



Réseau orienté utilisateurs d'Aruba pour l'éducation

Quelle est votre vision ? Faire de la technologie un élément central de votre campus ? Rassembler les services de communication disparates en un seul et même réseau ? Créer un réseau mobile véritablement omniprésent et sécurisé, qui soit au service de tous les étudiants, administrateurs et membres des facultés, 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 utilisateur d'Aruba intègrent des WLAN 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 à l'enseignement supérieur. On obtient ainsi une solution avec une gestion centralisée, conçue pour offrir la vitesse des réseaux câblés et la polyvalence des réseaux sans fil, tout en conservant une sécurité maximale et un coût total de possession réduit.

Fonctionnalités propres à Aruba

Aruba propose des innovations de pointe en matière de mobilité sur les campus. Les systèmes peuvent d'ailleurs être mis en œuvre de sorte à venir compléter le réseau existant.

802.11N ADAPTATIF

Les produits 802.11n à hautes performances d'Aruba garantissent la mise en œuvre d'un campus sans fil intégral. Aruba propose une solution adaptative s'intégrant facilement aux infrastructures existantes, tout en évoluant afin de répondre à une demande croissante des utilisateurs dans le domaine universitaire. Grâce à un système 3x3 entrée multiple, sortie multiple (MIMO), une conception permettant une mise à niveau rapide sur le terrain et le respect de la norme 802.3af Power-over-Ethernet (POE), les points d'accès 802.11n d'Aruba peuvent être utilisés pour l'accès sans fil, la détection des intrusions, l'analyse du trafic, la maille d'entreprise sécurisée ou les applications exploitant les points d'accès distants. Le mode de fonctionnement est fixé par un logiciel pouvant être téléchargé sur le réseau. Cet élément permet la réaffectation et la mise à jour des points d'accès sans aucune manipulation physique du périphérique.

UNE APPROCHE À L'ÉPREUVE DU TEMPS

L'architecture Aruba pose les bases de l'avenir des applications réseau. Les

puces au silicium reprogrammables qui la composent garantissent de grandes performances et une mise à jour conviviale. La plupart des écoles commencent par adopter un réseau sans fil basique et lui ajoutent des fonctions au fur et à mesure : protection sans fil contre les intrusions, voix sur Wi-Fi pour la maintenance et la sécurité publique, renforcement par réseau maillé sans fil de la fibre optique ou localisation du matériel prêt aux étudiants sur le campus. Grâce à Aruba, ces ajouts sont réalisés à l'aide d'une simple mise à jour du logiciel : plus besoin de travailler sur tout le réseau. Les mises à jour standard, tels les types de chiffrement et d'identification, s'effectuent facilement sans causer de perturbations sur le réseau.

SÉCURITÉ BASÉE SUR L'IDENTITÉ

En raison des déplacements des étudiants et du personnel enseignant sur le campus, il est essentiel de leur garantir l'accès à leurs ressources réseau dédiées, en y imposant toutefois quelques restrictions. Les méthodes de contrôle d'accès traditionnelles reposent sur le point d'entrée, ce qui est contraire à l'essence même des WLAN et de la mobilité. Le contrôle d'accès doit désormais prendre en compte l'identité de l'utilisateur, son rôle, le type de périphérique utilisé, son emplacement, l'heure ainsi que

Avantages :

- **802.11n adaptatif** : déployez la norme 802.11n selon vos besoins et laissez le réseau s'ajuster automatiquement
- **À l'épreuve du temps** : les mises à niveau permettent la prise en charge des futures applications
- **Sécurité basée sur l'identité** : les systèmes de sécurité suivent les utilisateurs tandis qu'ils se déplacent d'un endroit à l'autre du campus ou ailleurs
- **Compatibilité avec les applications** : système optimisé pour la prise en charge sans fil des données, de la voix et de la vidéo sur un réseau convergent
- **Gestion centralisée** : configuration, surveillance et dépannage aisés grâce au contrôle centralisé

tout élément personnel ou technique important. La mobilité doit devenir partie intégrante de l'infrastructure AAA (ex. : RADIUS, LDAP ou Active Directory). Seule l'architecture proposée par Aruba Networks répond à ces critères. A la différence des autres systèmes qui associent les stratégies à des SSID/VLAN spécifiques en vue de sécuriser et segmenter un réseau, Aruba met en œuvre un pare-feu dynamique à même d'associer des règles de sécurité propres à des rôles et utilisateurs distincts. La stratégie est liée à l'utilisateur. Elle s'applique donc où qu'il se trouve.

CONTINUITÉ DE SERVICE DES APPLICATIONS

Les universités et les écoles peuvent offrir une véritable valeur ajoutée à leur investissement Wi-Fi en exploitant cette architecture pour d'autres systèmes du campus : voix, vidéo, systèmes de surveillance et commandes des bâtiments. Le recours à un système unique et sécurisé permet de réaliser d'importantes économies. Grâce à sa compatibilité avec les applications, le système Aruba permet une parfaite convergence. Il assure la sécurité et la gestion du trafic en fonction du type d'application, du périphérique et de l'utilisateur. Les fonctions d'Aruba permettent aux universités d'exploiter les avantages de la convergence IP, et de rassembler les systèmes complexes et disparates en une seule infrastructure.

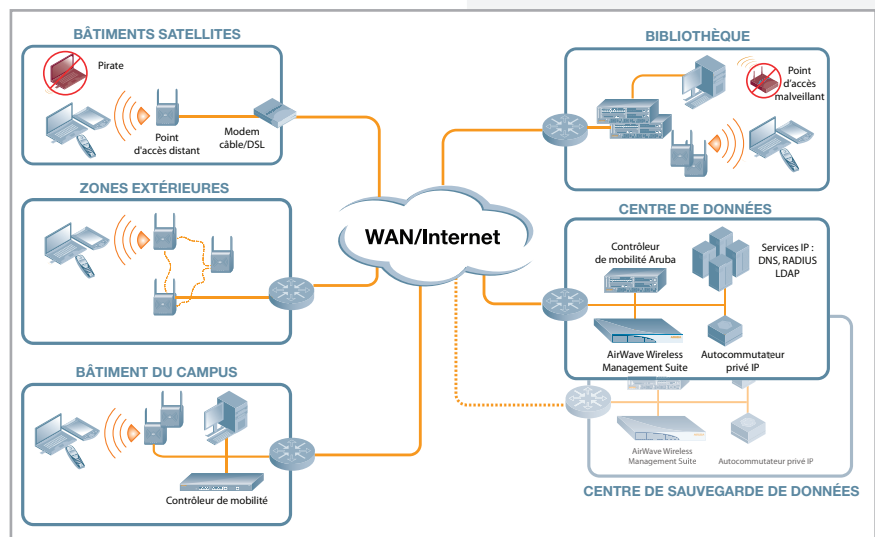
GESTION ET CONTRÔLE CENTRALISÉS

L'architecture réseau centralisée d'Aruba permet la surveillance, le contrôle et le dépannage du réseau à partir d'un même point, que le réseau s'étende sur un campus ou sur un continent entier. Pour les universités scindées en plusieurs pôles, les tâches peuvent être réparties entre les responsables informatiques des différentes institutions. Aruba propose une fonction « administrateur des administrateurs » permettant de répartir logiquement les informations selon la hiérarchie des administrateurs. L'infrastructure d'Aruba permet une capture des paquets à distance de sorte que les responsables informatiques n'aient pas à traverser le campus ou se rendre sur un autre site pour effectuer le dépannage. De plus, Aruba offre une vue complète en temps réel de l'environnement RF de chaque bâtiment composant le réseau du campus. L'administrateur réseau peut effectuer toutes les opérations de maintenance et les mises à niveau à partir d'un seul et même lieu. Il sera par ailleurs averti en cas d'intrusion ou d'événement de sécurité dès leur apparition.

Solution Aruba pour le secteur de l'éducation

La solution Aruba se compose de trois éléments essentiels (les points d'accès légers, les contrôleurs de mobilité centraux et les modules logiciels), auxquels s'ajoute un composant facultatif : l'AirWave Wireless Management Suite d'Aruba. Les points d'accès assurent une connectivité sans fil sécurisée aux périphériques. Ils se connectent sur des systèmes de réseaux LAN/WAN existants de manière à prendre en charge l'ensemble du trafic du réseau LAN sans fil (via un tunnel GRE ou un tunnel IPsec) vers un contrôleur de mobilité installé dans le centre de données ou dans un bâtiment local selon les exigences du flux. La configuration, la gestion, la continuité de service des applications et la sécurité sont centralisées sur le contrôleur de mobilité. Grâce aux modules logiciels pour les contrôleurs de mobilité, Aruba permet le déploiement d'une solution adaptée aux besoins actuels tout en autorisant l'ajout d'éléments complémentaires en cas de besoin.

Vous trouverez ci-dessous la présentation d'un réseau sans fil destiné aux campus disposant de services informatiques centralisés :



Centre de données : selon le nombre de sites distants et de points d'accès, un ou plusieurs contrôleurs de mobilité sont intégrés au centre de données. Ces contrôleurs peuvent également servir de terminaisons pour les points d'accès permettant la liaison sans fil au sein du bâtiment qui héberge le centre de données et les points d'accès installés dans les bureaux distants ou pour le télétravail. Le contrôleur principal peut prendre en charge jusqu'à 500 contrôleurs distants. Il est la seule interface exploitée pour la configuration et la gestion. Le contrôleur principal 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 peut être utilisé comme interface de gestion et de configuration.

Bâtiments du campus : un contrôleur de mobilité Aruba (contrôleur local) différent est installé selon le nombre de points d'accès requis sur chaque site. Tous les modèles de contrôleur Aruba exploitent le même logiciel et disposent des mêmes fonctions. Seul le nombre de points d'accès pris en charge varie (de 6 à 2 048 points d'accès). Chaque contrôleur local obtient sa configuration du contrôleur principal. La continuité des applications et les niveaux de sécurité PCI sont assurés au niveau de l'utilisateur par le contrôleur local. 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'en 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).

Zones extérieures : la plupart des points d'accès Aruba peuvent être déployés à l'extérieur, dans des zones couvertes. Ils pourront ainsi notamment être exploités par les vendeurs autour des stades, les caméras de surveillance, les cabines téléphoniques destinées aux appels d'urgence ou simplement par les étudiants souhaitant travailler à l'extérieur. Pour les endroits plus exposés, Aruba propose des points d'accès plus robustes. Au cas où le réseau Ethernet n'aurait pas été élargi aux zones extérieures, le point d'accès Aruba pourra établir une liaison avec un autre point d'accès Aruba relié au réseau et permettant un maillage (MESH). Le point d'accès agira toujours tel un point d'accès léger standard. Il sera en liaison avec le contrôleur grâce à au moins un autre point d'accès qui fera office de saut de réseau maillé.

Utilisateurs distants et bureaux temporaires : les points d'accès distants constituent une solution efficace pour assurer une liaison sécurisée et une gestion centralisée des sites ne nécessitant que quelques 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 plusieurs utilisateurs distants. Le trafic des applications peut être acheminé vers le centre de données ou localement. Dans les cas où davantage de points d'accès sont nécessaires sur le site distant, ils pourront être reliés à une source d'alimentation afin d'établir une liaison vers le point d'accès distant rattaché au réseau. L'installation sans fil peut donc s'effectuer rapidement, sans câblage Ethernet local ni ressources informatiques.



WWW.ARUBANETWORKS.COM

1344 Crossman Avenue. Sunnyvale, CA 94089 | Tél. +1 408.227.4500 | Fax. +1 408.227.4550