

JANVIER 2005

Du changement dans l'air

Fort impact de la communication sans fil sur l'architecture et la sécurité des réseaux

Retour vers le Futur

Pour bien appréhender la fonction d'un commutateur WLAN (Wireless LAN) dans un réseau sans fil, il est nécessaire de comprendre l'évolution des LANs filaires.

Dans les premiers LANs, la performance était le problème majeur. Malgré le développement des ponts et des commutateurs, l'adoption générale de LANs dans les entreprises n'a pas eu lieu.

D'autres développements tels que : câblage UTP structuré, commutateurs Ethernet, VLANs, management basé sur SNMP, management in-band et out-of-band, commutation niveau 3, réduction du coût par port – ont permis l'adoption étendue des LANs en milieu d'entreprise.

En d'autres termes, l'adoption des LANs avec fil ne s'est pas généralisée avant l'existence d'un ensemble d'éléments, apparemment sans rapport direct avec le transport de données sur le réseau, permettant de faciliter l'entrée dans le réseau.

En parallèle aux LANs avec fil, les WLANs entrent actuellement dans une phase de forte croissance à un rythme beaucoup plus rapide. Les analystes de l'industrie et les observateurs du marché s'accordent sur la généralisation des WLANs dans les entreprises au cours des prochaines années. Malgré les divergences des experts sur les étapes de cette évolution, ils sont d'accord sur deux facteurs :

1. L'adoption des WLANs interviendra plus rapidement que celle des LANs avec fil.
2. L'écosystème permettant une adoption rapide est prêt

Les premiers LANs sans fil

Dès leur apparition il y a quelques années, les LANs sans fil étaient confrontés aux mêmes obstacles que les LANs filaires, tels que la complexité de leur management et les coûts élevés de déploiement.

Le management des WLANs était complexe en raison de leur déploiement comme des extensions de LANs avec fil sous forme de points d'accès (APs) qui fonctionnaient en nœuds (nodes) IP indépendants du réseau. L'augmentation du nombre de nœuds gérables et la configuration manuelle des paramètres accentuant cette complexité.

En raison du coût élevé des APs, l'objectif des premiers déploiements était d'étendre la couverture avec moins d'APs. Pour cela, il fallait contrôler, avant déploiement, l'environnement de la fréquence radio (RF) du site et déployer les APs dans des espaces nécessitant plus de câblage structuré et de capacité d'alimentation.

De plus, deux problèmes particulièrement importants et spécifiques aux WLANs étaient la sécurité et la mobilité : l'air étant par définition un media non sécurisé et qui peut être exposé à tout nouveau type d'attaque. Les utilisateurs sans fil qui se déplacent dans le réseau conservent leurs privilèges et leurs contrôles d'accès, de sorte que la localisation et l'élimination de ces attaques sont très différentes par rapport aux environnements des LANs avec fil.

Des caractéristiques spécifiques accélèrent l'adoption des WLANs.

Très tôt il était évident que, pour assurer l'adoption générale des WLANs, il était nécessaire de disposer d'un ensemble d'éléments spécifiques centrés sur :

1. un coût moins élevé de déploiement
2. un management des réseaux plus facile
3. la sécurité

Il était également évident que, dans un environnement WLAN, une plateforme était nécessaire comme point de distribution de services pour faciliter le déploiement, le management et la sécurité. Par conséquent, le besoin était de créer et d'installer un écosystème WLAN permettant l'adoption généralisée de cette technologie dans les entreprises. D'où l'apparition du commutateur sans fil LAN.

Un commutateur WLAN est un dispositif centralisé dans un réseau, situé généralement au centre de données, auquel tous les APs sans fil sont connectés directement ou indirectement, en niveau 2/3. En raison de son emplacement centralisé et de son intelligence, le commutateur WLAN est complètement en phase avec l'environnement WLAN de l'entreprise. Il assure tous les services essentiels pour réduire les coûts, simplifier le management, et fournir les niveaux multiples de sécurité.

Réduction du coût de déploiement

Les facteurs entraînant tout particulièrement des coûts élevés de déploiement sont les études de site avant installation, la pose de nouveaux câbles et l'alimentation des APs ainsi que la reconfiguration de l'infrastructure réseaux existant.

La génération actuelle des commutateurs WLAN élimine par un logiciel de management RF intelligent les contrôles de site. Les commutateurs WLAN fournissent une alimentation normalisée à l'ETHERNET (IEEE 802.3af), évitant ainsi le besoin d'assurer l'alimentation à chaque point d'accès. Après déploiement, les APs sont automatiquement configurés par le commutateur WLAN qui fixe le niveau d'alimentation et les réglages des canaux afin d'optimiser les performances et la couverture de tout le système.

Le facteur d'innovation le plus important dans la réduction des coûts de déploiement vient sans doute de l'installation des APs dans l'espace utilisateur (sous le bureau ou intégration dans la prise murale LAN sans fil au lieu du plafond). L'approche la plus répandue, connue généralement sous l'appellation «architecture de maillage (grid)» permet la distribution dynamique de services sur le réseau IP existant sans changements physiques dans l'infrastructure existante. Basés sur l'architecture grid, ces nouveaux APs fournissent des services radio avec tous les autres services déployés au commutateur WLAN. Des APs légères, dispersés de façon très dense, assurent une connectivité haute performance avec une meilleure couverture.

Simplification par centralisation du management sans fil

Les caractéristiques d'auto-configuration et d'auto-réparation des réseaux sans fil facilite le management et la détection d'anomalies (troubleshooting). Le management réseaux est également facilité par la localisation précise de chaque utilisateur et la connaissance de toutes les caractéristiques de l'utilisateur et de l'AP telles que la localisation, l'adresse MAC (BSSID), le canal, le type radio, le fabricant, l'état actuel (status) sur le réseau et le nom du réseau.

Le commutateur WLAN centralisé intégrant les caractéristiques RF dans toute l'entreprise, il est facile de détecter des interférences entre les APs voisins et de reconfigurer automatiquement leur puissance et les réglages des canaux. Selon le même principe, au cas où le commutateur détecte un trou de couverture causé par la panne d'un AP, il envoie aux APs voisins une instruction qui augmente les puissances d'émission pour combler la perte.

Unification de sécurité avec fil et sans fil

Beaucoup ayant été écrit sur la sécurité WLAN, il n'est question ici que de signaler les facteurs essentiels permettant l'adoption rapide dans l'entreprise :

- | | |
|---------------------|---------------------------------|
| a) Authentification | d) Politique/Règles de sécurité |
| b) Autorisation | e) Sécurité RF |
| c) Chiffrement | |

Les WLANs doivent assurer l'authentification des employés, utilisateurs approuvés et contractants utilisant une variété de méthodes d'authentification telles que 802.1x, portail captif et VPN. Les utilisateurs de réseaux sans fil ne peuvent pas être traités comme les utilisateurs avec fil. Le contrôle d'accès d'utilisateurs sans fil privilégie l'emploi de certains critères déterminants comme la localisation, la méthode d'authentification, l'heure, le type d'installation afin de maintenir le niveau de sécurité par des modes d'accès différenciés.

Les WLANs doivent incorporer les meilleures techniques disponibles pour maintenir la sécurité sur l'ensemble des réseaux, c'est-à-dire, la sécurité ne doit pas limiter le chiffrement au niveau de l'AP, mais elle doit assurer l'isolation totale du trafic WLAN jusqu'à son passage du firewall au commutateur WLAN.

L'intégration d'un firewall et d'un VPN dans le WLAN permet de sécuriser chaque flot de trafic individuellement pour un coût nettement inférieur que par le déploiement de points de passage (gateways) VPN externes.

Les commutateurs les plus avancés comprennent un IDS sans fil à signature pour détecter toute la gamme d'attaques RF connues et également l'intelligence pour détecter des anomalies de fonctionnement dans le cas d'attaques d'origine inconnue. Enfin, la capacité à détecter et à éliminer des APs non-autorisés (« Aps voyous ») et à éradiquer toute connectivité sans fil du réseau non-autorisée constitue un atout majeur de la sécurité WLAN. Le repérage précis d'un « AP voyou » ou d'un AP d'interférence (par ex. un AP voisin) avec sa localisation précise est une dimension essentielle de la sécurité RF totale.

En fait, les commutateurs WLAN permettent maintenant aux entreprises de littéralement « bloquer l'air ».

Résumé

Il y a des parallèles entre le marché des LANs et des WLANs. Ce n'est que depuis le développement de caractéristiques apparemment non liées au transport de données sur des réseaux avec fil - donc complètement développé et prêt à l'emploi - que les LANs avec fil ont investi l'entreprise.

Les WLANs présentent aujourd'hui un ensemble de caractéristiques ad hoc nécessaires pour permettre leur véritable adoption dans les entreprises. La prochaine génération de commutateurs WLAN offriront la plateforme pour la distribution sécurisée de ces caractéristiques essentielles.

Devant la prolifération des installations clients avec Wi-Fi intégré, l'élimination des risques de sécurité des réseaux par la suppression de toutes connexions sans fil non-autorisées est l'une des raisons principales pour le déploiement des WLANs. D'autres avantages des WLANs comprennent l'amélioration de performance de trafic, la réduction importante des adaptations complémentaires chez le client et la diminution du nombre de ports réseaux physiques par employé, qui sont aussi des facteurs déterminants des WLANs. Les WLANs permettent également le déploiement VoIP en Wi-Fi dans l'entreprise, ce qui offre une meilleure couverture et une plus grande sécurité à un coût inférieur à celui de la voix mobile cellulaire. Malgré le niveau d'acceptation des commutateurs WLAN, ils n'offrent pas tous les mêmes critères d'égalité. Les commutateurs WLAN qui assurent le contrôle centralisé complet, les garanties de sécurité totale et la gamme complète des critères de performance optimisée permettent aujourd'hui le déploiement généralisé et l'adoption des réseaux sans fil partout dans l'entreprise, où les utilisateurs sont dorénavant dispensés d'opérations manuelles tout en étant bien connectés.

###



120, avenue Charles de Gaulle | Neuilly sur Seine Cedex | 92522
tel +1 72 92 05 56 | fax +1 71 92 05 57

www.arubanetworks.com