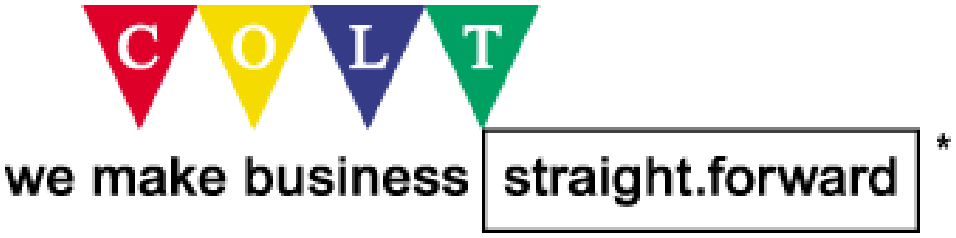
LIVRE BLANC

IP VPN
Réseau Virtuel, Solutions Réelles



* Donnons une longueur d'avance à votre entreprise

Avec la participation de

IP VPN
Réseau Virtuel, Solutions Réelles

SOMMAIRE

Introduction

La recherche permanente d'une plus grande productivité, la dispersion physique et géographique des sites des entreprises, la mobilité croissante des employés et le développement des applications de commerce électronique sont autant d'éléments qui favorisent le recours à des solutions de communications innovantes s'appuyant sur des architectures de réseau sans cesse plus performantes en terme de capacité, de souplesse, de rapidité, de sécurité et… d'économie.

Pour une entreprise en situation fortement concurrentielle, un des axes fondamentaux de l'amélioration de la productivité passe en effet par une circulation de l'information qui soit à la fois fiable, fluide, sécurisée, et rapide tant au sein de l'entreprise qu'entre l'entreprise et ses partenaires privilégiés (distributeurs, fournisseurs, sous-traitants, clients, …).

Le marché français des IP VPN est actuellement en pleine effervescence du fait d'évolutions technologiques très rapides et les acteurs de ce marché sont de plus en plus nombreux à proposer des offres variées répondant aux nouveaux besoins des entreprises.

Ces offres sont désormais adaptées aux exigences des grandes sociétés ayant une présence en France et à l'international mais aussi des PME multi-sites qui souhaitent améliorer leur communication interne et externe.

Aussi, qu'elles disposent déjà de réseaux basés sur des technologies X25 ou Frame Relay ou bien qu'elles souhaitent développer ex-nihilo un réseau le plus performant possible, les architectures de type IP VPN représentent une des voies incontournables pour les entreprises qui réfléchissent à l'évolution de leurs communications.

Un contexte de marché favorable à l'IP VPN

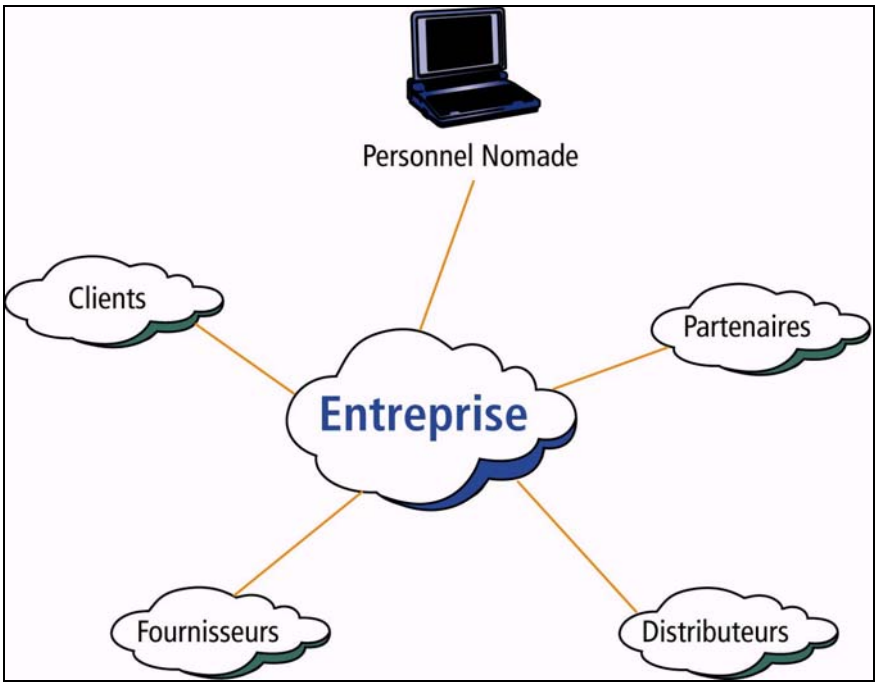
1. Positionnement sur un segment en forte croissance

Comme évoqué précédemment, les solutions de réseau de type IP VPN bénéficient d'un contexte favorable tant du point de vue des développements technologiques que de l'environnement économique et de l'évolution concurrentielle. La conjonction de ces phénomènes permet de prédire des débouchés en forte croissance à ce type de solutions ainsi que pour les services et applications associés.

Afin de mieux comprendre le positionnement des offres proposées par les opérateurs et les opportunités de marché qu'elles représentent, il est important de déterminer quels sont les différents facteurs contributifs de leur croissance.

1.1 Croissance du marché de la data

Tout d'abord du point de vue économique, il convient de mettre en évidence la part sans cesse plus importante du marché de la data dans l'ensemble des services des télécommunications. Cette tendance forte, observée par tous les opérateurs depuis 1999 et l'ouverture à la concurrence de ce marché, reflète les besoins des entreprises d'échanger avec leurs différents sites, partenaires, clients, fournisseurs, une masse d'information sans cesse croissante.



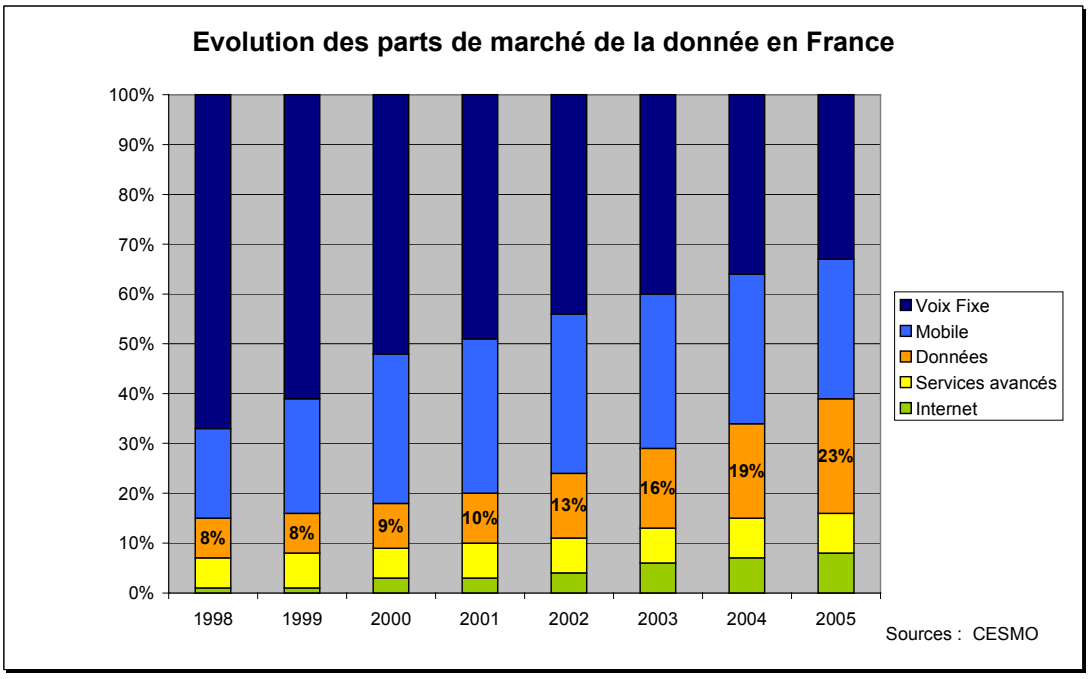
L'entreprise et son environnement de communication

Ces échanges sont facilités grâce à la généralisation des outils informatiques et la standardisation progressive des applications et protocoles.

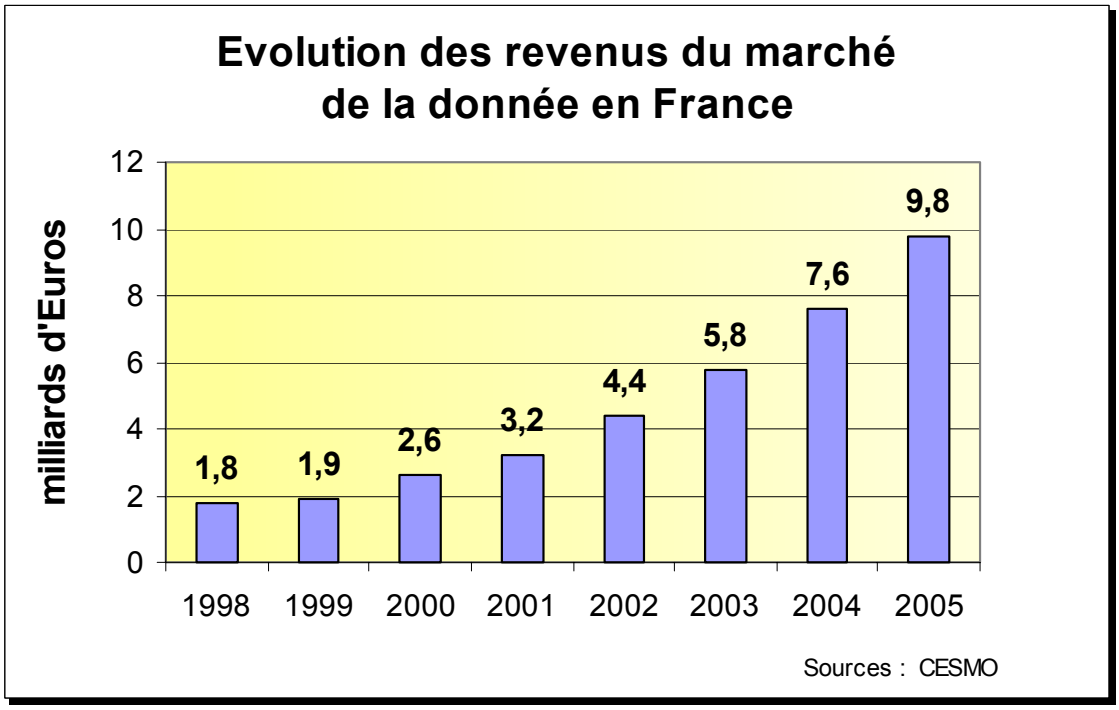
D'autre part, du fait de la concurrence et de l'innovation, l'entreprise moderne est chaque jour confrontée à de nouveaux défis d'organisation. La mise en place de nouveaux outils de productivité et de qualité nécessitent - là encore - des capacités importantes de la part des réseaux de communications. Qu'il s'agisse d'Extranets, d'Intranets, de gestion de la relation client (CRM), de gestion de la chaîne d'approvisionnement (SCM), de planification des ressources de l'entreprise (ERP) ou de simples documents de type Windows dont la demande en ressources croît perpétuellement, toutes les innovations reposant sur les communications d'entreprises nécessitent une interconnexion globale assurant à la fois performance, fiabilité et sécurité.

Ainsi le marché de l'IP VPN profite de la forte demande de capacité d'échange de données et bénéficie, chez les opérateurs, de l'engouement des entreprises pour le segment porteur de la donnée.

Le graphique ci-dessous montre l'évolution des parts de marché obtenues par les différents segments des télécommunications entre 1998 à 2000 (chiffres issus du rapport annuel de l'ART). Les parts de marché de 2001 à 2005 sont des prévisions CESMO.



CESMO estime que le marché global des télécommunications passera d'un taux de croissance annuel de 12% à un taux d'environ 7% après 2001. Le marché de la donnée, quant à lui, présentera des taux de croissance compris entre 19% et 27% d'ici 2005 et devrait représenter 4,4 milliards d'euros dès 2002.



Il s'agit donc d'une profonde modification structurelle du marché des télécommunications en France : hier tiré par le marché de la voix, le marché des télécoms doit aujourd'hui sa croissance globale aux activités à plus forte « valeur ajoutée » telles que les communications mobiles ou la donnée.

Notons que ce phénomène s'amplifie du fait des fortes baisses de tarifs engendrées par une concurrence accrue entre opérateurs sur le segment de la voix : la minute commutée ne permet pas de rentabiliser à elle seule l'activité des opérateurs alternatifs. Ces derniers se tournent naturellement vers le transport de la donnée, considéré avec les services qui lui sont associés **comme un très fort gisement de croissance**.

Les opérateurs alternatifs disposent, du fait de leur arrivée récente sur le marché, de réseaux modernes utilisant les nouvelles technologies, notamment IP, et remettent en cause l'avenir des protocoles d'« ancienne génération » tels que X25 et, dans une moindre mesure, le Frame Relay sur lesquels France Telecom avait bâti son réseau et détenait 80% de parts du marché de la donnée en 1997.

Suivant les évolutions du marché mondial des télécommunications, les opérateurs alternatifs, ont adopté, pour la majorité d'entre eux, un positionnement « données » et plus précisément, un positionnement IP, qui rend la concurrence effective sur ce marché.

1.2 Mutations technologiques

Au-delà de l'augmentation naturelle des échanges de données entre les sites des entreprises et leurs partenaires, l'apparition de nouveaux besoins liés à la recherche de productivité et d'efficacité des entreprises et le repositionnement stratégique des opérateurs sur le marché porteur de la donnée, il existe plusieurs **facteurs technologiques** favorisant l'avènement des architectures réseaux de type IP VPN.

A - Retrait des protocoles X 25 et FR au profit du protocole IP

Le premier facteur technologique est la **présence, au sein d'un nombre croissant d'entreprises, d'applications SI s'appuyant majoritairement sur le protocole IP.**

La prédominance naissante du protocole IP au sein même des applications de l'entreprise favorise naturellement le transport des données de façon native sur protocole IP.

Parmi les principales applications de l'entreprise, bon nombre sont nativement développées en s'appuyant sur le protocole IP (ou sont sur le point de migrer vers ce type de technologie) comme les applications de transfert de données asynchrones :

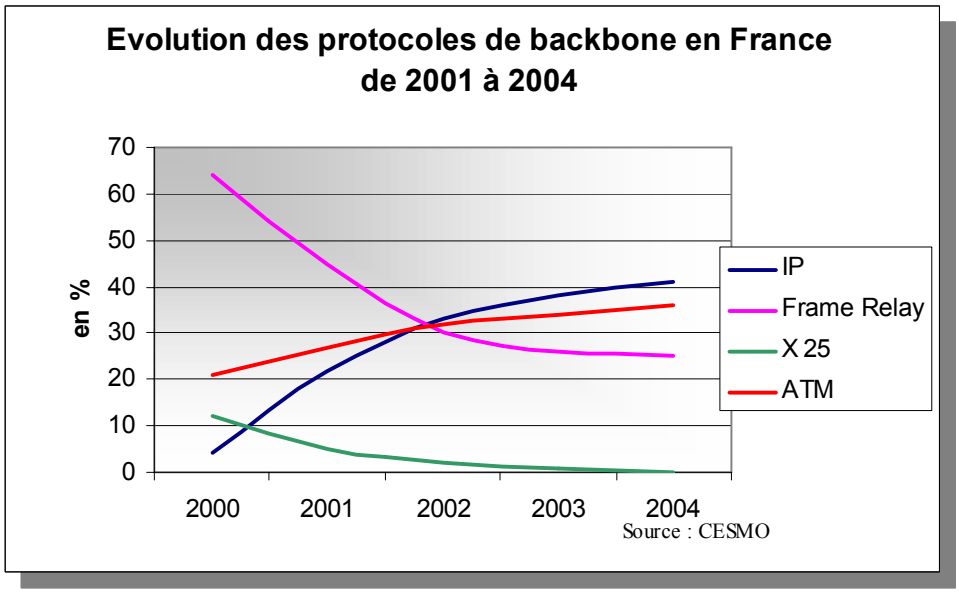
- fichiers électroniques
- e-mails
- navigation sur le web
- les applications Intranet, Extranet
- le transfert d'images (industrielles, médicales, géographiques, …)
- les outils de collaboration
- les applications de e-commerce
- les applications de CRM
- les ERP
- les applications de réalité virtuelle
- les réseaux dédiés au stockage, etc.

Ou encore des applications de type « temps réel », telles que la voix/ip, la vidéo, la visioconférence, l'audioconférence, etc.

Pour ce dernier type d'applications, dont la demande de la part des entreprises est encore faible en France, l'avenir des technologies IP permet d'envisager avec optimisme une convergence des applications voix et données qui s'intègreront dans un environnement de type IP VPN. Ces applications nécessiteront néanmoins des performances du réseau et une qualité de service incompatibles avec la notion de « best-effort » sur laquelle sont basés nombre de réseaux IP Internet et devront, en tout état de cause, s'appuyer sur des capacités bien maîtrisées.

Quoiqu'il en soit, cette évolution fondamentale vers le « tout IP » reflète les changements stratégiques dans les transformations des réseaux apparus chez les opérateurs historiques et mis en oeuvre par les nouveaux opérateurs alternatifs.

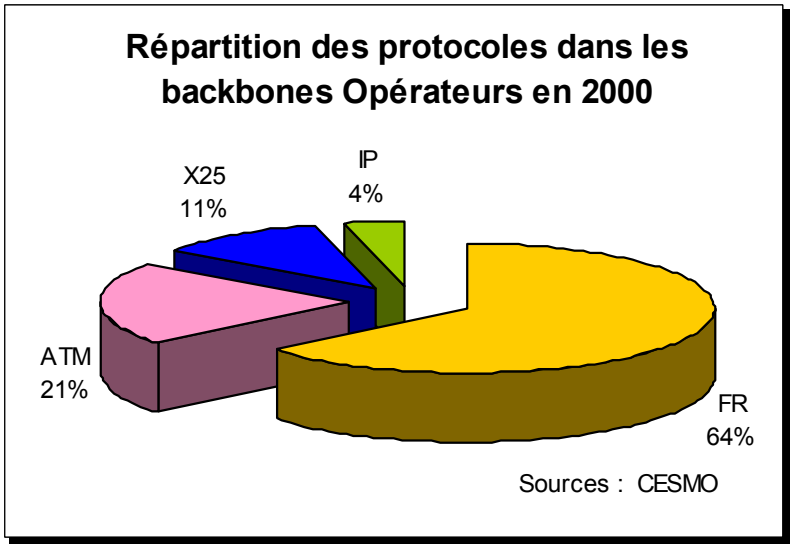
Le graphique ci-dessous présente les courbes d'évolution de chaque protocole de transport (backbone) entre 2000 et 2004 selon les estimations de CESMO :



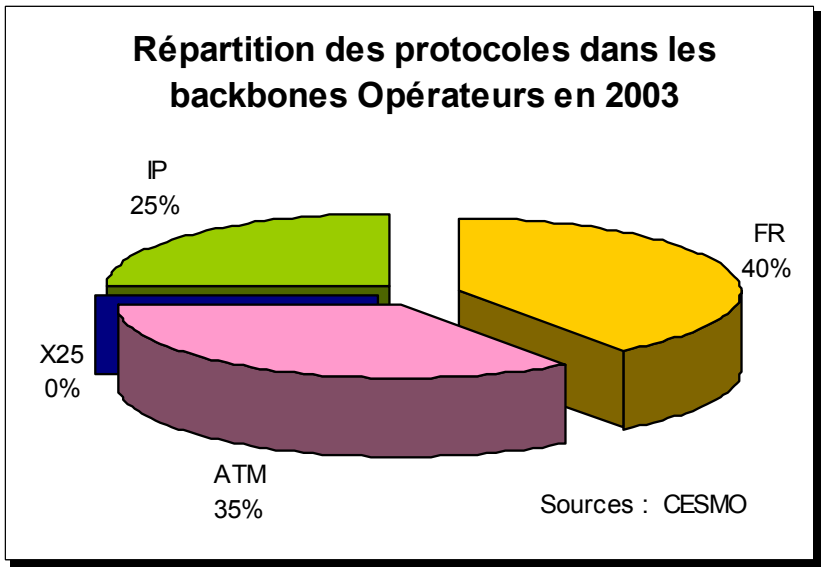
En 2000, le protocole le plus utilisé dans les backbones opérateurs était le Frame Relay. Globalement, le X25 et le Frame Relay sont désormais sur le déclin au profit des protocoles ATM et IP qui se répandent de plus en plus sur le marché. Le point de convergence entre le Frame Relay, l'ATM et l'IP en France devrait être atteint en milieu d'année 2002.

Si aujourd'hui le protocole X25 arrive en fin de cycle de vie, c'est bien qu'il ne correspond plus aux nouvelles applications du marché. En effet, sécurisés par des mécanismes de contrôle de flux et contrôle d'erreurs ralentissant le trafic sur le réseau, les réseaux utilisant X25 proposent de faibles débits et ne peuvent supporter les nouvelles applications gourmandes en bande passante.

De son coté, le Frame Relay accuse une chute relativement moins sensible en terme de parts de marché en raison du grand nombre de déploiements effectués au cours des années précédentes par les opérateurs. Le Frame Relay continue de répondre à certains besoins des entreprises et celles qui disposent d'un réseau Frame Relay ne peuvent pas toutes attendre d'une migration vers un réseau IP un retour sur investissement à court terme.



CESMO estime que le protocole IP qui représentait à peine 4% des réseaux d'opérateurs en l'an 2000, devrait s'imposer comme la principale technologie à l'horizon 2004 avec environ 40% des réseaux d'opérateurs devant l'ATM. La technologie Frame Relay ne devrait plus représenter à terme qu'un quart du marché contre environ 64% en l'an 2000.



Notons que si l'avenir semble appartenir au protocole IP, tant du point de vue « applicatif » que du point de vue « transport », l'émergence de cette technologie ne signifie pas la disparition totale et définitive du Frame Relay. A court terme, celui-ci sera de toutes façons encore largement utilisé par les opérateurs en tant que technologie de prolongement d'accès.

B - De nouvelles technologies d'accès à haut débit

Autre facteur technologique favorisant l'essor de l'IP VPN, les **nouvelles technologies d'accès au haut débit**. Le dégroupage de la boucle locale permet désormais l'introduction progressive d'une concurrence et la mise en œuvre de nouvelles technologies permettant des accès à haut-débit aux entreprises.

Grâce à l'ouverture du marché de la boucle locale en France en 2001, les technologies d'accès (en particuliers xDSL et BLR) sont nombreuses à se développer et permettent de plus en plus une couverture nationale et une capillarité importante sur le territoire français : **elles rendent ainsi l'IP VPN accessible à tous, du point de vue géographique comme du point de vue des coûts et facilite ainsi le déploiement d'architectures IP VPN par les entreprises.**

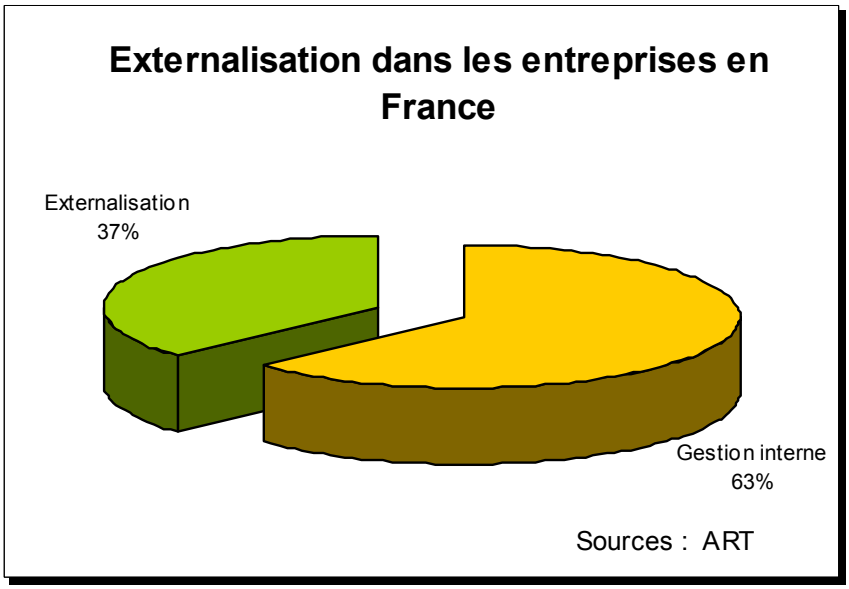
2. Des stratégies télécoms différentes

A l'aulne de cette double mutation technologique sur le marché de la donnée (suprématie émergente de l'IP et accès en hauts débits), les entreprises prennent progressivement conscience, après avoir mis en concurrence l'opérateur historique sur la téléphonie fixe, qu'elles pouvaient non seulement réaliser des économies sur ce poste de coût, mais aussi bénéficier de nouveaux services à valeur ajoutée.

Elles comprennent l'importance stratégique de leur problématique « réseau » et sont de plus en plus nombreuses à déléguer la gestion de toute ou partie de leur infrastructure (**externalisation**). Cette politique trouve sa pleine justification dans les nouveaux objectifs affichés par les entreprises de développement sous condition de rentabilité, de maîtrise et de réduction des coûts, et pour ce faire, de recentrage sur le métier d'origine.

2.1 Une externalisation de plus en plus forte

Comme le souligne une étude récente de l'ART (réalisée en 2000), les grandes entreprises françaises sont de plus en plus favorables à l'externalisation de tout ou partie de leur réseau. En France, 37% des entreprises déclarent en effet avoir délégué ce métier à un opérateur et ce pourcentage devrait augmenter progressivement dans les années à venir.



2.1.1 Dans les grandes entreprises françaises…

Les évolutions technologiques sont de plus en plus rapides et l'entreprise doit les suivre et apprendre à les maîtriser pour rester compétitive. Cela nécessite du temps et des investissements importants, deux choses incompatibles avec les priorités de toute entreprise qui doit rester concentrée sur son métier de base pour être performante.

En outre, les nouvelles solutions de type Extranet, ou d'utilisation d'applications en mode ASP, sont axées sur la mutualisation des ressources et poussent naturellement vers une gestion externalisée du réseau.

2.1.2 … et dans les PME aussi

L'unicité du lieu, du temps et de la production de l'entreprise, telle qu'elle était perçue jusqu'alors, laisse progressivement place à une organisation en réseau faisant appel à une multitude d'intervenants, partenaires - au sens large - de l'entreprise. La législation récente facilitant l'accès à une nouvelle forme d'entreprise (entreprises individuelles, essaimage, temps partiels, groupement d'entreprise, intégration verticale…) et la nécessaire réduction des coûts ont entraîné une remise à plat de l'organisation de la production et donc un accroissement de la sous-traitance à des coûts raisonnables, mieux maîtrisés et négociés.

L'externalisation doit permettre aux entreprises d'avoir accès à des services qu'elle ne pouvait se procurer auparavant, ou qu'elle devait réaliser elle-même en interne à des coûts mal maitrisés comportant des risques importants de gaspillage de ses ressources. Ceci est d'autant plus vrai dans les structures de taille moyenne qui ne peuvent allouer les ressources humaines, financières et organisationnelles suffisantes pour atteindre le même niveau de service que les grands groupes internationaux. L'externalisation représente alors une réelle opportunité d'accéder à des systèmes d'information qui leur étaient jusque là interdits.

2.2 Les motivations de cette externalisation

2.2.1 Réduction des coûts

Bien entendu, la réduction des coûts apparaît comme une des principales motivations de l'externalisation. Par ailleurs, les entreprises sont de plus en plus nombreuses à mettre en concurrence les opérateurs et favorisent ainsi l'émergence de nouveaux acteurs et de nouvelles offres sur le marché.

Ce contexte joue en faveur des offres d'IP VPN qui, reposant sur cette logique d'externalisation, permettent aux entreprises de maîtriser et de réduire leur budget télécom par rapport à des solutions de type Frame Relay.

2.2.2 Mais aussi, volonté de confier leur réseau à des opérateurs spécialistes

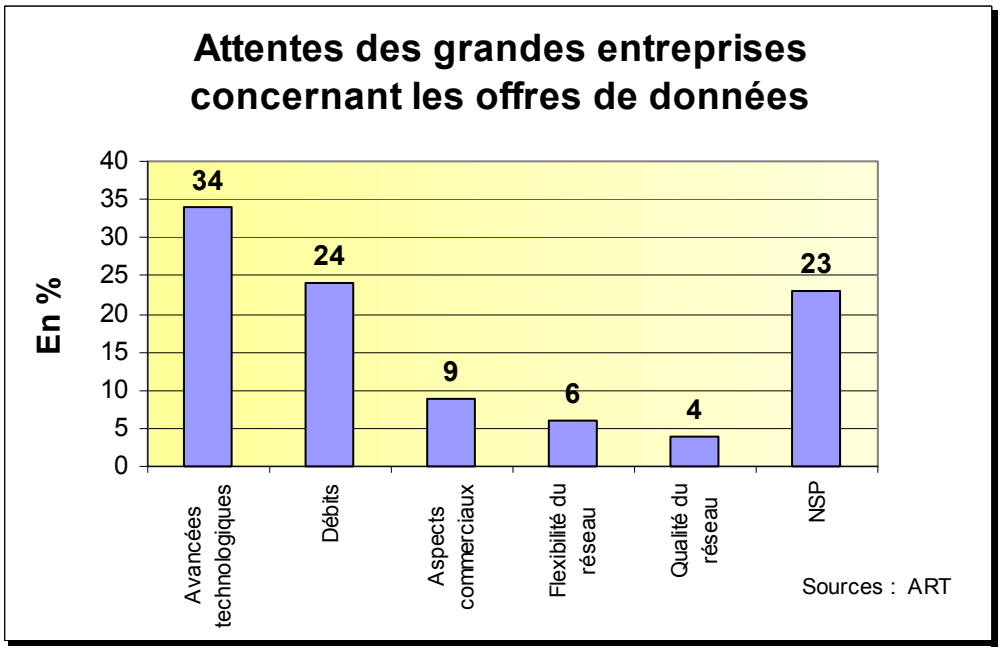
Au-delà des économies réalisées, l'entreprise montre une volonté de « coller » à son environnement économique et de disposer d'un réseau suffisamment flexible, capable de s'adapter à l'évolution économique de son métier.

En confiant la gestion de tout ou partie de son réseau à son opérateur, l'entreprise prend conscience de l'aspect stratégique de ce métier qui implique des compétences techniques dont elle ne dispose pas forcément en interne. Pour cela, l'entreprise se doit de sélectionner l'opérateur partenaire, dépositaire de sa confiance, qui puisse mettre en place la meilleure des solutions en rapport avec les besoins de l'entreprise (souplesse, flexibilité, moindre coût, évolution, …) et qui permette un contrôle permanent du service par l'entreprise.

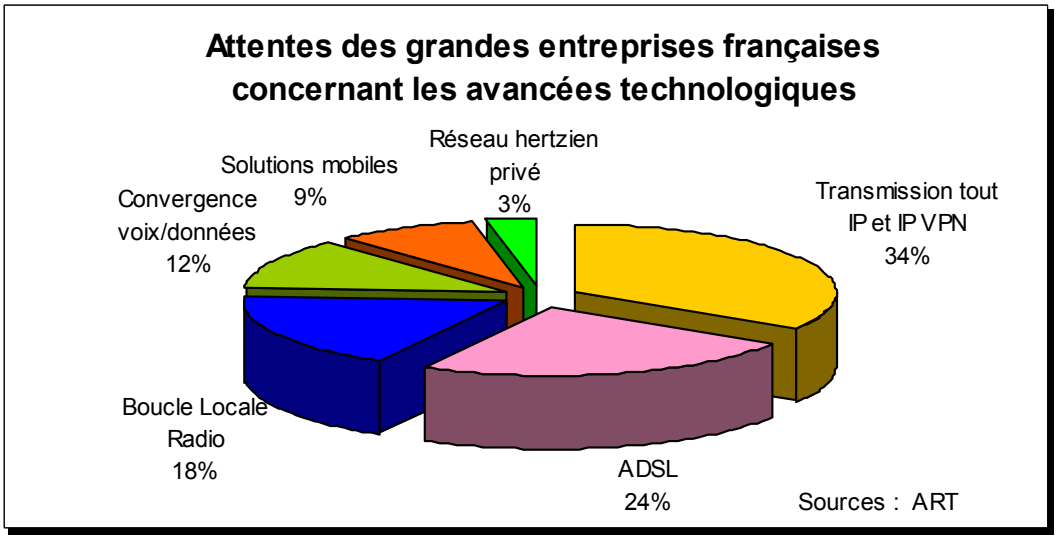
Là encore, l'IP VPN représente une réponse crédible à ce double objectif : disposer d'une solution réseau optimale et pouvoir la contrôler en permanence sans fournir l'effort financier, technique et humain ni détenir l'ensemble des compétences indispensables à sa réalisation.

2.3 Confiance dans le protocole IP

Ces objectifs sont révélateurs du fait que les grandes entreprises ont bien compris aujourd'hui l'importance des nouvelles technologies dans leur activité, sources de rentabilité et d'augmentation de la productivité. L'ART publie une étude qui illustre les priorités des entreprises françaises en matière réseau de données.



Ayant résolument adopté une logique applicative, 34 % des entreprises françaises comptent ainsi sur les progrès technologiques liés à l'IP VPN et aux nouvelles technologies d'accès ADSL et BLR pour augmenter leur compétitivité.



Les entreprises confortent ainsi le comportement des opérateurs dans leur positionnement tout IP et « nouvelles technologies d'accès ».

1.1 Besoins de haut-débit

Nous venons de l'évoquer, les stratégies télécoms des entreprises connaissent une profonde mutation qui repose en outre sur l'importance croissante des nouvelles technologies et des applications concrètes qui en découlent.

La recherche permanente de nouveaux gains de productivité : être plus réactif, mieux connaître son marché, avoir davantage de flexibilité (personnaliser le produit à la demande

du client par exemple)… passe par une meilleure exploitation des potentialités des nouvelles technologies de l'information et des communications.

Le haut débit devient par conséquent essentiel et stratégique pour l'entreprise car il permet la diffusion et le transport des applications de plus en plus volumineuses et cruciales pour le développement optimal de l'entreprise.

Un marché réel

1. Quelques chiffres sur le marché

Au-delà des visions prospectives sur les besoins des entreprises, quelles sont les réalités du marché des IP VPN en France ? Nombre d'analystes avaient prévu une forte croissance des IP VPN au niveau mondial et au niveau français dès l'année 2000. **Or, fin 2001, l'IP VPN commençait tout juste à décoller en France.**

1.1 Contexte

1.1.1 En 2000 : Période d'éducation de marché

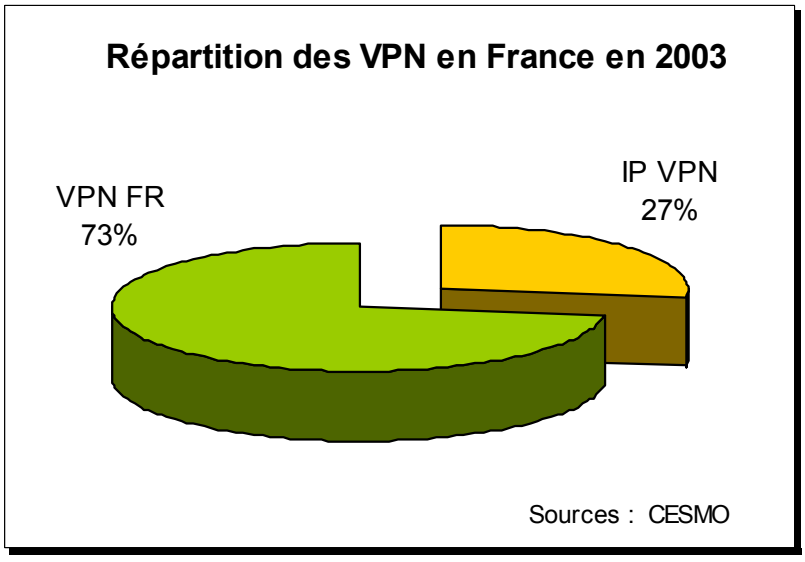
Ce retard apparent s'explique essentiellement par un manque d'offres disponibles sur le marché français en 2000. Les premières offres ne sont en effet apparues qu'à la fin du deuxième semestre et les opérateurs présents sur ce segment ont plutôt commencé leur activité avec des clients « tests » pour construire ou consolider ensuite leurs offres. Par ailleurs, le retard pris sur le dégroupage de la boucle locale ne permettait pas de faire la promotion de toutes les possibilités des IP VPN en termes d'accès haut débit.

Par conséquent, l'année 2000 et **le premier semestre 2001 ont plutôt fait l'objet d'une éducation de marché des entreprises.**

1.1.2 En 2001 : Phase de conquête client

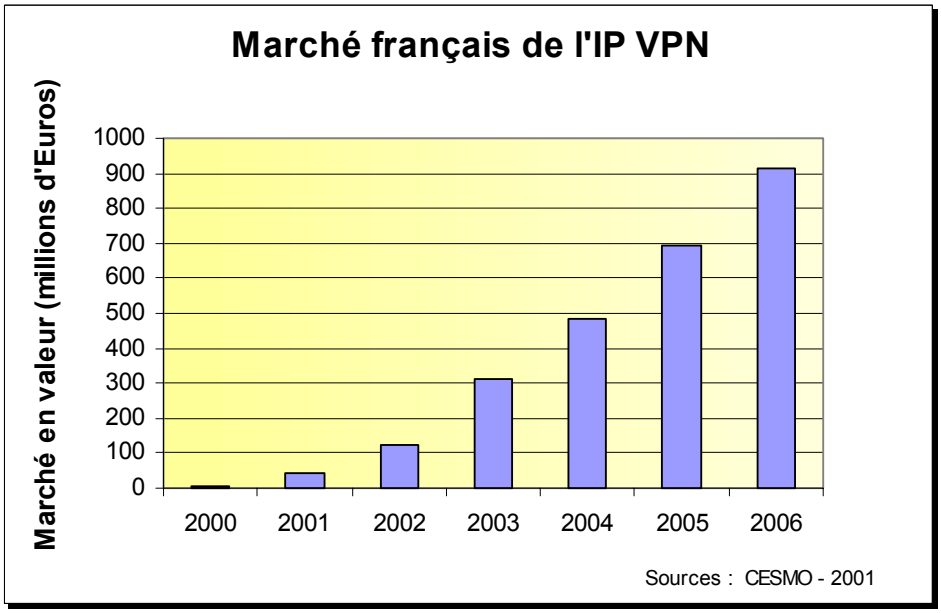
Aujourd'hui, les opérateurs sont en mesure de proposer des offres et **la demande est désormais bien réelle.**

Tenant compte du contexte du marché et de l'ensemble des facteurs favorables à la croissance du marché de l'IP VPN, CESMO estime qu'en 2003, l' **IP VPN représentera 27% des VPN des entreprises** (ces estimations n'intègrent pas les VPN ATM).



1.2 La quantification du marché

En terme de revenus générés par l'IP VPN, CESMO estime qu'ils étaient de l'ordre de 45 millions d'euros à fin 2001 et devraient atteindre 910 millions d'euros en 2006, soit une croissance exponentielle.

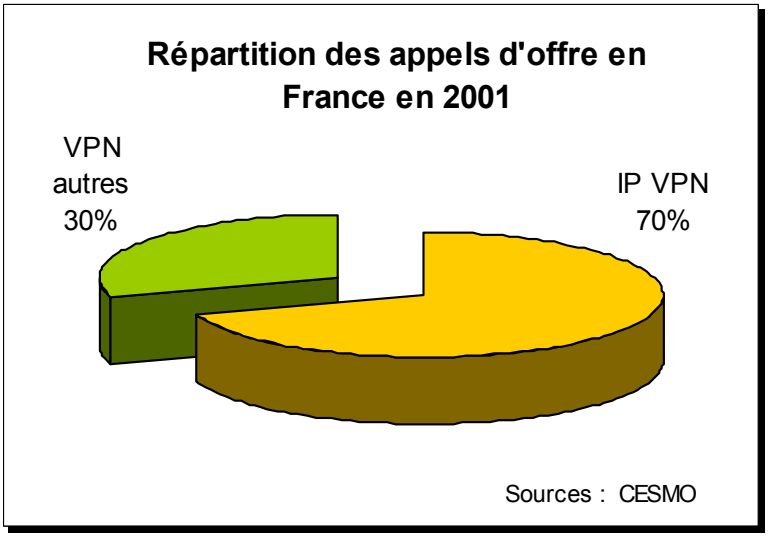


Ces prévisions optimistes sont, comme nous l'avons vu précédemment, justifiées par un contexte technologique et économique favorable.

2. Un intérêt prononcé de la part des entreprises

2.1 Vision sur la répartition des appels d'offres aujourd'hui

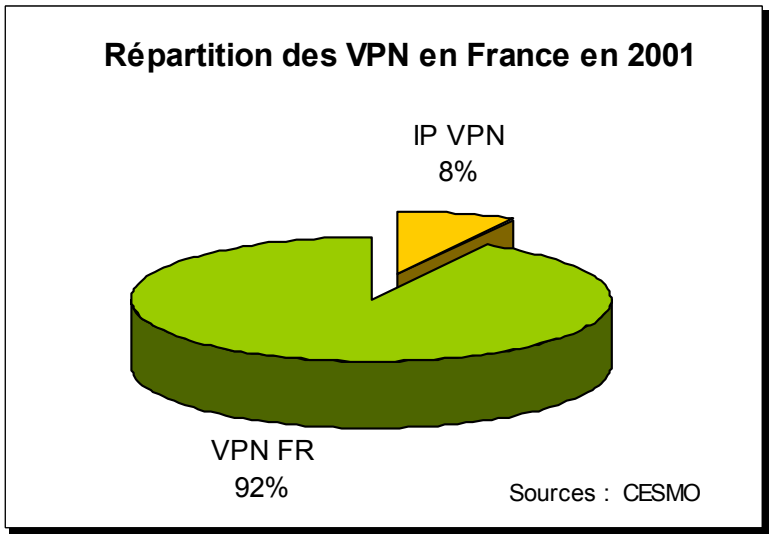
D'après les opérateurs, environ deux consultations d'appels d'offres sur la donnée sur trois en France concernent aujourd'hui la mise en place d'un IP VPN, ce qui confirme les besoins des entreprises :



Elles montrent donc un intérêt de plus en plus important pour les offres d'IP VPN dont les opérateurs font une grande promotion.

L'entreprise, qui connaît mal les fonctionnalités et les avantages dont elle pourra bénéficier via ces nouvelles offres, profite aujourd'hui des appels d'offre pour se familiariser avec les IP VPN.

Selon CESMO, fin 2001, l'IP VPN représentait 8% des VPN des entreprises (hors VPN ATM) contre 92% de VPN Frame Relay.



2.2 Quelles sont les raisons ?

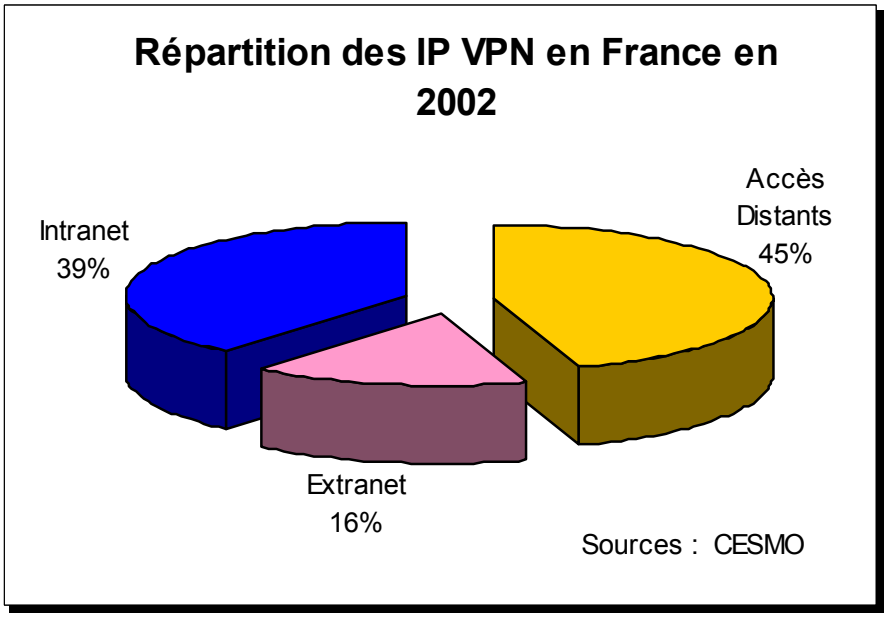
2.2.1 Une évolution des usages

A - L'accès distant pour les salariés

Confrontées à de nouvelles méthodes de travail, les entreprises voient, dans l'IP VPN, l'opportunité d'offrir de manière simple et sécurisée, des accès distants à ses salariés itinérants.

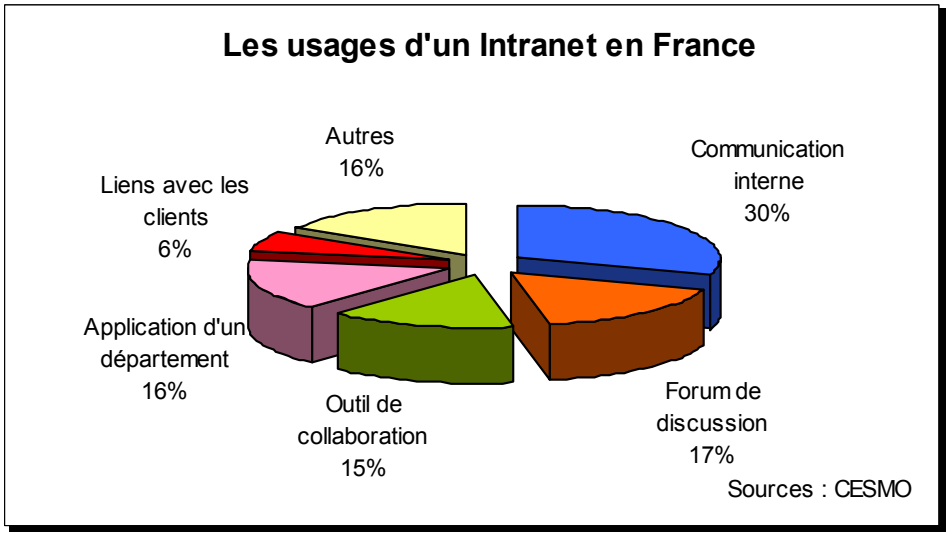
Ces nouvelles méthodes de travail sont en fort développement en France. Les **accès distants** favorisent non seulement la mobilité des salariés (nomades) en leur permettant de disposer d'un bureau virtuel depuis l'extérieur de l'entreprise mais favorisent également le travail collaboratif (travail synchrone ou asynchrone effectué par le salarié avec des équipes à distance, en utilisant des logiciels de travail de groupe (groupware).

La gestion de l'accès distant est donc devenue déterminante dans l'implémentation des IP VPN.



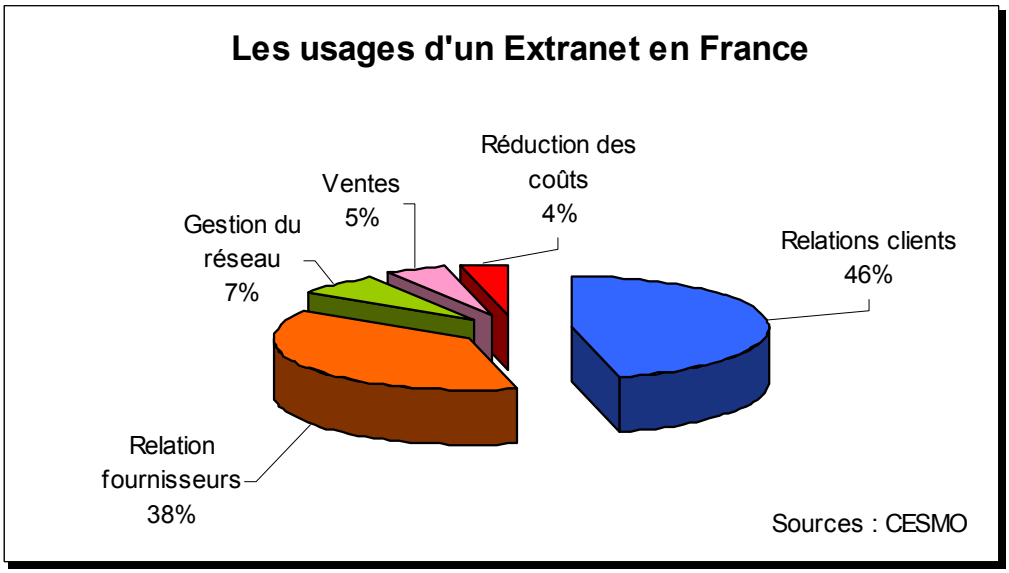
B - Intranet / Extranet

Autre raison essentielle de choix de mise en place d'un IP VPN pour une entreprise : l'Intranet ou Extranet. Pour la majeure partie des entreprises, la mise en place d'un **Intranet** a pour objectif de favoriser la communication interne ainsi que les discussions sous forme de forum. Grâce à l'Intranet, l'entreprise communique et joue la transparence avec ses salariés qui disposent ainsi de l'ensemble des informations en temps réel.



L'Intranet permet également d'encourager le travail collaboratif, de partager et transmettre les connaissances de l'entreprise (aussi bien les outils et les méthodes de travail que les références) et d'optimiser la veille stratégique et concurrentielle.

Parallèlement à la mise en place des Intranets, la mise en place d'un **Extranet** a pour objectif de favoriser la communication avec les fournisseurs et les clients :



Grâce aux **Extranets**, l'entreprise peut non seulement optimiser ses relations clients (Customer Relationship Management) mais simplifie et enrichit également l'ensemble des process liés à la Supply Chain Management.

- Les Extranets permettent le partage maîtrisé de l'information : c'est un facteur clé de productivité tant à l'intérieur de l'entreprise que dans le cadre d'une collaboration avec ses partenaires. Ce partage doit toutefois être contrôlé et maîtrisé : l'entreprise décide quelle information partager et avec quels acteurs. Ceci implique des communications sécurisées au sein de la « communauté d'intérêts » que forment l'entreprise et ses partenaires.

- Les Extranets développent la coordination des efforts : le seul partage d'informations ne permet pas de diriger tous les efforts de la « communauté d'intérêt » vers un objectif commun. La coordination des activités est un facteur de réussite. Ceci implique la mise en place d'une solution de communication globale, intégrant des outils de travail collaboratif, et permettant de maximiser l'efficacité des échanges au sein de la communauté.

- Enfin les Extranets peuvent engendrer une plus grande réactivité : la « communauté d'intérêt » est à même de réagir de manière rapide et flexible aux attentes des clients, en perpétuelle évolution. Il devient alors possible de diminuer le « time to market » des produits et de mieux réagir face à la concurrence. Cette réactivité est également importante afin de créer rapidement un réseau de communication avec un nouveau partenaire, que ce soit pour un projet commun de quelques mois ou pour des relations sur le long terme.

C - De plus en plus d'applications

Les offres d'IP VPN s'intègrent parfaitement à la tendance visant à l'unification et à la standardisation des interfaces telle qu'elle est observée dans les entreprises depuis plusieurs années. Les réseaux de données, autrefois simples infrastructures d'appui ou d'accès aux systèmes d'informations, prennent un rôle structurant dans de plus en plus de domaines stratégiques.

Jouant un rôle grandissant dans l'élaboration de processus concurrentiels tels que la relation client, l'e-business et le partage des connaissances, les offres d'IP VPN, grâce à notamment

à la différenciation des flux, permettent à l'entreprise de maîtriser ses priorités en termes d'applicatifs stratégiques.

D - Des perspectives (accessibilité des applications via ASP, voix sur IP, applications temps réel..)

De nombreuses applications voient actuellement le jour et donnent une illustration de ce que seront les futures applications profitant des réseaux VPN et des protocoles IP.
Si certaines de ces applications sont d'ores et déjà mise en œuvre par quelques entreprises, elles ne font pas encore l'objet d'une réelle et forte demande. Mais elles préfigurent l'avenir.

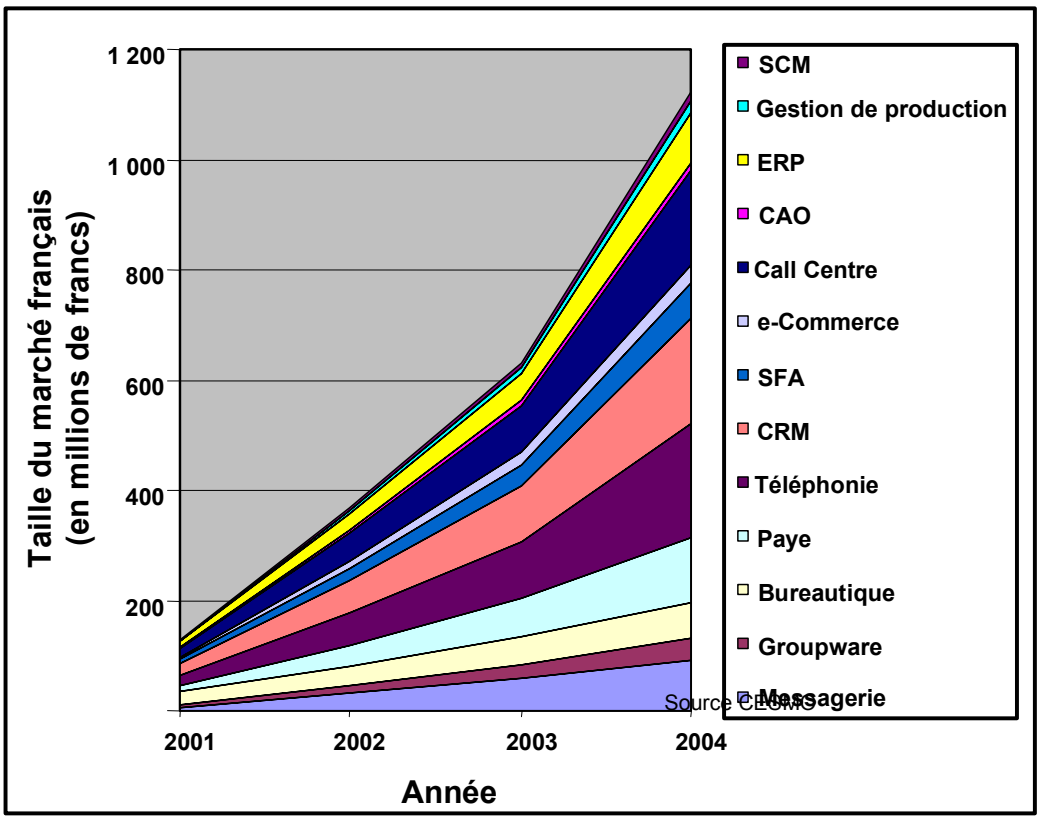
Parmi ces applications il est possible de distinguer :

- Les applications via ASP :

Les IP VPN, dans la mesure où ils permettent de **relier de manière flexible clients et fournisseurs,** semblent particulièrement bien adaptés aux nouveaux modes d'accès aux services applicatifs (mode ASP) qui se développent progressivement en France ou en Europe et qui permettent à l'entreprise de louer ses services applicatifs en ligne plutôt que de les acquérir.

Bien entendu, la richesse d'une offre ASP est fondée sur la capacité des réseaux à répondre parfaitement aux sollicitations de l'utilisateur. Aucun d'entre eux ne peut donc se permettre la moindre faiblesse technique sur l'élément qui structure l'ensemble de l'offre : la composante télécom.

En réalité, l'essor des offres commerciales ASP est non seulement lié aux fonctionnalités de réseau offertes par les VPN IP, mais aussi porté par celles–ci.



Le marché des ASP par type d'applications adressant les PME – PMI françaises

Les opérateurs qui tendent à développer autour d'eux des partenariats avec des éditeurs d'applicatifs ou des « content delivery network » travaillent dans ce sens et « remontent » ainsi dans la chaîne de services.

- La voix sur IP :

L'introduction des nouvelles technologies développe très fortement les perspectives de la Voix sur IP qui représente un fort enjeu économique pour les entreprises.

En effet, la voix sur IP permet de développer une solution de téléphonie a priori moins chère et intégrée à une solution télécom globale dans le cadre d'un réseau privé virtuel. La voix sur IP est une solution qui commence à être adoptée par les entreprises françaises.
Le marché devrait connaître une forte croissance à partir de 2003 avec une accélération de la **convergence voix-données**.

- Applications temps réel :

Les applications en temps réel, dont la voix mais aussi la video, l'audioconférence ou la vidéoconférence, sont des applications d'avenir sur les réseaux IP VPN car elles peuvent susciter outre des gains importants de productivité, des économies substantielles en termes de coût de communication entre les filiales ou avec les partenaires de l'entreprise.

Ces perspectives se heurtent encore toutefois à certaines contraintes techniques. Le dimensionnement des réseaux doit être réalisé avec une attention toute particulière du fait des débits importants que nécessitent ces applications et les temps de réponses très faibles indispensables pour permettre une communication réellement interactive et agréable entre les interlocuteurs. La voix sur IP n'est envisageable que si les délais de réponse n'excédent pas quelques millièmes de secondes, au-delà desquels une conversation téléphonique devient insupportable. De plus, pour assurer une qualité de service convenables aux applications en temps réel il convient de limiter au plus possible la déperdition d'information (perte de « paquets »).

Des bénéfices clients

1. Une réponse à des problématiques différentes

Récapitulons les principales problématiques qui peuvent inciter une entreprise à envisager la mise en place d'une solution d'IP VPN.

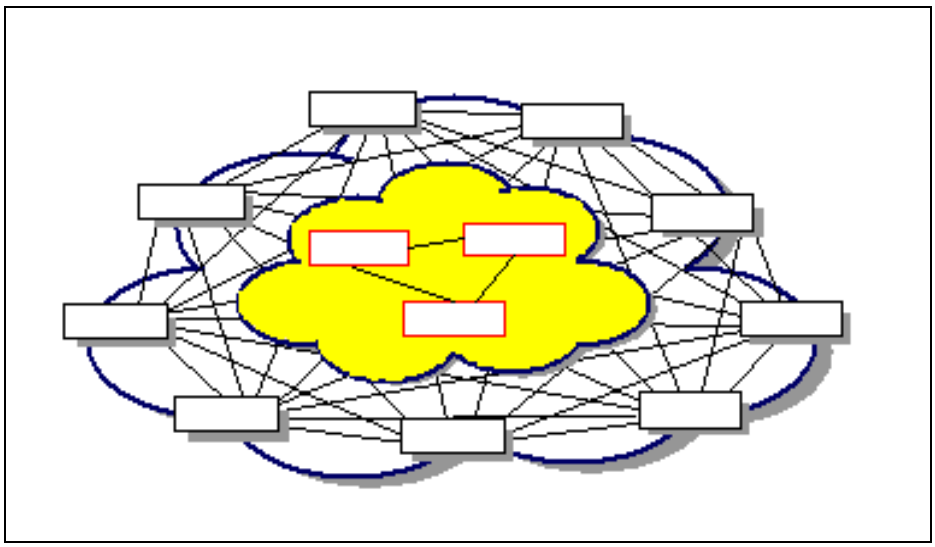
1.1 Problématique « d'accès Internet » et problématique de partage de l'information

1.1.1 En interne (entre sites distants)

L'axe numéro un consiste en l'amélioration et le développement de la communication interne à l'entreprise. Les solutions de communication doivent permettre un accès, pour tous les membres autorisés, aux applications SI de l'entreprise, n'importe où, n'importe quand, par tout type de terminal (fixe, mobile, PDA …), de façon fiable, rapide et sécurisée.

Cette souplesse était jusqu'alors impossible, incomplète ou bien très coûteuse à réaliser. En effet, les solutions traditionnelles ne permettent pas un accès à distance aisé, simple à mettre en oeuvre et économique. Le Frame Relay par exemple est peu adapté à des Intranet maillés de type « any-to-any », c'est à dire reliant tous les sites de l'entreprise les uns aux autres sans définir un lien permanent entre chaque site deux à deux. Le Frame Relay est une technologie orientée circuit : des CVP (Circuits Virtuels Privés) doivent être créés entre les deux extrémités souhaitant échanger des données, il s'agit donc d'une technologie « point-à-point ».

La figure ci-dessous représente un VPN Frame Relay et illustre bien cet aspect limitatif. Les équipements en noir représentent les routeurs CE (Customer Edge) dédiés à un site. Les équipements en rouge sont des commutateurs de type Frame Relay et constituent le backbone du réseau.



Représentation d'un réseau Frame Relay

La connectivité des solutions IP VPN représente un réel progrès dans la direction d'une meilleure souplesse et permet la connexion de l'ensemble des sites, même les plus petits et les plus éloignés sans engager des investissements disproportionnés.

1.1.2 En externe (avec clients et fournisseurs)

Nous avons déjà développé tous les avantages que représentent les Extranets dans la gestion et le développement de la relation client et la meilleure communication avec les partenaires.

Pour la même raison que précédemment, les technologies de type Frame Relay apparaissent comme peu adaptées aux Extranets. En effet, un réseau Frame Relay est un service orienté connexion, ses CVP définissent des connexions semi-permanentes qui contrarient les exigences de souplesse et de flexibilité requises dans le cadre d'un Extranet. Les modifications de topologie (ajout d'un site, suppression d'un site, …) ou l'augmentation de débit sont relativement complexes puisque ils nécessitent la création de nouveaux CVP. Même si la gestion est entièrement assurée par l'opérateur, elle est à l'origine de délais d'évolution plus importants qu'avec un IP VPN. De plus, si l'entreprise dispose d'une solution Frame Relay, ce n'est pas forcément le cas de l'ensemble de ses partenaires et des membres de la « communauté d'intérêt » qu'elle souhaiterait voir intégrés à son réseau.

Paradoxalement, l'objectif de créer une meilleure communication se heurte d'emblée aux outils déjà mis en place.

Les IP VPN permettent au contraire de développer rapidement une solution de type Extranet et d'en suivre l'évolution tout en économisant la mise en place d'un réseau physique coûteux et peu flexible qui réclamerait une profonde recomposition à chaque modification du périmètre de la « communauté d'intérêt » (disparition ou apparition d'un nouveau site, déménagement, …).

1.1.3 Et surtout un partage de l'information avec les travailleurs nomades

Le partage d'informations avec les travailleurs nomades est un autre objectif stratégique auquel peut répondre un IP VPN. L'accès aux ressources du système d'information doit être sécurisé. Cela implique la définition préalable de profils d'utilisateurs avec les autorisations d'accès associées et l'authentification des utilisateurs à la connexion. La gestion des liaisons et des autorisations est, grâce aux IP VPN, simplifiée. Elle permet souvent un pilotage depuis un tableau de bord web très accessible et assurant une grande réactivité.

Le personnel nomade et les télé-travailleurs peuvent dès lors être pris en compte dans une solution de réseau globale et être intégrés à l'entreprise de façon transparente, sans contrainte supplémentaire liée à la localisation. Le personnel nomade peut accéder à l'Intranet de l'entreprise en utilisant un PC portable doté d'un modem et en se connectant à un ISP par un appel local. Il n'y a donc pas de coût d'appel longue distance, ni d'équipements spécifiques à prévoir (mis à part le logiciel de sécurisation à installer sur le PC et le logiciel permettant de gérer le protocole de « tunneling » au niveau du serveur de sécurité et de la passerelle IP VPN). Là encore l'IP VPN apporte plus que les solutions de type Frame Relay qui sont peu adaptées aux accès commutés, ce qui est un facteur limitatif pour l'accès à distance des personnels nomades et des télé-travailleurs.

1.2 Problématique applicative

1.2.1 Gestion des applicatifs

Une autre problématique essentielle des entreprises est la gestion et l'intégration de nouvelles applications métiers au sein de leur organisation. Pour cela, les réseaux de communication doivent garantir une interopérabilité avec les applications anciennes et permettre la mise en place de nouvelles applications comme la voix sur IP, la vidéoconférence, les ERP, les outils de CRM, les applications hébergées en temps-réel, les applications interactives et collaboratives, etc. L'évolution vers un réseau IP VPN permet l'intégration de tous types de flux et apparaît comme une solution particulièrement souple de ce point de vue. De plus, la majeure partie des nouvelles applications est conçue sur la base du protocole IP et a pour but de fonctionner sur des réseaux IP.

Les opérateurs proposant des offres de IP VPN enrichissent par ailleurs leurs offres de classes de services. Elles permettent de différencier les flux applicatifs en fonction du type d'applications supportées et leur associent des priorités. Les applications critiques et stratégiques de l'entreprise ne sont ainsi jamais polluées par des flux moins importants (messagerie, web, …).

1.2.2 Accessibilité à de nouveaux applicatifs en mode ASP

L'émergence d'applications en mode ASP et l'intérêt que suscite en Europe cette nouvelle façon d'aborder les solutions applicatives permettant à l'entreprise de louer ses applications en ligne plutôt que de les acquérir, n'est pas sans répercussions sur le type de réseau de l'entreprise.

Au moment de faire le choix d'une solution réseau dans l'entreprise ou de son évolution, il convient sans doute, à la lumière des possibilités offertes par le mode ASP, d'opter pour un réseau multi accès, avec une forte capillarité et une grande souplesse de gestion qui relie de manière flexible clients et fournisseurs. Ces caractéristiques, qui peuvent être supportées par les solutions IP VPN, sont très avantageuses lorsqu'il s'agit de mettre en place des applications en mode ASP. Le développement de ce type d'offre est même conditionné par l'existence de ces réseaux hauts débits, aux temps de réponses courts, permettant une réelle interactivité entre le fournisseur de service (l'éditeur de l'application ASP) et l'entreprise utilisatrice du service.

2. Une solution flexible

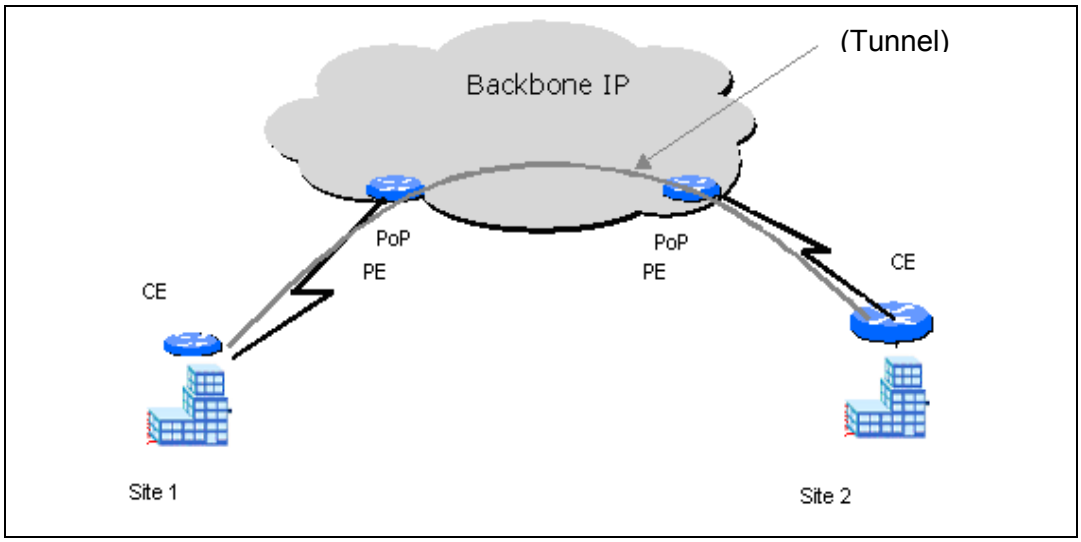
2.1 Simple à mettre en œuvre

En parcourant l'éventail des problématiques de l'entreprise et leur impact sur la configuration des réseaux de communication, il apparaît que la flexibilité de ces réseaux est une des caractéristiques essentielles tant pour leur mise en œuvre que pour leur évolution et l'évolution des usages.

Nous avons vu que les IP VPN fournissent une connectivité de n'importe quel terminal à n'importe quel terminal et qu'il n'est pas nécessaire de créer de lien spécifique entre 2 points : il s'agit d'une structure « any-to-any ».

Le backbone IP peut être considéré comme un « nuage » dans lequel chaque nouveau site qui se connecte est reconnu, c'est à dire qu'il voit et est vu de l'ensemble des autres sites connectés contrairement aux VPN Frame Relay qui ne fournissent de connectivité qu'entre des points terminaux prédéterminés.

Les IP VPN garantissent donc une simplicité dans la mise en œuvre supérieure aux autres solutions de VPN.



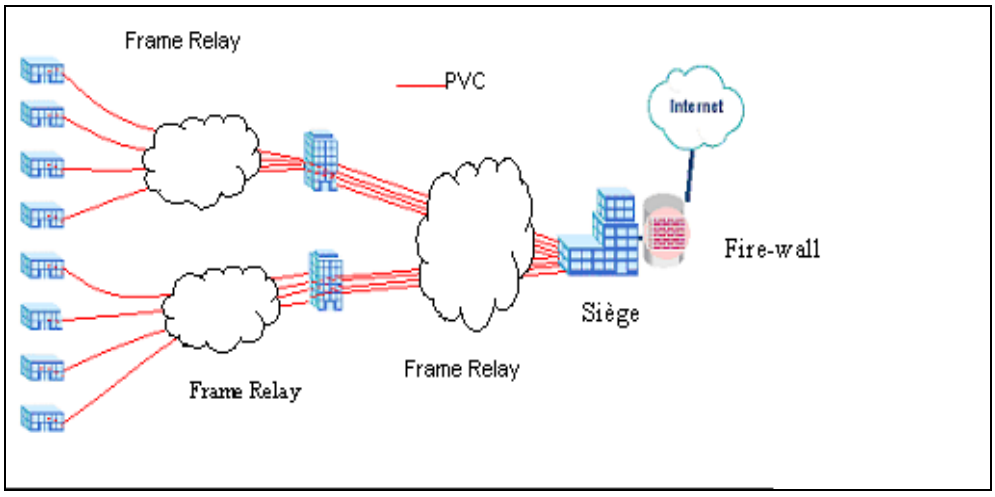
Un réseau IP natif

Le routeur situés dans les locaux des clients porte le nom de CE (Customer Edge) et le routeur de rattachement au POP le nom de PE (Provider Edge). Ces routeurs PE sont rattachés à des routeurs P (Provider) au cœur du backbone de l'opérateur.

2.2 S'adapte aux différentes structures d'entreprises

La mise en œuvre d'une solution de réseau dépend pour beaucoup de la structure de l'entreprise ou de sa « communauté d'intérêt » et la complexité de leur organisation géographique.

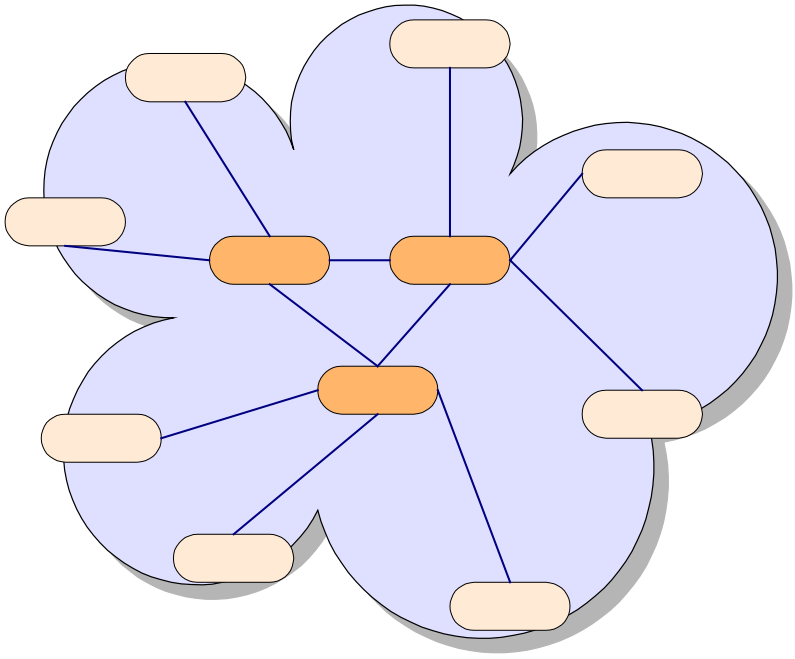
Dans le prolongement de notre comparaison avec le Frame Relay VPN, ce dernier est bâti sur un réseau constitué de deux parties : un **backbone** (réseau de transport) comprenant des commutateurs Frame Relay, reliés entre eux par des liens haut débit (typiquement de la fibre optique) et une partie **accès** permettant de relier les sites de l'entreprise à un des points de présence (POP) du backbone de l'opérateur. Ce type de réseau s'adapte parfaitement à une organisation « verticale » où des filiales de plusieurs rangs sont reliées au siège : les flux de communications « remontent » des filiales vers le siège et « redescendent » du siège vers les filiales.



Exemple d'architecture adaptée à la technologie Frame Relay

Dans ce type d'architecture, les filiales n'ont pas de besoins spécifiques d'échanger des flux directement entre elles, sans passer par le siège.

Un IP VPN peut parfaitement convenir à ce type d'organisation, mais il s'adapte également à une organisation plus éclatée, en « étoile », telle qu'une entreprise disposant de nombreux sites échangeant deux à deux des données (applications distribuées) car le réseau IP VPN est par essence maillé, comme l'illustre le schéma ci-dessous :



Structure « any-to-any » et maillée d'un réseau IP

2.2.1 Facilite l'ajout et suppression de sites

Cette souplesse liée à l'architecture « any-to-any » facilite les modifications (ajout d'un site, suppression, …), permet le déploiement rapide de nouvelles applications, facilite la création de plusieurs IP VPN par site (offre multi-VPN des opérateurs) et permet d'optimiser aisément les débits nécessaires à l'entreprise.

2.2.2 Facilite les accès distants

La solution IP VPN répond très bien aux exigences liées aux accès distants car elle permet aux travailleurs nomades de se connecter très facilement via un simple accès Dial Up tout en bénéficiant d'une connexion sécurisée.

3. Une solution pour tous

Les solutions IP VPN sont des solutions multi-accès et multi-applications, ce qui est un facteur facilitant grandement l'intégration et la gestion de réseaux.

3.1 Compatible avec toutes les applications

Ce type de réseau permet de véhiculer toutes les applications possibles notamment les applications distribuées mais aussi les applications les plus critiques et les plus exigeantes en terme de qualité de service (temps réel) telles que la vidéoconférence, la voix sur IP, etc.

Notons que les classes de service temps réel, disponibles aujourd'hui chez les opérateurs, sont pour le moment peu demandées par les entreprises françaises.

3.2 Compatible avec tous les types d'accès

Si les premières offres opérateurs ne proposaient essentiellement que des accès RNIS ou via LS, le dégroupage de la boucle locale et de la Boucle Locale Radio permettent aujourd'hui aux opérateurs d'IP VPN de proposer des accès haut-débit, soit en partenariat avec des opérateurs, soit en ayant eux-mêmes développé leur offre d'accès local haut-débit.

Aujourd'hui, plus de 80% des acteurs sont en mesure de proposer des accès DSL (malgré le développement très récent des offres en propre, s'appuyant souvent sur l'offre de l'opérateur historique) et plus d'un tiers d'entre eux des accès BLR via des partenariats. Dans ce domaine également, les IP VPN présentent plus d'avantages que les offres de type VPN Frame Relay qui sont moins aisément compatibles avec des technologies d'accès low cost tels que l'ADSL. L'IP VPN permet effectivement de réduire les coûts.

4. Une solution de tranquillité

Dans le cadre d'un politique d'externalisation, une offre IP VPN opérateur propose un périmètre d'externalisation plus large que les offre VPN Frame Relay : les opérateurs prennent en charge jusqu'aux routeurs situés dans les locaux de l'entreprise et proposent une gestion de bout en bout, tant du point de vue technique qu'humain. Ils fournissent une solution clé en main.

Ainsi l'entreprise a un prestataire unique, n'a pas d'investissement à réaliser et peut se recentrer sur son cœur de métier.

4.1 Des gains de temps et de compétences

Cette évolution fait gagner à l'entreprise du temps et des ressources qu'elle peut allouer à d'autres tâches et la libère des efforts d'acquisition de compétences indispensables à la gestion d'un réseau basé sur une solution développée en interne.

Chiffrer de façon détaillée les économies réalisées par le biais de la mise en place d'un IP VPN en terme de personnels ou de gain de temps, est un exercice qui dépend fortement des spécificités propres à chaque entreprise et chaque organisation. CESMO propose, dans le chapitre consacré aux coûts (§4.6), une estimation des économies réalisées sur la base d'une combinaison de différents éléments de coûts (coûts des équipements, coût de gestion du réseau, coût de l'accès, …) et reposant sur des mesures effectives.

Au-delà des économies réalisées, l'entreprise profite des compétences pointues et sans cesse mises à jour d'un opérateur qui lui apporte en outre le conseil amont et l'accompagnement dans le développement de sa solution.

4.2 Une qualité de service maitrisée

Cet apport de compétences doit s'accompagner d'une qualité de service et de sécurité. En s'appuyant sur le protocole DiffServ par exemple, les opérateurs offrent plusieurs classes de service associées à une qualité garantie de bout en bout.

La sécurité est assurée, selon les solutions adoptées par les opérateurs, sur IPSEc, ou sur une double authentification « client et utilisateur » reposant sur le protocole Radius, … Ces solutions sont généralement associées à des firewall managés par l'opérateur et qui permettent de sécuriser l'Intranet ou l'Extranet vis à vis d'attaques extérieures.

4.2.1 Supervision continue du réseau de l'entreprise

Un des avantages essentiels des IP VPN réside dans le fait que la gestion du réseau revient à la charge du fournisseur de service et non à l'entreprise utilisatrice du IP VPN. L'opérateur fournit le paramétrage de l'architecture mais aussi la supervision du service 24h/24 ainsi que les statistiques détaillées de l'utilisation du réseau. L'entreprise peut alors réellement se concentrer sur son métier d'origine tout en conservant un contrôle opérationnel permanent de la qualité du réseau qu'elle utilise et la gestion des droits utilisateurs grâce à des interfaces simplifiées du type Web.

4.2.2 La garantie de disposer d'engagements contractuels (SLA…)

Contrairement aux VPN basés sur l'Internet public, l'opérateur prend, sur les offres IP VPN opérateur, des engagements de qualité de service sous forme de SLA (Service Level Agreement) à l'image de ce qui se fait pour les solutions VPN Frame Relay.

La qualité du réseau ou de la classe de service est alors caractérisée par plusieurs paramètres mesurables tels que :

- la disponibilité de services
- le délai de transmission
- la gigue : variation du délai de transmission
- le débit : moyen ou maximum
- le rapport des « paquets » perdus

Le SLA est un contrat de service entre le fournisseur du réseau et l'entreprise définissant la qualité. Les SLA sont associés aux différentes classes de service offertes par l'opérateur :

best effort, qualité standard, temps réel, applications critiques…, chaque opérateur proposant un certain nombre de classes de service (généralement 3).

Ces classes de service permettent de prioriser les flux applicatifs de l'entreprise afin de fournir la bande passante nécessaire aux applications critiques. Les classes de service permettent de regrouper les applications possédant les mêmes caractéristiques et la même importance pour l'activité de l'entreprise, ce qui accroît les performances et optimise la bande passante disponible. Les utilisateurs gagnent en confort d'utilisation et l'entreprise en coût d'infrastructure. Sans classe de service, les applications non critiques peuvent dégrader les performances des flux critiques à moins que l'opérateur dimensionne le réseau de façon très large.

4.3 Une bande passante optimisée

4.3.1 Priorité donnée aux applications stratégiques de l'entreprise

Les contraintes de débits qui existent sur tout type de réseau sont critiques sur les IP VPN. Les utilisateurs ont tout intérêt à s'assurer auprès de l'opérateur de la qualité de son réseau en prenant des garanties de type SLA comme nous venons de le voir. Les opérateurs qui disposent de leur propre réseau de fibre optique présentent l'avantage de pouvoir réellement s'engager sans être dépendant de tel ou tel autre partenaire.

Ainsi, l'opérateur peut dimensionner l'IP VPN de façon adaptée aux besoins de l'entreprise, et en s'appuyant sur une analyse du trafic, lui apporter son conseil sur les priorités à associer à chaque type de flux, les applications critiques se voyant affecter une priorité maximale.

4.4 Une sécurité adaptée

4.4.1 IP VPN Internet

Lorsqu'il s'agit de service IP VPN via l'Internet public, la sécurité est considérée comme un élément critique qui doit être garanti – autant que faire se peut – par la combinaison de différentes méthodes et outils, qui sont :

- la **tunnellisation** : qui consiste à établir des connexions logiques point à point sur un réseau IP à libre accès avec ou sans cryptage.
- le **cryptage** : qui peut s'appliquer à une connexion « tunnelisée » et qui consiste à brouiller les données en les rendants illisibles aux personnes non autorisées afin d'assurer une sécurité encore renforcée (différents degrés de cryptage peuvent être appliqués selon le degré de confidentialité requis).
- enfin, les **pare-feu** (firewall) sont une assurance complémentaire contre les accès non autorisés aux données de l'entreprise et peuvent être mis en oeuvre et gérés soit par l'entreprise elle-même soit par le fournisseur de services.

4.4.2 IP VPN Opérateur

Dans le cas d'un service d'IP VPN proposé par un seul fournisseur de services possédant son propre réseau privé (IP VPN opérateur), le trafic entre les sites IP VPN peut être assuré

en toute sécurité. Les IP VPN opérateurs sont particulièrement recommandés pour les applications de type Extranet ou de commerce électronique sécurisé car les paramètres de sécurité peuvent être précisément détaillés et permettre de limiter les accès aux seules personnes ou sites souhaités.

L 'opérateur peut s'appuyer, selon les cas, sur différents protocoles de sécurisation et d'étanchéité des flux comme le protocole IPSec.

4.4.3 Des niveaux de services différents

Comme nous l'avons vu, les IP VPN qui supportent des QoS différenciées proposent généralement trois niveaux de « classes de service », chacun comportant ses propres paramètres QoS :

- voix et multimédia en temps réel : les standards QoS s'appliquent à la disponibilité du réseau, aux temps de transmission, à la perte de paquets et aux distorsions en cours de communication
- données vitales : les standards QoS s'appliquent à la disponibilité du réseau, aux temps de transmission, à la perte de paquets
- le meilleur effort (best effort) : les standards QoS s'appliquent seulement à la disponibilité du réseau

4.5 Une mise à disposition d'outils de reporting

4.5.1 Le principe

L'entreprise qui fait le choix d'externaliser sa solution réseau ne doit pas pour autant perdre la maîtrise de tout ou partie de son réseau.

C'est une des raisons pour lesquelles les opérateurs ont développé des outils de reporting pour le client qui permettent à l'entreprise de savoir exactement ce qui transite sur son réseau.

Ce reporting ne prend pas la même forme selon les opérateurs qui le proposent, mais il est accessible généralement via Internet. Les opérateurs de IP VPN proposent des reporting par VPN dans le cas où l'opérateur proposerait des solutions multi-VPN et des reportings par classe de service. Ainsi, il est possible d'effectuer un suivi du déploiement site par site et classe de service par classe de service.

Le reporting reprend également les indicateurs généraux sur le fonctionnement du backbone de l'opérateur : niveau de charge, temps de réponse entre chaque POP, taux perte de paquets, gigue … et les statistiques peuvent être disponibles sous forme de graphiques ou de tableurs afin de permettre au client de contrôler les usages de son réseau. Certains acteurs mettent en place des outils d'alarmes et de cartographie sophistiqués permettant de contrôler avec pertinence la qualité du service.

4.5.2 Consultable en ligne

Certains opérateurs proposent, via le Web, des services à valeur ajoutée facilitant les relations entre l'entreprise et l'opérateur : optimisation de forfait pour les accès nomades, gestion de commandes et de factures, etc.

L'entreprise dispose de statistiques exhaustives, ce qui permet de maîtriser la croissance du trafic, et donc d'avoir un réseau toujours correctement dimensionné. Les outils de suivi sont en général aisés à utiliser et ergonomiques. Les services client de ce type sont plus faciles à développer qu'avec une solution Frame Relay. Ces outils permettent également à l'entreprise de vérifier que l'opérateur respecte bien ses engagements.

4.6 Une maîtrise des coûts

4.6.1 Des forfaits mensuels

Enfin, la solution IP VPN doit garantir une maîtrise totale des dépenses en communication, le tout prenant en compte le coût associé au personnel nomade et les télé-travailleurs. Aujourd'hui les opérateurs facturent essentiellement au forfait en fonction du débit consommé.

4.6.2 Une réduction des côuts

Cet objectif de réduction des coûts est très souvent associé à l'IP VPN. C'est souvent la première motivation des entreprises. En effet ces solutions sont parfois plus économiques que les réseaux privés ou les réseaux privés virtuels Frame Relay. Ce n'est pourtant pas systématique et il n'est pas possible de s'épargner une étude précise des contraintes spécifiques à chaque entreprise.

La solution qui apparaît clairement comme la plus économique consiste à se baser sur une offre IP VPN Internet (Internet public), même si le coût des mécanismes de sécurité (authentification, chiffrement, etc.) à mettre en place n'est pas toujours insignifiant, surtout quand le nombre de sites est important.

Le comparatif entre les VPN Frame Relay et l'IP VPN Opérateur est plus délicat car il dépend réellement de chaque situation : nombre et situation géographique des sites, débits, applications stratégiques de l'entreprise, etc…

Au vu de son expérience du dépouillement d'appels d'offre IP VPN, CESMO estime que les coûts actuels d'un IP VPN Opérateur sont en général identiques ou légèrement inférieurs à ceux d'une solution Frame Relay, mais avec des services supplémentaires (any-to-any, …), ce qui induit un meilleur rapport qualité/prix.

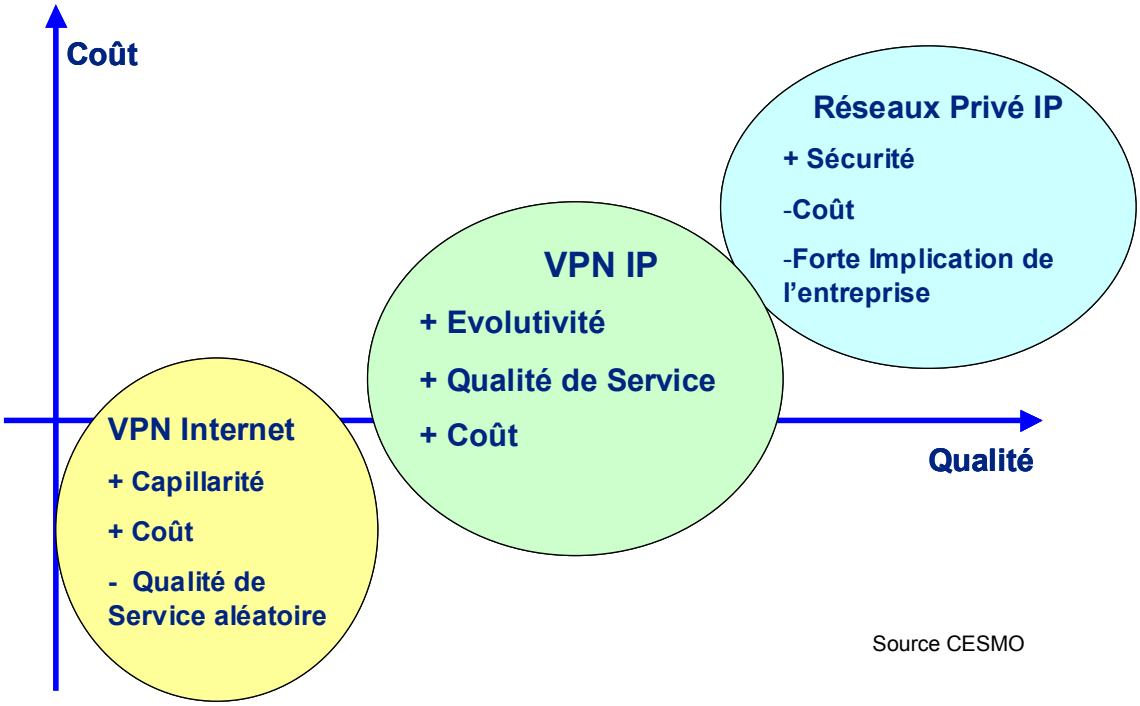
Les raisons de ces différences de coûts sont les suivantes :
- les équipements liés à l'IP VPN sont moins chers que les équipements FR
- le protocole IP est moins complexe à gérer (pour une solution FR, il faut tirer des circuits privés virtuels, ce qui n'est pas le cas pour IP). Ainsi, les ressources (techniques et humaines) nécessaires à l'installation d'une solution Frame Relay n'ont plus lieu d'être dans une solution IP. Cela réduit les coûts de revient de l'opérateur, et donc par conséquent les prix de vente.
- avec les classes de services, la bande passante est optimisée ce qui permet d'éviter un surdimensionnement des liens d'accès et les coûts qui lui sont associés (soit une économie d'environ 30%)

Au-delà des raisons qui tiennent essentiellement à la technologie IP, il existe aussi des raisons liées au type d'accès. Ainsi, au vu des réponses aux appels d'offres que CESMO étudie, il apparaît les différences de coûts suivantes :
- le VPN IP avec accès LS revient à environ 5% moins cher qu'un VPN FR avec accès LS

- le VPN IP avec accès ADSL revient entre 15 et 20% moins cher en moyenne et dans certains cas, l'économie réalisée avec un VPN IP accès ADSL peut aller jusqu'à 50% de la facture télécom avec accès LS.

Ces écarts devraient augmenter progressivement en raison : de la concurrence que se livrent les opérateurs, de l'amortissement des infrastructures déployées (amortissement des équipements IP, nombre de POP IP croissant permettant de réduire les coûts, nombre croissant de clients sur les infrastructures - le principe des IP VPN étant de faire partager aux clients la même infrastructure - les opérateurs vont donc pouvoir mieux rentabiliser leurs infrastructures et réduire ainsi leurs tarifs) et de l'essor des nouvelles technologies d'accès comme l'xDSL et la BLR.

Le schéma ci-dessous positionne les solutions IP VPN Internet, IP VPN opérateur et réseaux privés IP en terme de qualité de service et de coût :



Les réseaux IP VPN disposent, comme nous venons de le voir, de nombreux atouts et répondent aux besoins d'un nombre croissant d'entreprises de toute taille. Ils représentent un marché et une technologie dont l'expansion devrait être fortement croissante dans les années à venir et permettre à un plus grand nombre d'entreprises de disposer de solutions adaptées aux nouveaux modes de communications.

Conclusion

Les entreprises, de plus en plus favorables à l'externalisation de tout ou partie de leur réseau, bénéficient aujourd'hui d'offres IP VPN de plus en plus riches en terme de fonctionnalités.

Les opérateurs développent leurs offres en y implémentant sans cesse de nouveaux services, des possibilités croissantes en terme de diversité d'accès, de souplesse, de facilité de gestion, de garanties en terme de débit, disponibilité et sécurité et remontent dans la chaîne de valeur. Les opérateurs proposent désormais des solutions opérationnelles qui s'adaptent à l'ensemble des entreprises.

Les différences d'usage et de coûts dont bénéficient ces solutions représentent un intérêt bien compris des entreprises qui choisissent de plus en plus de migrer vers les IP VPN. Cette tendance devrait s'accroître encore dans les prochains mois et les prochaines années avec la baisse des coûts liée à la concurrence entre opérateurs et le développement des nouvelles technologies d'accès.

COLT, principal opérateur et fournisseur de solutions télécoms et Internet à valeur ajoutée

Décidé à garder sa position dominante sur un marché essentiellement centré sur les infrastructures, COLT a placé la valeur ajoutée au 1er plan de ses axes stratégiques de développement.

Créé en 1992, COLT commercialise une gamme complète de solutions à destination des entreprises, opérateurs et fournisseurs de services Internet : téléphonie, numéraux spéciaux, réseaux privés hauts débits, accès et hébergement Internet, …

COLT est aujourd'hui présent dans 32 villes - soit 13 pays européens - reliées entre elles par un réseau unique de 13 000 Km entièrement déployé, géré et supervisé par COLT. 11 centres d'hébergement sont également disposés sur ce réseau, actuellement renforcé par le déploiement d'une infrastructure DSL (dans le cadre du dégroupage en Europe).

Présent en France depuis 1997, COLT dispose d'une couverture nationale reposant sur différentes technologies (fibre optique, aDSL, sDSL, liaisons spécialisées…) pour apporter à toutes les entreprises une gamme de services de grande qualité.