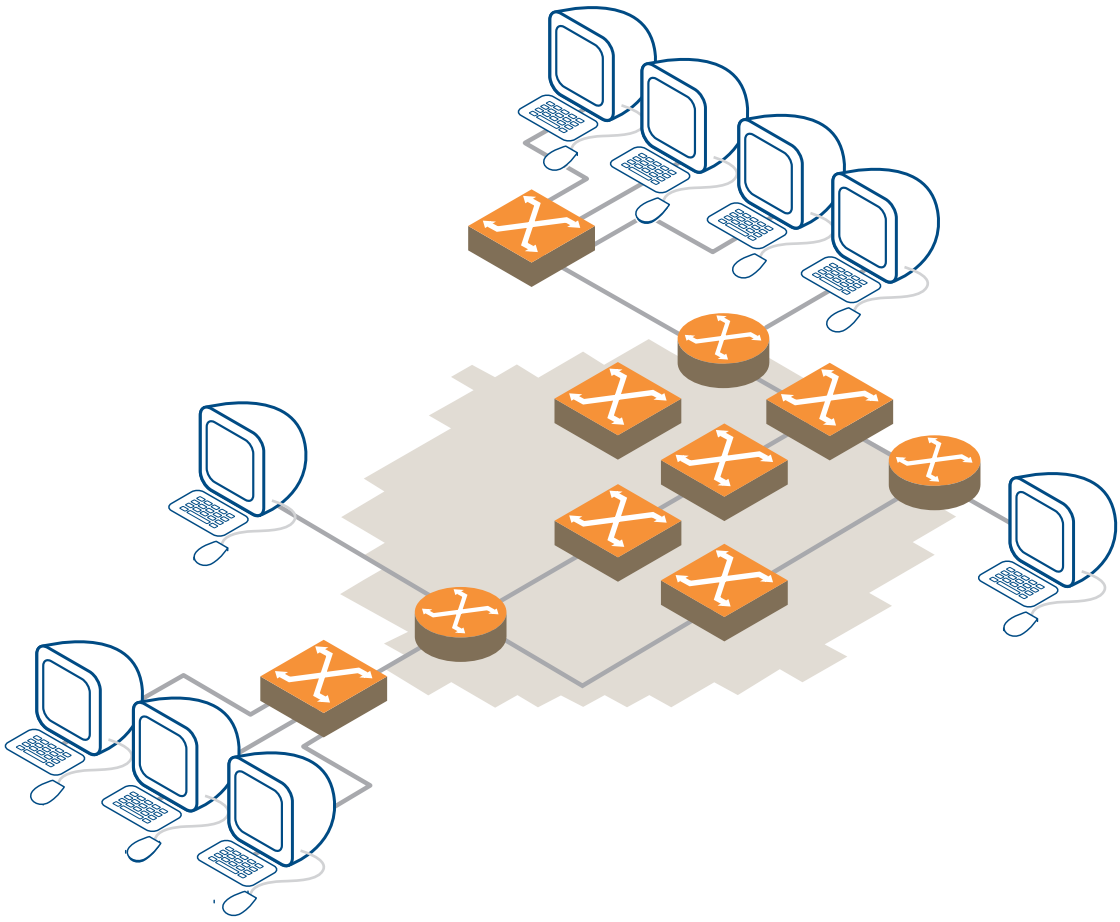
La Réalité des Réseaux IP

S'y retrouver dans la jungle des réseaux IP et WAN

Rapport réalisé par Ovum
à la demande de WorldCom



WORLDCOM

Ovum

Ovum est une société d'analyse et de conseil, un leader mondial specialisé dans l'informatique et les télécommunications; des secteurs dont l'évolution, et la convergence, ne cessent de s'accélérer. Nos connaissances et notre expérience nous permettent de présenter à nos clients une cartographie précise de ce nouvel environnement et de les aider à s'y retrouver. Résolument indépendants, nous leur offrons des conseils professionnels marqués du sceau de l'objectivité et de la perspicacité. Depuis nos bureaux répartis dans le monde entier - Londres, Boston, San Francisco, Buenos Aires, Séoul, Melbourne et Sydney - nos 300 collaborateurs consacrent leur énergie à aider nos clients à faire les choix qui correspondent à leurs besoins.

Activités de conseil - Ovum Consulting

Nos activités de conseil se basent sur nos activités d'analyse de marchés, de fournisseurs, de technologies et de solutions. Cette expertise nous permet de proposer à nos clients des conseils stratégiques adaptés à leurs besoins. Nous bénéficions d'une clientèle de premier ordre, en évolution permanente, constituée d'acteurs industriels, de décideurs et d'investisseurs - et les aidons à résoudre toutes les difficultés d'ordre industriel, technologique ou réglementaire.

Ovum bénéficie d'une excellente réputation basée sur la performance de ses analyses et de ses recommandations. Si vous souhaitez une aide à la décision pour assurer votre pérennité commerciale, utilisez les connaissances approfondies que nous avons déjá mises à disposition des organisations suivantes :

- Investisseurs
- Autorités gouvernementales
- Opérateurs réseaux (fixe, câble, sans fil, satellite)
- Fournisseurs de services (télécom, accés Internet, commerce électronique, services informatiques)
- Distributeurs télécom et réseaux
- Distributeurs informatique et commerce électronique
- Fournisseurs de service multimedia en ligne
- Utilisateurs informatiques et télécoms

Contactez-nous

Pour de plus amples informations sur nos publications et services de conseil, veuillez contacter Cathren Whelton, Consultante sur consult@ovum.com.

La réalité du Réseau IP est publiée par WorldCom.

www.wcom.com/fr/vpn

Introduction

Bienvenue dans la Réalité des Réseaux IP, rapport spécial commandé à la société Ovum, l'une des sociétés de conseil et d'analyse les plus réputées.

La raison pour laquelle nous avons demandé ce rapport est simple : vous aider à vous orienter dans le labyrinthe des solutions basées sur le protocole IP.

Demandez autour de vous et l'on vous répondra que tout est simple maintenant : l'Internet, un point c'est tout ! Pour WorldCom, les choses ne sont pas aussi simples, du moins pas encore. Si c'était le cas, vous ne seriez pas en train de lire ce rapport.

S'il existe une notion qui fait l'unanimité, c'est bien celle qui consiste à considérer le protocole Internet (IP - Internet Protocol) comme un composant fondamental de l'économie Internet, aussi bien pour aujourd'hui que pour demain. Mais comment en bénéficier? Comment configurer un réseau IP ? L'IP est supposé supporter tant d'applications et de services différents - certains très loin de ceux pour lesquels l'IP était prévu. La manière dont vous l'utilisez a une influence énorme sur ses performances. Par exemple : les applications pour lesquelles la notion de temps est primordiale, comme la voix ou la vidéo, exigent des garanties de qualité de service (Quality of Service - QoS) relatives au débit et aux temps de transmission. Dans le secteur public, les questions de sécurité ont une priorité plus grande. Associer des flux IP à des exigences qualitatives et de sécurité sur une seule voie d'accès de manière satisfaisante est devenu un véritable défi. Réseaux partagés (Extranets), réseaux locaux (Intranets), gestion de la relation client (CRM - customer relationship management), gestion de la chaîne d'approvisionnement (SCM - supply chain management), planification des ressources de l'entreprise (ERP - entreprise resource planning), tout doit être interconnecté correctement afin d'assurer à la fois performance et sécurité.

Il n'existe pas de solution unique pour toute entreprise ou toute situation. C'est pourquoi WorldCom dispose de toutes les solutions de réseaux IP dont vous pouvez avoir besoin, de la bande passante aux relais de trames (Frame Relay) et ATM (Asynchronous Transfert Mode), en passant par les réseaux privés virtuels IP (IP VPN - IP Virtual Private Networks) utilisant soit l'Internet soit notre infrastructure réseau propre. Vous pouvez ajouter à cela notre infrastructure réseau en France et dans le monde entier, nos services d'hébergement de premier ordre ainsi que nos solutions originales de centres d'appels.

Vous pourrez compter sur WorldCom quels que soient vos besoins.

Pour plus d'informations, contactez-nous au numéro suivant : 0805 100 100.

WorldCom France

Contents

1 Sommaire et principaux points d'analyse

Ce rapport permet aux entreprises de choisir la solution IP (Internet Protocol) qui convient à leur réseau. Il présente une analyse complète des différentes technologies en indiquant pour chacune d'entre elles points forts et points faibles. Nous espérons qu'il vous aidera a choisir le fournisseur capable de réellement prendre en charge votre réseau d'entreprise.

1.1 Sommaire

Les réseaux privés virtuels (VPN - Virtual Private Networks) sont des réseaux d'entreprises basés sur une infrastructure publique mise en place par des fournisseurs de services nationaux et internationaux. Le déploiement de réseaux privés sur des réseaux publics partagés permet aux entreprises de bénéficier des économies d'échelle et des capacités de connectivité offertes par les opérateurs de réseaux publics. Parmi les avantages offerts par une solution VPN, on peut citer une architecture souple avec une forte capacité d'évolution à des coûts de connexion et de gestion inférieurs à ceux des réseaux privés non virtuels. Les solutions VPN permettent aussi aux entreprises d'externaliser la gestion de leur réseau et de se concentrer sur leur activité principale.

Les VPN permettent à des utilisateurs distants d'accéder au réseau de leur entreprise et facilitent les connexions bi-directionnelles entre plusieurs bureaux locaux ou internationaux. Ils permettent aux entreprises, partenaires, fournisseurs et utilisateurs d'accéder à certaines parties de leurs réseaux locaux (intranets) respectifs via des réseaux partagés. Ils permettent aussi de déployer de nombreux types d'applications telles que les liaisons voix ou vidéo en temps réel, les logiciels critiques de gestion d'entreprise ou les applications interactives et d'arrière plan comme les navigateurs web, le transfert de fichiers et le courrier électronique (e-mail).

Ce rapport classe les solutions VPN et définit leurs avantages. Il donne également une brève description des réseaux et technologies sur lesquels les VPN se reposent, à savoir:

- Réseaux en relais de trames (Frame Relay)
- Réseaux en mode de transfert asynchrone (ATM - asynchronous transfer mode)
- Réseaux hybrides ATM/Frame Relay
- Réseaux IP public (Internet VPN)
- Réseaux IP privé (IP VPN) avec qualité de service (QoS)
- Lignes louées numériques.

Il analyse leurs avantages et leurs inconvénients en détail, décrit les services qu'ils peuvent offrir et définit une liste de paramètres destinés à faciliter les comparaisons entre technologies et applications. Le rapport conclut en illustrant avec des exemples concrets comment differents types de VPN répondent à différents besoins en matière de réseaux d'entreprise.

1.2 Principaux points d'analyse

1.2.1 Applications VPN

Les VPN peuvent supporter de nombreux types d'applications telles que les liaisons voix et données en temps réel, des applications interactives et d'arrière-plan comme les navigateurs web, le transfert de fichiers et le courrier électronique (e-mail), etc. Les réseaux basés sur IP peuvent supporter toutes ces applications, mais il faut tenir compte des compromis imposés par la nécessité de gérer différentes contraintes réseau telles que capacité de débit, temps de transmission, risque de distorsion et perte de paquets. Les technologies disponibles aujourd'hui rendent possibles les communications multimédia sur tous types de réseaux bien qu'ils subsistent des différences importantes en termes de configuration réseau et de QoS.

La section 6 de ce document présente, sous forme de tableau, une matrice des critères de choix les plus importants pour chaque type d'application.

1.2.2 IP VPN et Internet VPN

En dépit de fondements technologiques similaires, IP VPN et Internet VPN présentent une différence importante :

- Les Internet VPN acheminent le trafic réseau à travers l'infrastructure Internet publique
- Les IP VPN acheminent le trafic réseau à travers une infrastructure IP privée.

1.2.2.1 Internet VPN

Les principaux avantages des Internet VPN sont, entre autres, une couverture globale, le fait que l' utilisateur laisse à l'opérateur télécom la responsabilité de gérer routeurs et réseau, et une fourniture simplifiée des services longue distance. Ceci permet une réduction substantielles des coûts. En outre, cette offre est souple, rapidement déployée, peut être facilement modifiée et offre une forte capacité d'évolution.

1.2.2.2 IP VPN

Les IP VPN sont principalement utilisés pour connecter des réseaux locaux d'entreprise (Intranets ou LANs - Local Area Networks). Ils peuvent être utilisés comme base pour des contrats de type Accord sur les Engagements de Service (SLA - Service Level Agreement). Ceux-ci garantissent niveau de débits, délais d'attente, temps moyen de réparation, priorités de trafic ainsi que QoS. L'utilisation d'un réseau IP permet d'éliminer l'usage des circuits virtuels permanents (PVC - Permanent Virtual Circuit) associés aux protocoles orientés connexion comme le Frame Relay et l'ATM.

De plus, une nouvelle génération d' IP VPN basés sur la technologie de commutation multiprotocole avec étiquetage des flux (MPLS -multiprotocol label switching) peut supporter les communications voix et données en temps réel et les associer á des garanties contractuelles de qualité. L'un des avantages les plus significatifs des IP VPN réside dans le fait qu'ils sont parfaitement adaptés à la connectivité pour réseaux partagés (extranets) hautement sécurisés requises par les applications de commerce inter-entreprises (B2B - business-to-business - commerce).

1.2.3 Les VPN non IP se portent bien

Alors que toute l'industrie des télécom ne parle que de IP VPN, il est important de rappeler que n'importe quelle technologie VPN peut faciliter l'usage du protocole TCP/IP. IP est transmis au niveau de la couche Réseau et TCP au niveau de la couche Transport. Au dessous de ces niveaux, les communications sont supportées par les technologies apparternant à la couche de connexion physique de type Frame Relay, ATM, etc.

1.2.3.1 Frame Relay

Le Frame Relay, par exemple, peut gérer les pics de trafic soudains (bursting), acheminer les protocoles de type SNA (Systems Network Architecture), et facilement s'intégrer aux réseaux de type X.25 ou à des réseaux ATM. En outre, le Frame Relay peut transporter à la fois voix et données et offre un certain niveau de sécurité. Par rapport au X.25, Frame Relay est un protocole plus simple et moins cher. Il bénéficie de technologies de commutation simplifiées. Cette simplicité libére de la bande passante qui peut ainsi être utilisée à la fois pour transmettre plus de données et pour réduire les temps de transmission.

1.2.3.2 ATM

L'ATM remporte le prix de la flexibilité lorsqu'il s'agit de mettre en œuvre des réseaux à hautes performances. Son usage des circuits virtuels et la taille fixe des cellules ATM autorisent, dans un bon rapport qualité-prix, la transmission d'applications multimédia et différents niveaux de QoS sur un même réseau.

1.2.3.3 Solutions Hybrides Frame Relay/ATM

Les technologies modernes en matière de logiciels et de matériels permettent également des solution hybrides qui combinent ATM et Frame Relay. Cette approche est l'une des meilleures à adopter lors d'une migration d'un réseau Frame Relay vers un réseau ATM dans la mesure où elle pérennise les investissements Frame Relay initiaux. Cette approche bénéficie également du fait que l'infrastructure réseau hybride ainsi crée offre une forte capacité d'évolution.

Les clients possédant un réseau ATM peuvent bénéficier des services offerts par le Frame Relay chaque fois qu'un nœud ATM fait défaut, et vice versa.

1.2.3.4 Lignes louées

Les entreprises peuvent également louer des lignes numériques pour transférer leurs données. Bien que cette solution ne constitue pas, strictement parlant, un VPN - puisque chaque client dispose d'une infrastructure dédiée - elle utilise des ressources réseau qui sont partagées avec d'autres utilisateurs. Parmi les avantages des lignes louées, on peut citer un débit et un temps de transmission garantis. Les applications multimédia peuvent être supportées de manière cohérente avec des taux d'erreurs très bas; la fiabilité du service s'en trouve améliorée puisque les interférences durant la transmission sont réduites. De plus, les lignes louées ne subissent pas de déconnexion, ce qui arrive au cours de sessions Internet de longue durée. Elles sont toujours disponibles.

1.3 Choisir une solution VPN

Les entreprises utilisatrices des services VPN basent leur choix sur les critères suivants :

- performance
- coût
- sécurité
- Accords sur les Engagements de Service (SLA - Service Level Agreement).
- interopérabilité
- forte capacité d'évolution du réseau
- gestion du réseau
- facturation.

La section finale de ce document présente des exemples d'entreprises qui utilisent un VPN pour différentes applications et dont les exigences liées à leur métier sont très variées. Pour chacun de ces exemples, ce rapport vous explique les processus décisionnels qui ont abouti au choix d'une solution VPN.

2 Introduction aux communications de réseaux étendus (WAN - Wide Area Network)

Un réseau de communication relie au moins deux terminaux en leur fournissant les moyens d'échanger de l'information. Les deux principales raisons qui motivent l'utilisation d'un tel réseau sont les suivantes :

- Le réseau permet à ses utilisateurs de partager les ressources qu'il met à leur disposition à un meilleur rapport qualité-prix que s'ils utilisaient des lignes dédiées entre deux terminaux
- Le réseau n'est pas restreint à un nombre limité d'équipements et d'utilisateurs.

Il existe deux principaux types de réseaux.

- Un réseau local (LAN - Local Area Network) est limité à des zones géographiques réduites, généralement un immeuble ou un groupe d'immeubles.
- Un réseau étendu (WAN - Wide Area Network) dessert des zones géographiques plus larges - villes, régions, pays, voire continents.

La différence d'envergure géographique entre LANs et WANs a conduit à des solutions techniques différentes.

Les WANs sont composés d'un certain nombre de nœuds de commutation interconnectés. Ces nœuds acheminent l'information vers ses terminaux de destination en utilisant soit une technologie de commutation de circuits soit une technologie de commutation de paquets.

2.1 Réseaux WAN à commutation de circuits

Les réseaux téléphoniques publics sont les principaux utilisateurs de la technologie de commutation de circuits. Conçue pour gérer le trafic voix, cette technologie peut également gérer les données, quoique de façon non rentable.

Les réseaux à commutation de circuits créent un connexion dédiée pour chaque communication qu'ils gérent. Ils mobilisent un partie de leur resources pour toute la durée de cette communication. Ils nécessitent une bande passante fixe et n'utilisent pas de bits d'en-tête une fois l'appel établi. Pendant la communication, le débit est garanti, les informations ne sont pas stockées et il n'existe aucun délai autre que celui de la transmission. Si la personne appelée (le terminal de destination) est occupée, l'appel est bloqué. Les blocages d'appel interviennent également lorsque le réseau est surchargé.

2.2 Réseaux WAN à commutation par paquets

La commutation par paquets est plus efficace que la commutation de circuits pour gérer le trafic de données, particuliérement lorsque celui ci est enclin à des pics d'activité soudains. Dans les réseaux à commutation par paquets les informations sont transmises en petits blocs appelés paquets. Chaque

paquet contient, en plus des données à communiquer, des informations de contrôle sur le contenu et la destination du paquet.

Les réseaux à commutation par paquets peuvent utiliser deux types de technologie : circuits virtuels (orienté connexion) ou datagrammes (sans connexion).

2.2.1 Commutation de paquets en circuit virtuel

La commutation de paquets en mode circuit virtuel/orientés connexion établie un chemin dédié, ou circuit virtuel, entre ses points d'entrée et de sortie. Tous les paquets utilisant ce circuit virtuel empruntent le même chemin. La capacité de transfert de données de ce circuit n'est utilisée que s'il existe des données à transférer.

Plusieur utilisateurs peuvent utiliser le même circuit virtuel à travers la technologie dite de multiplexage statistique (statistical multiplexing). Les ressources réseau (bande passante) sont partagées de facon dynamique.

Dans les communications en circuit virtuel, l'appel doit être établi au préalable, l'émetteur étant notifié si la connexion est refusée. Le réseau est responsable de la livraison des paquets. En cas de saturation du réseau, les paquets sont stockés jusqu'à ce qu'ils soient livrés, ce qui entraîne un retard supplémentaire qui vient s'ajouter au délai de transmission. Lorsque le réseau est surchargé, l'appel peut être bloqué ou le temps d'acheminement des paquets augmenté.

2.2.2 Commutation de paquets par datagrammes

Les systèmes par commutation de paquets en mode datagramme ignorent le concept de connexion. Chaque paquet, ou datagramme, subit un traitement séparé et n'utilise pas de chemin dédié. Certains paquets peuvent avoir la même destination mais ne suivent pas nécessairement le même chemin. En cas de surcharge réseau, l'appel n'est pas bloqué; mais la livraison des paquets peut être retardée, voire interrompue. Dans la mesure où le réseau n'alloue pas de ressources spécifiques, il ne peut garantir qu'une qualité de service limitée.

2.3 Evolution des technologies de transport : X.25, Frame Relay, ATM et IP

2.3.1 De X.25 à Frame Relay

Entre les années 60 et le milieu des années 70, il existait de nombreux protocoles pour réseaux à commutation de paquets. En 1974, l'UIT (Union Internationale des Télécommunications) normalisa l'interface réseau et lui donna le nom de X.25.

Bien qu'à l'origine les protocoles pour réseaux à commutation par paquets étaient fondés sur le mode datagramme, le protocole X.25 utilise la technologie des circuits virtuels. Il est conçu pour acheminer des données au travers de lignes de transmission qui peuvent souffrir de bruit

de fond en utilisant le multiplexage statistique de paquets de longueur variable. Il n'est pas adapté à d'autres usages.

Frame Relay, une version simplifiée de X.25, vit le jour un peu plus tard. Il est basé sur les travaux de l'UIT sur la technologie RNIS (réseau numérique à intégration de services/ISDN - integrated services digital network).

Les principales différences entre X.25 et Frame Relay sont les suivantes:

- Frame Relay n'a pas de capacité de contrôle d'erreur au niveau liaison
- Les données de contrôle de l'appel Frame Relay empruntent une connexion logique distincte de celle utilisée par les données à transferer.

Cette facon simplifiée de transmettre des données permet au Frame Relay de réduire les temps de transmission et d'augmenter de manière importante le débit des transferts de données (jusqu'à 2 Mbit/s par rapport à 64 Kbit/s pour X.25). Le Frame Relay s'adapte beaucoup mieux que l'X.25 aux applications sensibles aux temps de transmission et nécessitant des vitesses de transfert élevées.

2.3.2 ATM (Asynchronous Transfert Mode - mode de transfert asynchrone)

Traditionnellement, les réseaux dédiés à la voix et ceux dédiés aux données ont toujours été indépendants les uns des autres en raison de leur différences en matière de qualité de service (QoS) et de qualité-prix.

Les réseaux téléphoniques publics commutés (PSTN - public switched telephone networks -) assurent un flux continu des données, ce qui s'est avéré le mieux adapté aux applications sensibles aux temps de transmission comme la téléphonie. La technologie de réseau numérique à intégration de services (ISDN - integrated services digital network) elle aussi garantit des débits continus d'information.

PSTN et ISDN correspondent à une vision du monde réseau, qui, au milieu des années 80, considérait que la technologie des circuits virtuels pouvait maximiser l'utilisation des ressources réseaux tout en permettant de supporter des applications dont les exigences en matière de performance réseau sont très variées. Cette vision conduit au développement de la technologie ATM, basée sur les transmissions en circuit virtuel.

Les réseaux ATM gèrent des paquets de taille fixe (dit cellules) transmis sur des circuits virtuels en garantissant une qualité de service (QoS) spécifiée en termes de temps d'attente, de vitesse et de taux d'erreur. La taille des cellules fixées à 53 octets est le résultat d'un compromis entre les experts spécialisés en communications voix et ceux spécialisés en communications de données.

2.3.3 IP

Les réseaux téléphoniques et les réseaux publics de transmission de données sont tous construits autour d'une même topologie dite maillée. Chaque terminal peut avoir accès à tout autre terminal présent sur le réseau. Le maillage présente un degré de fiabilité élevé dans ce sens qu'il permet de dérouter le trafic vers d'autres nœuds, liens ou même d'autres réseaux en cas de panne sur un lien ou un nœud de transmission.

Depuis la fin des années 60 aux Etats-Unis, les réseaux utilisés par les organisations de défense et les institutions académiques sont basés sur une topologie maillée qui utilise le protocole internet (IP - Internet Protocol). Ce protocole n'est pas basé sur le concept de connection. L'IP transfère des données sous forme de datagrammes de format variable, allant jusqu'à 64 Ko. Il ne peut garantir
la qualité du transfert en termes de délai d'acheminement ou de débit car il est basé sur la notion de meilleur effort (best effort).

Le protocole de contrôle de transmission (TCP - Transfer Control Protocol), défini en 1974, est un protocole de couche supérieure qui s'associe à l'IP pour assurer la fourniture et la séparation des paquets en séquences. La souplesse de l'IP associée à TCP, et aux nouvelles techniques d'adressage, est un atout considérable pour le succès d'Internet.

L' Internet est un réseau de réseaux. Il est constitué de liens point à point qui relient des réseaux régionaux. Basé sur IP, Internet peut supporter une grande variété d'applications telles que Telnet, FTP (File Transfer Protocol), connexion à distance et courrier électronique (e-mail). La popularité d'Internet est principalement due à la libre circulation de ses protocoles, et à leur mise en place logicielle disponible depuis n'importe quel ordinateur individuel.

La simplicité, la souplesse et le faible coût des réseaux IP sont autant de raisons qui poussent les utilisateurs à déployer de nouveaux types applications sur ce type de réseaux. Les applications aussi sophistiquées que le World Wide Web, dont le succès n'est plus à démontrer, ont prouvé que les datagrammes peuvent être le fondement de services complexes. Les applications Web, par exemple, ont favorisé l'essor des transactions commerciales électroniques. L'Internet permet aussi de bénéficier de la téléphonie multimedia à moindre coût, en plus de la transmission des données audio et vidéo en flux (streaming).

2.4 Conclusion

Les industriels veulent utiliser les technologies et infrastructures de communications IP pour transmettre et recevoir toutes sortes d'applications, de la voix au courrier électronique en passant par le multimédia. Ils veulent exploiter cette capacité de manière rentable, fiable et sécurisée et, de plus en plus, sur des zones géographiques très étendues. Ils réalisent que posséder leur propre réseau privé devient chaque jour un peu moins rentable et qu'il est bien plus lucratif d'utiliser les ressources des grands opérateurs télécom pour un VPN.

3 Vue d'ensemble des réseaux d'entreprises virtuels privés (VPN) et étendus (WAN)

Globalisation, entreprises virtuelles, télétravail et commerce électronique sont autant de facteurs qui exercent une forte pression sur les réseaux WAN traditionnels. Cependant, de nouvelles technologies, et l'évolution des solutions WAN traditionnelles, donnent aux entreprises un très grand choix dans la constitution de leur réseau.

3.1 Introduction aux VPN

Les réseaux d'entreprise étendus (WAN) utilisent traditionnellement soit des lignes louées soit le propre réseau de l'entreprise. Les WAN privés sont principalement utilisés pour relier des réseaux vocaux ou locaux. Seules les plus grandes entreprises peuvent s'offrir ce type de technologie.

La mondialisation de l'économie a eu pour effet d'augmenter la demande d'accès, à partir de sites distants, aux réseaux locaux et privés. Le développement du commerce électronique a poussé les entreprises à partager leurs ressources avec leurs partenaires commerciaux et leurs clients au travers de réseaux partagés (Extranets). La technologie WAN traditionelle doit évoluer pour répondre à ces nouvelles exigences. L'une des stratégies considerée par la majorité des grandes entreprises, en réponse à ces exigences, est l'adoption des VPN pour remplacer et/ou suppléer les WAN privés.

Un VPN est un réseau d'entreprise déployé sur une infrastructure réseau partagée gérée par des fournisseurs de services réseau nationaux et internationaux. En tant qu'alternative aux réseaux dédiés de type WAN, il permet non seulement de satisfaire aux même exigences que les WANs en matière de support de protocoles multiples, de fiabilité, et de forte capacité d'évolution, mais encore d'y satisfaire à moindre coût et avec plus de souplesse. Ceci permet aux PME d'accéder aux services disponibles sur un WAN, et de se rendre accessible depuis n'importe quel point du globe, sans avoir pour autant à posséder l'infrastructure réseau requise.

Un VPN peut utiliser la plupart des technologies de transport actuellement disponibles, notamment les réseaux IP soit public (Internet) soit privé, c'est à dire gérés par des founisseurs de services télécom. Il peut également utiliser les réseaux Frame Relay et ATM de ces même fournisseurs.

3.2 Les avantages des VPN

Les VPN offrent les avantages suivants :

- souplesse et forte capacité d'évolution des architectures réseau comparées aux WAN classiques
- plus efficace pour répondre à des besoins de connectivité variés
- moins cher que les WAN privés sur le plan de la gestion, de la bande passante et des investissements
- retour sur investissement plus rapide
- et sans doute le plus important, la gestion du réseau revient à la charge du fournisseur de service VPN et non à l'entreprise qui utilise le VPN. Cela permet à cette dernière de se concentrer sur son métier au lieu de s'occuper de la gestion de son réseau.

3.3 Classification des VPN

Plusieurs critères permettent de classer les VPN. Nous avons défini deux types de classification respectivement basées sur le type d'applications supportées par le VPN et sur l'implémentation des couches ISO (OSI - open systems interconnexion).

3.3.1 Classification en fonction du type d'applications

3.3.1.1 VPN pour accès nomade

Les VPN permettent à des utilisateurs distants d'accéder au réseau de leur entreprise. Les employés nomades détachés pour de longues périodes hors de l'entreprise, ainsi que ceux travaillant individuellement ou en groupe sur des sites reculés, ont besoin d'accéder aux informations de leur entreprise. Les accès nomades sont également nécessaires aux télétravailleurs, aux représentants commerciaux et à toute personne travaillant régulièrement à l'extérieur de l'entreprise.

3.3.1.2 Intranet VPN

Les Intranet VPN autorisent des connexions bi-directionnelles entre différents bureaux, au niveau national ou international, de filiale à filiale ou de filiale à siège social. Les communications doivent être sécurisées et rentabilisées sans que les installations ne soient attribuées de manière permanente à l'une des filiales.

3.3.1.3 Extranet VPN

Le commerce électronique inter-entreprises nécessite qu'une entreprise ait accès au réseau local (intranet) d'une autre entreprise dans le cadre de transactions entre elle-mêmes. On appelle Extranet VPN le type de VPN qui permet à des entreprises, partenaires, fournisseurs et utilisateurs de partager certaines parties de leur réseau local respectif.

3.3.2 Classification en fonction des couches ISO

Les principales technologies qui permettent d'exploiter les applications et services VPN sont les suivantes :

- Réseaux en relais de trames (Frame Relay)
- Réseaux en mode de transfert asynchrone (ATM - asynchronous transfer mode)
- Réseaux hybrides ATM/ Frame Relay
- Réseaux IP public (Internet VPN)
- Réseaux IP privé (IP VPN) avec qualité de service (QoS)
- Lignes louées numériques.

La section suivante (section 4) contient une description de ces différentes technologies.

4 Technologies pour réseau virtuel privé (VPN)

Cette section propose un tour d'horizon de chacune des six solutions VPN prédominantes :

- Réseaux en relais de trames (Frame Relay)
- Réseaux en mode de transfert asynchrone (ATM - asynchronous transfer mode)
- Réseaux hybrides ATM/ Frame Relay
- Réseaux IP public (Internet VPN)
- Réseaux IP privé (IP VPN) avec qualité de service (QoS)
- Lignes louées numériques.

4.1 Frame Relay

Le Frame Relay est un protocole de réseau étendu (WAN) orienté connexion. Il agit au niveau de la couche liaison de données, la seconde couche du modèle de référence pour l'interconnexion de systèmes ouverts ISO (OSI - open systems interconnection). Il est fondé sur une technologie de commutation par paquets qui permet aux terminaux de partager de manière dynamique les ressources disponibles sur la base de la technologie dite de multiplexage statistique. Des paquets de longueur variable sont utilisés afin d'obtenir des transferts de données plus efficaces et plus souples. Ces paquets sont ensuite commutés entre les différents segments du réseau jusqu'à leur destination.

Un réseau Frame Relay est composé des éléments suivants :

- points terminaux tels que PCs, serveurs, ordinateur principal
- équipement d'accès (FRAD - Frame Relay Access Device) tels que passerelles et routeurs
- matériel réseau tels que commutateurs et routeurs de réseau. Les liaisons sont généralement supportées par des lignes T1/E1 soit dédiées soit partagées et/ou des multiplexeurs 56K.

Un réseau Frame Relay offre un service orienté connexion. Cela signifie qu'en cas de demande de communication, il établi un circuit entre chacun de deux points d'entrée et de sortie de la communication. Cette communication utilise un circuit virtuel, c'est à dire une connexion logique entre les deux points d'entrée et de sortie. Les standards du sérvice définissent deux types principaux de circuits logiques : permanents et commutés.

4.1.1 Circuits virtuels permanents

Les circuits virtuels permanents (PVC - Permanent Virtual Circuit) définissent des connexions semi-permanente utilisées pour des transferts de données volumineux et fréquents. La communication n'exige pas de configuration d'appel et se trouve toujours à l'état de transmission ou d'attente. Dans ce dernier cas, la connexion est active mais aucune donnée n'est transférée. L'équipement réseau peut démarrer le transfert des données dès que nécessaire parce que le circuit est établi en permanence.

4.1.2 Circuits virtuels commutés

Les circuits virtuels commutés (SVC - switched virtual circuit) sont des connexions temporaires utilisées dans les situations n'exigeant que des transferts de données sporadiques. Contrairement aux communications CVP, une session CVC consiste en une configuration d'appel qui "réserve" un circuit virtuel et une fin d'appel qui libère le circuit virtuel.

4.1.3 Gestion

Le matériel de transmission et de commutation d'un réseau Frame Relay est hébergé par un opérateur télécom. Les abonnés d'un VPN sont facturés en fonction de leur utilisation du réseau. Ils sont dispensés de la gestion et de la maintenance du matériel et des services nécessaires au réseau Frame Relay.

4.2 ATM

Comme le Frame Relay, l'ATM est un service à commutation de paquets orienté connexion qui utilise des circuits virtuels pour transférer des données. Les ressources sont partagées par multiplexage statistique. La grande difference avec la technologie Frame Relay est l'utilisation de cellules de longueur fixe (53 octets) pour le transfert d'informations. Le format fixe des cellules garantit que les informations prioritaires, telles que la voix ou la vidéo, ne vont pas trop être retardées par de longs paquets. Ce format permet aussi une commutation plus rapide et plus efficace. L'ATM offre des vitesses de 2 Mbit/s à 622 Mbit/s. Il est peu efficace pour des débits moindres dans la mesure où l'information requise pour acheminer les paquets représente une part non négligeable de chaque cellule.

Un réseau ATM est composé d'un commutateur ATM et de points terminaux ATM.

4.2.1 Commutateur ATM

Un commutateur ATM prend en charge le transit des cellules via un réseau ATM. Il accepte une cellule entrante à partir d'un terminal ATM ou d'un autre commutateur ATM. Il la lit, met à jour les informations de l'en-tête de cellule, puis dirige la cellule vers sa destination suivante.

4.2.2 Terminal ATM

Un terminal ATM comprend un adaptateur d'interface réseau ATM. Les postes de travail, les routeurs, les unités de services numériques, les commutateurs de réseaux locaux (Local Area Network - LAN) et les codeurs-décodeurs vidéo sont des exemples de terminaux ATM.

4.2.3 Interfaces ATM

Les commutateurs ATM sont interconnectés par des liaisons ou interfaces ATM point à point. Il existe trois types d'interfaces :

- les interfaces réseau utilisateur (UNI - user-network interface) connectent les systèmes terminaux d'ATM (tels que les hôtes et les routeurs) à un commutateur ATM.
- Les interfaces de nœud inter-réseau (NNI- network-network node interface) connectent des commutateurs ATM
- les interfaces large bande inter-opérateurs (B-ICI - broadband-inter carrier interface) connectent des réseaux ATM publics.

4.2.4 L'ATM utilise des circuits virtuels permanents

Une des caractéristiques clés de l'ATM est la manière dont les connexions sont établies sur le réseau. L'ATM utilise des circuits virtuels permanents (PVC - permanent virtual circuits) qui permettent d'établir une connexion de bout en bout. Ce sont des routes de réseau préconfigurées ce qui supprime la nécessité d'établir un circuit (configuration d'appel) à chaque fois que l'utilisateur souhaite effectuer une transmission vers un site distant. Lorsqu'il est sollicité, le service ATM connaît déjà la route que suivra chaque cellule sur le réseau et commence immédiatement à acheminer les cellules de message, chacune contenant l'adresse PVC dans son en-tête. Chaque cellule suit la même route et est ré-assemblée à l'extrémité de destination.

4.2.5 Circuits virtuels commutés : une alternative à l'ATM

Les circuits virtuels commutés (CVC / switched virtual circuit - SVC) sont une alternative à la mise en place d'un réseau ATM. Ils exigent que le réseau effectue une connexion virtuelle à chaque fois qu'un site distant est sollicité. Il existe des assignations temporaires effectuées

sur demande et qui ne font appel aux ressources réseau qu'en cours d'utilisation, ce qui améliore potentiellement le rapport qualité-prix pour certaines applications dans lesquelles il existe un trafic peu fréquent vers un site distant.

4.3 Hybrides ATM/Frame Relay

Les entreprise mixent reseaux ATM et Frame Relay pour les cinq principales raisons suivantes :

1. Frame Relay est bien adapté à de nombreuses applications, dont l'interconnexion de réseaux locaux (LAN), la migration SNA (Systems Network Architecture), et l'accès distant. Cependant, d'autres applications telles que les communications multimédia avec qualité de service (QoS) garantie, sont mieux servis par des réseaux ATM.

2. Une vaste gamme de débits peut être supportée, de 64 Kbit/s à 622 Mbit/s.

3. Les clients ATM peuvent bénéficier des connexions Frame Relay lorsque le nœud ATM n'est pas disponible, et vice versa.

4. ATM peut être utilisé à la place du Frame Relay si ce dernier n'est pas disponible dans certaines zones géographiques, et vice versa.

5. Lors de la migration du Frame Relay vers ATM, l'interconnexion pérennise les investissements Frame Relay originels

Il existe deux scénarios d'interconnexion ATM-Frame Relay :

- interconnexion réseau
- interconnexion service.

L'interconnexion réseau facilite le transport entre deux unités (ou entités) Frame Relay via un réseau de structure ATM. La fonction d'interconnexion réseau (IWF - interworking function) facilite la transparence du transport du trafic utilisateur et le trafic de signalisation PVC Frame Relay via ATM. On l'appelle parfois tunnellisation (tunnelling). En d'autres termes, le réseau ATM est utilisé à la place des Lignes Louées pour connecter deux réseaux Frame Relay. Cela signifie que l'encapsulage multiprotocole et les autres procédures des couches supérieures sont transportés de manière transparente, comme ce serait le cas sur des Lignes Louées.

L'IWF peut être soit externe aux réseaux, soit, plus vraisemblablement intégrée au commutateur de réseau ATM ou au commutateur Frame Relay. Chaque PVC Frame Relay peut être supporté par un PVC ATM ; ou encore tous les PVC Frame Relay peuvent être multiplexés sur un PVC ATM unique.

Cette méthode de connexion des réseaux Frame Relay peut permettre une réduction des coûts par comparaison aux Lignes Louées. Ceci est particulièrement vrai lorsque l'interface de nœud inter-réseau (NNI) Frame Relay fonctionne avec un faible pourcentage d'utilisation. L'interaction réseau comprend également un scénario dans lequel un ordinateur hôte ATM émule Frame Relay dans la sous-couche de convergence spécifique au service. L'interaction du service permet à un utilisateur ATM d'interagir de manière transparente avec un utilisateur Frame Relay, sans que chacun d'eux sache que l'autre extrémité utilise une technologie différente. L'interaction de service ATM-Frame Relay pour les PVC est translationnelle entre les deux protocoles. En d'autres termes, le service IWF n'achemine pas le trafic de manière transparente mais fonctionne plutôt comme un convertisseur de protocole entre des équipements différents.

4.4 Internet VPN

Les Internet VPN permettent d'utiliser l'Internet public de manière sécurisée, comme s'il s'agissait d'un réseau privé. Ils permettent des connexions site à site au sein d'une entreprise, des connexions extranet entre partenaires commerciaux et des connexions pour utilisateurs distants (tels que les télétravailleurs et/ou le personel en déplacement). La connexion peut être à haut débit puisqu'ils peuvent être construits à partir de toute méthode d'accès disponible pour l'Internet public, y compris

- Ligne Louée
- Frame Relay
- Ligne d'abonné numérique (DSL - digital subscriber line)

- Réseau numérique à intégration de services (ISDN - integrated services digital network)
- Réseau téléphonique public commuté (PSTN - public switched telephone network).

4.4.1 Multiples fournisseurs

Les Internet VPN peuvent soit être mis en place et gérés par une entreprise en interne soit partiellement ou totalement mis en place et géré par un fournisseur de services. Ces services sont offerts par des Fournisseurs d'accès à Internet (ISP - Internet service provider) internationaux ou locaux. Ces ISP peuvent être des entreprises de télécommunications ou des fournisseurs de services spécialisés qui s'associent à des ISP locaux pour fournir une couverture géographique étendue.

4.4.2 La sécurité est un problème important

Le meilleur avantage de l'Internet public est son ubiquité, mais ceci au détriment de la sécurité. L'Internet est un réseau de libre accès avec une affectation dynamique des ressources, ce qui signifie que chaque paquet d'informations transmis peut être acheminé par plusieurs chemins, sur différents réseaux exploités par des ISP. Ce routage soulève des problèmes de sécurité, et la sécurisation de l'adressage est d'une importance essentielle dans tout service VPN qui utilise l'Internet public comme structure de base. La sécurité des données peut être complexe à gérer et cette gestion représente l'un des principaux avantages des solutions administrées par des fournisseurs de services par rapport à ceux mis en place en interne par une entreprise.

Dans les services de Internet VPN, la sécurité est généralement assurée par une association de méthodes, dont les principales sont la tunnellisation (tunnelling), le cryptage et les pare-feu (firewalls).

La tunnellisation est une technique qui propose des "connexions" logiques point à point sur un réseau IP à libre accès. Il offre en lui-même un certain niveau de sécurité mais est généralement associé à un cryptage afin de garantir des fonctions de sécurité plus avancées. Lorsqu'un cryptage est appliqué à une connexion 'tunnel', les données sont brouillées ce qui ne les rend lisibles qu'aux personnes autorisées. Il existe différents degrés de cryptage selon le degré de confidentialité requis. Dans les applications pour lesquelles la confidentialité n'est pas un obstacle, les tunnels peuvent être utilisés sans cryptage. Les pare-feu assurent une protection contre les accès non autorisés aux données de l'entreprise et peuvent être mis en œuvre et gérés par l'entreprise elle-même ou par le fournisseur de services.

Il existe un certain nombre de protocoles pour la tunnellisation des Internet VPN Internet. Le plus connu, IPSec (IP Security), est un protocole VPN de couche 3 offrant des fonctionnalités de tunnellisation et de sécurité, notamment le cryptage, l'authentification et la gestion des clés. Les autres protocoles en vigueur sont les suivants :

- PPTP (Point-to-Point Tunnelling Protocol - Protocole de Tunnelling Point-à-Point)
- L2TP (Layer 2 Tunnelling Protocol - Protocole de Tunnelling de couche 2)
- L2F (Layer 2 Forwarding).

Il s'agit pour chacun d'eux de protocoles de couche 2 qui supportent le tunnelling de bout en bout ; en revanche, ils ne supportent pas le cryptage standard et la gestion des clés.

4.4.3 Au-delà du "Best effort"

Autre limitation importante de l'Internet : il est par nature de type 'best effort' et dépourvu de tout contrôle de la qualité (QoS). Cependant, certains fournisseurs de services peuvent proposer des services VPN Internet qui ne sortent pas de leur propre infrastructure réseau. Quoique cette infrastructure fasse toujours partie de l'Internet, les ISP qui la possèdent peuvent employer des méthodes de prioritisation du trafic, comme la mise en file d'attente par type de service (class-based queuing) et ainsi offrir un certain niveau de QoS.

Les organismes de normalisation n'ont toujours pas finalisé les spécifications relatives à la garantie QoS sur les réseaux IP. Bien que le protocole de réservation de bande passante (RSVP - resource ReSerVation (set-up) protocol) existe déjà depuis quelques années, il semble communément admis que sa complexité constitue un obstacle à son adoption par la majorité.

4.4.4 Une solution pour l'accès à distance

Outre la connectivité de site-à-site, les VPN Internet revêtent une importance particulière pour les applications d'accès distant des entreprises, motivée par les exigences croissantes des télé-travailleurs et du personel nomade qui ont besoin d'accéder à leur réseau local. La sécurité est assurée par des logiciels (généralement utilisant IPSec) installés sur le PC ou les portables des utilisateurs distants. Ces derniers se connectent à l'intranet de leur entreprise en appelant le point de présence (PoP - point of presence) local de leur fournisseur d'accès. S'agissant généralement d'un numéro local, et le coût fixe mensuel étant généralement peu élevé, cette solution convient bien aux utilisateurs dont les besoins en accès à distance ne cessent de croître. La principale alternative pour l'accès à distance consiste à fournir une connexion temporaire via un modem et un serveur d'accès à distance. Cette solution implique davantage de dépenses d'investissement et entraîne des coûts d'appel longue distance ou international plus élevé.

4.5 IP VPN avec QoS

Cette expression s'utilise en référence aux IP VPN qui peuvent garantir la fourniture d'un niveau de service. La qualité de service (QoS) d'un IP VPN diffère de celle d'un Internet VPN dans la mesure où le trafic est routé à travers un seul réseau IP privé, c'est-à-dire détenu et géré par un seul fournisseur de services utilisant TCP/IP, et non pas l'Internet public. Toutes les caractéristiques de QoS peuvent ainsi être appliquées et rendent possible la fourniture d'un environnement beaucoup plus sécurisé que l'Internet. Les IP VPN peuvent supporter des débits de 64 Kbit/s à 45 Mbit/s à mesure que la demande croît. Le IP VPN avec QoS est parfois appelée IP VPN privé ou IP VPN d'entreprise.

4.5.1 Applications intranet et extranet

Le IP VPN avec QoS fournit une solution complète pour la création d'un WAN. Traditionnellement, elle assure la connectivité pour un reseau local intranet, connectant le siège social aux filiales au sein d'une entreprise dispersée géographiquement. Cette solution peut également être retenue pour la création d'un extranet, reliant les entreprises à ses partenaires commerciaux.

4.5.2 L'usage du MPLS est essentiel

Contrairement aux Frame Relay VPN, qui fournissent une connectivité entre des points terminaux prédéterminés, un IP VPN fourni une connectivité de n'importe quel terminal à n'importe quel terminal.

Les premiers services VPN IP se présentaient comme un réseau secondaire venant se greffer sur un réseau Frame Relay principal. De tels services étaient difficiles à mettre en œuvre et à gérer en raison de l'utilisation sous-jacente de PVC. Aujourd'hui, la plupart des services IP VPN s'appuient sur une technologie IP ou ATM et utilise le protocole MPLS. Celui ci crée une architecture de couche 3 sans connexion et permet d'obtenir une plate-forme souple et évolutive qui peut supporter le QoS. Ces services MPLS se distinguent de ceux fournis par les technologies IP VPN plus anciennes. Dans la mesure où les utilisateurs ne voient qu'une interface d'accès IP côté réseau, la technologie principale utilisée par le fournisseur de services leur est transparente.

Avec MPLS, un label est affecté à chaque paquet lorsqu'il entre sur le réseau IP/ATM du fournisseur de services. Les labels contiennent des instructions pour le routage et la gestion des paquets tout au long de leur cheminement à travers le réseau. En empruntant le réseau, seuls les labels sont lus par les routeurs et les commutateurs, ce qui réduit les temps de transmission de bout en bout. La QoS est gérée pour chaque classe de trafic au travers :

- d'un contrôle du chemin emprunté par les paquets en fonction du type de trafic
- d'un ensemble de techniques d'ingénierie de trafic, comme la surveillance de la charge du trafic et le contrôle des mises en file d'attente.

L'utilisation du protocole MPLS dans les services VPN IP avec QoS s'est considérablement accrue l'année dernière. Cette augmentation a donné naissance à une nouvelle génération de services hautement évolutifs, lesquels permettent de proposer des QoS différenciées. Cela signifie que les différentes classes de trafic - notamment les trafics voix et données vitales de l'entreprise - peuvent chacune être transportée avec leurs propres niveaux de QoS.

4.5.3 Trois niveaux de 'classes de service'

Les VPN IP qui supportent les QoS différenciés proposent généralement trois niveaux de 'classes de service' (Class of service - CoS), 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.

4.6 Lignes louées

Les lignes louées (parfois appelées circuits privés) sont des connexions dédiées qu'un opérateur télécoms exploite directement entre deux sites clients, fournissant une connexion permanente à un débit determiné. Elles sont essentiellement des chemins réservés privés à travers le réseau du fournisseur de services loués par l'entreprise utilisatrise pour le transport de son trafic réseau. Ce service s'apparente à celui des lignes téléphoniques dans la mesure où il est disponible en permanence, mais son coût ne varie pas selon l'utilisation qui en est faite ; en effet, une ligne se loue au mois, quelle que soit la fréquence de son utilisation. Les lignes louées peuvent être installées sur toutes distances. Le tarif varie selon le débit (bande passante) et la situation géographique des deux extrémités de la ligne.

4.6.1 Lignes louées numériques

Les lignes louées sont analogues ou numériques. Numériques, elles offrent une solution plus souple en termes de bande passante et de qualité de QoS).

Lorsqu'un opérateur loue une ligne numérique, il fournit généralement à l'utilisateur des interfaces de transfert de données (e.g. V.35), à certains emplacements, là où le client peut connecter ses routeurs d'accès. La disponibilité des lignes louées numériques dépend de la topologie du réseau de l'opérateur. La connexion au réseau nécessite un équipement de transmission de données tel qu'un routeur, ainsi qu'une Unité de service de canal/unité de service de données (CSU/DSU - channel service unit/data service unit) pour fournir l'interface réseau.

4.6.2 Liaisons point-à-point et point-à-multiples points

Le service point-à-point constitue le type d'application de lignes louées de base le plus sécurisé. Un circuit dédié connecte un site à un autre via une ligne privée et transmet les données à une vitesse constante équivalente à la bande passante du circuit. La configuration la plus répandue consiste à relier deux LAN géographiquement séparés pour faciliter la transmission de la voix et des données sur le même circuit.

Les lignes louées numériques peuvent aussi s'appliquer aux communications point-à-multiples points. Une liaison point-à-point permet d'établir la connexion entre un site terminal et un PoP. A partir du PoP, la fonction de multiplexage permet de connecter un site (centralisé) unique avec plusieurs site distants. D'où l'idée qu'une telle configuration pourrait constituer une alternative aux topologies des Frame Relay VPN ou ATM VPN.

4.6.3 Débits de transmission variables

Les lignes louées numériques utilisent généralement un circuit partagé T1/E1 ou à bande passante supérieure, allant de débits de 64 Kbit/s jusqu'á 274 Kbit/s (DS0-T4 aux Etats-Unis, DS0-E4 en Europe). La location d'une ligne réseau à fibres optiques, avec hiérarchie numérique synchrone (SDH - synchronous digital hierarchy) ou réseau optique synchrone (Sonet - synchronous optical network) autorise des vitesses de transmission STS (signal de transport synchrone - synchronous transport signal aux Etats-Unis) ou STM (synchronous transport module - module de transport synchrone en Europe), c'est-à-dire jusqu'à 622 Mbit/s.

5 Principaux critères de choix pour réseaux virtuels privés (VPN)

L'objectif des utilisateurs, lors du choix d'un VPN, est de trouver le bon équilibre entre avantages technologiques et coûts. L'analyse qui mène à ce choix repose sur de nombreux critères (performance, coût, sécurité, niveau garanti de service, interopérabilité, capacité d'évolution, gestion du réseau, ubiquité et facturation) décrits dans cette section.

5.1 Performance

- débit - désigne le volume de données qu'un canal de communication peut acheminer (généralement indiqué en bits par seconde ou bits/s)
- délai moyen d'acheminement (ou latence) - désigne le temps moyen nécessaire à un paquet pour aller de l'émetteur au récepteur à travers une connexion réseau
- délai maximum (ou deadline) - désigne le retard de livraison maximum acceptable. Ce paramètre s'applique à l'ensemble de la connexion au niveau de la couche application
- distorsion - désigne une variation aléatoire des caractéristiques de délai d'acheminement d'un paquet
- perte de paquet - désigne le pourcentage de paquets non parvenus
- pics de trafic (burst) - désigne la capacité du système à s'adapter à une demande substantiellement supérieure à la moyenne
- compression - consiste à réduire la taille des données à transmettre en leur appliquant un algorithme spécialisé afin d'économiser les ressources de transmission et la bande passante
- contrôle d'erreur - il existe deux types de contrôle d'erreur. La détection d'erreurs avec demande de répétition (ARQ - automatic request for repetition) permet au destinataire de demander à l'émetteur de lui envoyer à nouveau les données incorrectes. La correction d'erreurs sans voie de retour (FEC - forward error correction) achemine des informations complémentaires en même temps que les données á transmettre. Ces informations supplémentaires peuvent être utilisées par le destinataire pour contrôler et corriger les données d'origine
- taux d'erreurs sur les bits (BER - bit error rate) - est une mesure fondamentale pour évaluer la qualité des réseaux de communications.

5.2 Coûts

- coûts du service
- coûts de location
- coûts d'entretien
- frais de licence
- coûts du niveau de cryptage
- coûts d'administration.

5.3 Sécurité

- tunnelling - création de circuits virtuels via Internet par l'encapsulage d'un type

de paquet dans un autre, de sorte que les données peuvent être transférées via des chemins virtuels

- cryptage - désigne une procédure employée pour convertir du texte pur en texte crypté afin d'éviter toute lecture de ces données par une personne autre que le destinataire

- authentification - désigne la procédure qui garantit que les données proviennent effectivement de la source qu'elles revendiquent.

5.4 Capacité du fournisseur à garantir des Accords sur les Engagements de Service (SLA - Service Level Agreement).

- fiabilité - caractéristique de tout système qui produit régulièrement les mêmes résultats, et de préférence répond voire dépasse ses spécifications

- temps d'installation - désigne le délai nécessaire pour que le réseau soit entièrement fonctionnel

- limites de responsabilité - définit les problèmes de logiciel et ceux pouvant survenir entre opérateurs

- disponibilité du service - désigne la période de temps au cours de laquelle le service est disponible, par exemple, 24 heures par jour, 99.99% du temps

- temps de réponse du service - indique la rapidité avec laquelle le fournisseur VPN doit répondre aux problèmes des clients

- mise à niveau (upgrade) - indique la fréquence et les coûts de mise à niveau lorsque celle ci doit intervenir.

5.5 Interopérabilité

- compatibilité avec d'autres systèmes (y compris intégration avec des équipements existants)

- complexité de l'intégration avec d'autres systèmes

- facilité de migration vers d'autres technologies.

5.6 Capacité d'évolution

Un réseau évolutif peut supporter un nombre croissant d'utilisateurs et/ou de services sans que ses performances en soient affectées. La capacité d'évolution peut être requise à différents niveaux :

- bande passante - capacité supplémentaire

- fourniture de nouveaux services

- couverture géographique - extension à de nouvelles zones.

5.7 Gestion du réseau

- contrôle de la gestion de performance - généralement effectué par des outils logiciels associés (certains avec une interface utilisateur Web)

- maintenance

- support client (centre d'assistance)

- récupération après sinistre - vitesse de réponse, actions sur le site des utilisateurs, sur le site du fournisseur de services ou dans le pool d'équipements loués

- formation utilisateur - y compris la formation d'origine, de suivi et de mise à jour.

5.8 Ubiquité

- nombre de points de connexion de Couche 2 ou de Couche 3

- couverture géographique

- restrictions gouvernementales (par exemple, pour le cryptage).

5.9 Facturation

- notamment la fréquence, les augmentations, les remises sur volume, le remboursement pour cause de pannes, et le coût de l'accès en ligne en temps réel aux données.

6 Classification des services et applications pouvant utiliser un réseau virtual privé (VPN)

En général, on peut identifier trois niveaux de service pour vérifier que les applications VPN obtiennent les ressources et la performance réseau dont elles ont besoin : transfert en temps réel, transfert asynchrone de données critiques et transfert de données ordinaires.

6.1 Transfert en temps réel

Les services en temps réel comprennent le trafic sensible au retard tels que :

- voix
- vidéo
- flux audio et vidéo professionnels
- vidéoconférence
- audioconférence.

6.2 Transfert asynchrone de données critiques

Ce type de service est utilisé pour les applications d'entreprise telles que les bases de données client-serveur. Il assure aux applications critiques d'entreprise la bande passante nécessaire à leur niveau de performance souhaité.

Les applications critiques d'entreprise incluent :

- l'accès au web
- les applications interactives telles que les jeux proposés en-ligne
- les applications telnet et de connexion à distance
- les outils de collaboration tels que la conception et fabrication assistées par ordinateur (CAD/CAM)
- le transfert d'images médicales, géographiques, militaires
- les applications intranet
- l'accès aux données et applications extranet
- les applications de commerce électronique
- les applications de réalité virtuelle
- les systèmes de gestion de la relation client (CRM - customer relationship management)
- les systèmes de planification des ressources d'entreprise (ERP - entreprise resource planning)
- les réseaux dédiés au stockage.

6.3 Transfert de données ordinaires

Les applications plus ordinaires utilisent la bande passante non consommée par les applications critiques. Ce type de service s'applique au trafic d'arrière-plan tel que :

- le transfert de fichiers
- la navigation web
- le courrier électronique
- des données diverses.

Les applications en temps réel exigent une performance réseau homogène. Cela rend difficile l'utilisation de ces applications via des réseaux IP, dans lesquelles la qualité du service est fondée sur la notion de meilleur effort (best effort). Les réseaux IP étaient à l'origine conçus pour acheminer des données pour lesquelles la notion de temps réel n'était pas importante puisque les paquets de données pouvaient arriver à tout moment.

Les risques de distorsion peuvent généralement être contrôlés à l'aide de buffers mais au prix d'un délai supplémentaire. L'échange doit être dimensionné avec précaution car les usagers du téléphone, par exemple, ne peuvent supporter des délais supérieurs à 200 millisecondes, au-delà desquels une conversation téléphonique devient un

LOGICIELS APPLICATIFS	CRITÉRES DE SERVICE										
	Débit	Temp de latence	Retard Max.	Distorsion (jitter)	Perte de Paquet	Pics de Paquet (bursting)	Compression	Contrôle d'erreur	Tunnelling (si IP)	Authentication	Cryptage
Voix	D	C	C	C	C	N	D	D	D	N	D
Vidéo	C	C	C	C	C	N	C	C	D	N	D
Flux audio	D	D	D	D	D	D	C	D	C	D	D
Flux vidéo	C	C	C	C	C	D	C	C	C	D	D
Accès au Web	D	N	N	N	N	C	D	D	C	C/D	C/D
Service interactif	C	N	D	N	C	D	C	D	C/D	C/D	C/D
Telnet	D	N	D	N	D	C	D	D	C/D	C	C
Connexion à distance	N	N	N	N	N	D	N	N	C	C	C
Outils collaboratifs	C	D	D	N	D	C	C	C	C	C	C
Transfert d'images	C	N	N	N	D	C	C	D	D	D	D
Intranet	D	D	D	N	N	C	C	D	N	C	D
Accès Extranet	D	N	N	N	N	C	D	D	C	C	C
Réalité virtuelle	C	C	C	D	D	C	C	D	C	D	D
Commerce électronique	D	N	N	N	N	C	D	D/N	C	C	C
Transfert de fichiers	D	N	N	N	N	C	C	D/N	C	D	D
Courrier électronique	N	N	N	N	N	C	D	D	C	C	C
Utilisation du Web	N	N	N	N	N	C	D	D	C	N	N
Systèmes de gestion de la relation client	C	D	N	N	D	C	C	C	C	C	C
Systèmes de planification des ressources de l'entreprise	D	N	N	N	D	C	C	C	C	C	C
Systèmes de gestion de la chaîne d'approvisionnement	C	N	C	N	D	C	D	C	C	C	C
Réseau local dédié au stockage	C	N	N	N	D	C	C	C	C	C/D	C/D

Tableau 6.1 Caractéristiques clés pour les applications VPN

C pour critique (vital), D pour désirable (souhaitable, exigé ou non), N pour non important (sans importance).

problème. Une perte excessive de paquets affecte également la qualité du service des applications en temps réel. Généralement, une perte de paquets supérieure à 5% lassera les utilisateurs. Alors que certaines applications, telles que la diffusion de vidéo, les outils de CAO ou les jeux, exigent un haut débit permanent; d'autres, telles que les applications web, le commerce ou le courrier électronique, nécessitent plus simplement que le réseau puisse gérer les pics de trafic.

Pour certaines applications, telles que le transfert d'images ou le commerce électronique, la sécurité peut être un véritable problème.

Le tableau 6.1 ci-dessus illustre l'importance des paramètres de performance et de sécurité pour chaque application mentionnée dans ce rapport. Trois critères sont utilisés:
C pour critique (vital), D pour désirable (souhaitable, exigé ou non), N pour non important (sans importance).

7 Comparaisons entre technologies pour réseaux virtuels privés (VPN)

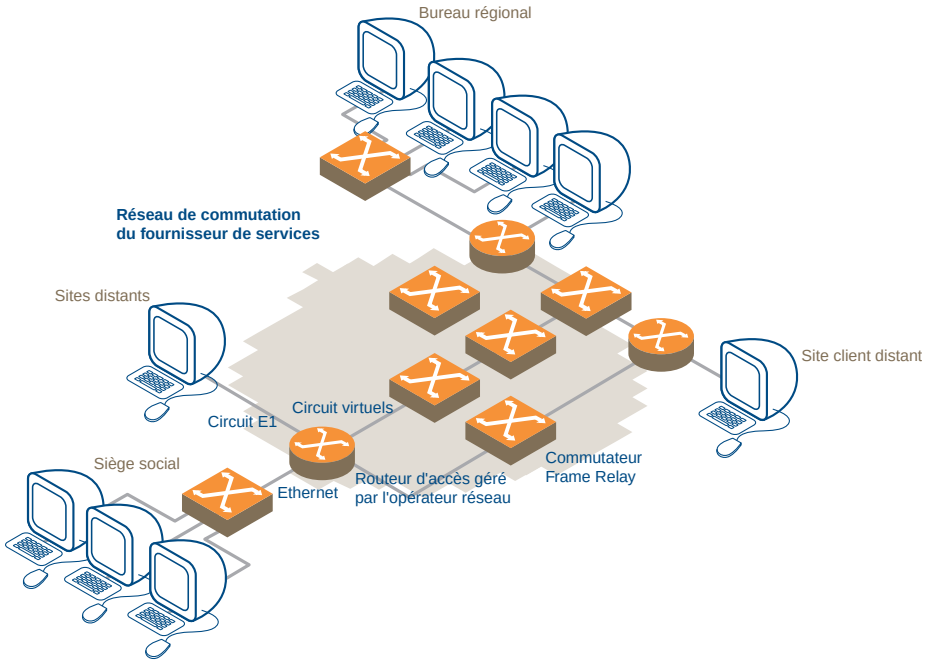


Figure 1 - Frame Relay VPN

7.1 Avantages, inconvénients et services supportés par les VPN Frame Relay

Parmi les caractéristiques clés supportées par la technologie Frame Relay on trouve :

- La possibilité de faire face à des pics de trafic soudains (Bursting): Un circuit virtuel défini pour gérer une certaine capacité peut généralement gérer le trafic qui excède cette capacité. Le service Frame Relay définit un débit minimal garanti (CIR - committed information rate), c'est-à-dire le débit que le réseau accepte de gérer pour une connexion Frame Relay particulière. Lorsque le débit réseau excéde le débit défini par le CIR, on appelle ce phénomène un pic de trafic. Par exemple, un circuit virtuel garantissant une bande passante de 128Kbit/s mais béficiant d'une vitesse d'accès de 256Kbit/s acheminera toujours le trafic à la vitesse de 128Kbit/s mais pourra parfois gérer des pics à 256Kbit/s. La capacité à s'adapter aux pics de trafic soudains dépend de la capacité réseau du fournisseur de services

- La mise en file d'attente (Queuing) : un grand nombre de mécanismes de mise en attente peut être offert par le réseau Frame Relay afin de gérer le trafic de données prioritaires par rapport à celui d'informations de moindre importance. Ces mécanismes incluent la mise en file d'attente prioritaire, la mise en file d'attente définie sur des critères déterminés par le client et la mise en file d'attente en fonction de critères définis de manière dynamique

- L'interopérabilité avec les réseaux ATM, X.25 et SNA : le Frame Relay peut faciliter l'acheminement du trafic SNA à partir de sites distants vers le système central

(mainframe), conjointement avec le trafic X.25 et le trafic asynchrone existant. Les standards Frame Relay ont été développés pour inter-agir avec d'autres services tels que l'ATM. A mesure que de nouvelles applications apparaissent et/ou que le trafic augmente, les réseaux peuvent migrer vers la technologie appropriée sans rendre l'équipement de réseau existant complètement obsolète

- Le Frame Relay peut gérer à la fois le trafic voix et le trafic de données
- Le Frame Relay offre une sécurité implicite : une structure basée sur un circuit virtuel permanent garantit que les paquets ne sont acheminés que vers le port possédant l'adresse de destination correcte. En outre, le Frame Relay supporte la compression et la correction d'erreurs sans voie de retour (forward error correction).

Les protocoles Frame Relay offrent également les avantages suivants:

- C'est un protocole simple qui nécessite moins de données de contrôle, ce qui signifie que davantage de bande passante est attribuée aux données à transmettre plutôt qu'aux données qui gèrent la transmission
- Excellente fiabilité
- Commutation simplifiée, entraînant une réduction des délais
- Les circuits virtuels et le multiplexage statistique entraînent une réduction significative des coûts
- Souplesse et forte capacité d'évolution et rétablissement après sinistre du réseau.

En raison de sa structure, la capacité d'évolution du Frame Relay est plus élevée que celle d'un réseau fixe point à point. L'utilisateur final ne se rend pas compte des ajouts et modifications au réseau, ce qui permet aux gestionnaires réseau de modifier facilement la topologie du réseau et d'étoffer ses capacités à mesure que les applications qui l'utilisent deviennent plus exigeantes en trafic et que de nouveaux sites viennent s'ajouter au réseau.

Dans de nombreux cas, l'utilisateur final ne se rend également pas compte que le trafic est routé vers des sites de rétablissement après sinistre. Frame Relay est plus adapté aux applications qui offrent les caractéristiques suivantes :

- trafic périodique
- trafic variable et/ou imprévisible
- grands volumes de transaction
- transmission de documents et autres transferts de données qui peuvent générer des pics de trafic soudains et exigent une augmentation de la bande passante disponible (l'accès au service Frame Relay commence á 56Kbit/s).

Le Frame Relay est particulièrement adapté aux besoins de réseaux hétérogènes qui supportent un grand nombre d'applications différentes, certaines très exigeantes en trafic et d'autres nécessitant des débits plus modeste. Cette diversité permet d'exploiter efficacement toutes les capacités du Frame Relay.

La technologie Frame Relay présente cependant certains inconvénients, à savoir :

- à l'origine, le Frame Relay était conçu pour des applications de données. Il ne supportait pas les données de type voix en raison des problèmes relatifs aux temps de traitement imposés par le réseau
- La transmission de paquets de longueurs variables n'est pas adaptée aux applications sensibles au temps de transmission telles que la voix et la vidéo
- faibles vitesses de transmission car le Frame Relay supporte des débits maximaux de 2Mbps
- il est sujet à des erreurs dans le cas de circuit affectés de bruit parce qu'il bénéficie pas de facilités de contrôle d'erreur
- l'intégrité des données et le contrôle de flux ne sont pas garantis, comme avec le réseau X.25 (plus lent).

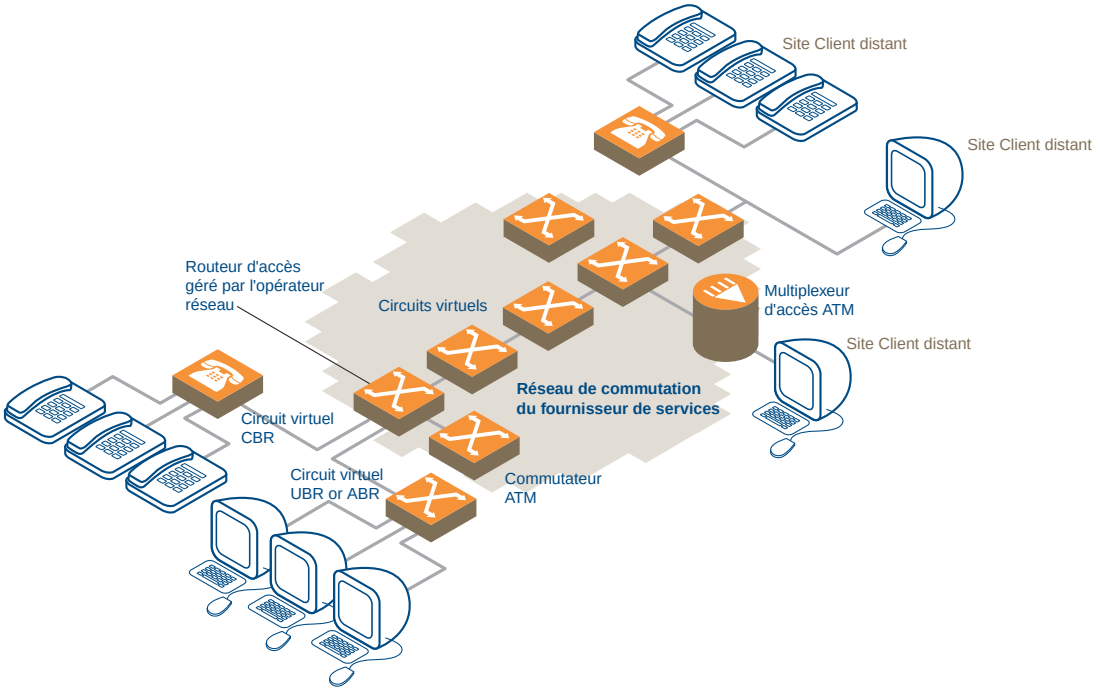


Figure 2 - ATM VPN

7.2 Avantages, inconvénients et services supportés par les ATM VPN

Parmi les avantages et bénéfices du service ATM, on trouve :

- l'attribution dynamique de la bande passante pour faire face aux pics de trafic (attribution limitée par le fournisseur de services)
- l'utilisation de circuits virtuels qui, en raison du multiplexage statistique, permettent, notamment à hauts débits, un très bon rapport qualité-prix par rapport aux communications commutées par circuit
- une vaste gamme de critères de qualité de service (QoS) pour les applications multimédias, ce qui permet de répondre, sur un même réseau, aux différentes exigences des applications en matière de débit et de délai
- une forte capacité d'évolution tant en termes de débit qu'en matière de taille du réseau
- la souplesse - ATM peut être configuré pour répondre aux différentes exigences de performance d'une application
- une haute performance permise par une commutation matérielle
- des opportunités de simplification offerte par une architecture de connexion virtuelle commutée
- la fiabilité et la redondance
- l'interopérabilité avec d'autres technologies telles que Frame Relay et l'adaptation à des protocoles de couche supérieure tels que TCP/IP.

Par comparaison avec Frame Relay, conçu à l'origine pour les transferts de données seulement, ATM est optimisé pour supporter un large spectre de types de trafic avec une qualité (garantie) de service. Cinq classes de services sont supportées :

- Débit constant (CBR - constant bit rate) - Le CBR émule la commutation de circuit et définit un débit constant des cellules ATM. Il est adapté aux applications sensibles aux délais de traitement telles que le trafic téléphonique et la visioconférence
- Débit variable - Temps Réel (VBR-RT / Variable Bit Rate - Real Time) - Le service VBR-RT ne varie pratiquement pas en matière de délai d'attente, et s'adapte facilement aux variations du trafic. La transmission de données vidéo et voix compressées interactives avec détection de la parole sont des exemples d'applications VBR-RT
- Débit variable - Différé (VBR-NRT / Variable Bit Rate - Non-Real-Time) - Le VBR-NRT fonctionne également sur une base de connexion mais se distingue du CBR et du VBR-RT par le fait que l'acheminement des cellules peut souffrir de délais d'attente variables. Le VBR-NRT est identique au service Frame Relay mais offre des débits supérieurs. Il est particulièrement adapté aux applications de données qui génèrent des pics de trafic telles que l'interconnexion de réseaux locaux (LAN), la conception et fabrication assistées par ordinateur (CAD/CAM) et le multimédia
- Débit non spécifié (UBR - Unspecified Bit Rate) - L'UBR peut être utilisé pour des applications qui demandent une garantie de transport sur la base du meilleurs effort (Best effort), tel que celle fournie par TCP. Avec cette approche, le réseau transporte les cellules ATM dès que la bande passante est disponible et que l'utilisateur fournit des données. Cependant, le réseau peut se débarrasser des données utilisant le service UBR au profit de données utilisant d'autres types de service
- Débit disponible (ABR - Available Bit Rate) - L' ABR offre un contrôle de flux basé sur le débit. Il est particulièrement adapté à l'acheminement de données telles que le transfert de fichiers et le courrier électronique (e-mail). Il est identique au service VBR-NRT à l'exception des garanties du débit. Il propose des débits variables en fonction de la disponibilité du réseau.

L'ATM présente cependant les inconvénients suivants :

- souplesse au détriment de l'efficacité
- sa couche supplémentaire d'adressage ajoute de la complexité et entraîne une certaine inefficacité à bas débits
- la complexité des mécanismes permettant d'atteindre une qualité de service (QoS) définie entraîne des coûts plus élevés
- l'encombrement du réseau peut entraîner des pertes de cellules
- les cellules éliminées ne sont pas retransmises
- actuellement, pour des réseaux utilisés par une seule application, il est souvent possible de trouver une technologie plus adaptée
- un grand nombre de possibilités promises par l'ATM reposent sur des standards qui restent encore à définir.

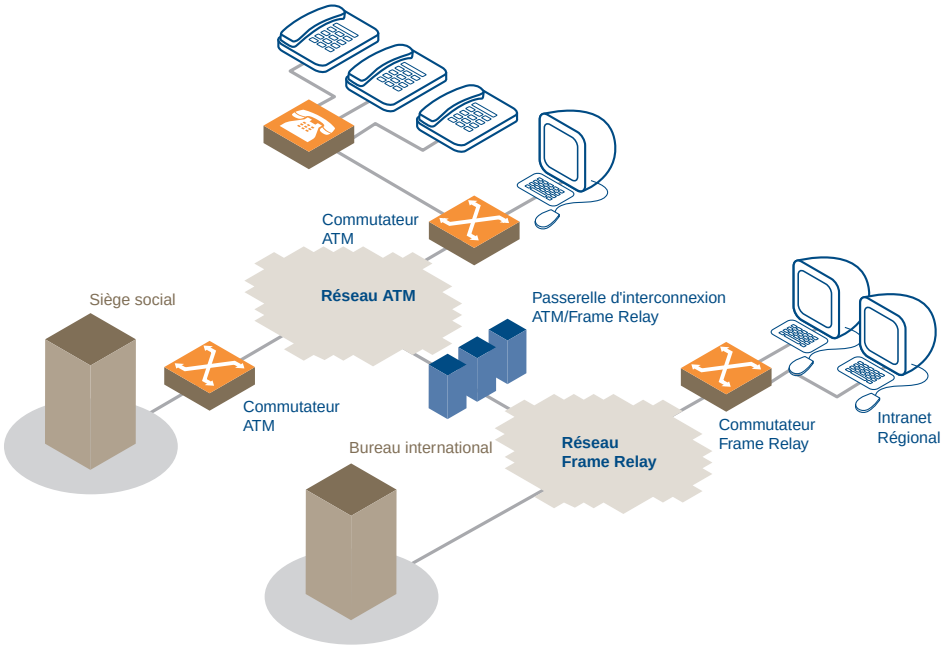


Figure 3 - Interconnexion ATM/Frame Relay

7.3 Avantages, inconvénients et services supportés par des VPN d'interconnexion ATM/Frame Relay

Le Frame Relay et l'ATM possèdent chacun des caractéristiques uniques. L'un ne peut pas offrir toutes les fonctions de l'autre. C'est pourquoi l'utilisation des deux technologies est un avantage pour le déploiement d'applications auxquelles elles sont chacune le mieux adaptée, offrant des services VPN à la fois souples et permettant une forte capacité d'adaptation.

En permettant aux terminaux existants l'accès à des applications reposant sur les technologies Frame Relay et ATM, un VPN d'interconnexion protège les investissements déjà effectués. Ceci favorise la séparation du côté "client" et du côté "serveur" du réseau, ce qui permet à chaque coté d'utiliser les ressources correspondant le mieux à leurs exigences en matière de débit et de contraintes budgétaires.

Parmi les autres avantages offerts par l'interopérabilité ATM/Frame Relay on distingue :

- une meilleure capacité d'évolution qui s'étend de la simple ligne T1 partagée jusqu'aux débits de type module de transport/transfert synchrone (STM - synchronous transport/transfer module)
- les clients ATM peuvent se reposer sur l'infrastructure Frame Relay en cas d'indisponibilité d'un nœud ATM, et vice versa
- l' ATM peut être utilisé à la place du Frame Relay si celui-ci est pas disponible dans une certaine zone géographique, et vice versa.

L'implémentation VPN de Couche 2 (Layer 2) offre une excellente sécurité car les mesures de sécurité peuvent être prises au niveau des équipements terminaux. Cependant, en Couche 2, les algorithmes de sécurité peuvent être "propriétaires" et entraîner ainsi des problèmes d'interopérabilité.

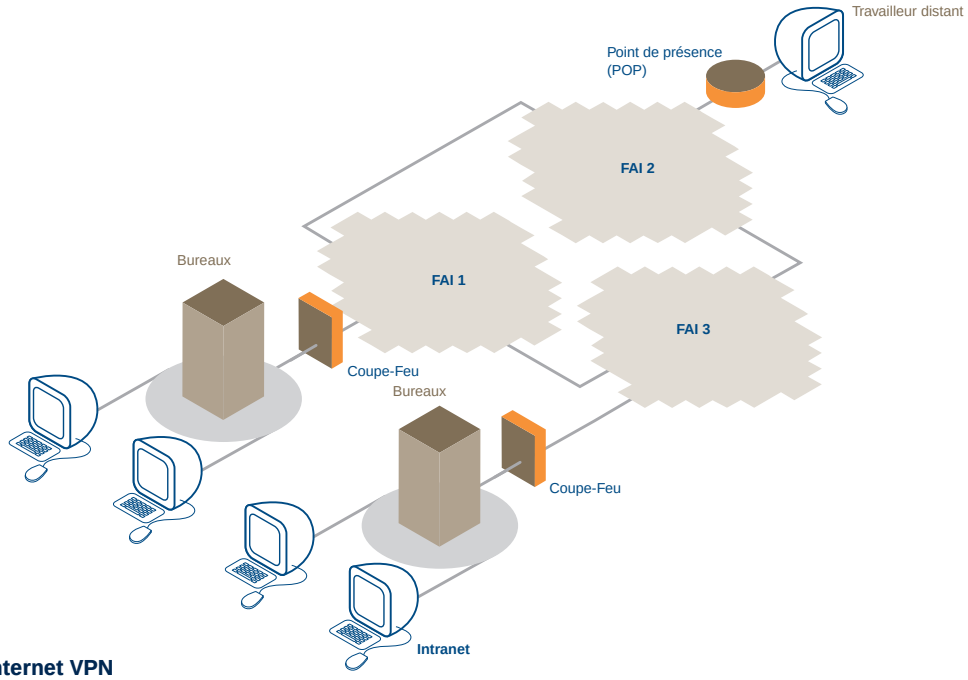


Figure 4 - Internet VPN

7.4 Avantages, inconvénients et services supportés par les Internet VPN

Le principal avantage des Internet VPN est la couverture mondiale. Ils permettent á chacun d'être accessible depuis n'importe quel point du globe sans infrastructure supplémentaire. Les Internet VPN présentent également les avantages suivants :

- Ils ne nécessitent pas de routeurs réseaux spécifiques
- Ils ne nécessitent pas d'administration système, de configuration, et de support technique pour routeurs. Il n'est plus nécessaire de créer et d'assurer la maintenance des tables de routage
- Ils suppriment des coûts de services longue distance, ce qui permet des économies substantielles
- Ils supportent une grande variété d'applications ce qui permet aux utilisateurs de ne pas avoir à payer pour d'autres types de réseaux
- Ils peuvent être utilisés par quiconque sans investissement important préalable
- Leur faibles coûts offrent les même opportunités aux petites comme aux grandes entreprises
- Ils sont d'un déploiement rapide et souple, sont facilement modifiables et offrent une forte capacité d'évolution (ils peuvent répondre de manière dynamique à des besoins variés)
- Les utilisateurs ont un vaste choix de distributeurs et de fournisseurs de services Internet
- La disponibilité de personnel technique et d'expertise dans le monde entier

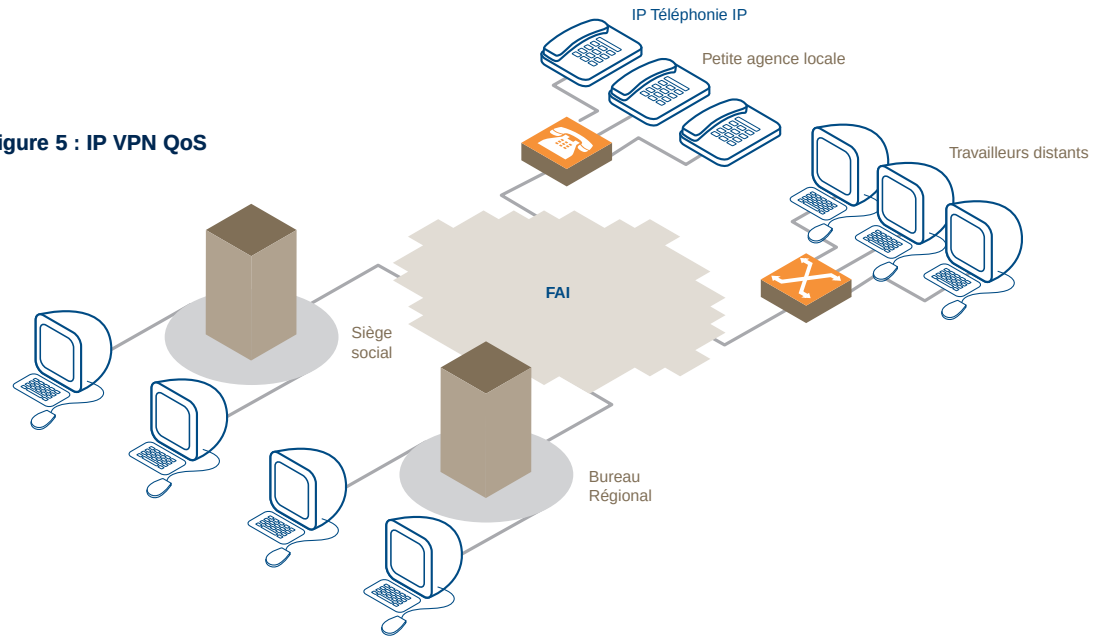
Les Internet VPN sont tout à fait adaptés à l'accès à distance et aux communications entre sites géographiquement très dispersés, applications pour lesquelles le critère de coût prend une importance suprême.

Cependant, l'utilisation de l'Internet public pour créer un WAN d'entreprise présente des inconvénients, notamment lorsque plusieurs FAI (fournisseurs d'accès Internet) sont impliqués dans le service. Ceci entraîne :

- la nécessité de mettre en place un stratégie de sécurité qui couvre l'ensemble des fournisseurs et de leurs services
- le fait que divers fournisseurs offrent des niveaux de service variés, certains d'entre eux avec un niveau de garantie limité, voire sans aucune garantie de service
- des délais d'accès et d'acheminement variables.

Ces problèmes rendent généralement les Internet VPN inadaptés aux applications professionnelles critiques ou en temps réel.

Figure 5 : IP VPN QoS



7.5 Avantages, inconvénients et services supportés par les IP VPN avec QoS

L'emploi d'un seul fournisseur de services IP possédant son propre réseau privé signifie que le trafic entre les sites IP VPN peut être assuré en toute sécurité. En outre, un fournisseur de services unique utilisant les technologies assurant la qualité du service (QoS), peut définir des contrats de niveau de service (SLA - Service Level Agreement) détaillés. Ces SLA peuvent se définir sur la base des critères suivants : performances relatives à la fourniture et au dépannage du service, à la disponibilité du réseau et paramètres QoS tels que temps de latence, fluctuations et perte de paquets.

Cependant, les contrats de type SLA pour services IP VPN sont encore en plein développement et nombreux sont ceux qui n'incluent pas la boucle d'accès réseau, ce qui ne leur permet par de garantir le service sur l'ensemble de la transmission.

L'utilisation d'une structure IP supprime les circuits virtuels permanents (PVC) statiques associés à des protocoles orientés connexion tels que Frame Relay et ATM, créant ainsi une topologie de réseau entièrement maillé tout en réduisant vraiment la complexité et le coût du réseau.

Une nouvelle génération de IP VPN utilisant la technologie de commutation multiprotocole par étiquette (MPLS - multiprotocol label switching) peut définir une base QoS sur laquelle elle délivrera à la fois voix et vidéo en temps réel et transferts de données plus classiques. La capacité des IP VPN à supporter les applications voix et données haute priorité, ainsi que les applications basse priorité (telles que le courrier électronique et les communications HTTP), est très importante. Elle signifie que de nombreuses entreprises peuvent satisfaire leurs besoins en communications internes via un seul VPN; ce qui conduit à une réduction importante de leurs coûts et de leurs efforts de gestion.

A mesure que la voix sur IP (VoIP) devient plus courante dans les réseaux offerts par les opérateurs télécoms et que les autocommutateurs IP privés (IP PABX) remplacent les autocommutateurs privés plus traditionnels, les IP VPN peuvent de plus en plus offrir des services VoIP. Ils offrent une plate-forme de convergence des applications voix et données telles que la messagerie unifiée, le cliquer/parler (click to talk) et la co-navigation (co-browsing). L'évolution rapide de la VoIP associée au développement et à l'application de nouveaux protocoles tels que SIP (Session Initial Protocol) va générer de nombreuses applications centrées sur la voix ou combinant voix et données. Ces applications s'intégreront facilement à un environnement IP VPN.

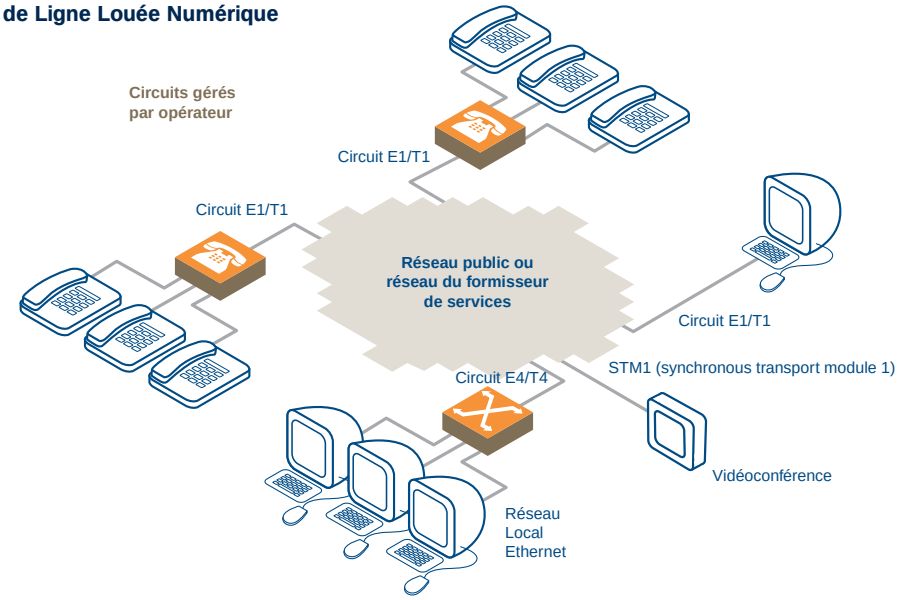
Les IP VPN sont particulièrement adaptés aux connexions extranet très sécurisées destinées aux applications de commerce inter-entreprise. Les entreprises peuvent autoriser leurs partenaires commerciaux, fournisseurs et clients à accéder à leur réseau à partir d'une connexion de réseau IP privé. Les paramètres de sécurité peuvent être définis de façon très détaillée. L'accès peut être limité à un seul ordinateur source ou cible avec des adresses IP et des numéros de port TCP/UDP spécifiques.

L'utilisation des technologie MPLS et QoS pour une vaste gamme de trafics ont fait des IP VPN une solution adoptée par une majorité d'utilisateurs en quête d'un WAN d'entreprise sécurisé offrant un niveau élevé de performance. Les VPN IP utilisant la technologie MPLS ne sont pas encore mâtures mais permettront de combiner la plupart des attributs offerts par d'autres technologies á savoir:

- le QoS de l'ATM
- le débit minimal garanti (CIR) du Frame Relay
- la sécurité du Frame relay et de l'ATM
- la souplesse, la robustesse de capacité d'évolution et de connexion des Internet VPN.

Les IP VPN vont finir par devenir la solution de choix pour les réseaux d'entreprises.

Figure 6 : Solutions de Ligne Louée Numérique



7.6 Avantages, inconvénients et services supportés par les Lignes Louées Numériques

Les Lignes Louées sont adaptées à des réseaux dont les exigences en matière de trafic ne sont pas élevées et qui supportent des débits stables et prolongés, tels que les transferts de fichiers volumineux, entre un nombre limité de sites.

Les principaux avantages des Lignes Louées sont le contrôle et la confidentialité qu'elles garantissent à l'utilisateur. Elles ne posent pas de problème de disponibilité comme c'est le cas de Frame Relay ou de l'ATM. Elles sont disponibles en permanence et n'exigent pas qu'une communication soit établie avant d'acheminer le trafic. Ceci permet :

- de garantir le débit et de rapide délais d'acheminement
- de supporter des applications multimédias avec un débit constant et des taux d'erreur très faibles
- un meilleure fiabilité du service parce que :

  les Lignes Louées ne souffrent pas des déconnexions qui peuvent intervenir lors de longues sessions Internet

  les interférences dues aux connexions bruyantes sont réduites

  elles ne sont jamais occupées, toujours prêtes au transfert de données

  leur gestion est centralisée

- la ligne est contrôlée par l'utilisateur

L'inconvénient des Lignes Numériques Louées dédiées est que l'utilisateur paie pour la bande passante contractuellement définie même s'il ne l'utilise pas. Autre inconvénient majeur : leur coût est défini sur la base de la distance couverte par les lignes louées. Elles sont extrêmement coûteuses pour des réseaux qui couvrent de longues distances ou qui connectent plusieurs sites á grande échelle. Les Lignes Louées à faible débit manquent également de souplesse par comparaison à d'autres types de solutions tels que le Frame Relay lorsque l'on souhaite modifier la topologie du réseau.

L'ajout d'un nouveau site, par exemple, exige la fourniture d'un nouveau circuit et d'interfaces de bout en bout pour chaque point avec lequel le nouveau site doit communiquer. Si les nouveaux sites à ajouter sont nombreux, les coûts peuvent s'élever très vite. Par comparaison, les technologies telles que le Frame Relay exigent seulement une ligne d'accès au bureau central le plus proche et la définition de circuits virtuels pour chaque site avec lequel le nouveau site souhaite communiquer.

Cependant, les avantages présentés par les Lignes Louées permettent le support de nombreuses applications :

- la connexion de noeuds et d'équipements réseau
- l'interconnexion de réseaux locaux
- l'interconnexion de réseaux distribués
- l'interconnexion de PABX distribués
- l'interconnexion de réseaux de recherche
- la liaison des entreprises à des serveurs informatiques
- la liaison d'agences de voyages avec les centres de réservation
- l'accès à des journaux en ligne
- un accès rapide à Internet
- l'interconnexion de serveurs avec Internet
- la visioconférence
- le télétravail
- l'accès à des applications/des serveurs distants
- la réception du courrier électronique en temps presque réel.

8 Exemples d'entreprises utilisatrices de réseaux virtuels privés (VPN)

8.1 Entreprise A

L'entreprise A est l'un des leaders mondiaux du secteur des livraisons et du transport. Elle emploie plus de 200 000 personnes sur plus de 1 500 sites et offre ses services dans plus de 200 pays. Elle possède son propre réseau privé mais, en raison de sa croissance récente et de ses besoin en services plus complexes, sa demande en communications a largement augmenté.

Son réseau doit principalement gérer un trafic de données, et, dans une moindre mesure, le trafic voix. Le trafic de données est généré par des applications variées y compris des applications à pics de débit soudains, le courrier électronique (e-mail) et le transfert de fichiers volumineux. Ces besoins ont conduit à la mise en place d'un VPN basé sur la technologie Frame Relay qui offre une solution optimale pour les raisons suivantes :

- la rapidité est l'un des paramètres les plus importants, et la préférence est donc donnée à une technologie qui repose sur le routage et la commutation au niveau de l' équipement réseau
- le service bénéficie de débits élevés et de délais de traitement courts
- le client souhaite définir lui-même le débit minimal garanti (CIR - committed information rate)
- le réseau doit pouvoir gérer les pics de débit soudains
- l'utilisation de circuits virtuels est d'un meilleur rapport qualité-prix que les lignes dédiées.

L'entreprise A a développé un accord sur les engagements de service (SLA - Service Level Agreement) détaillé pour chacun des services empruntant le réseau. Ce contrat prend en compte les critères suivants : sécurité, capacité de réponse, transmission, disponibilité, maintenance, et délai de réparation. En outre, l'entreprise A souhaitait réduire ses coûts de contrôle et de fonctionnement et éviter le recrutement et l'emploi d'une équipe spécialisée.

Les principaux critères de choix du fournisseur de service ont été le type de services disponibles, le prix de ces services et surtout la représentation de fournisseur au niveau mondial.

8.2 Entreprise B

L'entreprise B est l'une des principales sociétés de communication mondiales avec 150 agences dans presque 100 pays. Bien qu'elle dispose de son propre réseau privé, elle a décidé de développer une solution VPN afin de répondre à ses besoins croissants en capacité réseau. Les principales raisons de sa migration vers un VPN sont les suivantes:

- souplesse et rapport qualité-prix
- diffusion sécurisée de documents
- permettre aux employés basés dans différents pays de travailler facilement sur un même projet.

L'entreprise souhaite utiliser le VPN pour:

- le transfert de fichiers
- le courrier électronique
- échanger des données critiques
- échanger des données variées
- les flux vidéo en continu
- la vidéo en temps réel.

L'entreprise est consciente du fait que la solution VPN optimale devra être basée sur la technologie ATM en raison de la capacité de celle-ci à gérer le multimédia en combinant haut débits, délais minimums, qualité et sécurité.

D'autres critères sont également entrés en compte lors du choix du fournisseur de services, dont :

- couverture mondiale
- prix
- support clientèle
- capacités à s'engager sur les paramètres de service, à savoir : disponibilité, maintenance, et délai de réparation
- image.

8.3 Entreprise C

L'entreprise C est une grande companie industrielle avec plus de 100 000 employés dispersés dans le monde entier. Elle veux permettre à ses principaux clients d'effectuer des commandes en ligne. Outre la passation de commandes, l'entreprise C veut également permettre à ses clients d'accéder à son réseau partagé (Extranet) afin de:

- procéder à des transactions en ligne
- contrôler l'état d'avancement de leurs commandes
- consulter l'historique de leurs commandes
- consulter l'état des arriérés de commande
- surveiller l'état de leur compte
- accéder au réseau 24h/24h.

L'entreprise C ne possède pas de réseau WAN privé au niveau mondial et a donc besoin de développer son Extranet via un fournisseur de services VPN. Elle ne désire pas gérer le réseau et veut un contrat d'engagement de service (SLA) principalement fondé sur les critères suivants : disponibilité du service, temps de réponse en cas de problème et délais de mise à niveau. Les exigences en matière de débit et de rapidité de transfert ne sont pas prioritaires car les communications voix et vidéo en temps réel ne sont pas indispensables. Le principal problème est la sécurité du réseau.

Dans la mesure où le réseau doit permettre le déploiement d'applications qui ne nécessitent pas de transferts de données en temps réel mais qui exigent que ces transferts soient effectués en toute sécurité, l'entreprise a opté pour un Internet VPN proposé par un fournisseur de services international. L'entreprise C conclut qu'une solution Internet VPN peu coûteuse en gestion offre une capacité de connexion assez sécurisée en s'appuyant sur des protocoles de cryptage, d'authentification et de tunnellisation. En outre, sa mise en place permettra à l'entreprise C d'offrir des services de commerce électronique inter-entreprise (B2B e-commerce) à ses principaux clients.

Les autres critères de sélection pris en compte par l'entreprise C sont les suivants: couverture mondiale, prix et capacités à s'engager sur la qualité du service VPN.

8.4 Entreprise D

L'entreprise D est une entreprise de taille moyenne en pleine croissance qui emploie environ 350 personnes réparties dans 6 bureaux sur 5 continents. Ses agences étaient, à l'origine, reliées entre elles par une solution Internet VPN que l'entreprise avait elle-même mis en place pour répondre à ses besoins en matière de courrier électronique mais il était devenu difficile de gérer plusieurs FAI (Fournisseurs d'accès Internet) à la fois. De plus la croissance de l'entreprise avait créé de nouveaux besoins que cette solution interne ne pouvait satisfaire, à savoir :

- la mise en place d'une importante application de gestion de la relation client, commune à toute l'entreprise, rendait essentielles les garanties de qualité de service (QoS)
- l'entreprise faisait face à des coûts croissants du trafic téléphonique international entre ses filiales et souhaitait mettre en place une solution capable de supporter ses communications voix internes
- la mise en place prévue d'agences supplémentaires dans le monde entier demandait une infrastructure capable de s'étendre rapidement et de faire face à la croissance du trafic à travers la mise en place rapide de nouveaux noeuds réseau.

L'entreprise envisageait deux types de solution : Frame Relay ou IP VPN QoS. Elle choisi l'IP VPN qui, à coût pratiquement égal, présentait une plus grande souplesse pour l'extension du réseau et l'ajout de nouveaux sites. Les capacités d'interliaision offertes par la solution IP VPN, notamment, permettraient de faire face à une croissance élevée du trafic données et voix entre les filiales. En outre, une solution entièrement gérée par un fournisseur de services permettait aux ressources du support technique informatique de se consacrer à la mise en place de nouvelles applications vitales pour l'entreprise.

WORLDCOM
Tour Franklin,
La Défense 8
92800 Puteaux
www.worldcom.com/fr

Cisco® Powered Network