications. Quand des chemins optiques SLP ne sont pas possibles, des chemins optiques MHPs sont installés.

Selon [28], le problème de la conception de la topologie virtuelle peut être formulé comme un problème de programmation linéaire entier avec les demandes de trafic, les contraintes de longueur d'onde et de ressources. L'idée est qu'une matrice des trafics demandés est divisée en matrices individuelles pour réduire la complexité de la conception de la topologie virtuelle. Les matrices individuelles sont ensuite formulées l'une à la suite de l'autre. L'objectif final de cette approche est d'optimiser l'utilisation des ressources du réseau d'infrastructure et de maximiser le nombre de réseaux OVPN établis.

Le désavantage des approches basées sur la topologie virtuelle est que celles-ci sont inextensibles et non dynamique, parce que la topologie est construite en se basant sur les demandes fixes de réseaux OVPN. Ainsi, lorsqu'il y a une extension de la bande passante pour un réseau OVPN, cela veut dire que l'ancien réseau OVPN doit être supprimé et qu'un nouveau réseau OVPN doit être crée. De plus, cette approche ne donne pas une architecture complète pour le contrôle et la gestion des réseaux OVPN sur les routeurs PE-ONE et aussi pour les réseaux d'accès entre périphériques CD et routeurs PE-ONE.

1.3. GMPLS : la technique de tunnellisation optique

L'établissement des tunnels sur les réseaux d'infrastructure non optiques est fait par la technique de commutation d'étiquette (typiquement le protocole MPLS - *MultiProtocol Label Switching* [13]). Une étiquette dans le protocole MPLS est un entier (sur 32bits) ajouté à l'en-tête d'un paquet. En se basant sur ce nombre, un routeur LSR (*Label Switching Router*) fait simplement acheminer (*forward*) les paquets correspondants aux différentes étiquettes. En conséquence, les paquets ayant la même étiquette sont transférés de la même façon. Cette propriété fait que les paquets sont transmis via le réseau d'infrastructure comme dans un tunnel.

L'idée du protocole MPLS généralisé GMPLS (*Generalized MPLS* [18]) est que tout ce qui peut identifier un flux de trafic peut être utilisé comme une étiquette. Par exemple, dans une fibre optique dont la bande passante est divisée en longueurs d'onde, la totalité de bande passante d'une longueur d'onde donnée pourrait être assignée à un flux de trafics optiques et les routeurs LSR aux extrémités de la fibre doivent simplement convenir de la fréquence à utiliser, qui devient une étiquette GMPLS. Contrairement aux étiquettes non généralisées, les données à l'intérieur d'un flux de trafic optique n'ont pas du tout besoin d'être marquées d'une valeur d'étiquette;

au lieu de cela, la valeur d'étiquette est implicite dans le fait que les données sont transportées sur une fréquence convenue. En outre, une représentation de la valeur d'étiquette est nécessaire dans le protocole de signalisation de sorte que les messages de contrôle entre les routeurs LSR puissent convenir de la valeur l'utilisation.

Différentes propriétés des trafics peuvent servir d'étiquette généralisée dans la commutation des flux de trafics optiques :

- **Étiquette de fibre (Fibre Label)**: Un lien entre deux routeurs LSR peut se composer d'un faisceau de fibres optiques. Les routeurs LSR peuvent assigner une fibre en entier à un flux de trafic et il s'agit alors simplement de convenir de la fibre à utiliser. Dans ce cas, la valeur d'étiquette est l'index de la fibre sélectionnée dans le faisceau. L'interprétation des index de fibre/port est un sujet local pour les routeurs LSR sur un lien. Quand deux routeurs LSR utilisent les schémas de numérotation différents, un protocole de gestion des liens comme le protocole LMP (*Link Management Protocol*) [20] est utilisé pour fournir un mécanisme qui permet aux routeurs LSR d'échanger et de corréler l'information de numérotation.
- **Étiquettes de longueur d'onde (Wavelength Label)**: Quand la bande passante d'une fibre optique est subdivisée par la technique WDM (*Wavelength Division Multiplexing*), un routeur LSR peut assigner une longueur d'onde simple au flux de trafic demandé. Dans ce cas-ci, la valeur d'étiquette est la fréquence de la longueur d'onde sélectionnée.
- **Étiquettes de gamme d'onde (Waveband Label)**: Si des longueurs d'onde consécutives sont groupées ensemble dans une gamme d'ondes, pour toutes les commuter de la même manière, l'étiquette est une paire de fréquences indiquant les longueurs d'onde inférieures et supérieures de la gamme d'ondes sélectionnée.
- **Étiquettes d'intervalle de temps (*Time-slot Label*)**: Quand la bande passante d'une longueur d'onde est subdivisée en intervalles de temps par la technique TDM (*Time Division Multiplexing*), un commutateur optique peut satisfaire la demande d'un flux de trafic particulier en assignant un ou plusieurs intervalles de temps.
- **Attributions de bande passante**: Pour tous les types d'étiquettes du protocole GMPLS décrits précédemment, la valeur d'étiquette implique directement la bande passante disponible correspondant au flux de trafic. Par exemple, si une étiquette dénote un intervalle de temps simple de la technique SONET VT-6, la bande passante disponible est la bande passante d'un intervalle de temps VT-6. Il en est de même pour l'étiquette de longueur d'onde, l'étiquette de gamme d'ondes et l'étiquette de fibre. Cette propriété est tout à fait différente pour les étiquettes non généralisées et découle de propriété fondamentale de la nature des réseaux optiques.

1.4. Problèmes du transport optique

Deux contraintes bien connues dans le transport optique sont la continuité de longueur d'onde[1] et la distinction de longueur d'onde[2]. La contrainte de continuité de longueur d'onde peut être éliminée si les nœuds (commutateurs OXC (*optical cross-connect*)) sont équipés de convertisseurs de longueurs d'ondes. Un convertisseur de longueurs d'ondes est un dispositif qui convertit la longueur d'onde d'un signal optique traversant un commutateur OXC. Dans les commutateurs OXC sans possibilité de conversion de longueur d'onde, un signal entrant au port p_i sur la longueur d'onde λ peut être optiquement commuté à n'importe quel port p_j, mais doit être sur la même longueur d'onde λ. Mais avec des convertisseurs de longueur d'onde, ce signal peut être optiquement commuté vers n'importe quel port p_j sur une autre longueur d'onde λ'. C'est-à-dire, la conversion de longueur d'onde permet à un chemin optique d'employer des longueurs d'onde différentes le long des liens physiques.

Une limite du transport optique est l'absence de file d'attente (queue) des trames optiques pour la commutation sur un commutateur OXC. Dans les réseaux non optiques, le mise en file d'attente est réalisée à l'aide d'une mémoire RAM (*Random Access Memory*). Chose, qu'on ne peut pas faire dans les réseaux optiques, par la limite de la technologie optique actuelle. Ceci limite la commutation dynamique dans ces réseaux. La seule façon de mettre une trame optique en file d'attente actuellement est de les convertir en paquets électroniques, de les enregistrer temporairement dans une mémoire RAM en attendant de les commuter. À la sortie du commutateur OXC, les paquets électroniques sont re-convertis en trames optiques pour être transportés aux nœuds suivants. Néanmoins, à cause de la grande différence entre la vitesse de transmission optique et la vitesse des traitements électriques, un blocage (*bottleneck*) électronique se produit.

La bande passante exigée pour une connexion à un client dans un réseau OVPN est normalement plus basse que la capacité de transport d'un canal optique OC (*Optical Channel*). Pour exploiter efficacement la bande passante des canaux optiques, un canal optique peut être partagé sur plusieurs connexions. La technique de combinaison des flux de trafic en basse bande passante dans un flux de trafic à haute bande passante s'appelle le *grooming*[3] de trafic (Traffic Grooming) [30]. Dans les réseaux non optiques, un réseau d'infrastructure est vu comme un réseau d'autoroutes où des paquets peuvent, comme les voitures, entrer ou sortir en nombre qui n'est pas limité d'avance. Bien sûr, quand le nombre de paquets est plus élevé que la capacité du réseau, un blocage se produit. Dans ces cas, certains paquets sont enlevés et des demandes de retransmission des paquets perdus sont émises. À l'opposé, un canal optique (concrètement, un *ligthpath*) est plutôt vu comme un train ayant

---

[1] Un chemin optique doit employer la même longueur d'onde sur tous les liens le long de son chemin, du nœud de source au nœud de destination.

[2] Tous les chemins optiques employant le même lien (fibre) doivent recevoir des longueurs d'onde distinctes.

[3] Nous n'avons pas trouvé le mot français correspondant à « grooming ». Alors nous l'utilisons directement en anglais.

plusieurs wagons (qui sont les intervalles de temps). Le partage d'un chemin optique entre plusieurs connexions correspond alors à l'inscription d'un ou plusieurs intervalles de temps sur une longueur d'onde donnée pour chaque connexion. La position des intervalles de temps sur une longueur d'onde est importante. Sur chaque nœud intermédiaire, la position des intervalles de temps d'une connexion peut être changée sur la même longueur d'onde ou sur les longueurs d'onde différentes si les échangeurs d'intervalles de temps et les convertisseurs des longueurs d'onde sont adéquatement équipés. La technique de *grooming* de trafics est alors considérée comme un problème de planifications des intervalles de temps d'une longueur d'onde pour des connexions et de commutation des intervalles de temps pour une connexion sur chaque commutateur OXC.

1.5. Objectifs du projet de recherche

On voit des analyses précédentes que le réseau OVPN est important pour interconnecter des sites de clients en partageant la bande passante disponible d'un réseau d'infrastructure optique. Cependant, il existe des différences considérables entre les techniques de transport optique et non optique. Une transformation des modèles VPN non optiques en modèles VPN optiques est donc complexe. En outre, des limitations dans la technologie optique actuelle augmentent les difficultés d'une telle transformation. La définition d'une architecture OVPN complète est alors nécessaire pour supporter des services OVPN.

Les objectifs de notre projet de recherche sont :

1. ***Concevoir une architecture OVPN complète***. Un réseau OVPN complet se compose d'un ensemble de connexions d'accès entre les sites des clients et un réseau de fournisseurs ainsi qu'un ensemble de connexions internes dans le réseau du fournisseur. La concaténation des connexions d'accès et des connexions internes, le triplet (connexion d'accès, connexion interne, connexion d'accès), forme un ensemble de liens virtuels qui interconnectent les sites des clients participants dans le réseau OVPN. Le modèle VPN proposé est basé sur le contrôle et la gestion par le fournisseur, alors il est totalement transparent pour le client.
2. ***Optimiser l'exploitation et l'utilisation efficace des chemins optiques***. L'exploitation et l'utilisation efficace des chemins optiques dans le réseau de fournisseurs est un critère important dans l'architecture OVPN proposée et c'est la technique de *grooming* de trafics qui sera appliquée dans ce modèle. Dans la carde de notre projet de recherche, la technique TG se compose de la planification et de la commutation des trafics. Le but est l'optimisation de l'utilisation des ressources qui consiste à minimiser le nombre de canaux optiques utilisés et à maximiser la bande passante utilisée de chaque canal optique.
3. ***Appliquer la technologie multiagents dans l'architecture OVPN***. L'établissement des connectivités entre des sites de client aussi bien que l'optimisation de la technique TG dans l'architecture OVPN ne sont pas seulement le résultat des efforts chaque nœud individuel, mais aussi la coopération et la

coordination des nœuds entre eux. En considérant leur comportement, il y a un lien conceptuel important entre l'architecture OVPN et les systèmes multiagents. Un nouveau point important pour notre proposition est donc l'intégration de la technologie multiagents dans l'architecture OVPN. Ceci permet un contrôle et une gestion des réseaux OVPN qui soit plus intelligente, plus flexible et plus dynamique. La technologie multiagents est aussi prouvée dans l'optimisation de la technique TG.

4. ***Développer une application spécifique pour notre architecture OVPN***. Une application proposée pour notre architecture OVPN est l'interconnexion des stations du réseau sans fil par le réseau optique. En effet, puisque le nombre d'utilisateurs des services sans fil (comme des téléphones cellulaires ou des ordinateurs portables munis de cartes sans fil (*wireless*)), tout comme le nombre de services de transport sans fil, augmentent de plus en plus rapidement, le besoin de bande passante est alors de plus en plus critique et demande aux chercheurs en télécommunications de proposer des solutions. En profitant de la capacité de bande passante du réseau optique, l'interconnexion des stations des réseaux sans fil par le réseau optique est faisable dès maintenant. Notre architecture OVPN montrera une solution efficace pour l'établissement et la gestion des services de réseau intelligents, flexibles et dynamiques connectant des stations du réseau sans fil. Le document présentera une spécification de l'application du réseau OVPN dans l'interconnexion des stations de base du réseau sans fil.

1.6. Conclusion

Il est évident que la tendance actuelle est le remplacement de l'infrastructure de non optique en une infrastructure optique. Cependant, à cause des différences importantes dans les techniques de transport et des limites de la technologie optique actuelle, l'architecture et les fonctions OVPN doivent changer considérablement par rapport à l'architecture et aux fonctions VPN non optiques. Il y a déjà eu certaines propositions en vue d'une architecture OVPN, mais elles ne sont pour l'instant que des idées primitives et incomplètes. Une architecture OVPN complète sur laquelle des services OVPN puissent être fournis aux utilisateurs est vraiment nécessaire et c'est le but de la recherche présentée dans cette proposition. Dans ce projet, nous allons présenter une architecture OVPN, y compris ses opérations, en détail. Différentes techniques pour augmenter l'efficacité du service OVPN sont aussi ajoutées à l'architecture OVPN comme la technologie multiagents et l'optimisation du *grooming* de trafics. Pour prouver l'applicabilité de notre proposition, un modèle de service d'interconnexion de stations sans fil à travers un réseau OVPN sera discuté et installé.

2. Architecture, composantes et opérations OVPN

On a vu au chapitre 1 qu'un réseau VPN est un ensemble de connexions reliant les sites de clients qui veulent échanger des informations ou des données. L'établissement et la gestion des réseaux VPNs sont alors nécessaires et doivent se baser sur un cadre d'applications (*framework*) où les composantes et les opérations VPN ont été standardisées. Ce chapitre définira ainsi une architecture OVPN (une architecture VPN sur le réseau d'infrastructure optique). Les composantes de l'architecture et les opérations OVPN sont aussi décrites.

2.1. L'architecture OVPN

Comme l'architecture OVPN de référence présentée en [26], l'architecture OVPN sur le réseau optique est construite de dispositifs ONE (Optical Network Element) tel qu'illustré dans la Figure 2-1. Il y a deux types de dispositifs ONE : Les dispositifs ONE de périphérie du fournisseur (appelé routeur PE-ONE, *Provider Edge ONE*) et les dispositifs ONE dans le réseau du fournisseur (appelé commutateur P-ONE, *Provider ONE*). Les routeurs PE-ONE sont les dispositifs qui connectent aux réseaux de clients et qui ont les fonctions requises pour un VPN optique, tandis que les commutateurs P-ONE sont définis comme les commutateurs OXC (*Optical Cross-Connect*) qui ne se connectent pas directement aux sites de clients. Par conséquent, un commutateur P-ONE n'a pas besoin de sauvegarder l'état des réseaux OVPN et alors il est transparent pour le réseau OVPN.

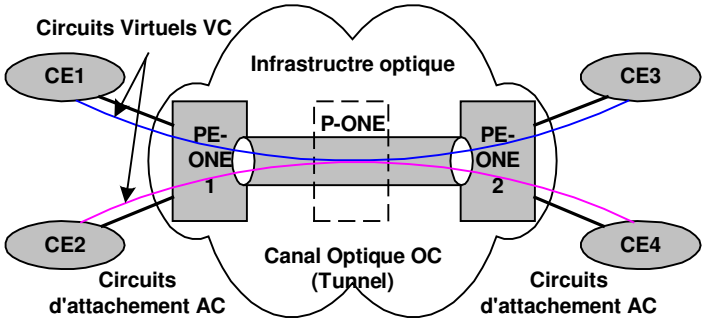

Figure 2-1 : L'architecture OVPN

Les dispositifs de périphérie du client (CE, *Customer Edge*) (ex. CE1, CE2 …) sont les dispositifs qui s'attachent aux réseaux de fournisseurs à travers des routeurs PE-ONE. Dans un réseau OVPN, les périphériques CE sont attachés aux routeurs PE-ONE par des circuits d'attachement (AC, *Attachment Circuit*). Les circuits d'attachement peuvent être des liens physiques ou logiques. Sur les réseaux de fournisseurs, les routeurs PE-ONE sont reliés ensemble par des canaux optiques (OC, *Optical Channel*). Ainsi, le rôle de chaque routeur PE-ONE est de faire correspondre (au sens de *mapping*) un circuit d'attachement à un canal optique en se basant sur de l'information locale. De cette façon, une connexion d'un périphérique CE à un autre est le

résultat d'une concaténation AC-OC-AC qui s'appelle le circuit virtuel (VC, *Virtual Circuit*). Les paquets transmis d'un périphérique CE à un autre sont alors entièrement déterminés par le circuit virtuel.

2.2. Les composantes OVPN

Dans un réseau OVPN, quand un paquet non optique arrive à un routeur PE-ONE (PE1), il est modulé en une trame optique et transportée à un autre routeur (PE2). Sur le routeur PE2, la trame optique est démodulée pour obtenir le paquet non optique original puis transféré au périphérique CE correspondant. Un tel modèle fonctionnel divise l'architecture OVPN en un ensemble de composantes fonctionnelles. Cette division permet d'exhiber les rôles joués les diverses composantes et mécanismes utilisés dans l'architecture proposée.

2.2.1. Circuits d'attachement

Dans un réseau OVPN, un périphérique CE s'attache à un routeur PE-ONE par des circuits d'attachement (AC, *Attachment Circuit*). Un circuit d'attachement peut être une ligne physique louée (tel que une ligne FR ou ATM) ou une ligne logique de couche 2 ou 3 (tel que un tunnel L2TP, un chemin MPLS LSP ou un réseau VLAN, etc.) Le périphérique CE peut être un routeur, un commutateur ou un serveur que les clients utilisent pour s'attacher à un réseau OVPN. Le rôle des circuits d'attachement est de transporter des données entre des périphériques CE et des routeurs PE-ONE.

Un flux de données traverse un circuit virtuel d'abord sur un circuit d'attachement (AC1) (d'une périphérique CE (CE1) à un routeur PE-ONE (PE1)) et ensuite sur un autre circuit d'attachement (AC2) (d'un autre routeur PE-ONE (PE2) à une autre périphérique CE (CE2)). Par rapport à un flux de données spécifiques, le premier circuit d'attachement s'appelle le circuit d'attachement d'entrée (IAC, *Ingress AC*) et le dernier circuit d'attachement est appelé le circuit d'attachement de sortie (EAC, *Egress AC*). Cette notion de circuit d'attachement d'entrée ou de sortie est relative à un flux de données spécifiques et ne dénote que la direction du flux au cours d'un transport.

Les circuits d'attachement participent à la construction des circuits virtuels entre deux périphériques CE. Les circuits d'attachement sont identifiés par leur identificateur « AC id » qui est unique pour chaque routeur PE-ONE, mais pas nécessaire unique par rapport à d'autres routeurs PE-ONE. Dans le réseau de fournisseur, chaque circuit d'attachement est alors identifié par un duplex « PE-ONE address, AC id ». Les routeurs PE-ONE distribuent automatiquement ses identificateurs AC (*AC id*) à d'autres routeurs PE-ONE pour établir des circuits virtuels. Le protocole utilisé pour la distribution des identificateurs est le protocole LMP [20].

2.2.2. Canaux optiques

Si un circuit d'attachement est utilisé pour transporter des données d'un périphérique CE à un routeur PE-ONE et vice versa, un canal optique s'emploie à transporter des trames optiques entre des routeurs PE-ONE. Un canal optique est conçu comme un tunnel entre deux routeurs PE-ONE dans le réseau de fournisseur. Avec la technique TDM (*Time Division Multiplexing*), un intervalle de temps (*time-slot*) sur une longueur d'onde est

considéré comme l'unité la plus petite pour porter des données. Alors, le volume le plus petit d'un canal optique est un intervalle de temps (ex. OC1). Un canal optique peut être composé d'un ensemble d'intervalles de temps sur une longueur d'onde, d'une longueur d'onde entière, d'une gamme d'onde ou d'une fibre optique au complet.

La location et la maintenance des canaux optiques est le travail des routeurs PE-ONE. L'information sur l'état d'un canal optique particulier est maintenue sur deux routeurs PE-ONE, qui sont ses terminaux, mais pas chez d'autres routeurs PE-ONE et pas non plus dans les dispositifs P-ONE. D'un routeur PE-ONE, il est possible d'établir plusieurs canaux optiques séparés vers d'autres routeurs PE-ONE. De même, entre deux routeurs PE-ONE, il est possible d'établir plus d'un canal optique. Les canaux optiques alors sont distingués par leur identificateur « OC id ». En effet, un canal optique est caractérisé par sa fibre, sa gamme d'onde (*waveband*), sa longueur d'onde et son groupe d'intervalles de temps sur la longueur d'onde. L'identificateur complet d'un canal optique est alors représenté par le n-tuplet « fibre id, waveband id, wavelength id, group de time-slots ».

Une propriété intéressante du canal optique est la capacité d'emboîtement : les canaux optiques de faible bande passante sont emboîtés dans un canal optique de bande passante élevée. Par exemple, les canaux optiques au niveau des intervalles de temps ayant la même longueur d'onde peuvent être emboîtés dans un canal optique au niveau de la longueur d'onde. À son tour, les canaux optiques au niveau de la longueur d'onde peuvent être emboîtés dans un canal optique au niveau de la fibre. Cette technique d'emboîtement des flux de trafic s'appelle la tunnellisation optique.

La technologie de tunnellisation utilisée dans le réseau optique se base sur le protocole GMPLS [18]. Dans le protocole GMPLS, tout ce qui peut identifier uniquement de chaque flux de trafic peut servir d'étiquette. L'étiquette utilisée pour la commutation optique peut être alors une fibre, une longueur d'onde, un groupe de longueurs d'onde (*waveband)* ou un intervalle de temps. En conséquence, les dispositifs ONE doivent avoir la structure adéquate pour commuter différentes quantités de flux de trafic.

Il est possible d'établir des canaux optiques multiples entre deux routeurs PE-ONE. Dans ce cas, il est souhaitable d'assigner un flux de trafics particuliers à un canal optique particulier à partir des caractéristiques particulières du flux de trafics et/ou du canal optique. Par exemple, des canaux optiques différents peuvent être associés à différentes qualités de service (QoS) et les flux de trafics différents exigent différents niveaux de QoS. La classification des différents QoS du canal optique est présentée dans [28].

2.2.3. Circuits virtuels

Dans un réseau OVPN, un flux de données doit d'abord passer sur un circuit d'attachement d'entrée (AC1), puis sur un canal optique (OC), enfin sur un circuit d'attachement de sortie (AC2). La concaténation de ces trois éléments (AC1, OC, AC2) produit un lien logique qui connecte directement deux sites de clients. Ce lien logique s'appelle le circuit virtuel (VC, Virtual Circuit). Ainsi, l'identification d'un circuit virtuel est déterminée par un triplet (circuit d'attachement d'entrée, canal optique, circuit d'attachement de sortie).

Un circuit virtuel est établi par une mise en correspondance (*mapping*) d'un circuit d'attachement d'entrée avec un canal optique sur un routeur PE-ONE et une autre mise en correspondance du canal optique avec un circuit d'attachement de sortie sur un autre routeur PE-ONE. Si les circuits d'attachement sont de la même technologie (comme les deux ATM, Ethernet ou FR), le canal optique fournit un transport homogène; autrement il fournit un transport hétérogène. Un exemple de transport hétérogène est le suivant : si un périphérique CE1 s'attache à un routeur PE1 par le protocole ATM, mais le périphérique CE2 attache au routeur PE2 par le protocole FR, alors le routeur PE1 doit fournir une fonction d'encapsulation du protocole ATM dans le protocole FR en transportant des données du routeur PE1 au routeur PE2. De telles techniques d'encapsulation ne sont pas l'objet de ce document.

2.2.4. Routeur PE-ONE

Dans l'architecture OVPN, le seul routeur PE-ONE possède les fonctions OVPN telles que l'allocation de circuits d'attachement, la location de canaux optiques, la mise en correspondance (*mapping*) d'un canal optique avec une paire de circuits d'attachement pour produire un circuit virtuel et la tunnellisation des circuits virtuels à travers le réseau du fournisseur. Les objets à gérer sur un routeur PE-ONE sont alors des circuits d'attachement et des canaux optiques.

L'assignation de l'identificateur pour déterminer de façon non ambiguë des circuits d'attachement et des canaux optiques est des plus importantes. Comme nous l'avons décrit précédemment, un circuit d'attachement est identifié par une étiquette « AC id » et un canal optique « OC id ». L'identificateur d'un circuit d'attachement ou d'un canal optique doit être unique sur chaque routeur PE-ONE, mais pas nécessairement pour les autres routeurs PE-ONE. Alors, dans un réseau OVPN, l'adresse du routeur PE-ONE est ajoutée comme préfixe de l'identificateur de chaque circuit d'attachement ou canal optique : « PE-ONE adr, AC id » et « PE-ONE adr, OC id ». Dans le cas où il faudrait distinguer des circuits d'attachement et des canaux optiques dans les réseaux OVPN différents, l'identificateur du réseau OVPN est ajouté : « OVPN id, PE-ONE adr, AC id » et « OVPN id, PE-ONE adr, OC id »

La détermination d'un canal optique correspondant à une paire de circuits d'attachement dépend de la bande passante des circuits d'attachement. Normalement, un canal optique correspondant à un intervalle de temps (la bande passante la plus petite) est sélectionné pour une paire de circuits d'attachement, parce que la bande passante demandée pour une connectivité de clients dans un réseau OVPN est souvent inférieure de la capacité d'un intervalle de temps. Cependant, si le routeur PE-ONE est capable de multiplexer des circuits d'attachement dans un intervalle de temps, alors le canal optique correspondant à l'intervalle de temps devient un tunnel qui port des circuits virtuels ayant les mêmes extrémités.

2.3. Les opérations OVPN

Sur un réseau optique, un ou plusieurs canaux (optiques ou non optiques) sont réservés pour le contrôle et la gestion de la transmission des données. Ces canaux s'appellent « canaux de contrôle ». Un canal de contrôle peut être intrabande (*in-band*) ou hors bande (*out-of-band*) (selon que les signaux de contrôle et les données sont transportées sur la même ligne physique ou non). Avec la technique GMPLS, les canaux de contrôle entre deux nœuds adjacents n'utilisent plus la même ligne physique que la ligne de données. Par exemple, un canal de contrôle peut être une longueur d'onde, une fibre, un lien Ethernet ou un tunnel IP. De nouvelles techniques pour l'établissement et la gestion des lignes de données ont été aussi développées (comme le protocole LMP [20]).

Similairement, l'établissement, la gestion et la maintenance des circuits virtuels dans des réseaux OVPN sont réalisés à partir des canaux de contrôle. Les circuits virtuels connectent des sites de clients dans un réseau OVPN sont des triplets de « AC, OC, AC ». Les opérations nécessaires pour l'architecture OVPN sont alors la découverte automatique ou « auto-découverte » de la topologie, l'allocation des circuits d'attachement, la location des canaux optiques et la maintenance des circuits virtuels.

2.3.1. Auto-découverte de la topologie

L'auto-découverte de la topologie est importante pour l'établissement et la gestion des circuits virtuels dans l'architecture OVPN. C'est un processus automatique qui crée la topologie virtuelle entre des routeurs PE-ONE participant à un réseau OVPN. Quand un nouveau routeur PE-ONE participe à un réseau OVPN, un processus d'auto-découverte se produit pour annoncer aux autres routeurs PE-ONE, sa participation au réseau et, en même temps, demander des informations nécessaires de ces autres routeurs PE-ONE. Le processus peut être établi par l'échange de messages « *Config* » du protocole LMP [20]. Le scénario d'un processus d'auto-découverte est illustré dans la Figure 2-2.

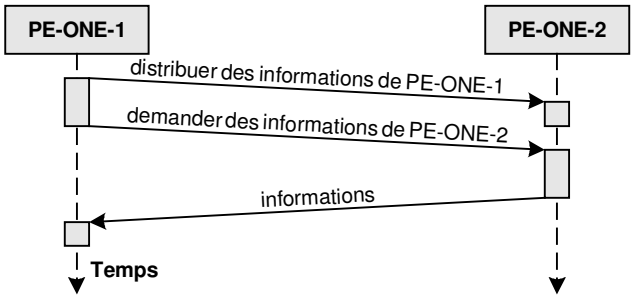

Figure 2-2 : Scénario de l'auto découvert de la topologie

2.3.2. Allocation des circuits d'attachement

Dans la plupart des cas, l'allocation des circuits d'attachement AC (*Attachment Circuits*) a lieu individuellement sur le routeur PE-ONE. Ce sont les cas où la technique d'attachement « CE, PE-ONE » est

différente de la technique de transport sur les réseaux de fournisseurs. Par exemple, des lignes FR ou ATM sont la technique d'attachement « CE, PE-ONE », tandis que le transport de données dans les réseaux de fournisseurs est entièrement optique sur des canaux optiques. On a un autre cas lorsque les circuits d'attachement sont précisés par des paramètres spécifiques comme la qualité de service (QoS), la garantie de largeur de bande, etc. Différents types de circuits d'attachement sont alors distingués. La Figure 2-3 illustre le scénario de l'allocation des circuits d'attachement.

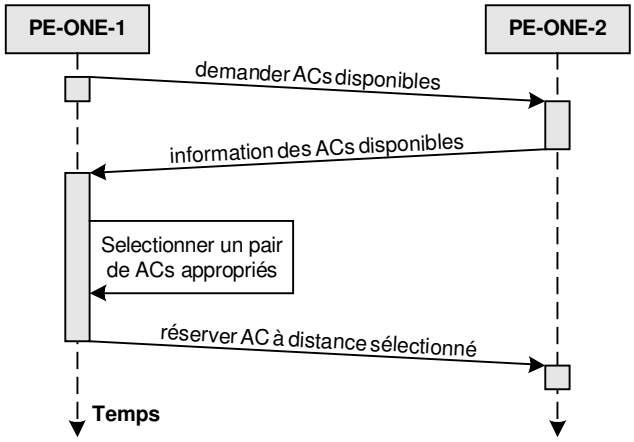

Figure 2-3 : Scénario de l'allocation des circuits d'attachement

Il y a également des cas où l'allocation des circuits d'attachement ne doit pas être établie individuellement. Par exemple, si un circuit d'attachement est aussi un canal optique, les circuits d'attachement pourraient être installés à la suite de l'installation d'un canal optique, plutôt qu'être fournis auparavant. Dans ces cas, le circuit virtuel est considéré comme un canal optique CE-CE.

2.3.3. Location de canaux optiques

Un fournisseur de services réseau peut posséder des ressources optiques; il peut alors établir des canaux optiques pour interconnecter des routeurs PE-ONE participant à un réseau OVPN. Cependant, le problème de signalisation et de configuration d'un canal optique n'est pas l'objectif de cette thèse. Nous considérerons que les canaux optiques utilisés sont loués d'un quelconque fournisseur de ressources optiques. La location d'un canal optique dépend des caractéristiques (comme la bande passante, la qualité de service, etc.) des deux circuits d'attachement aux extrémités du canal optique. Un canal optique peut être loué sur la base d'un ensemble de circuits virtuels. Dans ce cas, la bande passante du canal optique loué doit être capable de porter tous les circuits virtuels.

Les informations échangées entre deux routeurs PE-ONE qui se connectent par un canal optique se composent de :

- L'identificateur du circuit d'attachement local auquel le canal optique doit être lié.

- L'identificateur du circuit d'attachement distant auquel le canal optique doit être lié.
- Les caractéristiques du canal optique (comme la qualité de service, la bande passante etc.)

L'identificateur sélectionné pour échanger entre deux routeurs PE-ONE doit faire sens au routeur PE-ONE distant et peut être transféré par le protocole de signalisation pour permettre au routeur PE-ONE distant de lier le canal optique à un circuit d'attachement approprié. Celui-ci peut être l'identificateur du canal optique ou l'identificateur du circuit d'attachement distant. Si on emploie l'identificateur du canal optique, celui-ci doit être unique à chacun de deux routeurs PE-ONE. Si on utilise plutôt l'identificateur du circuit d'attachement, celui-ci se doit seulement être unique au routeur PE-ONE distant.

2.3.4. *Grooming* de circuits virtuels

Le transport de données dans le réseau d'infrastructure optique est organisé en hiérarchie où les flux de trafics de basse bande passante sont combinés dans un flux de trafics de bande passante élevée. Selon la définition de [30], cette technique s'appelle *grooming* des trafics. Le but de la technique de *grooming* est d'exploiter efficacement la capacité de bande passante des longueurs d'onde et ainsi réduire le coût d'utilisation du réseau.

Dans l'architecture OVPN, les circuits virtuels qui sont dans le même réseau OVPN et qui ont les mêmes extrémités sont combinés dans le même tunnel en transmettant à travers un réseau d'infrastructure optique. Cependant, les circuits virtuels de différents réseaux OVPN qui ont les mêmes extrémités peuvent aussi être combinées dans le même tunnel. Dans ce cas, l'identificateur des circuits virtuels se compose de l'identificateur du réseau OVPN et de l'index du circuit virtuel dans le réseau OVPN : « OVPN id, VC idx ». Notez que l'identificateur du réseau OVPN est unique pour chaque routeur PE-ONE.

La technique de *grooming* peut être généralisée sous des formes différentes. Dans ce document, la technique de *grooming* est considérée comme la planification des circuits virtuels VC dans quelques canaux optiques OC et la commutation des circuits virtuels sur chaque nœud. Le but principal de la technique est de réduire le coût de service, d'optimiser l'utilisation de bande passante et d'augmenter la qualité de service. L'optimisation de la technique TG est présentée dans le chapitre 4.

2.3.5. Maintenance des circuits virtuels

La maintenance des circuits virtuels dans un réseau OVPN est réalisée par l'envoi périodique de messages « *Hello* » d'un routeur PE-ONE aux autres routeurs PE-ONE ou aux périphériques CE pour vérifier si la connexion est bien en fonction ou non (Figure 2-4). Cette technique s'appelle la technique « *Keep-live* ». Un circuit virtuel est en bon état si l'émetteur (un routeur PE-ONE) reçoit périodiquement des messages de réponse d'un autre routeur PE-ONE. Si un dépassement de temps (*time-out*) apparaît, il y a alors une interruption sur le circuit virtuel concerné.

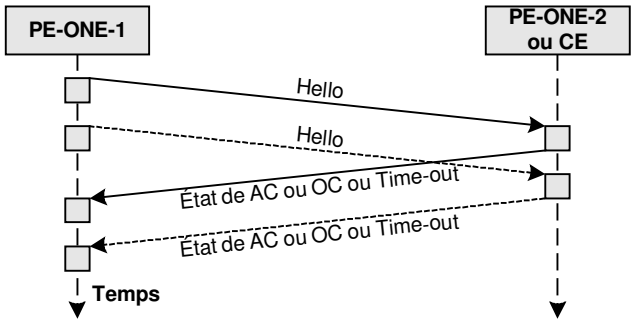

Figure 2-4 : Scénario de la maintenance de circuits virtuels

La interruption d'un circuit virtuel peut être causée par l'interruption d'un de deux circuits d'attachement ou du canal optique. Dans ce cas, un circuit d'attachement ou un canal optique est rétabli pour remplacer celui qui est interrompu. Cependant, si les ressources appropriées ne sont pas disponibles, un nouveau circuit virtuel peut être établi pour remplacer celui qui est coupé. En tant que telles, les techniques de restauration ne sont pas l'objet de ce document.

2.4. Conclusion

Ce chapitre a présenté une architecture VPN générale sur le réseau d'infrastructure optique (OVPN). C'est un réseau VPN basé sur le fournisseur; le fournisseur étant responsable de gérer et de contrôler toutes les fonctions OVPN. Seuls les routeurs PE-ONE dans le réseau de fournisseur ont les fonctions OVPN. De plus, nous avons vu qu'un réseau OVPN est un ensemble de connexions reliant les sites de clients qui participent à un réseau OVPN. De ce point de vue, les composants d'un réseau OVPN qui doivent être gérées sont les circuits d'attachement, les canaux optiques et les circuits virtuels. Les opérations nécessaires sont l'auto-découverte de la topologie, l'allocation des circuits d'attachement, la location des canaux optiques et la maintenance des circuits virtuels. Cependant, les descriptions précédentes sont encore formelles et brutes. Des définitions plus fines de ces fonctions et opérations internes sont présentées dans le chapitre suivant.

3. Technologie multiagents dans l'architecture OVPN

L'application de la technologie multiagents aux réseaux privés virtuels n'est pas nouvelle. Dans le projet EUREOSCOM et ACTS MIAMI [40], la technologie multiagents a été utilisée pour automatiser la négociation des ressources de réseau en répondant aux demandes de connexions temporaires de l'utilisateur. Dans ces projets, trois types agents sont considérés : les assistants de client (agents PCA), les fournisseurs de services de réseau (agents SPA) et les fournisseurs de ressources de réseaux (agents NPA). Les agents PCA assistent les utilisateurs dans la recherche et la sélection des offres de services de réseau de la part des agents SPA. Les agents SPA déterminent ensuite les services requis puis recherchent et sélectionnent des offres de ressources réseau de la part des agents NPA. La négociation automatique entre ces agents permet d'établir un réseau VPN entre les utilisateurs.

Contrairement au modèle d'agent précédent, l'intégration de la technologie multiagents dans notre architecture OVPN se fera dans le modèle fonctionnel interne du système de services OVPN. Pour offrir des services OVPN multiples, un routeurs PE-ONE peut participer à plusieurs différents réseaux OVPN. Cependant, ceci peut causer une ambiguïté dans la gestion de l'espace d'adressage ou dans la numérotation des éléments (tels que les circuits virtuels, les canaux optiques, etc.). Nous avons proposé dans l'article [29] une utilisation de routeurs virtuels (VR, *Virtual Router*) pour gérer et contrôler séparément d'un routeur PE-ONE qui est partagé à différents réseaux OVPN. Les routeurs virtuels communiquent et coopèrent ensemble pour établir et maintenir des connexions appartenant aux différents réseaux OVPN. En nous basant sur leur fonctionnement, nous pouvons constater que le système de fourniture de services OVPN a un rapport avec un système multiagent. L'intégration de la théorie des systèmes multiagents dans l'architecture OVPN va permettre de profiter de leurs avantages tels que les techniques de communication, de coordination, etc. Ainsi, les services OVPN offerts seront plus flexibles et plus efficaces.

3.1. Théorie des systèmes multiagents

Un système multiagents peut être considéré comme un groupe d'agents interactifs travaillant ensemble pour réaliser un ou plusieurs objectifs. Pour maximiser l'efficacité du système, chaque agent doit pouvoir raisonner au sujet des actions des autres agents en plus de ses propres actions. Un environnement dynamique et imprévisible crée le besoin pour qu'un agent utilise des stratégies flexibles. Cependant, plus les stratégies sont flexibles, plus il est difficile de prévoir ce que des autres agents vont faire. Pour cette raison, des techniques de communication et de coordination ont été développées pour aider les agents interactifs effectuant des actions complexes qui exigent un travail d'équipe. Ces techniques doivent s'assurer que les plans des différents agents n'entrent pas en conflit, en guidant les agents dans la poursuite des buts du système.

L'agent est l'élément le plus important dans un système multiagents. Une définition plus compréhensive des agents (donné par Wooldridge et Jennings (1995)) [39] est qu'un « agent est une composante matérielle ou, plus habituellement, un système informatique basé sur logiciel, qui a les propriétés suivantes: *Autonomie* - les agents fonctionnent sans intervention directe des humains ou des autres agents et sont capables de contrôler leurs actions et états internes; *Capacités sociales* - les agents interagissent avec d'autres agents (peut-être humains) par divers types de langage de communication; *Réactivité* - les agents perçoivent leur environnement et répondent de façon opportune aux changements; *Proactivité* les agents n'agissent pas simplement en réponse à leur environnement, ils peuvent exhiber le comportement dirigé vers un but en prenant l'initiative ». La Figure 3-1 illustre l'architecture de base d'un agent. Les flèches y montrent des flux de données. Les capteurs reçoivent les entrées de l'environnement et fournissent des données au composant cognitif, lequel calcule et décide quelles actions exécuter pour enfin commander aux effecteurs d'exécuter les actions.

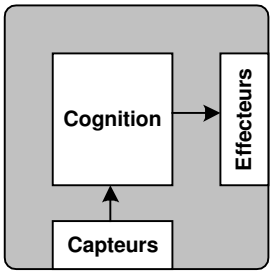

Figure 3-1 : L'architecture de base d'un agent

Deux tendances principales dans la définition des agents sont identifiées. Certains chercheurs considèrent et définissent l'agent en isolation, alors que d'autres les conçoivent principalement comme des entités agissant en relation avec d'autres agents, d'où le paradigme des systèmes multiagents. On peut également identifier une vaste catégorie d'agents; mais les plus populaires maintenant sont l'agent d'information et l'agent personnel (tous des agents logiciels). Un agent d'information est un agent qui a accès à une ou plusieurs sources d'information, qui peut les rassembler, les filtrer, choisir l'information appropriée sur un sujet et présenter cette information à l'utilisateur. Les agents personnels (ou agents d'interface) sont des agents qui agissent en tant qu'assistant personnel à l'utilisateur, pour faciliter des tâches pénibles comme le filtrage et la classification des e-mails, pour interagir entre l'utilisateur et le système d'exploitation, pour gérer la planification des activités quotidiennes, etc.

Il y a deux approches principales pour concevoir les agents [39]: l'approche traditionnelle « *top-down* » et, plus récemment, l'approche « *bottom-up* ». Les agents construits selon ces approches s'appellent souvent l'agent *délibératif* et *réactif* respectivement. La caractéristique principale de l'approche traditionnelle est que les capacités cognitives (perception, modélisation du monde, planification du projet, etc.) sont modulaires. Ainsi, la capacité cognitive de l'agent est fonctionnellement décomposée. De cette façon, on peut commencer par la conception de l'architecture globale de l'agent, pour ensuite développer séparément les différentes composantes. D'autre part,

selon l'approche « *bottom-up* », on devrait commencer par installer les comportements simples de l'agent, en couvrant la gamme complète de la perception à l'action, puis ajouter de façon incrémentale des comportements plus sophistiqués. Ainsi, la modularité comportementale est employée, au lieu de la modularité fonctionnelle.

3.2. Une architecture OVPN intégrant la technologie multiagents

Sur le plan du comportement, la technologie multiagents et l'architecture OVPN sont étroitement liées entre elles. Les agents peuvent améliorer le fonctionnement d'un réseau OVPN et, également, l'architecture OVPN peut être un environnement dans lequel des capacités des agents sont pleinement utilisées. On peut dire que la technologie multiagents est le point de croisement où l'intelligence artificielle et les systèmes distribués se rencontrent [38]. Les agents sont capables d'exécuter une gestion dynamique d'un réseau OVPN dans laquelle les routeurs PE-ONE (nos agents) se comportent intelligemment (négocier, apprendre, prévoir, coopérer, etc.) de façon à optimiser les fonctions OVPN.

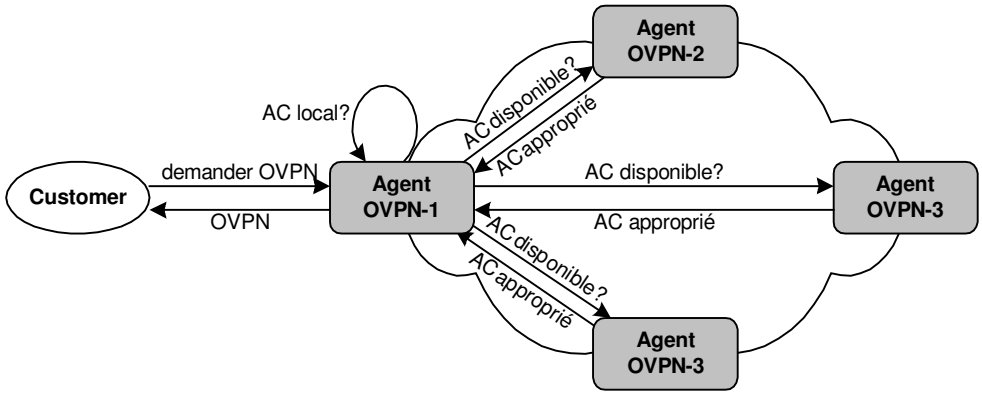

Figure 3-2 : Un exemple de la communication et la coordination des OVPN-agents

La Figure 3-2 montre comment une solution peut être trouvée pour un problème spécifique en utilisant la coordination des agents. L'agent 1, après avoir reçu une demande du réseau OVPN du client, la divise en quatre plus petites tâches. La tâche 1, soit chercher des circuits d'attachement locaux appropriés, est traitée à l'interne alors que les autres sont envoyées aux agents responsables pour chercher des circuits d'attachement distants appropriés. Les résultats, les circuits d'attachement distants ainsi trouvés, sont alors envoyés à l'agent de source et une solution complète est offerte par cet agent.

L'intégration de la technique d'agent dans l'architecture OVPN se base sur l'approche descendante (*top-down*). A partir des fonctions OVPN, différents types d'agents sont définis. Ensuite les capacités cognitives sont modularisées puis localisées dans ces agents. Il y a trois types d'agents à définir sur un routeur PE-ONE: l'agent de contrôle (*Controlling Agent*) qui gère (c'est-à-dire qui ajoute ou enlève) des agents OVPN, l'agent de *grooming* (*Grooming Agent*) qui optimise la transmission des flux de trafic et enfin l'agent OVPN (OVPN Agent) qui établit et

maintient des circuits virtuels dans un réseau OVPN. La Figure 3-3 illustre l'interaction de ces agents dans un routeur PE-ONE.

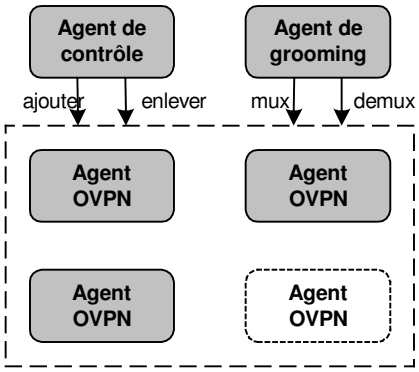

Figure 3-3 : Interaction des différents types agents sur un routeur PE-ONE

3.3. Agent de contrôle

Il n'y a qu'un seul agent de contrôle sur un routeur PE-ONE. Son rôle est de gérer des agents OVPN correspondant à différents réseaux OVPN. Quand un routeur PE-ONE participe à un réseau OVPN, l'agent de contrôle va créer un nouvel agent OVPN. Cet agent OVPN joue le rôle du routeur PE-ONE dans ce réseau OVPN. Lorsque le routeur PE-ONE veut quitter de ce réseau OVPN, l'agent OVPN est enlevé par l'agent de contrôle. Un tel modèle de fonctionnement rend l'agent de contrôle comme un agent personnel qui est sensible au changement de l'environnement (les demandes du réseau OVPN, l'état des réseaux OVPN, etc.)

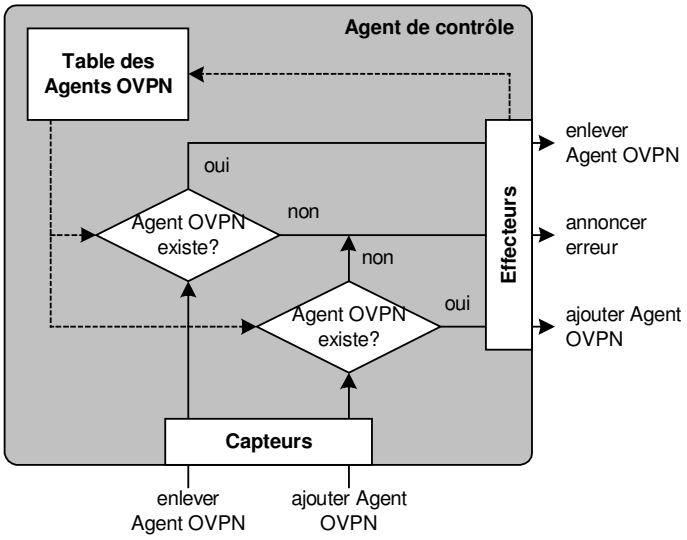

Figure 3-4 : Structure interne d'un agent de contrôle

Chaque agent de contrôle possède une table des agents OVPN. La table représente la participation du routeur PE-ONE dans différents réseaux OVPN. Lorsque le routeur PE-ONE veut participer à un réseau OVPN,

l'agent de contrôle doit vérifier si le réseau OVPN existe dans la table des agents OVPN; si non, un nouvel agent OVPN est créé. Il en est de même quand le routeur PE-ONE veut quitter un réseau OVPN : l'agent de contrôle doit aussi vérifier l'existence du réseau OVPN dans la table des agents OVPN; si oui, l'agent OVPN correspondant est enlevé.

3.4. Agent de grooming

Le transport de données dans le réseau d'infrastructure optique est hiérarchique. À l'entrée (d'un routeur PE-ONE) du réseau d'infrastructure optique, les trafics de clients sont combinés dans certains canaux optiques. Ce processus peut être répété dans le noyau du réseau d'infrastructure optique en multiplexant des canaux optiques de basse bande passante dans des canaux optiques de bande passante élevée. À la sortie du réseau d'infrastructure optique, un processus inverse est exécuté, les trafics des clients sont démultiplexés des canaux optiques. L'agent de *grooming* alors est défini pour faire de telles fonctions.

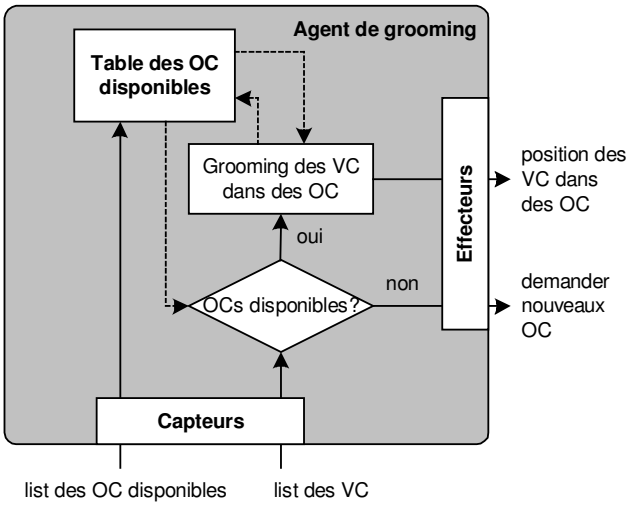

Figure 3-5 : Structure interne d'un agent de *grooming*

Dans l'architecture OVPN, un agent de *grooming* existe uniquement sur un routeur PE-ONE. Les circuits virtuels qui ont les mêmes extrémités (routeurs PE-ONE) sont multiplexés dans des canaux optiques par l'agent de *grooming*. Les circuits virtuels combinés dans le même canal optique peuvent être dans le même réseau OVPN ou non. La combinaison des circuits virtuels dans des canaux optiques peut être statique ou dynamique dépendant le changement des flux de données dans réseaux OVPN au cours du temps. Le *grooming* de trafic considéré dans ce document se compose de la planification et de la commutation des circuits virtuels qui sera décrit en détail dans le chapitre 4.

La Figure 3-5 illustre la structure interne de l'agent de *grooming*. Normalement, en se basant sur l'ensemble de circuits virtuels qui sont à multiplexer, l'agent de *grooming* va commander des canaux optiques disponibles pour *grooming*. Cependant, l'information au sujet des canaux optiques disponibles peut être récupérée d'avance

et sauvegardée dans une table des canaux optiques disponibles. Les objectifs de la technique de *grooming* est d'optimiser l'efficacité de l'utilisation de la bande passante, d'assurer la qualité de transport et de réduire le coût de service. Le coût de service considéré dans ce document (chapitre 4) se compose de le coûte d'échange d'intervalle de temps et le coût de conversion de longueur d'onde. Celui-ci dépend alors de la capacité des échangeurs d'intervalle de temps et des convertisseurs de longueur d'onde dont sont équipés les nœuds. Autrement dit, avant d'assigner un intervalle de temps à un circuit virtuel, il faut prendre en compte la stabilité du circuit virtuel (le moins échange d'intervalle de temps et le moins conversation de longueur d'onde pour ce circuit virtuel sur des nœuds intermédiaires). Ceci est résolu par la coopération et la coordination des nœuds en *grooming* (voir chapitre 4.4).

L'optimisation du *grooming* dans ce document se base sur le réseau neuronal Hopfield. Le principe de cette méthode est que la meilleure solution correspond à l'énergie minimale (voir chapitre 4.1). Comme toutes les autres méthodes d'optimisation, l'optimisation du *grooming* prend un certain temps pour trouver une solution optimale. Cependant, puisque le temps pour prendre une décision dans la planification et la commutation de trafics sur le réseau optique est limité, la décision prise est souvent approximativement optimale. Pour améliorer l'efficacité de la méthode, notre proposition dans ce cas est que l'agent de *grooming* continuera de calculer pour déterminer la solution optimale. Le résultat va être utilisé pour les prochaines fois (sans recalculer) quand le pattern de trafics (circuits virtuels) est semblable avec celui de cette fois. Ce-ci peut être vu comme la capacité d'apprentissage de l'agent de *grooming*.

3.5. Agent OVPN

Les agents OVPN sont crées, détruits et gérés par un agent de contrôle. Un agent OVPN est crée quand le routeur PE-ONE correspondant participe dans un réseau OVPN et il est enlevé lors que le routeur PE-ONE quitte du réseau OVPN en question. Le rôle des agents OVPN est de découvrir de la topologie virtuelle d'un réseau OVPN, d'établir et de maintenir l'ensemble les connexions dans un réseau OVPN. La Figure 3-6 illustre la structure interne d'un agent OVPN.

Un agent OVPN se compose de plusieurs modules internes dont chacun exprime une fonction OVPN typique. Ces modules sont responsables d'exécuter les activités internes de l'agent. La coordination des modules permet à l'agent d'accomplir les tâches exigées. Les composantes de l'agent OVPN sont illustrées dans la Figure 3-7 et leurs fonctions sont présentées dans les sections suivantes

3.5.1. Module d'auto-découverte de la topologie

Quand un agent OVPN est produit, son module d'auto-découverte distribue automatiquement aux autres routeurs PE-ONE une annonce au sujet de la participation du routeur PE-ONE actuel dans le réseau OVPN. Lorsqu'ils répondent à cette annonce, les autres routeurs PE-ONE envoient leurs informations nécessaires au

nouveau routeur PE-ONE. De cette façon, la topologie virtuelle d'un réseau OVPN est établie. Les informations partagées entre les agents OVPN sont les sites de clients connectés et les circuits d'attachement disponibles. Le processus d'auto découvert peut être exécuté par l'envoie du message « *Hello* » du protocole LMP.

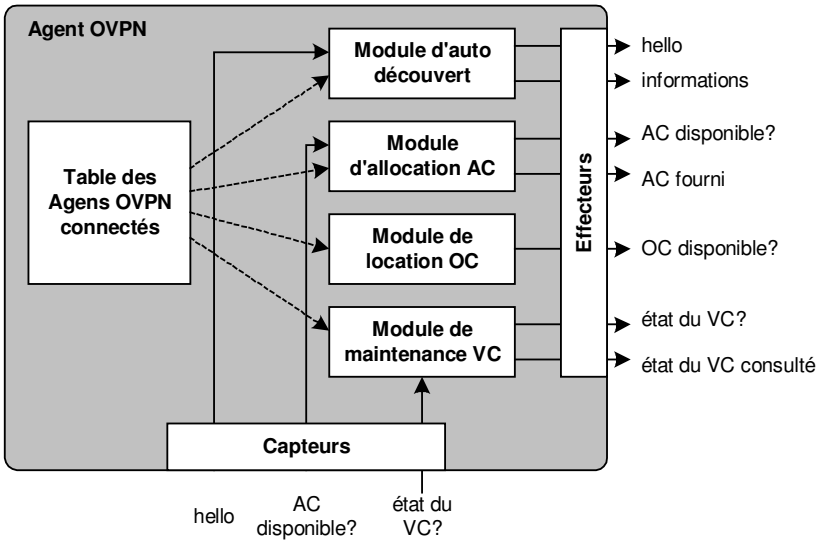

Figure 3-6 : Structure interne d'un agent OVPN

3.5.2. Module d'allocation des circuits d'attachement

Le module d'allocation des circuits d'attachement est responsable de sélectionner une paire de circuits d'attachement appropriés pour un circuit virtuel en se basant sur les informations reçues dans la phase d'auto-découverte. En réalité, de telles informations changent tout le temps parce que les circuits d'attachement peuvent être utilisés par d'autres circuits virtuels et par différents réseaux OVPN. Le module d'allocation des circuits d'attachement alors doit vérifier s'il existe un AC approprié sur un routeur PE-ONE distant et ensuite doit réserver ce circuit d'attachement.

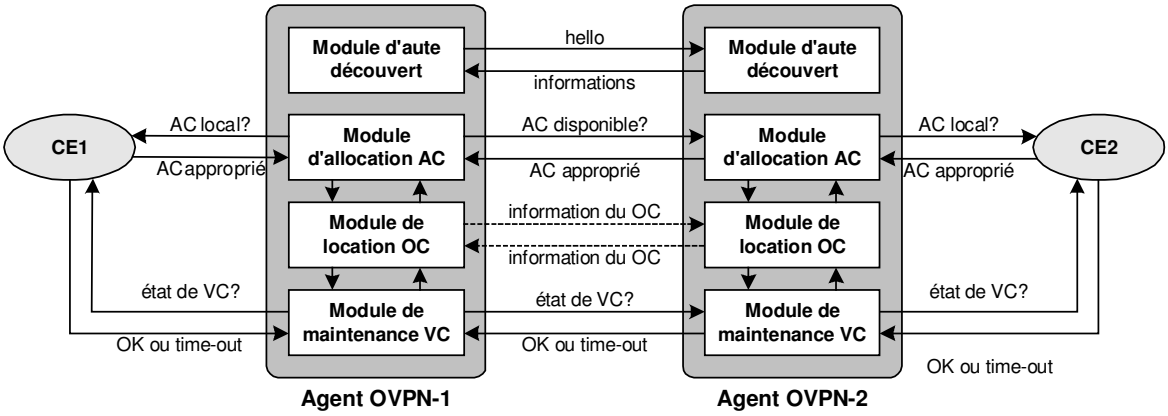

Figure 3-7 : Modules et leurs fonctions dans chaque agent OVPN

3.5.3. Module de location des canaux optiques

La détermination d'un canal optique correspondant à une paire de circuits d'attachement est le rôle du module de location des canaux optiques. Les canaux optiques utilisés pour les réseaux OVPN sont loués d'un ou de plusieurs fournisseurs de canaux optiques. La recherche et la location des canaux optiques sont le travail de l'agent de *grooming* et les informations des canaux optiques disponibles sont enregistrées dans une table des canaux optiques disponibles. Le module de location des canaux optiques contacte alors son agent de *grooming* pour déterminer un canal optique approprié pour une paire de circuits d'attachement sélectionnés. Si un canal optique approprié est trouvé, un circuit virtuel est alors établi par la concaténation deux circuits d'attachement avec le canal optique.

3.5.4. Module de maintenance des circuits virtuels

La maintenance des circuits virtuels est nécessaire dans l'architecture OVPN pour assurer la qualité de service. Puisque la ligne de contrôle et la ligne de transport des données sont physiquement distinctes, les routeurs PE-ONE utilisent normalement la technique « keep-live » pour vérifier l'état des lignes de transport des données entre eux. Dans un réseau OVPN, la maintenance de circuits virtuels est la responsabilité du module de maintenance des circuits virtuels. Le module de maintenance des circuits virtuels sur un routeur PE-ONE envoie un message « *Hello* » périodiquement au module de maintenance des autres routeurs PE-ONE. Le dépassement de temps (*time-out*) pour la réponse va indiquer qu'il y a une interruption sur le circuit virtuel concerné. La restauration du circuit virtuel coupé peut se faire être par un rétablissement de la partie interrompue (soit le circuit d'attachement ou le canal optique) ou par l'établissement d'un tout nouveau circuit virtuel.

3.6. Conclusion

Essentiellement, l'architecture OVPN est un système distribué où les routeurs PE-ONE sont des entités séparées dans le contrôle et dans la gestion. Chacun dispose de sa propre base de connaissance et peut alors prendre lui-même des décisions dans la planification ou la commutation des trafics (voir chapitre 4). Cependant, les routeurs PE-ONE peuvent travailler en groupe en établissant des circuits virtuels ou en échangeant des informations au sujet du *grooming* des trafics. Par leur fonctionnement, le rôle des routeurs PE-ONE dans une architecture OVPN est semblable avec les agents dans un système multiagents. L'utilisation de la théorie des systèmes multiagents dans la conception de l'architecture OVPN profite alors des avantages de la théorie des systèmes multiagents comme les techniques de communication et de coordination, etc. Basé ainsi sur la technologie multiagents, le réseau OVPN produit sera alors plus flexible et plus efficace.

4. Optimisation du *grooming* des trafics OVPN

La technique de *grooming* des trafics dans le réseau optique est un ensemble de méthodes qui combinent des trafics de basse bande passante dans des trafics de bande passante élevée dans le but de satisfaire certains objectifs comme la réduction du coût d'utilisation de réseau [30]. Un circuit virtuel dans un réseau OVPN peut être considéré comme un exemple du trafic de basse bande passante et les canaux optiques dans le réseau d'infrastructure comme un exemple du trafic de bande passante élevée. La technique de *grooming* peut être exprimée sous les formes différentes telle que la planification des trafics, la commutation des flux de données, la conversion de longueur d'onde ou l'échange des intervalles de temps (*time-slots*).

Avec la technique de *grooming* installée sur des routeurs PE-ONE (concrètement, sur les agents de *grooming* des routeurs PE-ONE) dans l'architecture OVPN, un ensemble de circuits virtuels arrivant à un routeur PE-ONE sont planifiés et combinés dans les canaux optiques appropriés pour aller vers d'autres routeurs PE-ONE. L'efficace du multiplexage dépend évidemment de la capacité de *grooming* des routeurs PE-ONE et à leur coopération/coordination sur le réseau d'infrastructure. La coopération et la coordination considérées dans ce document se basent simplement sur l'échange des informations de bande passante disponible entre les nœuds. Des techniques d'échanges plus complexes seront examinées dans l'avenir.

La méthode utilisée pour l'optimalisation de la planification et de la commutation des trafics est le réseau neuronal Hopfield. L'avantage des méthodes par réseaux neuronaux est la capacité de traitement en parallèle, ce qui réduit considérément le temps de calcul pour trouver une solution optimale. Cependant, à cause du temps limité pour prendre une décision dans la planification ou la commutation des trafics sur le réseau optique, les solutions *approximativement* optimales plutôt qu'optimales sont acceptables. En outre, les propositions actuelles en vue d'optimiser du *grooming* de trafics ne sont elles-mêmes qu'approximativement optimales [30]. Il existe toujours un compromis entre le temps de traitement et la découverte d'une solution optimale.

Ce chapitre va présenter deux techniques de *grooming* : la planification et la commutation de trafics. La présentation de chacune suit la démarche suivante : La formulation du problème à optimiser est d'abord décrite; une transformation des fonctions objectives en fonctions d'énergie du réseau neuronal Hopfield est ensuite exécutée; enfin, la simulation et l'analyse des résultats expérimentaux sont discutées. Cependant, le principe et l'algorithme d'optimisation du réseau neuronal Hopfield sont présentés tout d'abord.

4.1. Principe de l'optimisation par le réseau de Hopfield

Le principe d'optimisation du réseau Hopfield se base sur la minimisation d'une fonction d'énergie. Si un problème peut être représenté sous la forme d'une fonction d'énergie, avec la propriété que la meilleure solution a la plus basse énergie, alors le réseau qui correspond à la fonction d'énergie peut être utilisé pour minimiser et

fournir une solution optimale ou approximativement optimale [35]. La fonction d'énergie du réseau Hopfield se présente comme suit :

$$E = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} W_{ij} O_i O_j - \sum_{i=1}^{N} I_i O_i + \sum_{i=1}^{N} \theta_i O_i \qquad \text{Eq. 1}$$

Où E est l'énergie de réseau, W_{ij} est le poids de la connexion du nœud i au nœud j, O_i est le niveau d'activation du nœud i, I_j est l'entrée externe arrivant sur le nœud i et θ_i est le seuil du nœud i.

Sur le nœud i, le changement d'énergie après chaque cycle d'apprentissage est :

$$\Delta E_i = -\left(\frac{1}{2}\sum_{i=1}^{N} W_{ij} O_j + I_i - \theta_i\right)\Delta O_i \qquad \text{Eq. 2}$$

Où $\Delta O_i = O_i(n+1) - O_i(n)$.

Supposons que la valeur d'activation de O_i est binaire. Alors, les changements de la valeur d'activation d'un nœud (ΔO_i) sont 1, 0 ou –1. Dans le premier cas, quand la somme des entrées sur le nœud i est supérieure au seuil θ_i, la valeur d'activation du nœud i change de 0 à 1. Par l'équation Eq. 2, $\Delta E_i<0$. Dans le deuxième cas, si la valeur d'activation du nœud i ne change pas, alors $\Delta E_i=0$. Dans le dernier cas, si la somme des entrées sur le nœud i est inférieur au seuil θ_i, alors la valeur d'activation du nœud i change de 1 à 0. Par l'équation Eq. 2, encore une fois, $\Delta E_i<0$. On peut voir que la fonction d'énergie n'augmente jamais. Quand la fonction d'énergie devient stable, un niveau d'énergie minimal a été trouvé. C'est le principe d'optimisation du réseau neuronal Hopfield.

Normalement, il faut prendre un certain temps pour trouver une solution optimale, dépendant du temps de convergence du réseau neuronal Hopfield qui est utilisé. Cependant, le temps pour une décision de *grooming* dans le transport optique est limité. Alors une solution approximativement optimale est souvent acceptable. Pour améliorer l'efficacité de *grooming*, nous proposons une technique d'apprentissage pour l'agent de *grooming*: Le processus de calcul de la solution optimale continuera, bien que la décision de *grooming* a été faite sur la base d'une solution *approximativement* optimale. Mentionnons que la solution optimale trouvée sera alors utilisée pour les prochaines étapes de décision qui aura lieu quand le nouveau pattern de trafics qui arrive est semblable au pattern de trafics dont la solution a été optimisée. Cependant, cette technique n'est pas présentée dans le présent document. Elle sera considéré dans le futur.

4.2. Algorithme d'optimisation du réseau Hopfield

En se basant sur le principe d'optimisation décrit ci-dessus, l'algorithme d'optimisation du réseau neuronal Hopfield se présente donc comme suit :

1. Initier une matrice de nœuds avec le poids de connexion et le seuil de chaque nœud.

2. Au moment 0,

$$O_{ij}(0) = 0$$

où $O_{ij}(0)$ est le niveau d'activation du nœud (ij) au moment 0.

3. Au moment t (t>0), si $I_j = 1$ (il y a un trafic arrivant),

$$O_{ij}(t+1) = f_{max}(\sum_{kh} W_{ijkh} O_{kh} - \theta_{ij})$$

où

$$f_{\max} = \begin{cases} 1 & for \quad the \quad \max imal \quad activation \\ 0 & for \quad others \end{cases}$$

4. Répéter l'étape 2 jusqu'à équilibre (i.e. les niveaux d'activation du reste nœuds ne changent plus). Les patterns d'activation à équilibrage présentent alors la solution optimale au problème.

4.3. Optimisation de la planification des trafics

Dans l'architecture OVPN, chaque circuit virtuel ou chaque canal optique est caractérisé par trois attributs : la bande passante, le temps de départ (qui correspond au moment où ce circuit ou ce canal a commencé à fonctionner) et la durée de vie. Si on suppose que les circuits virtuels sont uniformes et que la capacité de bande passante de chaque canal optique est un multiple de la bande passante du circuit virtuel, alors, chaque canal optique peut être divisé (en bande passante) en plusieurs couches dont la bande passante de chacune est égale à celle de chaque circuit virtuel. Pour préciser le temps de départ et la durée de vie des circuits virtuels, chaque canal optique est divisé en périodes de temps (*time-intervals*) où un circuit virtuel est présenté comme sur une séquence de périodes de temps occupés sur un canal optique. La planification des circuits virtuels dans un canal optique est alors représentée comme l'ordonnancement des circuits virtuels dans le canal optique. La Figure 4-1 illustre un exemple où un circuit virtuel, qui commence à 0h avec une durée de vie de 3h (se terminant au début de ti3) et une bande passante de 50Mb, est planifié dans un canal optique, qui commence à 0h avec une durée de vie de 4h et une bande passante de 155Mb (OC3).

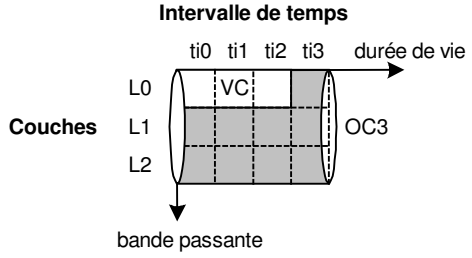

Figure 4-1 : Division d'un canal optique en couches et en périodes de temps

4.3.1. Formulation

Considérons un ensemble de N circuits virtuels VC à planifier et certains canaux optiques OC disponibles. L'état des circuits virtuels (représenté par le temps de départ et la durée de vie) est représenté par une matrice binaire *vcm*, comme dans la Figure 4-2, où chaque ligne correspond à un circuit virtuel et chaque colonne réfère à une période de temps. Dans ce cas, la matrice d'état des circuits virtuels est interprétée comme suit : vcm_{ix}=1 si la période de temps x sur la ligne i appartient à circuit virtuel VC i et vcm_{ix}=0 sinon. L'état des canaux optiques est aussi représenté par une matrice binaire *ocm* (Figure 4-3) où ocm_{jx}=1 si la période de temps x sur la couche j des canaux optiques est disponible et ocm_{jx}=0 sinon. Pour représenter le résultat de la planification, une autre matrice binaire *m* est utilisée où m_{ij}=1 si le circuit virtuel VC i est planifié dans la couche j des canaux optiques et m_{ij}=0 sinon.

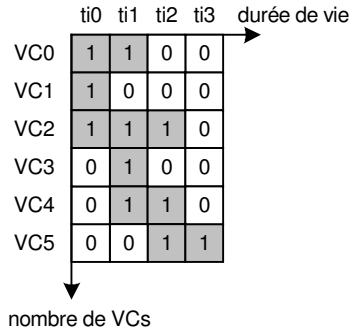

Figure 4-2: Matrice binaire des circuits virtuels

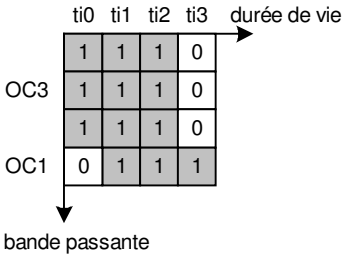

Figure 4-3: La matrice binaire des canaux optiques

L'optimisation de planification des circuits virtuels VC dans les canaux optiques est considérée comme étant la maximisation du nombre de périodes de temps occupées par les circuits virtuels sur chaque canal optique. Il nous faut donc minimiser la fonction objective suivante :

$$f = \sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix} \qquad \text{Eq. 3}$$

Avec les contraintes

1. Un circuit virtuel se situe sur une seule couche

$$\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{h=1}^{M} m_{ij} m_{i,h\neq j} = 0 \qquad \text{Eq. 4}$$

2. Les circuits virtuels situés sur la même couche ne se superposent pas

$$\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{N}\sum_{x=1}^{T} m_{ij} m_{k\neq i,j} vcm_{i,x} vcm_{k\neq i,x} = 0 \qquad \text{Eq. 5}$$

3. Les circuits virtuels planifiés doivent bien se situer dans les canaux optiques disponibles.

$$\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix}(1-ocm_{jx}) = 0 \qquad \text{Eq. 6}$$

La solution la plus simple est d'énumérer tous les cas de planification possibles et sélectionner le cas optimal. Avec N circuits virtuels VC à planifier sur M couches, il y a N^M cas possibles. Quand N et T augmentent, alors le nombre de cas de planification augmente plus rapidement. Ceci prend beaucoup de temps pour trouver une solution optimale (voir la Table 1).

4.3.2. Transformation

Pour utiliser un réseau Hopfield dans un but d'optimisation, le précédent problème de la planification des trafics doit être formulé comme une fonction d'énergie. Nous pouvons transformer une fonction objective en une fonction d'énergie par l'approche de la fonction de pénalité [36]. Alors, la fonction objective Eq. 3 et les contraintes Eq. 4 - Eq. 6 sont transformés ainsi:

$$\begin{aligned} E = &-A_1\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix} + A_2\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix}(1-ocm_{jx}) \\ &+ A_3\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{h=1}^{M} m_{ij} m_{i,h\neq j} + A_4\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{N}\sum_{x=1}^{T} m_{ij} m_{k\neq i,j} vcm_{ix} vcm_{k\neq i,x} \end{aligned} \qquad \text{Eq. 7}$$

or

$$\begin{aligned} E = &-A_1\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix} + A_2\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{x=1}^{T} m_{ij} vcm_{ix}(1-ocm_{jx}) \\ &+ A_3\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{N}\sum_{h=1}^{M} m_{ij} m_{kh} C_{ik}(1-C_{jh}) + A_4\sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{k=1}^{N}\sum_{h=1}^{M}\sum_{x=1}^{T} m_{ij} m_{kh} vcm_{ix} vcm_{kx} C_{jh}(1-C_{ik}) \end{aligned} \qquad \text{Eq. 8}$$

où C est une matrice binaire constante : C_{ik}=1 si i=k et C_{ik}=0 sinon.

Le réseau Hopfield utilisé pour l'optimisation de la planification est une matrice à deux dimensions comme dans la Figure 4-4. La ligne représente N circuits virtuels VC participant à la planification et la colonne représente M couches nécessaires pour planifier les circuits virtuels. Le nombre de couches dépend de l'intersection maximale sur une période de temps des circuits virtuels (sur une colonne). Par exemple, dans la Figure 4-3, l'intersection maximale des périodes de temps ayant la valeur 1 est 4 (sur la colonne 2). Alors, le nombre de couches nécessaires pour le processus de planification est 4.

De l'équation Eq. 8, l'extraction du poids des connexions entre les nœuds et le seuil des nœuds est :

$$\theta_{ij} = A_1\sum_{x=1}^{T} vcm_{ix} - A_2\sum_{x=1}^{T} vcm_{ix}(1-ocm_{jx}) \qquad \text{Eq. 9}$$

$$W_{ijkh} = -A_3 C_{ik}(1 - C_{jh}) - A_4 C_{jh}(1 - C_{ik}) \sum_{x=1}^{T} vcm_{ix} vcm_{kx} \qquad \text{Eq. 10}$$

La Figure 4-5 illustre un exemple d'optimisation de la planification des circuits virtuels dans les canaux optiques. Correspondant à un circuit virtuel sélectionné i pour planification, tous les nœuds sur la ligne i sont excités. Cependant, le seul nœud qui correspond à l'activation maximale est gagnant (par la contrainte 2 - Eq. 5). Quand un nœud s'active, il va alors inhiber les autres sur la même ligne. Par la contrainte 3 - Eq. 6, il est possible d'avoir plus d'un nœud activé sur une colonne; c'est-à-dire que plusieurs trafics peuvent se situer sur la même couche mais ils ne doivent pas se superposer.

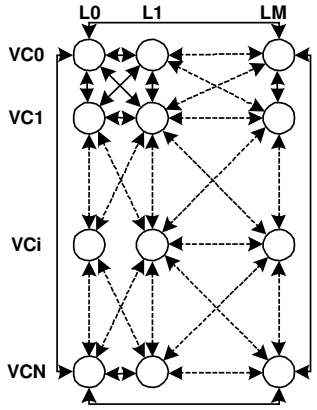

Figure 4-4: Réseau neuronal Hopfield utilisé pour la planification

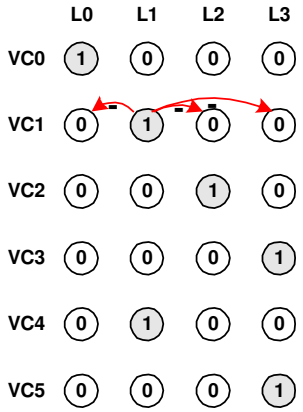

Figure 4-5 : Un exemple de la planification optimale

4.3.3. Simulation et analyse des résultats

Pour vérifier notre approche, nous avons effectué une simulation dont le code a été écrit en Java et exécuté sur un ordinateur ADM 950MHz avec 256Mb RAM.

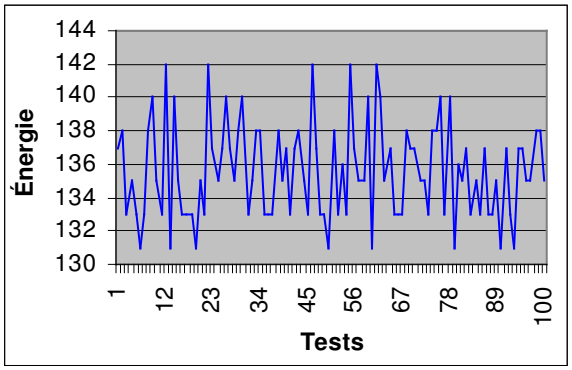

Figure 4-6: Énergie minimale trouvée du réseau Hopfield

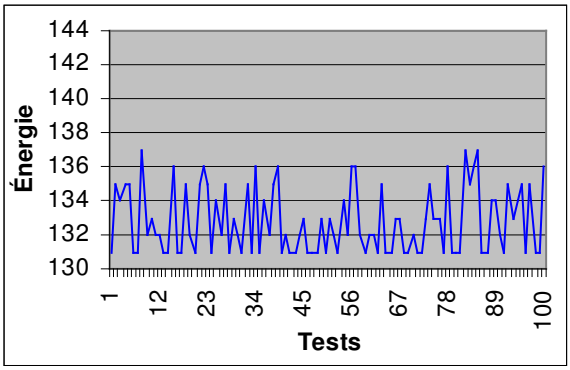

Figure 4-7: Énergie minimale trouvée de la machine Boltzmann

En utilisant le réseau Hopfield, le résultat expérimental est présenté dans Figure 4-6 : le taux d'énergie minimum atteint est 7% et l'énergie minimale moyenne est de 135.6. Ce résultat est faible car la plupart des énergies s'arrêtent sur une valeur minimale *locale*.

Pour sortir des points minimaux locaux, nous avons utilisé une machine Boltzmann qui produit des augmentations aléatoires subites. En utilisant cette machine, l'énergie atteint un taux minimal de 39% et l'énergie minimale moyenne est de 132.82 (Figure 4-7). On constate que la machine Boltzmann donne un meilleur résultat que le réseau Hopfield (Figure 4-9), mais la vitesse de convergence (réduction d'énergie) de cette machine est moins grande que celle du réseau Hopfield (Figure 4-8).

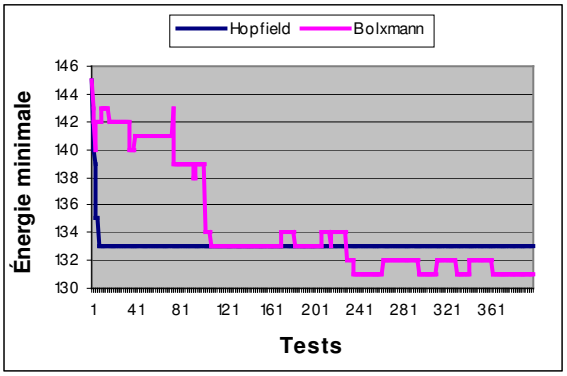

Figure 4-8 : Comparaison de la réduction de l'énergie du réseau neuronal Hopfield et de la machine Boltzmann

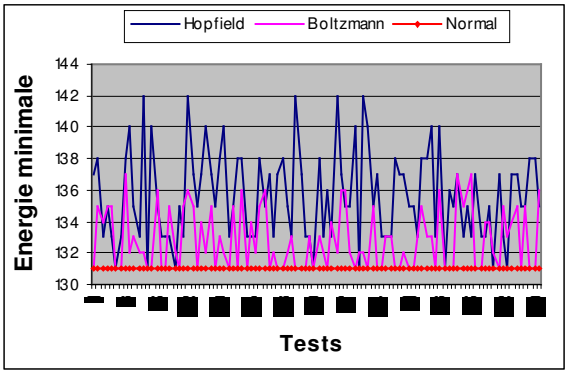

Figure 4-9 : Comparaison de l'énergie minimale trouvée de Hopfield, Boltzmann et l'algorithme simple

Pour trouver une solution optimale, la machine de Boltzmann prend plus de temps que le réseau Hopfield (Table 1). Cependant, comparativement à l'algorithme simple, le temps pour trouver une solution optimale de la machine Boltzmann est acceptable (Figure 4-10).

Dimension de trafic	Hopfield	Bolzmann	Simple
6x4	0 ms	10 ms	70 ms
10x10	10 ms	20 ms	151 ms
15x15	10 ms	661 ms	667850 ms

Table 1 : Temps pour trouver une solution optimale par rapport à la dimension de trafics

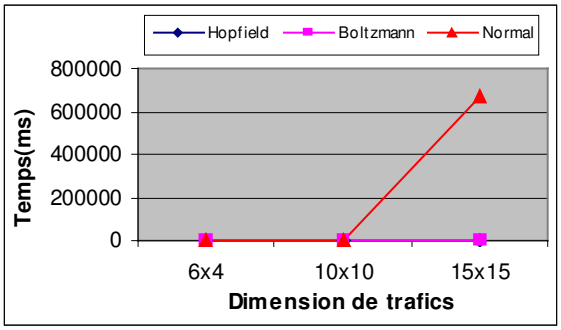

Figure 4-10: Comparaison du temps pour trouver une solution optimale

4.4. Optimisation de la commutation des trafics[4]

La capacité de la bande passante d'une longueur d'onde dans le réseau d'infrastructure optique est normalement beaucoup plus grand par rapport à celle du circuit virtuel. Pour exploiter cette capacité, une longueur d'onde est alors divisée en intervalles de temps (par la technique TDM) où chaque circuit virtuel occupe un intervalle de temps ou une séquence d'intervalles de temps.

Pour formuler le problème nous émettons les hypothèses suivantes :

- Les circuits virtuels sont uniformes.
- Chaque circuit virtuel occupe un seul intervalle de temps.
- Les dispositifs ONE sont équipés de convertisseurs de longueur d'onde et d'échangeurs d'intervalles de temps. Alors, un circuit virtuel correspondant à un intervalle de temps d'une longueur d'onde qui arrive à l'entrée d'un dispositif ONE peut être commuté sur un autre intervalle de temps d'une autre longueur d'onde à la sortie du dispositif ONE.

L'optimisation de la commutation des circuits virtuels peut alors être considérée comme étant la minimisation du nombre de longueurs d'onde utilisées et la maximisation de la bande passante utilisée par chaque longueur d'onde.

4.4.1. Formulation

Examinons un commutateur optique comme dans la Figure 4-11. Supposons qu'il y a deux ports (une d'entrée et une de sortie). Chaque port supporte W longueurs d'onde dont chacune est divisée en M intervalles de temps. Alors, le commutateur peut être représenté par N=W*M points d'accès d'entrée (IAP, Input Access Point) et N points d'accès de sortie (OAP, Output Access Point). Un trafic arrivant à un point d'accès d'entrée peut avoir plusieurs différentes possibilités de commutation au point d'accès de sortie. Il est alors important de trouver un point d'accès de sortie approprié correspondant au coût minimal (qui se compose du coût de commutation et du coût d'utilisation).

La sélection d'un point d'accès de sortie correspondant à un circuit virtuel arrivant à un point d'accès d'entrée dépend des conditions suivantes :

- Il doit être situé sur un port de sortie bien déterminée à l'avance.
- Il est disponible, c'est-à-dire qu'il n'est pas utilisé par un autre circuit virtuel.
- Il correspond au coût d'utilisation minimal.

---

[4] Cette partie a été publiée à la conférence RIVF'04, 02-05 Février 2004, Hanoi, Vietnam [34].

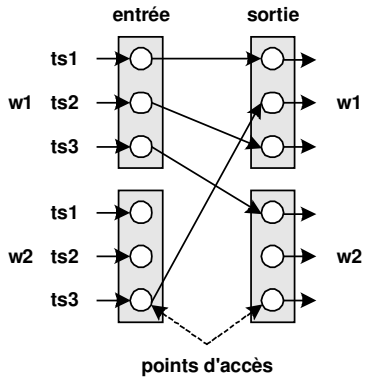

Figure 4-11: Modèle logique du commutateur optique

Le point d'accès à un port est déterminé uniquement par la position d'un intervalle de temps sur une longueur d'onde. La position du point d'accès est importante parce qu'elle montre si la commutation d'un circuit virtuel a fait l'échange entre les intervalles de temps ou/et entre les longueurs d'onde ou non. L'échange entre les intervalles de temps ou entre les longueurs d'onde dans un commutateur optique est la responsabilité des équipements particuliers : l'échangeur d'intervalles de temps et le convertisseur de longueurs d'onde. Supposons que la capacité de ces équipements est totale. Alors, un circuit virtuel arrivant à un point d'accès d'entrée peut être commuté sur n'importe quel point d'accès de sortie.

Les équipements particuliers ajoutés ont des coûts différents. Il s'ensuit que le coût de commutation du circuit virtuel varie selon que la commutation échange des intervalles de temps ou des longueurs d'onde du circuit virtuel ou non. Supposons que *fc* est le coût de commutation lorsqu'il n'y a pas d'échange d'intervalle de temps et de longueur d'onde du circuit virtuel, que *sec* est le coût de commutation pour échanger l'intervalle de temps mais pas la longueur d'onde du circuit virtuel, et que *wec* est le coût de commutation pour échanger la longueur d'onde mais pas l'intervalle de temps du circuit virtuel. Si la commutation échange à la fois l'intervalle de temps et longueur d'onde, alors le coût de commutation est *swec*=*sec*+*wec*.

Posons qu'une matrice binaire *vc* représente l'état de commutation des circuits virtuels: vc_{ij}=1 lorsqu'un circuit virtuel arrivant sur le point d'accès d'entrée i est commuté au point d'accès de sortie j. Le but est de minimiser le coût de commutation et le nombre de longueurs d'onde utilisées pour un ensemble de T de circuits virtuels qui arrivent. Il nous faut alors minimiser la fonction objective suivante :

$$f = \sum_{i=1}^{N}\sum_{j=1}^{N} vc_{ij}\delta_{ij} + \sum_{i=1}^{N}\sum_{j=1}^{N}\phi_{ij} \qquad \text{Eq. 11}$$

Où δ est une matrice constante pour le coût de commutation et ϕ est une fonction pour calculer le nombre de longueurs d'onde utilisées.

Cette fonction objective doit satisfaire les conditions suivantes :

1. Les circuits virtuels arrivant sur les points d'accès d'entrée sont tous commutés sur des points d'accès de sortie. Il est à noter que des points d'accès de sortie peuvent être disponibles ou non et qu'il est alors important de sélectionner un point d'accès de sortie disponible pour la commutation par rapport à un circuit virtuel. Pour représenter l'état disponible des points d'accès de sortie, nous utilisons une liste *d* : d_j=1 si le point d'accès de sortie j est disponible et d_j=0 sinon. Alors :

$$\sum_{i=1}^{N}\sum_{j=1}^{N} d_j vc_{ij} = T \qquad \text{Eq. 12}$$

   Il est à noter que la valeur 0 d'un élément de la liste *d* signifie que l'intervalle de temps correspondant est occupé par un circuit virtuel quelconque sur le nœud actuel ou qu'il est occupé par un autre circuit virtuel sur le (ou les) prochain(s) nœud(s). Ce dernier cas est pour éviter un échange d'intervalles de temps ou même une conversion de longueur d'onde sur le (ou les) prochain(s) nœud(s), parce que ceci augmente le coût de service. Ainsi, l'information au sujet de la bande passante disponible des canaux optiques est échangée entre les nœuds pour mettre à jour des matrices *ocm*.

2. Un circuit virtuel arrivant sur un IAP est commuté à un seul point d'accès d'entrée.

$$\sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{h=1}^{N} vc_{ij} vc_{i,h\neq j} = 0 \qquad \text{Eq. 13}$$

3. Il n'existe pas deux circuits virtuels arrivant sur deux différents points d'accès d'entrée et qui sont commutés sur un même point d'accès de sortie.

$$\sum_{i=1}^{N}\sum_{k=1}^{N}\sum_{j=1}^{N} vc_{ij} vc_{i\neq k,j} = 0 \qquad \text{Eq. 14}$$

La solution la plus simple pour l'optimisation de la commutation est d'énumérer tous les cas de commutation possibles et de sélectionner le cas correspondant au coût minimal de commutation et au nombre minimal de longueurs d'onde utilisées. Avec T circuits virtuels arrivant sur N points d'accès d'un commutateur, il y a N*(N-1)*…*(N-T+1) cas de commutation possibles. Quand N et T augmente, le nombre de cas de commutations possibles augmente plus rapidement encore, alors, cela prend beaucoup de temps pour trouver une solution optimale.

4.4.2. Transformation

Pour utiliser un réseau Hopfield dans un but d'optimisation, le précédent problème de commutation des circuits virtuels doit être formulé comme une fonction d'énergie. Nous pouvons transformer une fonction objective en une fonction d'énergie en utilisant l'approche de la fonction de pénalité [36]. Alors, la fonction objective Eq. 11 et les contraintes Eq. 12 - Eq. 14 sont transformés comme suit :

$$E = E1+E2+E3+E4+E5 \quad \text{Eq. 15}$$

où

$$E_1 = A_1 \sum_{i=1}^{N} \sum_{j=1}^{N} vc_{ij} \delta_{ij} \quad \text{Eq. 16}$$

$$E_2 = A_2 \sum_{i=1}^{N} \sum_{j=1}^{N} \phi_{ij} \quad \text{Eq. 17}$$

$$E_3 = A_3 \left(\sum_{i=1}^{N} \sum_{j=1}^{N} d_j vc_{ij} - T \right)^2 \quad \text{Eq. 18}$$

$$E_4 = A_4 \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{h=1}^{N} vc_{ij} vc_{i,h \neq j} \quad \text{Eq. 19}$$

$$E_5 = A_5 \sum_{i=1}^{N} \sum_{j=1}^{N} \sum_{k=1}^{N} vc_{ij} vc_{k \neq i,j} \quad \text{Eq. 20}$$

où A_i (i=1..5) sont les coefficients des composantes participant dans la fonction d'énergie.

Le réseau Hopfield utilisé pour l'optimisation a la même taille que la matrice *vc* où les colonnes sont étiquetées par les points d'accès d'entrée et les lignes représentent la position des points d'accès de sortie (Figure 4-12). Quand il y a un circuit virtuel arrivant sur un point d'accès d'entrée i, les nœuds sur la colonne i sont excités. Cependant (par la contrainte Eq. 13) il y a un seul nœud qui gagne (soit le plus activé) et celui-ci montre le point d'accès de sortie sur lequel le trafic est commuté (Figure 4-13). De plus, par la contrainte Eq. 14, il existe un seul nœud activé sur une ligne. Alors, quand un nœud activé, il inhibe tous les autres sur la même colonne et la même ligne.

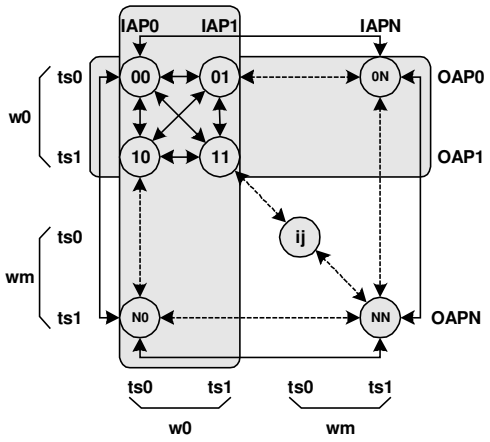

Figure 4-12: Réseau Hopfield utilisé pour l'optimisation

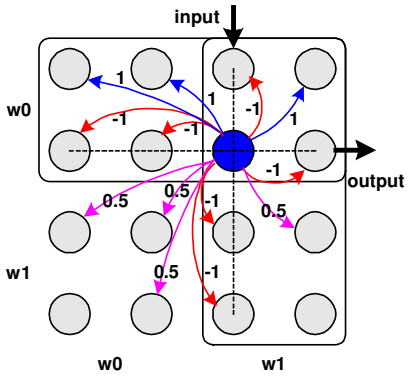

Figure 4-13: Excitation et inhibition d'un neurone aux autres

Pour réduire le nombre de longueurs d'onde utilisées, la tendance est de combiner les circuits virtuels dans certaines longueurs d'onde, au lieu qu'ils soient distribués sur toutes les longueurs d'onde. Autrement dit, quand un nœud est activé, il excite beaucoup d'autres nœuds qui sont sur la même longueur d'onde que d'autres. Alors, Eq. 17 est remplacé par:

$$E_2 = A_2 \sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{k=1}^{N}\sum_{h=1}^{N} vc_{ij} vc_{k\neq i, h\neq j} D_{ik} D_{jh} \qquad \text{Eq. 21}$$

où D est une matrice constante représentant l'influence de l'activation d'un nœud sur les autres.

De Eq. 15, l'énergie du nœud (ij) est

$$E_{ij} = \left(A_1\delta_{ij} + A_2 \sum_{k=1}^{N}\sum_{h=1}^{N} vc_{k\neq i, h\neq j} D_{ik} D_{jh} + A_3(d_j - T) + A_4 \sum_{h=1}^{N} vc_{i, h\neq j} + A_5 \sum_{k=1}^{N} vc_{i\neq k, j} \right) vc_{ij} \qquad \text{Eq. 22}$$

Alors, nous avons le poids de la connexion du nœud (ij) au (kh) et, à l'inverse.

$$W_{ij,kh} = A_2(1-C_{ik})(1-C_{jh})D_{ik}D_{jh} + A_4C_{ik}(1-C_{jh}) + A_5C_{jh}(1-C_{ik}) \qquad \text{Eq. 23}$$

où C est une matrice binaire constante: C_{ik}=1 si i=k et C_{ik}=0 sinon, et le seuil du nœud (ij) est

$$\theta_{ij} = A_1\delta_{ij} + A_3(d_j - T) \qquad \text{Eq. 24}$$

4.4.3. Simulation et analyse des résultats

L'algorithme d'optimisation de la commutation a été simulé en Java sur un PC AMD950 avec 256Mb RAM. Le commutateur utilisé dans le test se compose de 6 longueurs d'onde dont chacune est divisée en 4 intervalles de temps. Par conséquent, le commutateur a 6*4=24 points d'accès en entrée (ou en sortie). Nous avons alors utilisé un réseau neuronal avec 24*24=576 neurones tous connectés les uns aux autres. Examinons un ensemble de trafics de T (T≤24) arrivant aléatoirement sur des points d'accès d'entrée IAP; la réduction d'énergie à travers des cycles d'apprentissage est illustrée comme par la Figure 4-14.

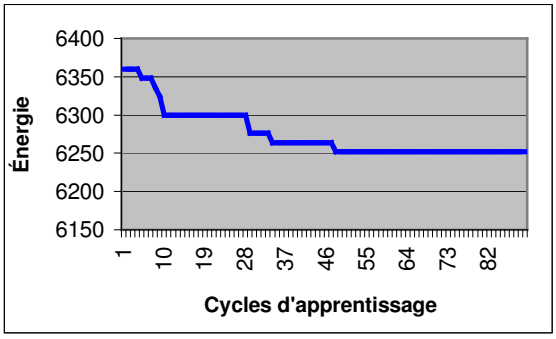

Figure 4-14: Réduction de l'énergie à travers des cycles d'apprentissage

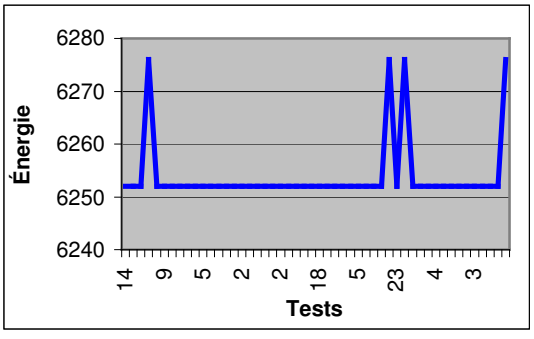

Figure 4-15: Énergie minimale trouvée

Nous pouvons voir qu'après quelques cycles d'apprentissage, l'énergie de réseau devient stable. Aux points ayant la plus basse énergie, la solution optimisée est trouvée. Cependant, la question reste de savoir si ces points stables de la fonction d'énergie correspondent vraiment à la solution optimale ou non. Pour répondre à la question, nous avons répété cette expérimentation plusieurs fois en changeant l'ordre des modèles étudiés. Nous obtenons le diagramme des énergies minimales de réseau correspondant à différents ordres de patterns d'apprentissage (Figure 4-15). Nous voyons que l'énergie minimale dépend de l'ordre des patterns d'apprentissage d'entrée. Tel qu'illustré sur le diagramme, l'énergie peut tomber dans un minimum local, mais, dans la plupart des cas, elle se situe sur le minimum global. Sur 50 tests, l'énergie est tombée dans un minimum local seulement quatre fois. Ce taux de minimum local (4/50*100 = 8%) est acceptable.

Le temps pour trouver une solution optimale dépend du nombre de points d'accès: le nombre de longueurs d'onde et le nombre d'intervalles de temps sur chaque longueur d'onde. Supposons que le nombre d'intervalles de temps sur chaque longueur d'onde est constant (il est de 4 dans notre expérimentation). La Figure 4-16 illustre comment le temps requis pour trouver une solution optimale augmente avec le nombre de longueurs d'onde.

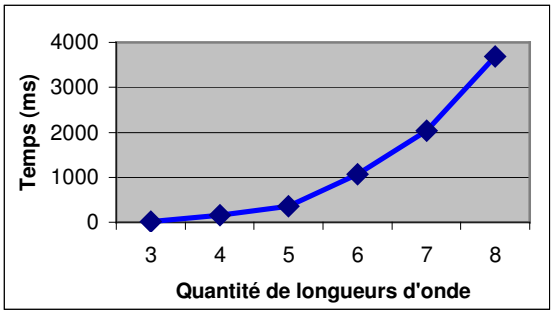

Figure 4-16: Temps pour trouver une solution optimale dépend du nombre de longueurs d'onde

4.5. Conclusion

L'optimisation du *grooming* des trafics va entraîner des bénéfices quant au coût d'utilisation des réseaux OVPN et à l'efficacité d'utilisation des ressources de réseau (telle que la bande passante). Cependant, la planification et la commutation des trafics OVPN dans les descriptions précédentes sont essentiellement des décisions individuelles des routeurs PE-ONE. Leur coordination se limite aux échanges d'informations concernant l'état disponible de la bande passante (exprimé dans la matrice d'état des canaux optiques pour la planification (Chapitre 4.3) ou dans la liste d'états disponibles des intervalles de temps sur un port pour la commutation (Chapitre 4.4). Ainsi, l'optimalisation considérée dans ce chapitre est presque locale. Des études sur l'optimalisation globale (qui se compose des communications et des coordinations des routeurs PE-ONE) seront réalisées dans l'avenir.

5. Réseaux sans fil étendus à travers connexions OVPN

Cette section concerne l'étude de l'allocation des circuits virtuels dans des réseaux dits *hybrides* composés de réseaux sans fil et de réseaux filaires. Les réseaux sans fils sont de plus en plus présents et offrent plusieurs avantages, dont la mobilité des usagers. Cependant ces réseaux coexistent en général avec les réseaux filaires tels que les réseaux optiques. D'autre part, les nouvelles applications (ex. multimédia) demandent de plus en plus de bande passante. Ce qui fait les réseaux optiques sont un bon candidat pour supporter ces réseaux hybrides.

Contrairement aux réseaux sans fil locaux, qui permettent à des utilisateurs d'être mobiles dans une zone restreinte, les réseaux sans fil étendus permettent des connectivités dans une zone plus large, pour les utilisateurs mobiles. Les réseaux sans fil étendus peuvent par exemple employer des réseaux cellulaires pour la transmission de données. Un ordinateur portable avec un modem sans fil se relie à une station de base par des ondes radio. Les radios portent des données à un centre de commutation mobile (*Mobile Switching Center*), où elles vont être transmises sur un réseau public approprié comme l'Internet. En utilisant des connexions louées au sein du réseau public, la communication est établie entre les terminaux. Pour les réseaux sans fil étendus qui emploient les réseaux téléphoniques cellulaires existants (ex. GSM), il est également possible de faire des appels téléphoniques (vocaux) par le biais du réseau public.

Avec l'accroissement de plus en plus rapide du nombre d'utilisateurs des services sans fil ainsi que du volume de données à transporter, une tendance actuelle vise le remplacement des réseaux publics non optiques (comme l'Internet) par l'infrastructure optique pour satisfaire des demandes de bande passante de plus en plus élevées. Le modèle de services OVPN devient alors une solution efficace pour établir des connexions supportant des réseaux sans fil étendus à travers une infrastructure optique. En outre, étant donné le caractère mobile des services sans fil, ces connexions OVPN se doivent d'être dynamiques pour s'adapter aux changements et aussi réduire la redondance. Ce chapitre va considérer l'adaptabilité du réseau OVPN par rapport de la mobilité du terminal sans fil à travers un réseau hybride étendu.

5.1. Stratégie d'adaptabilité du réseau OVPN

Considérons un exemple d'interconnexion de stations sans fil par un réseau OVPN comme la Figure 5-1. Dans l'exemple, une connexion OVPN (un circuit virtuel) est établie entre les stations de base 1 et 3 (à travers les routeurs PE-ONE 1 et 3). En utilisant cette connexion, un terminal mobile dans la zone radio de la station 1 peut communiquer avec un autre connectant à la station 3. Supposons que le terminal mobile se déplace de la zone radio d'une station de base à celle d'une autre. Dans cet exemple, le terminal mobile va quitter la zone radio de la station 1 et entrer dans celle de la station 2. Alors la station 1 va envoyer un message à la station 2 pour lui demander de prendre en charge la communication de ce terminal mobile. Autrement dit, la connexion actuelle de

la communication pourra être changée. Ce problème est connu sous le nom de problème « *handoff* » ou « *handover* ».

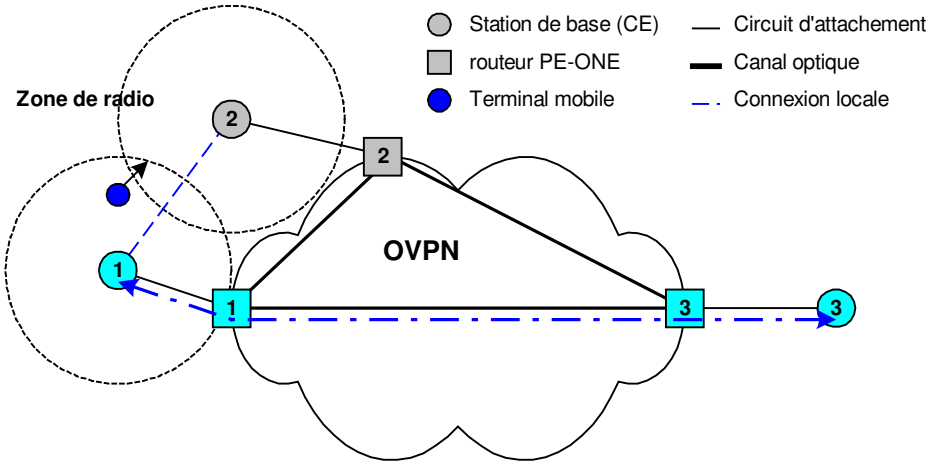

Figure 5-1 : OVPN utilisé dans l'interconnexion deux stations sans fil

S'il existe un lien (comme un lien FR ou une connexion IP) disponible entre la station 1 et 2 (Figure 5-2), celui-ci pourrait être employé pour transporter des données entre la station 1 et 3. Dans ce cas, il n'y a rien à changer dans le réseau OVPN actuel. La station 1 est toujours responsable de lier le terminal mobile à la station 3

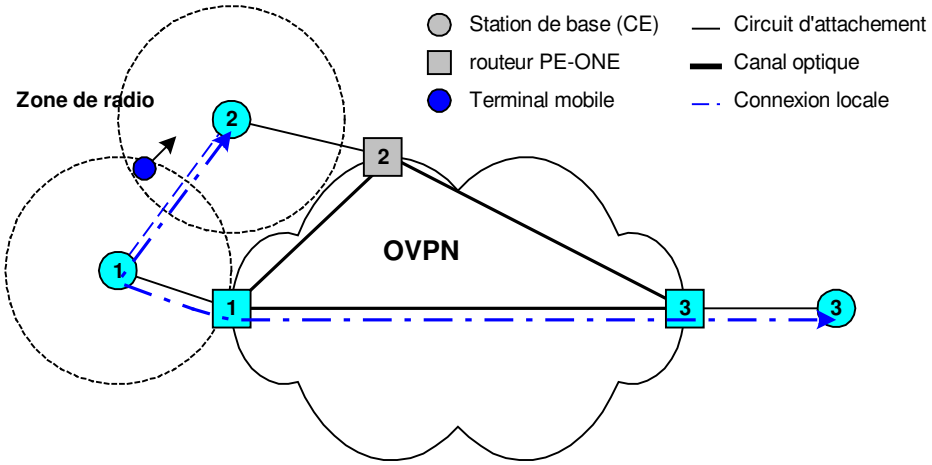

Figure 5-2 : Changement du parcours en utilisant un lien local

Par contre, s'il n'y a pas de lien disponible entre les stations 1 et 2, la station 2 doit établir un nouveau circuit virtuel à la station 3. Il y a deux possibilités : s'il existe un circuit d'attachement disponible entre la station 2 et le routeur PE-ONE 1, ce circuit d'attachement sera alors utilisé pour transporter des données entre le terminal mobile et la station 3 (Figure 5-3). Le réseau OVPN dans ce cas change seulement le circuit d'attachement au routeur PE-ONE 1 de la station 2, au lieu de la station 1. Le routeur PE-ONE 1 est alors responsable de reconfigurer la mise en correspondance (*mapping*) du nouveau circuit d'attachement avec le canal optique utilisé.

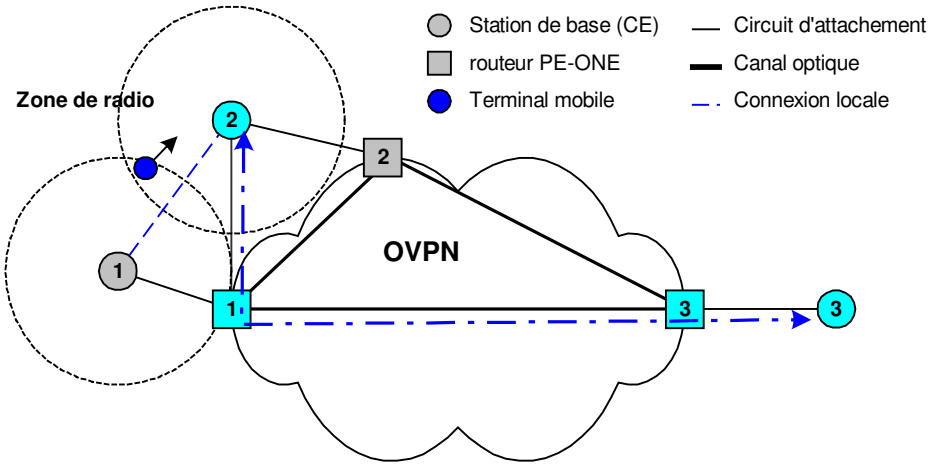

Figure 5-3 : Changement du parcours en changeant le circuit d'attachement

S'il n'y a pas de circuit d'attachement entre la station 2 et le routeur PE-ONE 1, le routeur PE-ONE 2 est responsable d'établir un circuit virtuel à la station 3. Il existe aussi deux possibilités : soit le routeur PE-ONE 2 établit un circuit virtuel directement à la station 3 (Figure 5-4), soit il établit un canal optique au routeur PE-ONE 1 et réutilise le circuit virtuel du routeur PE-ONE 1 à la station 3 (Figure 5-5). Il existe sans doute d'autres possibilités, mais on peut les réduire aux deux cas précédents. La sélection de l'une des deux solutions précédentes dépend de la disponibilité des canaux optiques et du temps pour les établir afin qu'il n'y ait pas d'interruption dans le transport des données.

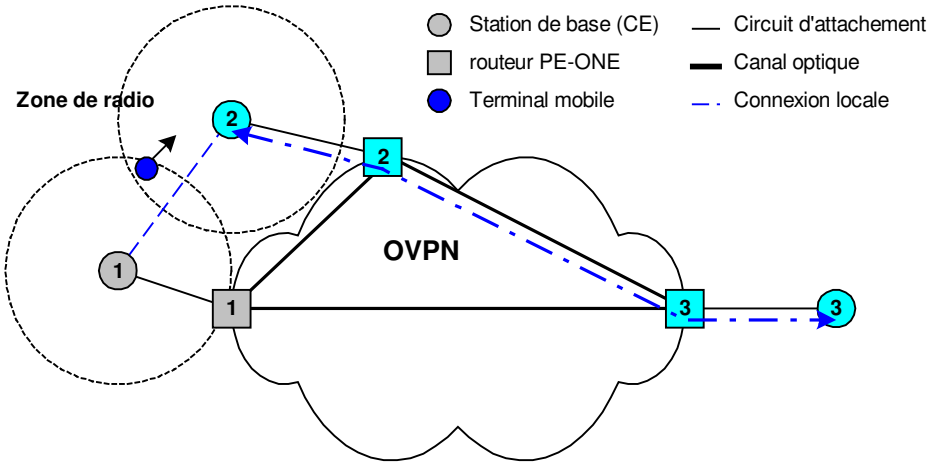

Figure 5-4 : Changement du parcours en changeant le circuit virtuel

Dans la première solution (Figure 5-4), le canal optique entre les routeurs PE-ONE 1 et 3 est libéré et un canal optique entre les routeurs PE-ONE 2 et 3 est établi. Le routeur PE-ONE 3 remet alors en correspondance le circuit d'attachement (de lui à la station 3) avec le nouveau canal optique (entre les routeurs PE-ONE 2 et 3). Le

routeur PE-ONE 2 met aussi en correspondance le circuit d'attachement (de lui à la station 2) avec le nouveau canal optique (entre les routeurs PE-ONE 2 et 3).

Pour la deuxième solution (Figure 5-5), un canal optique entre les routeurs PE-ONE 1 et 2 est établi. Le routeur PE-ONE 1 remet alors en correspondance le canal optique (entre les routeurs PE-ONE 1 et 3) avec le nouveau canal optique (entre les routeurs PE-ONE 1 et 2). Une commutation entièrement optique est souvent établie et demande alors que deux canaux optiques était homogènes (pour la bande passante, la longueur d'onde et les intervalles de temps). Si des processus électriques (comme la conversion de longueur d'onde ou l'échange des intervalles de temps) doivent être utilisés, alors la qualité de service du réseau OVPN n'est plus assurée.

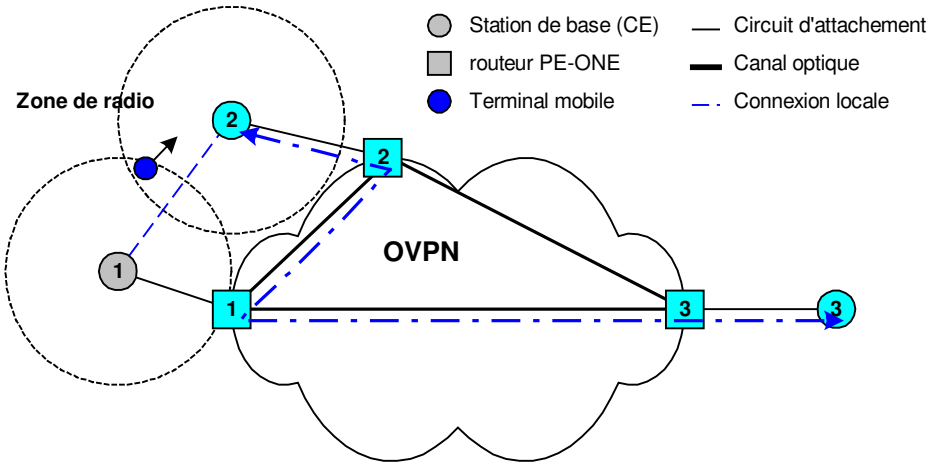

Figure 5-5 : Changement du parcours en ajoutant un nouveau canal optique

5.2. Principe de changement d'une connexion

Dans l'interconnexion des stations sans fil par réseau OVPN, le mouvement du terminal mobile cause évidemment un changement de la topologie du réseau OVPN. Pour éviter l'interruption du transport des données, un principe de changement des circuits virtuels est proposé à la Figure 5-6. Supposons que les données actuellement échangées entre deux nœuds 1 et 2 sont transportés par le circuit virtuel VC 1 et qu'on veuille l'échanger pour le circuit virtuel VC2. Tout d'abord, les données vont être transportées sur les deux circuits virtuels VC1 et VC2. Lorsque les données arrivées au nœud 2 sur les deux circuits virtuels sont identiques (stables), le transport sur le circuit virtuel VC1 est terminé. Le circuit virtuel VC2 est maintenant responsable de transport des données et le processus de changement des circuits virtuels est terminé.

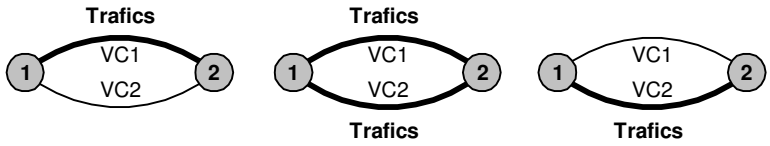

Figure 5-6 : Principe de changement d'une connexion

Dans l'exemple précédent, l'application du principe de changement des circuits virtuels est entièrement identique (Figure 5-7). D'abord, le routeur PE-ONE 2 participe dans le réseau OVPN en question. Par le processus d'auto-découverte, le routeur PE-ONE 2 reconnaît ses voisins et commence à établir un circuit virtuel de la station 2 à la station 3 (par le processus d'établissement de circuits d'attachement et le processus d'établissement de canaux optiques). Les données échangées entre le terminal mobile et la station 3 sont alors transportées sur les deux circuits virtuels (VC 1-3 et VC 2-3). Lorsque le transport des données sur les deux circuits virtuels est stable, le circuit virtuel VC 1-3 est enlevé ainsi que le routeur PE-ONE 1. Le transport des données se fait maintenant entièrement sur le circuit virtuel VC 2-3.

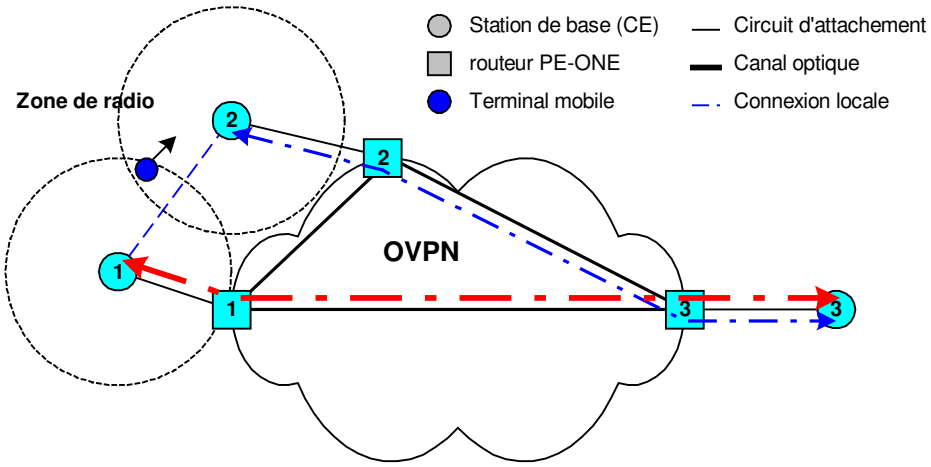

Figure 5-7 : Un exemple de changement des circuits virtuels

5.3. Contrainte de temps de configuration

Le changement des circuits virtuels est affecté par la contrainte de temps de configuration : le temps de configuration d'un nouveau circuit virtuel doit être inférieur ou égal du temps que le terminal mobile passe sur la zone de recouvrement (*overlap*) pour assurer de ne pas produire une interruption de communication. Si d est la longueur du chemin où le terminal mobile passe sur la zone de recouvrement, v_{tm} est la vitesse de mouvement du terminal mobile, t_{VC} est le temps d'établissement d'un nouveau circuit virtuel, alors

$$t_{VC} \leq \frac{d}{v_{tm}} \qquad \text{Eq. 25}$$

Considérons un terminal mobile qui se déplace dans la zone de recouvrement de deux stations de base comme dans la Figure 5-8. Supposons que la direction de mouvement du terminal mobile et la ligne entre deux stations de base 1 et 2 forment un angle α. La longueur du chemin (d) où le terminal mobile passe sur la zone de recouvrement alors est déterminée par l'équation :

$$d^2 - 2R_1 \cos(\alpha - \beta)d + R_1^2 - R^2 = 0 \qquad \text{Eq. 26}$$

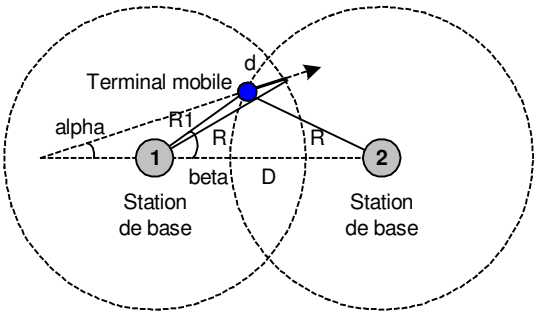

Figure 5-8 : Un exemple du chemin à travers la zone de recouvrement

Où R1 est la distance entre la station 1 et le terminal mobile, R est le rayon de la zone radio de chaque station, D est la distance entre deux stations de base. Cosin(α-β) dans l'équation Eq. 26 est calculé par la formule suivante :

$$\cos(\alpha-\beta)=\cos(\alpha)\left(\frac{R_1^2+D^2-R^2}{2R_1D}\right)+\sin(\alpha)\sqrt{1-\left(\frac{R_1^2+D^2-R^2}{2R_1D}\right)^2} \qquad \text{Eq. 27}$$

5.4. Simulation

Nous allons développer une simulation pour démontrer l'adaptabilité du réseau OVPN par rapport à des changements régulier des connexions. Le rôle du réseau OVPN dans cette simulation est de supporter des connexions d'un réseau sans fil étendu. À cause du caractère mobile des terminaux sans fil (comme le cellulaire ou le portable sans fil), la topologie du réseau OVPN qui supporte leurs communications change en fonction de mouvement des terminaux sans fil. Puisque l'architecture OVPN est un modèle décentralisé de contrôle et de gestion, les décisions quant au changement de connexions entre chaque composant OVPN (nœud - agent) doivent alors se faire à temps. Cela montre la robustesse du réseau OVPN.

5.5. Conclusion

Avec l'intégration de la technique d'agents, le réseau OVPN devient flexible et intelligent grâce à l'autonomie et la coordination des nœuds OVPN (qui ont des fonctions OVPN) sur une infrastructure optique. Les connexions OVPN sont temporaires, parce qu'elles se basent sur des ressources disponibles temporellement d'un réseau public. Le réseau OVPN est alors approprié pour soutenir des services mobiles comme le réseau sans fil étendu, où le mouvement des terminaux sans fil amène des changements de la topologie du réseau OVPN. Ce chapitre a considéré une problématique de mobilité des connexions OVPN. La stratégie de changement d'une connexion, le principe de changement et la contrainte de temps pour le changement sont discutés. Une simulation est également proposée mais seulement à l'étape de la spécification. Le but de la simulation est de démontrer l'applicabilité de l'architecture OVPN dans la réalité : dans ce chapitre, c'est l'application du service OVPN pour soutenir des réseaux sans fil étendus.

6. Conclusion

Le réseau privé virtuel VPN est une solution efficace pour établir des connexions privées à travers un réseau public. Pour l'infrastructure non optique, plusieurs types de réseaux VPN ont été proposés et ont été appliqués dans les services de télécommunication. Une tendance actuelle est le remplacement des infrastructures publiques non optiques en infrastructures publiques optiques pour profiter la capacité de bande passante des fibres optiques. Cependant, à cause de la différence considérable quant au caractère du signal de transport de données (trames optiques, au lieu des paquets non optiques) et par conséquent de la technique de routage (canaux optiques, au lieu des tunnels IP), la transformation des modèles VPN non optique en modèles VPN optiques exige beaucoup de modifications. Il existe aussi certaines propositions pour une architecture VPN sur l'infrastructure optique (architecture OVPN), mais elles ne sont pas suffisantes et complètes pour être considéré comme une carde d'applications sur lequel on peut contrôler et gérer des services OVPN. Notre étude propose alors une approche pour une architecture OVPN intégrant la technologie des agents.

Si on considère les fonctions de contrôle et de gestion des services OVPN, l'architecture OVPN est semblable à un système multiagents, où les nœuds OVPN (qui ont des fonctions OVPN) sont des entités autonomes qui communiquent entre elles et se coordonnent pour établir des connexions OVPN. L'intégration de la technologie des agents dans l'architecture OVPN permet alors d'améliorer la flexibilité et l'intelligence des services OVPN. Cet avantage a été démontré dans l'application du service OVPN pour soutenir des réseaux sans fils étendus. L'adaptabilité s'exprime alors comme des changements dynamiques de la topologie du réseau OVPN par rapport aux mouvements des terminaux sans fil dans un réseau sans fil étendu. L'avantage de la technique d'agents est aussi représenté par l'optimisation de la planification et de la commutation des trafics OVPN.

Cependant, l'aspect cognitif est encore limité dans les propositions précédentes. Par exemple, dans la planification et la commutation des trafics OVPN, la décision est plutôt individuelle et non basée sur une coopération réelle entre les agents. Bien que la connaissance utilisée par chaque agent soit mise à jour par d'autres agents, la communication et la coordination entre les agents sont encore faibles. Dans l'avenir, nous travaillerons à renforcer la coopération entre les agents dans la planification et la commutation afin d'augmenter l'efficace globale du réseau, au lieu de l'efficacité locale tel que présenté dans le document. Une simulation est aussi développée pour démontrer l'adaptabilité des services OVPN dans le réseau étendu sans fil. L'adaptabilité de notre architecture OVPN va ainsi être confirmée.

7. Références

VPN non-optique

[1] Jeremy De Clercq and others, A Paquetwork for Provider Provisioned CE-based Virtual Private Networks using Ipsec, Internet Draft, draft-ietf-ppvpn-ce-based-00.txt, July 2001

[2] CY Lee and others, CE-based Virtual Private LAN, Internet Draft, draft-lee-ce-based-vpl-02.tx, Mars 2003

[3] Luca Martini and others, Encapsulation Methods for Transport of ATM Over IP and MPLS Networks, Internet Draft, draft-ietf-pwe3-atm-encap-04.txt, December 2003

[4] Claude Kawa and others, Paquet Relay over Pseudo-Wires, Internet Draft, draft-ietf-pwe3-paquet-relay-00.txt, October 2002

[5] Luca Martini and others, Encapsulation Methods for Transport of Ethernet Paquets Over IP/MPLS Networks, Internet Draft, draft-ietf-pwe3-ethernet-encap-05.txt, December 2003

[6] Kireeti Kompella and others, MPLS-based Layer 2 VPNs, Internet Draft, draft-kompella-ppvpn-l2vpn-00.txt, June 2001

[7] Marc Lasserre and others, Virtual Private LAN Services over MPLS, Internet Draft, draft-lasserre-vkompella-ppvpn-vpls-01.txt, March 2002

[8] Himanshu Shah and others, IP-Only LAN Service (IPLS), Internet Draft, draft-ietf-l2vpn-ipls-00.txt, November 2003

[9] Loa Andersson and others, L2VPN Paquetwork, Internet Draft, draft-ietf-l2vpn-l2-paquetwork-03.txt, October 2003

[10] Mike Capuano, VPLS: Scalable Transparent LAN Services, White Paper, Juniper Networks, Inc., 2003

[11] E. Rosen and others, BGP/MPLS VPNs, RFC2547, March 1999

[12] Paul Knight and others, Network based IP VPN Architecture using Virtual Routers, Internet Draft, draft-ietf-l3vpn-vpn-vr-01.txt, September 2003

Protocoles

[13] E. Rosen and others, Multiprotocol Label Switching Architecture, RFC3031, January 2001

[14] E. Rosen and others, Use of PE-PE IPsec in RFC2547 VPNs, Internet Draft, draft-ietf-ppvpn-ipsec-2547-00.txt, July 2001

[15] D. Farinacci and others, Generic Routing Encapsulation (GRE), RFC2784, March 2000

[16] Yakov Rekhter and others, Use of PE-PE GRE or IP in RFC2547 VPNs Internet Draft, draft-ietf-ppvpn-gre-ip-2547-00.txt, July 2001

[17] J. Lau and others, Layer Two Tunneling Protocol "L2TP", Internet-Draft, draft-ietf-l2tpext-l2tp-base-00.txt, July 2001

[18] Eric Mannie and others, Generalized Multi-Protocol Label Switching Architecture, Internet-Draft, draft-ietf-ccamp-gmpls-architecture-07.txt, May 2003

[19] Neil J. and Adrian F., MPLS in Optical Networks, MPLS Architect at Data Connection Ltd., October 2001

[20] J. Lang and others, Link Management Protocol (LMP), Internet Draft, draft-ietf-ccamp-lmp-10.txt, October 2003

[21] Eric C. Rosen and other, OSPF as the PE/CE Protocol in BGP/MPLS IP VPNs, draft-ietf-l3vpn-ospf-2547-01.txt, Internet Draft, February 2003

[22] Hamid Ould-Brahim and others, Using BGP as an Auto-Discovery Mechanism for Provider-provisioned VPNs, Internet Draft, draft-ietf-l3vpn-bgpvpn-auto-00.txt, May 2003

Réseaux optiques WDM

[23] Semih B. and Altan K., All-Optical Networking

[24] D. Coudert and H. Rivano, Lightpath Assignment for Multifibers WDM Networks with Wavelength Translators, MASCOTTE project, CNRS-I3S/INRIA/UNSA, B.P. 93, 06902 Sophia Antipolis Cedex, FRANCE.)

VPN sur le réseau WDM

[25] Virtual Private Networks Over Wavelength Division Multiplexed Networks: A Survey, http://www.dataconnection.com

[26] Hamid O. B. and others, BGP/GMPLS Optical VPNs, Internet Draft, draft-ouldbrahim-bgpgmpls-ovpn-00.txt, April 2001

[27] Byrav R. and Ashok R., Design of virtual private networks (VPNs) over optical wavelength division multiplexed (WDM) networks, Department of Computer Science and Engineering, University of Nebraska – Lincoln, Lincoln, Nebraska USA

[28] Yang Q., Krishna S. and Bo Li, Architecture and Analysis for providing Virtual Private Networks (VPN) with QoS over Optical WDM Networks, School of Electrical and Electronic Engineering, Nanyang Technological University Singapore, 639789

[29] Vo, Viet Minh Nhat, "Information model for a virtual private optical network (OVPN) using virtual routers (VRs)", OPTO Canada- Ottawa, 26 February 2002

Grooming de trafics

[30] Eytan Modiano and Philip J. Lin, Traffic Grooming in WDM Networks, IEEE Communications Magazine, July 2001

[31] S. Thiagarajan, A.K. Somani, Capacity Fairness of WDM Networks with Grooming Capabilities, Telecommunications Grooming - Optical Networks, 2001

[32] George N. Rouskas, Routing and Wavelength Assignment in Optical WDM Networks, Department of Computer Science, North Carolina State University

[33] R. Dutta, G.N. Rouskas, Traffic grooming in WDM networks: past and future, IEEE Network, 2002

[34] Vo, Viet Minh Nhat, Traffic Switching Optimization in Optical Routing using Hopfield Networks, RIVF'04, 02-05 Février 2004, Hanoi, Vietnam

Optimisation par réseau Hopfield

[35] Michail G. Lagoudakis, Neural Networks and Optimization Problems - A Case Study: The Minimum Cost Spare Allocation Problem, The Center for Advanced Computer Studies, University of Southwestern Louisiana

[36] Lillo, W., Loh, M., Hui, S., Zak, S. "On Solving Constrained Optimization Problems with Neural Networks: A Penalty Method Approach", in IEEE Transactions on Neural Networks, 4, 6, 1993, pp. 931–940.

Système multiagents

[37] "International Conference on Autonomous Agents", Proceedings of the Fifth International Conference on Autonomous Agents, May 28-June 1, 2001

[38] Ferber, J., Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence, February 1999.

[39] Adina Magda Florea, Introduction to Multi-Agent Systems, University of Bucharest, 1998

[40] Jean-Pierre Briot and Yves Demazeau, Principes et architecture des systèmes multi-agents, Lavoisier 2001

Réseau sans fil

[41] Li-Yun Chiang and Sing-Ling Lee, An Efficient Handoff Algorithm in Wireless ATM Networks, Department of Computer Science and Information Engineering National Chung Cheng University, Chiayi 62107, Taiwan, Republic of China

[42] Jun-Zhao Sun and others, Mobility management techniques for the next generation wireless networks, Machine Vision and Media Processing Unit, Infotech Oulu, University of Oulu, Finland

[43] Jun-Zhao Sun and Jaakko Sauvola, Mobility and Mobility Management: a Conceptual Framework, MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu, University of Oulu, Finland

8. Annexe : Lexique

- FR – *Frame Relay* (Relais de trames) : Mode de transfert de données qui se base sur la commutation par paquets et permet de transmettre, à haut débit et sur de grandes distances, de grandes quantités de données.
- ATM - *Asynchronous Transfer Mode* (Mode de transfert asynchrone) : Mode de transfert de données qui permet d'acheminer à haut débit des paquets dont la principale caractéristique est la taille fixe de chaque paquet.
- BGP - *Border Gateway Protocol* (Protocole BGP): Protocole de routage externe utilisé pour connecter des systèmes autonomes et permettant d'échanger des informations entre des réseaux qui ont des politiques de routage différentes.
- OSPF - *Open Shortest Path First* (Protocole OSPF): Protocole employé pour le routage dans un groupe de routeurs selon la technologie d'état de lien dans laquelle les routeurs envoient des informations au sujet des connexions et des liens directs avec des autres routeurs.
- MPLS - *MultiProtocol Label Switching* (Protocole de commutation par étiquette) : Technique de transmission qui assigne une étiquette à chaque flux de données. L'étiquette fournit des informations sur le chemin qu'il doit parcourir, de façon à ce qu'il puisse être commuté ou routé plus rapidement sur des réseaux utilisant différents types de protocoles.
- GMPLS – *Generalized MPLS* (MPLS généralisé) : GMPLS est une généralisation de MPLS. L'étiquette de commutation est y généralisée par n'importe quoi qui est suffisant pour identifier un flux de trafic. Dans le réseau optique, l'étiquette peut être une fibre, une gamme d'ondes (*waveband)*, une longueur d'onde ou un time-slot
- OXC - *Optical Cross Connect* (Répartiteur optique ou Brasseur optique) : Commutateur optique qui commute des signaux optiques au niveau des fibres, des gammes d'ondes, des longueur d'ondes ou des time-slot d'un port d'entrée vers des ports de sortie.
- TDM – *Time Division Multiplexing* (Multiplexage par temps): Technique qui assigne des trafics de faible bande passant dans les intervalles de temps précis d'un porteur de bande de manière élevée afin qu'ils puissent être reconnus par le récepteur.
- WDM - *Wavelength-division multiplexing* (Multiplexage en longueur d'onde) : Technique qui combine des canaux correspondant aux différentes longueurs d'onde dans une fibre optique

- SONET/SDH - *Synchronous Optical Network* / *Synchronous Digital Hierarchy* (Réseau optique synchronique) : Mode de transmission de données sur fibre optique dans lequel des canaux sont intégrés progressivement et synchroniquement, par multiplexage TDM, à certains canaux plus grands.
- TG - *Traffic Grooming* (Grooming de trafics) : Ensemble des techniques qui combinent des trafics de faible bande passante dans les trafics de bande passante élevée pour satisfaire divers objectifs comme la réduction du coût d'utilisation de réseau.
- VPN - *Virtual Private Network* (Réseau privé virtuel) : Réseau privé qui se base sur l'infrastructure d'un réseau publique pour transmettre des données qui sont protégées grâce à l'utilisation de techniques de numérotation ou d'encapsulation.
- OVPN – *Optical VPN* (VPN optique): Réseau privé qui se base sur l'infrastructure d'un réseau optique publique.
- ONE – *Optical Network Element* (Élément du réseau optique) : Routeur ou commutateur optique (comme OXC) dans le réseau optique qui peut router ou commuter des trafics vers différents niveaux de bande passante.
- PE-ONE – *Provider Edge ONE* (Dispositif de périphérique du client): Dispositifs ONE à la périphérie du réseau du fournisseur qui se connectent aux réseaux des clients et aux autres dispositifs ONE et qui ont les fonctions requises pour un VPN optique.
- P-ONE – *Provider ONE* (Dispositif de fournisseur) : Dispositifs ONE à l'intérieur du réseau du fournisseur qui connectent uniquement à d'autres dispositifs ONE.
- CE – *Customer Edge* (Dispositif de périphérique du client) : Équipement de clients qui s'attachent aux réseaux de fournisseurs.
- AC – *Attachment Circuit* (Circuit d'attachement) : Lien logique ou physique entre CE et PE-ONE.
- VC – *Virtual Circuit* (Circuit virtuel) : Lien logique entre deux dispositifs CE à travers le réseau du fournisseur.
- OC – *Optical Channel* (Canal optique) : Lien optique logique qui correspond à un intervalle de temps (time-slot) ou un groupe d<intervalles de temps sur une longueur d'onde, ou à une longueur d'onde ou un gramme d'onde sur une fibre optique, ou encore à une fibre au complet.
- LP - Lightpath (Chemin optique) : Par la technique WDM, les rayons laser correspondant à différentes longueurs d'onde sont employés pour établir les connexions fixes bout à bout, s'appelle les lightpaths dans ce contexte, dans le réseau [24]. Alors, le ligthpath est le canal optique correspondant à une longueur d'onde.