



Réseau orienté utilisateurs d'Aruba pour le secteur de la santé

Quelle est votre vision ? Faire de votre hôpital un véritable centre d'excellence en matière de soins aux patients ? Mettre à la disposition des médecins et du personnel soignant la meilleure technologie possible afin d'optimiser l'efficacité de l'établissement ? Créer un réseau véritablement omniprésent et sécurisé, qui soit au service de tout le personnel soignant, des administrateurs et des patients, partout, sur n'importe quel dispositif et conformément à leurs besoins ?

Aruba a mis au point une nouvelle approche révolutionnaire pour vous aider à atteindre votre objectif. Les réseaux orientés utilisateurs d'Aruba intègrent des réseaux locaux sans fil adaptatifs, une sécurité basée sur l'identité et des services de continuité des applications ; tout cela au sein d'un système cohésif à hautes performances destiné aux hôpitaux, cliniques, médecins et cabinets à domicile. Il en résulte un réseau centralisé rassemblant les applications professionnelles sur le réseau local, le réseau étendu et Internet. Les utilisateurs sont donc plus productifs et la sécurité n'est pas compromise. A la différence des autres solutions, les réseaux orientés utilisateurs d'Aruba exploitent les réseaux existants afin de préserver l'investissement initial et d'éviter toute modification susceptible d'en perturber le fonctionnement.

Fonctionnalités propres à Aruba

HIPAA ET CONFIDENTIALITÉ POUR LE PATIENT

La réglementation HIPAA et les normes analogues dans d'autres pays exigent des professionnels de la santé qu'ils garantissent la confidentialité des informations propres aux patients. La sécurité basée sur l'identité d'Aruba permet le respect de la réglementation HIPAA et un accès sécurisé aux applications professionnelles partout et depuis n'importe quel périphérique. Grâce au pare-feu certifié ICSA, Aruba met en place des stratégies individuelles permettant de suivre les utilisateurs au fil de leurs déplacements au sein de l'hôpital, dans les cliniques et même jusque dans leurs consultations à domicile. De plus, avec une sécurité basée sur l'identité, les anciens dispositifs (anciens appareils VoWLAN, lecteurs de codes à barres uniquement compatibles avec le protocole WEP) sont pris en charge en toute sécurité et en toute conformité avec la réglementation HIPAA.

La réglementation HIPAA exige également la mise en place de systèmes de sécurité permettant la détection et le blocage des attaques par radio (points d'accès malveillants). Aruba intègre un système de

prévention des intrusions sans fil. Les points d'accès d'Aruba font office de contrôleurs d'ondes. Les capteurs de sécurité tiers deviennent donc superflus.

CONTINUITÉ DE SERVICE DES APPLICATIONS

Le fonctionnement en continu des applications cliniques mobiles (DME/DMI, DMP ou saisie informatique des ordonnances) est essentiel dans le secteur sanitaire. De plus, le système VoWLAN permet de joindre le personnel soignant plus efficacement qu'à l'aide de téléphones portables. Pour une prise en charge efficace des services cliniques et vocaux, le réseau doit permettre l'installation d'un système de qualité de service sans fil et câblé. Il doit aussi pouvoir prioriser les modèles de trafic afin d'en optimiser les performances.

Aruba propose des fonctionnalités pour réseaux adaptatifs sans fil permettant d'optimiser la fréquence radio pour l'accès aux applications stratégiques et sensibles à la latence, et ce, même dans les environnements les plus difficiles. Cela inclut une itinérance rapide (<10 ms) lors des transferts entre les points d'accès, une détection et correction

Avantages :

- **Connectivité mobile** : permet la mise en place d'un réseau omniprésent dans les hôpitaux, les cliniques et les cabinets médicaux
- **Sécurité mobile** : garantit la protection des données du patient et le respect de la réglementation HIPAA
- **Continuité de service des applications** : services permanents pour les aspects stratégiques du secteur sanitaire
- **Coût total de possession réduit** : plate-forme à hautes performances intégrée et dédiée au secteur sanitaire ne nécessitant pas l'installation de dispositifs supplémentaires

Solution pour le secteur de la santé

automatique des trous de couverture avec équilibrage de charges dans les zones à haute densité d'AP. La solution Aruba est parfaitement compatible avec la voix puisqu'elle exploite un pare-feu applicatif afin d'en sécuriser le flux et lui accorder la priorité le cas échéant. Le trafic vocal acquiert sa priorité grâce aux balises de qualité de service 802.1p et DSCP. Cette hiérarchisation suit les utilisateurs au fil de leurs déplacements au sein du réseau. Le système Aruba détecte automatiquement les protocoles vocaux les plus répandus (SIP, SVC et SCCP) et accorde la priorité au trafic vocal. Une priorisation supplémentaire peut être effectuée grâce au système Call Admission Control (contrôle d'admission d'appels voix, CAC). Le système CAC définit une limite pour les appels vocaux par point d'accès. En présence d'un nombre d'appels supérieur, ceux-ci sont automatiquement transférés vers les points d'accès voisins afin d'assurer une qualité optimale de la voix.

Pour garantir à ses clients davantage de fiabilité et de performances, Aruba s'est associé aux plus grands fournisseurs de systèmes destinés au secteur de la santé. Chaque application a ainsi pu être testée avant d'être proposée au client. Parmi les partenaires d'Aruba, on compte les experts en solutions de surveillance des patients Welch Allyn et Dräger Medical, SpectraLink/Polycom, Avaya, Ascom et Vocera pour les systèmes vocaux et d'appel infirmier, ainsi que les spécialistes du suivi des actifs AeroScout, Ekahau et Inner Wireless/Pango.

GESTION CENTRALISÉE

Le déploiement et la gestion d'un réseau sans fil permanent peuvent s'avérer fastidieux si ces opérations ne sont pas correctement réalisées. La gestion centralisée du réseau et des stratégies proposée par Aruba est conçue pour permettre un déploiement et un contrôle aisés.

Grâce à la gestion centralisée d'Aruba, les données de configuration sont diffusées automatiquement et en toute sécurité sur le réseau, via les points d'accès et les contrôleurs, à distance ou localement. Une seule interface est prévue pour la mise en œuvre et la protection des stratégies sous-jacentes garantissant l'intégrité, la sécurité et le fonctionnement du réseau dans son intégralité. La fonction de contrôle centralisé prend également en compte les profils de performances utilisés par les points d'accès d'Aruba en vue d'en optimiser leur fonctionnement et assurer la prise en charge des applications stratégiques. Cette approche permet la mise en place d'un réseau évolutif et accessible à un public profane.

PERFORMANCES ET ÉVOLUTIVITÉ

Le réseau local sans fil doit répondre aux exigences actuelles, mais il doit aussi permettre l'évolution et l'ajout de périphériques et d'applications mobiles. Le nombre d'utilisateurs et de périphériques, le chargement instantané des applications pendant les heures de pointe et la mobilité des utilisateurs sur les réseaux LAN, WAN ou sur Internet constituent les principaux écueils d'un tel système. Aruba Networks innove et propose une solution permettant d'automatiser la configuration RF, de décharger les serveurs AAA et de faire évoluer les VLAN afin de faire face à une utilisation évolutive. De plus, Aruba propose des plates-formes puissantes, évolutives et dédiées offrant un débit tel qu'il permet d'exploiter réellement les applications existantes, l'infrastructure informatique et les clients standard en place. Conçus pour répondre aux exigences des clients d'aujourd'hui et de demain, la plupart des produits Aruba exploitent une structure logicielle modulaire et évolutive pouvant être améliorée au fil du temps selon la mise à disposition de nouvelles fonctions.

Solution Aruba Networks pour le secteur de la santé

La solution Aruba se compose de quelques éléments essentiels (les points d'accès légers, les contrôleurs de mobilité centraux et leurs modules logiciels), auxquels viennent s'ajouter certains composants facultatifs comme un système d'analyse de gestion et des dispositifs de prévention des menaces. Les points d'accès assurent une connectivité sans fil sécurisée aux périphériques et se connectent sur des systèmes de réseaux LAN/WAN existants de manière à prendre en charge l'ensemble du trafic du réseau local sans fil (via un tunnel GRE ou IPsec) vers un contrôleur de mobilité installé dans le centre de données. La configuration, la gestion, la continuité de service

des applications et la sécurité sont centralisés sur le contrôleur de mobilité. Grâce aux modules de sécurité pour les contrôleurs de mobilité, Aruba apporte la sécurité nécessaire et garantit le respect des normes.

Vous trouverez ci-dessous la présentation d'un réseau sans fil destiné au secteur de la santé, en présence de services informatiques centralisés :

Centre de données : au moins un contrôleur de mobilité est installé dans le centre de données. Il peut être utilisé comme point de configuration et de gestion pour tout le réseau. Ces contrôleurs peuvent également

servir de terminaisons pour les points d'accès permettant la liaison sans fil au sein du pôle hospitalier et les points d'accès distants exploités par les télétravailleurs et cabinets a domicile. Le contrôleur principal prend en charge jusqu'à 500 contrôleurs distants. Il peut également prendre le relais d'un contrôleur installé sur un site distant en cas de panne. Dans le cas des déploiements de plus grande envergure, plusieurs contrôleurs principaux peuvent se répartir la gestion des contrôleurs locaux et des points d'accès sur les sites distants. Le système de gestion de la mobilité (Airwave) peut être utilisé comme interface de gestion et de configuration.

CHU/centres médicaux/grandes cliniques : un contrôleur de mobilité Aruba (contrôleur local) différent est installé selon le nombre de points d'accès pris en charge varie (de 4 a 512 points d'accès). Chaque contrôleur local obtient sa configuration du contrôleur principal. La continuité de service des applications et les niveaux de sécurité sont assurés au niveau de l'utilisateur par le contrôleur local. Différents profils sont affectés en fonction de stratégies de groupes définies dans le système d'identification. Il est également possible de rediriger les invités vers la zone démilitarisée. Les contrôleurs

locaux offrent également un système de protection sans fil contre les intrusions. Le cas échéant, l'activation des services d'identification et/ou des requêtes d'accès direct au centre de données est possible. Chaque contrôleur local calibre automatiquement la couverture RF afin d'optimiser les performances et d'éviter les trous de couverture. De plus, pour permettre une couverture sans fil dans les zones où le câblage s'avérerait trop difficile ou trop coûteux, les points d'accès Aruba peuvent assurer la liaison par Wi-Fi grâce au réseau maillé d'entreprise sécurisé (MESH).

Cabinets médicaux et a domicile : des points d'accès distants autonomes (Remote AP) constituent une solution efficace pour assurer une liaison sécurisée et une gestion centralisée des sites ne nécessitant qu'un ou deux points d'accès. Ces derniers peuvent être directement connectés par Ethernet à un réseau Internet public/privé ou au réseau LAN. Les points d'accès distants détectent automatiquement le contrôleur principal. Ils établissent un tunnel VPN sécurisé vers le centre de données et élargissent la liaison sans fil à l'utilisateur. Le trafic des applications peut être acheminé vers le centre de données ou localement.

