Technologie de réseaux simultanés

Surmonter les défis associés à la communication de données critiques

Résumé

Les données ont commencé à faire partie des communications critiques au début des années 1990. De nos jours, le simple texte et les images de basse résolution côtoient les applications Internet et multimédias (voix, flux de données vidéo, etc.) friandes de bande passante. Tout cela doit maintenant être rapidement accessible aux utilisateurs mobiles d'une manière fiable, sécuritaire et transparente sur une multitude de technologies de réseaux sans fil.

Chaque réseau sans fil se définit par des critères de rendement, de couverture, de gestion et sécurité, de fiabilité et de coût. Ces critères s'appliquent autant aux réseaux de données privés (radiocommunication professionnelle [PMR], traditionnelle ou de nouvelle génération, et large bande) qu'aux réseaux publics ou partagés (cellulaire, satellite et large bande), chacun ayant ses propres avantages et inconvénients.

Il est maintenant possible de réunir les meilleures caractéristiques de différents réseaux en créant un « réseau de réseaux » par l'entremise d'un réseau privé virtuel mobile (VPN mobile). Les VPN mobiles apportent la sécurité tout en permettant l'itinérance (*roaming*) et la persistance d'application et de session. Mais, jusqu'à ce jour, les utilisateurs ne pouvaient accéder qu'à un seul réseau à la fois.

L'introduction de la technologie de réseaux simultanés permet maintenant aux administrateurs TI de prendre avantage de tous les réseaux existants simultanément, peu importe le type de ceux-ci. Chaque application peut donc tourner sur le réseau lui étant le mieux adapté. Aussi, si pour une raison quelconque un réseau devient inaccessible, l'utilisateur peut toujours passer par un autre. En d'autres mots, il est garanti que les applications consommant beaucoup de bande passante utiliseront les connexions les plus rapides, et qu'en aucun moment, celles-ci n'affecteront les plus délicates applications de données critiques qui elles, sont transmises sur le réseau le plus sécuritaire et le plus fiable disponible.

Communication de données critiques
Un seul réseau ne peut répondre à tous les besoins

Les communications critiques apparurent dans les années 1930 sous la forme de transmission de voix bidirectionnelle seulement. La transmission des données a commencé dans les années 1990 avec l'arrivée d'applications sur des appareils tels les terminaux numériques mobiles (TNM). Les ordinateurs portatifs et les assistants numériques (PDA) jouent présentement un rôle de plus en plus important dans la communication de données critiques pour les travailleurs mobiles. Ceci n'est pas prêt de changer avec la prolifération des applications de toutes sortes.

Aujourd'hui, les applications de données critiques ont évolué et se retrouvent parmi une des quatre catégories suivantes (voir Illustration 1) :

- **Texte** — ***transmission de simples messages textes à des vitesses ne dépassant pas 9,6 kb/s***. Aussi minimaliste que cela puisse paraître, c'est suffisamment de bande passante pour bon nombre d'applications indispensables, mais peu exigeantes, telles que les requêtes au FBI CJIS (texte seulement), l'accès aux bases de données de permis de conduire et d'immatriculation de véhicules, la localisation automatique des véhicules (AVL) — avec l'aide des technologies GPS —, la répartition assistée par ordinateur (RAO) de première génération, et les systèmes de gestion des pannes comme ceux utilisés par les services publics.

- **Images — *transmission d'images à basse résolution à des vitesses d'au moins 96 kb/s.*** Les applications utilisées par la sécurité publique et du militaire nécessitent la transmission d'images fixes au personnel sur le terrain, tels que des photos anthropométriques et des cartes. Elles comprennent aussi la transmission sans fil de rapports à partir d'un véhicule, les demandes de partage d'images avec le FBI CJIS (avec clichés anthropométriques), l'identification mobile des empreintes digitales, la répartition assistée par ordinateur de deuxième génération, et les applications Intranet (par exemple, le système d'archivage et de transmission d'images [PACS] des hôpitaux).

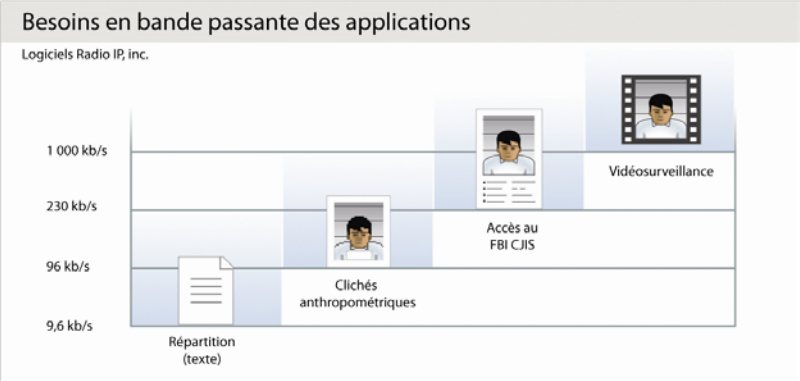

Illustration 1

- **Fureteur** — exigeant un débit de transmission sans fil de 230 kb/s, les utilisateurs mobiles peuvent accéder à Internet ou à l'intranet de leur organisation.

- **Multimédia** — La quatrième et dernière catégorie d'applications de données critiques — à ce jour — est le multimédia au plein sens du terme avec les flux de données vidéo en temps réel (vidéosurveillance et caméra embarquée, etc.) et potentiellement la VoIP, qui demande un beaucoup de bande passante. Ce segment de marché naissant comprend les très prisées nouvelles applications de vidéosurveillance, qui s'installe rapidement grâce à l'utilisation de caméras sans fil se connectant à distance par radio. Ces applications permettent aux unités mobiles d'interagir pleinement avec les unités fixes, les connectant ainsi au LAN câblé de leur organisation. Les utilisateurs mobiles peuvent désormais accomplir toutes leurs tâches, tout en étant à l'extérieur, en se connectant à distance aux applications de leur ordinateur de bureau incluant les dossiers de santé électroniques (télémédecine), les rapports d'électrocardiogrammes et la répartition assistée par ordinateur de troisième génération.

La croissance de la bande passante et de la capacité des réseaux sans fil a stimulé l'évolution des applications de données critiques. Le côté positif est que les réseaux modernes peuvent prendre en charge beaucoup plus d'application de mobilité que leurs prédécesseurs. Toutefois, les nouvelles applications multimédias requirent beaucoup de bande passante, attisant la demande pour la mise en place de réseaux encore plus performants.

Lorsqu'il est temps de jumeler applications de données et réseaux, il n'existe aucune solution unique. Un réseau sans fil spécifique peut ne pas convenir certaines applications — l'environnement doit satisfaire les exigences de chaque application. L'architecture d'un réseau à bande étroite offrant une couverture fiable aux données ne conviendra pas nécessairement aux applications multimédia, alors que certains réseaux à large bande peuvent ne pas fournir la couverture requise pour les applications texte critiques.

L'évolution des réseaux de données sans fil

Les communications critiques d'aujourd'hui utilisent différents réseaux de données sans fil, dont la capacité peut être évaluée et comparée à l'aide des cinq mesures suivantes : *Rendement*, *couverture*, *gestion et sécurité*, *fiabilité*, et *coût*.

- ***Rendement*** : fonction du temps d'attente et de la bande passante qui exprime à quelle vitesse le réseau transporte les données de l'émetteur au récepteur.

- ***Couverture*** : définition de la portée du réseau. En termes géographiques, le réseau d'un état ou d'une province couvre un grand territoire comparativement à un réseau urbain. La couverture fait aussi référence à la continuité du service à l'intérieur du territoire d'un réseau donné. En réalité, la couverture d'un réseau est habituellement inversement proportionnelle au rendement de ce dernier.

- ***Gestion et sécurité*** : indique à quel point une organisation peut décider de la façon dont le réseau fonctionne et qui l'utilise, et donc, par conséquent, son niveau de sécurité. Les réseaux privés, par définition, offrent une gestion plus flexible et sont plus sécuritaires que les réseaux publics puisque l'organisation est propriétaire de l'infrastructure réseau et le maîtrise totalement.

- ***Fiabilité*** : « Est-ce que ce réseau est fonctionnel en cas de désastre ? » Dans la communication pour la sécurité publique, où l'environnement doit garantir en tout temps le transfert des données, la notion de fiabilité est essentielle. l'infrastructure réseau ne doit pas être accessible au public.

- ***Coût*** : ce critère est crucial. Si le coût n'avait pas d'importance, on couvrirait entièrement un large territoire d'appareils Mesh, mais une telle idée serait prohibitive et donc, pas vraiment réaliste.

Les réseaux de données sans fil tombent habituellement dans deux catégories principales: privé ou public (ou partagé). Les réseaux dont la propriété et l'exploitation sont privées permettent aux organismes de décider des utilisateurs autorisés et sous quelles conditions. Il existe trois principaux types de réseaux de données sans fil privés :

- **Réseaux traditionnels de radiocommunication professionnelle (PMR)** — Des systèmes comme Motorola DataTAC, Dataradio G2 et Harris EDACS offrent une grande couverture et un niveau plus élevé de fiabilité et de sécurité. Cependant, leur débit est limité à environ 9,6 kb/s en raison des limitations de leur bande passante étroite. Considérées « traditionnelles », ces infrastructures ont probablement été payées au fil des ans.

- **Réseaux PMR de nouvelle génération** — Les réseaux comme Motorola ASTRO 25 HPD, Dataradio G3, et Harris OpenSky procurent un rendement supérieur à celui de leurs prédécesseurs en raison d'un débit de données plus élevé. Ils utilisent désormais le protocole IP de façon à offrir une meilleure interopérabilité avec les LAN et les autres technologies sans fil. La gestion, la couverture et la fiabilité sont excellentes, mais leur débit est toujours limité à environ 32 kb/s.

- **Réseaux privés à large bande** — Bien des organismes qui transmettent des données critiques complètent leur infrastructure sans fil avec des points d'accès WiFi (802.11a/b/g/n) leur permettant d'atteindre un débit tournant autour du mégabit, mais en ne couvrant qu'un rayon limité à environ 90 mètres (300 pieds), soit à peu près l'équivalent d'un parc de stationnement. Les réseaux Mesh sont similaires aux réseaux WiFi, mais se distinguent par leur déploiement rapide sur de plus grands territoires. Le réseau WiMAX quant à lui, offre le même débit que le WiFi mais sur des distances pouvant atteindre 16 kilomètres (10 milles), le coût devient rapidement un critère à considérer. Les réseaux de données privés LTE (*Long Term Evolution*) sont des réseaux

multimégabits ayant une meilleure couverture. Ces réseaux en sont encore à leurs premiers balbutiement mais promettent de hauts débits sur de vastes territoires, et à un coût tout aussi élevé.

Il y a une multitude de types de réseaux publics (ou partagés) couramment utilisés pour les communications critiques :

- **Réseaux cellulaires** — Ces réseaux couvrent de vastes territoires à un débit équivalant à celui des réseaux à large bande. Les coûts d'accès sont minimes puisque la seule exigence est d'obtenir une carte réseau sans fil bon marché. Aussi, la plupart du temps, il est avantageux de « louer » l'accès à un réseau public appartenant à un fournisseur que d'exploiter sa propre infrastructure privée. Cependant, le fournisseur de service peut changer les prix à tout moment. Il y a aussi le risque inhérent à l'utilisation exclusive de tels réseaux pour les communications de la sécurité publique. Les réseaux cellulaires ne font pas la différence entre des données critiques ou non. Ceci rend vulnérables les communications au moment précis ou le rendement et la fiabilité sont cruciaux notamment quand le trafic est élevé lors de catastrophes naturelles ou non. Elles sont aussi vulnérables au « syndrome de la demande élevée ». Par exemple, vers 14h, lorsque le trafic sur le réseau atteint un sommet dans les grandes villes, certains fournisseurs restreignent la bande passante ou réduisent la taille maximale des paquets de données de façon arbitraire afin de desservir un plus grand nombre d'utilisateurs. Finalement, la gestion et la sécurité des utilisateurs sont problématiques en raison de la nature partagée du réseau et de l'absence d'accès restreints pour l'obtention d'un appareil compatible.

- **Réseaux satellites** — les réseaux satellites offrent une couverture très étendue, plus particulièrement dans les régions éloignées, là où il n'existe aucune autre infrastructure réseau et où leur installation serait beaucoup trop dispendieuse. Cependant, le débit dans les communications satellite est synonyme de délais, les clients doivent se procurer des modems coûteux et le coût du « temps d'antenne » est faramineux.

- **Réseaux publics à large bande** — les réseaux WiFi à haute vitesse sont omniprésents, et on retrouve de plus en plus de réseaux WiMAX. Les réseaux LTE, la prochaine génération de réseaux de communication, en sont encore à leurs premiers balbutiements mais promettent d'être moins dispendieux que les réseaux LTE privés. Mais ici, comme avec les autres réseaux publics, il y a des problèmes de garanties offertes en matière de rendement, de fiabilité, de gestion et de sécurité comparativement aux réseaux privés. La gestion des coûts demeure entre les mains du fournisseur de service.

Il n'existe pas de solution parfaite en ce qui concerne les réseaux sans fil. Chaque technologie répond à des besoins spécifiques. Peu importe le réseau choisi, il y aura des compromis à faire (voir Illustration 2).

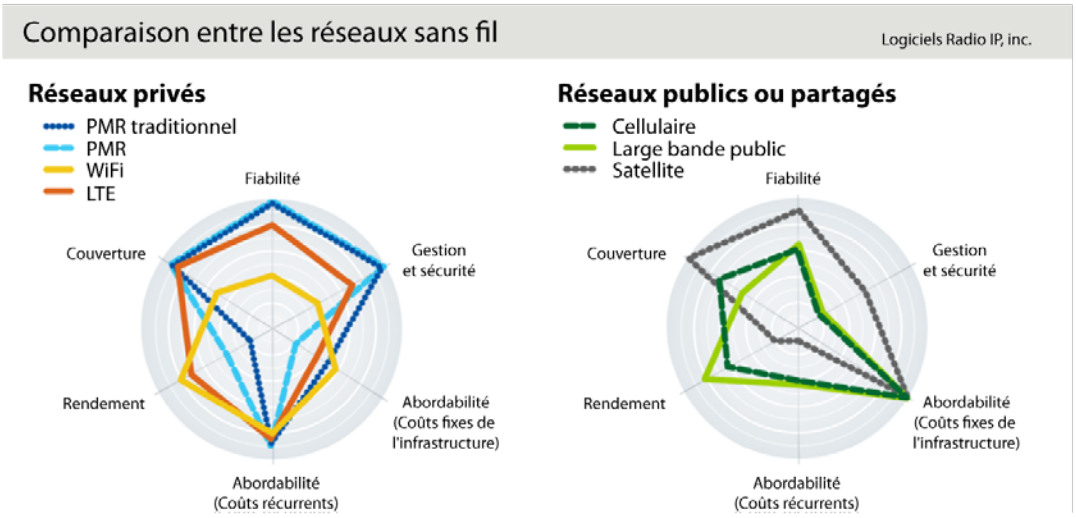

Illustration 2

Les défis de la communication de données critiques

Quand vient le temps de répondre aux besoins de communication de données critiques des utilisateurs, les administrateurs TI sont confrontés à trois défis fondamentaux :

- Premièrement, l'administrateur TI doit s'assurer que les utilisateurs ont accès à toutes les applications et à toutes les ressources nécessaires pour accomplir leur travail, et ce, sans compromettre la sécurité des appareils mobiles des utilisateurs, des données transmises et de l'infrastructure TI dans son ensemble. Ceci requiert la mise en place de mécanismes garantissant une authentification performante des utilisateurs et des appareils, un chiffrement des données solide, et potentiellement la prise de mesures protégeant des cyber-attaques.

- Deuxièmement, les réseaux doivent être gérés de façon à donner aux utilisateurs une mobilité fiable et facile à utiliser. Cela comprend une itinérance transparente entre réseaux tout en empêchant que les bris ou mises à niveau de la connectivité n'affectent en aucun cas l'intégrité de la session, ce qui obligerait l'utilisateur à s'authentifier de nouveau au retour de la connexion.

- Troisièmement, l'itinérance est une fonction importante permettant d'ouvrir tout un monde de nouvelles possibilités aux organismes quant à l'accès à une multitude de technologies réseau (IP, non IP, large bande, bande étroite, etc.). Cela se traduit, pour les utilisateurs, en une meilleure couverture et davantage de flexibilité. Les organismes, quant à eux, bénéficient d'une meilleure utilisation des ressources et une rationalisation des coûts. Ainsi, les administrateurs TI peuvent mettre en place des politiques de haut niveau concernant la priorité d'utilisation d'un réseau par rapport à un autre selon des critères tels que le coût ou la bande passante nécessaire pour une application ; par exemple, sur le réseau PMR, on pourrait donner priorité à la répartition tandis que le réseau WiFi servirait au transfert de masse de données.

L'inconvénient avec les connexions sécuritaires fixes est qu'elles ne permettent ni l'itinérance, ni la persistance de session. Sur certains réseaux, les connexions sécuritaires fixes n'optimisent pas le rendement du sans-fil lorsque nécessaire, peuvent demander la création d'applications compatibles avec un fureteur et typiquement, elles n'obligent pas l'authentification des appareils.

Les VPN mobiles (réseaux privés virtuels mobiles) permettent l'itinérance ou le changement de réseau. Le problème avec ces derniers était jusqu'à maintenant, que les utilisateurs étaient limités à l'utilisation d'un seul réseau à la fois.

La solution VPN mobile idéale n'accepte aucun compromis

Une solution VPN mobile permet aux administrateurs TI de surmonter en même temps tous ces défis tout en respectant les budgets souvent restreints qui font maintenant partie de notre économie. Les VPN mobiles maximisent la flexibilité, l'accessibilité et la sécurité. Comme la sécurité s'effectue au niveau du réseau, une gestion cohérente peut être exercée en tout temps. Les VPN mobiles livrent une solide persistance d'application et de session, ainsi qu'une simplicité et une utilisation transparente pour les utilisateurs.

Cependant, retenons que les VPN mobiles ne s'équivalent pas tous. Certains ne sont pas compatibles avec tous les réseaux. Par exemple, certains fournisseurs tenteront de convaincre les organismes de laisser tomber une infrastructure privée qui a coûté cher aux contribuables parce qu'elle n'est pas compatible avec leur solution — une situation qui va à l'encontre des intérêts des organismes de sécurité publique et de maintien de l'ordre. Les infrastructures privées, par leur nature même, offrent un haut niveau décisionnel et sont habituellement la seule ligne de communication fiable en cas de désastre.

On demande aux administrateurs TI, de toutes les manières possibles et imaginables, de faire des compromis : des concessions au niveau de la couverture et du rendement, et plus particulièrement au niveau des coûts. Les

administrateurs pourraient devoir compromettre la sécurité et la gestion de leurs réseaux par certains fournisseurs qui n'offrent pas l'interopérabilité entre tous les systèmes pouvant potentiellement être utilisés. Auparavant les utilisateurs finaux ne pouvaient transmettre de données sur plus d'un réseau à la fois. Les administrateurs TI ont besoin d'une solution de VPN mobile modulaire, permettant la redondance et facile à gérer.

Une autre situation que doivent affronter les administrateurs TI est l'utilisation d'une « solution de segmentation de tunnel », une méthode adoptée par certaines organisations pour contourner cette limitation d'accès à un seul réseau à la fois. La segmentation de tunnel permet à des applications d'éviter le VPN mobile pour se connecter directement à un serveur sans la création d'un tunnel crypté. Cette méthode représente une faille de sécurité majeure sur un réseau, car elle crée un point d'entrée non sécurisé autant sur le client mobile que sur le serveur.

La solution VPN mobile idéale doit aider les organismes transmettant des données critiques à atteindre leurs objectifs de couverture, de rendement, de fiabilité, de sécurité et de gestion, tout en optimisant le rendement du capital investi en technologie, et ce, sans compromis. La solution doit jumeler les applications les plus appropriées pour leurs besoins en couverture, rendement, fiabilité, sécurité et gestion. Ce VPN mobile doit aussi permettre aux organisations de tirer avantage du rendement de la large bande passante qu'offrent certains réseaux tout en continuant de bénéficier de la couverture, de la gestion et de la sécurité d'autres réseaux. Il faut donc créer un « réseau de réseaux ». Ainsi, les administrateurs TI n'auraient plus à recourir à la segmentation de tunnel qui atténue la sécurité du réseau. Cette solution doit aussi optimiser le débit des données sur les réseaux à bande étroite pour permettre aux administrateurs TI d'améliorer le rendement de leur infrastructure.

La solution VPN mobile idéale doit améliorer la productivité et la mobilité des utilisateurs à l'aide d'une itinérance sécuritaire et transparente, et faciliter la gestion des parcs de véhicules par les administrateurs TI. Elle doit offrir aux administrateurs TI la liberté de choisir la technologie (applications, réseaux et appareils) qu'ils désirent utiliser aujourd'hui comme demain.

Technologie de réseaux simultanés

La technologie de réseaux simultanés fut conçue comme une solution « sans compromis ». Elle permet d'utiliser une multitude de réseaux sans fil simultanément sans perdre la capacité d'itinérance transparente lors de la perte de signal d'un réseau. La technologie de réseaux simultanés permet de réunir les caractéristiques les plus intéressantes d'une multitude de réseaux pour obtenir un rendement et une fiabilité supérieure. Les administrateurs TI peuvent maintenant jumeler les applications aux technologies. Cette technologie garanti, par exemple, que les applications de données critiques, comme la répartition assistée par ordinateur (RAO), transmettront leurs données sur les réseaux les plus fiables). Les applications utilisant beaucoup de bande passante, mais nécessitant moins de sécurité et de la continuité, peuvent utiliser n'importe quel autre réseau sans fil public tel que le cellulaire ou le large bande. Mieux encore, ces applications peuvent désormais être transmises simultanément sans se nuire l'une l'autre : le flux de données vidéo, friand de bande passante, s'exécute sur les réseaux 3G ou WiFi, pendant que la répartition utilise les réseaux PMR hautement fiables tels que P25 ou TETRA.

la technologie de réseaux simultanés permet de scinder un tunnel VPN mobile en une multitude de routes virtuelles faisant appel à des profils d'itinérance(*voir illustration 3*) intelligents qui définissent la priorité des réseaux sans fil à utiliser pour établir une connexion. Une fonction avancée et unique du logiciel vérifie continuellement l'état du réseau pour garantir que le profil d'itinérance utilise constamment le réseau ayant le niveau de priorité la plus élevée pour cette route virtuelle (voir illustration 4). Elle gère donc les changements dans la couverture des réseaux pour éviter tout impact sur l'état de la connexion.

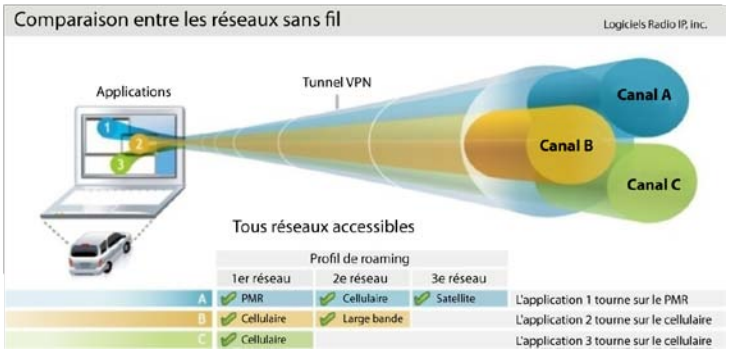

Illustration 3 – Mulitples profils de roaming

La gestion supérieure de politiques de groupes permet aux administrateurs TI de créer des groupes de clients et de leur associer des politiques. Elle permet de respecter les besoins et budgets spécifiques des organismes. Cette répartition intelligente des ressources permet à chacun des organismes de définir le réseau qui transmettra les données selon la priorité des applications, des paramètres d'exploitation ou des exigences concernant l'authentification, et ce, de façon spécifique pour chacun des groupes de l'organisme ou parmi les autres organismes.

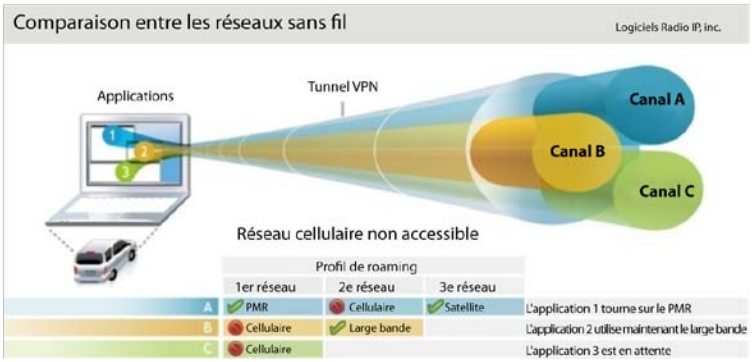

Illustration 4 – Gérer les changements dans la couverture d'un réseau

Le modèle d'échange de données de la technologie de réseaux simultanés garantit que les données de chacune des applications critiques sont transmises sur le réseau le plus adapté et que l'utilisateur accède de façon transparente à tous ces réseaux. Du point de vue de l'administrateur TI, ça représente un équilibre idéal entre la couverture, le rendement, la gestion, la fiabilité et le coût.

Conclusion

La technologie de réseaux simultanés de Logiciels Radio IP optimise le rendement et la couverture dans la communication sans fil de données critiques. À l'aide de la sélection de différents chemins réseau, la gestion et la sécurité sont améliorées dans l'ensemble du système tout en minimisant les coûts grâce à un meilleur usage de l'infrastructure existante.

Les utilisateurs bénéficient d'un accès plus étendu au réseau, et l'utilisation transparente et fiable de l'environnement mobile augmente la productivité et la mobilité des ces derniers. Pour les administrateurs TI, ceci représente une architecture de réseau critique « sans compromis » qui remplit ses promesses de manière efficace, économique et fiable.