Architecture Cisco SWAN :

la nécessité d'intégrer les réseaux sans fil aux réseaux filaires

Le succès des réseaux locaux sans fil (WLAN) place les administrateurs de réseaux devant de nouveaux défis : ils doivent répondre à la demande croissante en WLAN d'entreprise provenant des utilisateurs finaux enthousiasmés par la liberté et la souplesse de la connectivité sans fil, comme des dirigeants convaincus de l'avantage compétitif que confère à leur organisation la mobilité des applications vitales pour leur activité.

L'entreprise ne peut plus se permettre d'ajourner le déploiement des WLAN, car, en l'absence de réseaux sans fil autorisés, ses collaborateurs risquent de les créer eux-mêmes en établissant des points d'accès « illégaux », c'est à dire non-autorisés. Ces points d'accès illégaux sont autant de faiblesses de sécurité qui mettent en danger l'intégrité du réseau tout entier. Pour réduire le risque des déploiements illégaux qui exposent le réseau filaire aux intrusions, l'administrateur réseau doit installer des WLAN d'entreprise autorisés qui lui permettront d'exercer le contrôle indispensable sur ses infrastructures filaires et sans fil, et d'assurer la bonne protection de son réseau.

Les administrateurs de réseaux doivent également intégrer les WLAN aux réseaux filaires existants et dimensionner les réseaux sans fil pour qu'ils prennent en charge des centaines, voire des milliers d'utilisateurs installés sur le campus comme dans des sites distants répartis sur des zones géographiques considérables. Ils doivent également fournir un support de haute disponibilité capable de répondre aux attentes de ces utilisateurs habitués aux performances des réseaux filaires. Alors que ses budgets se resserrent, l'entreprise exige de l'administrateur réseau qu'il livre en tout lieu des applications informatiques mobiles de qualité entreprise sans sacrifier ni la sécurité, ni la mobilité, ni le contrôle du réseau, tout en garantissant le coût d'acquisition total le plus bas possible. En matière de WLAN, la bonne solution doit exploiter au maximum tout ce qui peut exister en matière d'outils, de connaissances, de ressources et d'infrastructure filaire pour régler les problèmes vitaux de sécurité, de déploiement et de contrôle des réseaux locaux sans fil.

Cisco Structured Wireless-Aware Network

L'architecture Cisco® SWAN (Structured Wireless-Aware Réseau) est la solution idéale pour les administrateurs réseaux qui doivent déployer, exploiter et gérer des centaines, voire des milliers de points d'accès dans le cadre d'un déploiement WLAN aussi bien dans le campus que dans les succursales d'entreprise, les grands centres commerciaux, les installations de fabrication ou les centres de soins de santé. Cet ensemble offre aux organisations de taille moyenne et aux grandes organisations des niveaux de sécurité, d'évolutivité, de fiabilité, de facilité de déploiement et de gestion identiques à ceux auxquels les réseaux LAN filaires les ont habituées.

Disponible à partir du dernier trimestre 2003, l'architecture Cisco SWAN réunit huit grandes composantes :

- la plate-forme IOS Cisco®
- des points d'accès WLAN de la gamme Cisco Aironet
- des cartes clients WLAN de la gamme Cisco Aironet
- des cartes clients compatibles Cisco
- un CiscoWorks WLSE 2.x
- la solution Cisco Wireless Security Suite
- le serveur ACS (Access Control Server) Cisco Secure 3.2
- les produits de commutation et de routage pour réseaux LAN supportant le sans fil (wireless-aware) Cisco (disponibles à partir de 2004)

L'intégration de ces produits et de ces technologies, déjà récompensés, forme une solution hautement évolutive, sécurisée et facile à gérer qui simplifie le déploiement et l'administration des WLAN et maximise les temps de fonctionnement des réseaux sans fil. L'ensemble fournit :

- l'intégration des services de réseau LAN filaires et sans fil grâce à l'infrastructure Cisco et à la plate-forme Cisco IOS,
- la gestion simplifiée de centaines, voire de milliers de points d'accès centraux ou à distance,
- WDS (Wireless Domain Services) pour le service d'authentification local IEEE (Institute of Electrical and Electronics Engineers Inc) 802.1X et la prise en charge du Fast Secure Roaming,
- la détection et la localisation des points d'accès illégaux,
- le balayage et le contrôle des fréquences radio,
- la détection des interférences afin d'isoler et de localiser les interférences réseau,
- des processus simplifiés de déploiement de WLAN avec assistance à l'analyse de site,
- l'assistance à la rationalisation de la gestion et de l'exploitation de réseaux WLAN,
- des outils améliorés de dépannage et de diagnostic pour des performances proactives et le suivi des défaillances,
- une disponibilité élevée grâce à des réseaux locaux sans fil à restauration automatique,

- le suivi des politiques de sécurité,
- la fourniture en continu de solutions améliorées de sécurité réseau.

Intégration des services de LAN et Wireless LAN grâce à l'infrastructure Cisco et au Cisco IOS

L'architecture Cisco SWAN (Structured Wireless-Aware Network) intègre les services de réseau WLAN qui deviennent ainsi une véritable extension du réseau filaire Cisco. L'ensemble utilise les fonctions classiques de gestion des commutateurs et des routeurs de la plate-forme Cisco IOS en intégrant la gestion des points d'accès Cisco et des cartes clientes. La fourniture de bout en bout des services de réseau WLAN – détection des points d'accès illégaux, mobilité, qualité de service (QoS), administration de réseau, etc. – est dès à présent disponible pour les points d'accès et les cartes clientes, et le sera dès 2004 sur certains commutateurs et routeurs LAN Cisco.

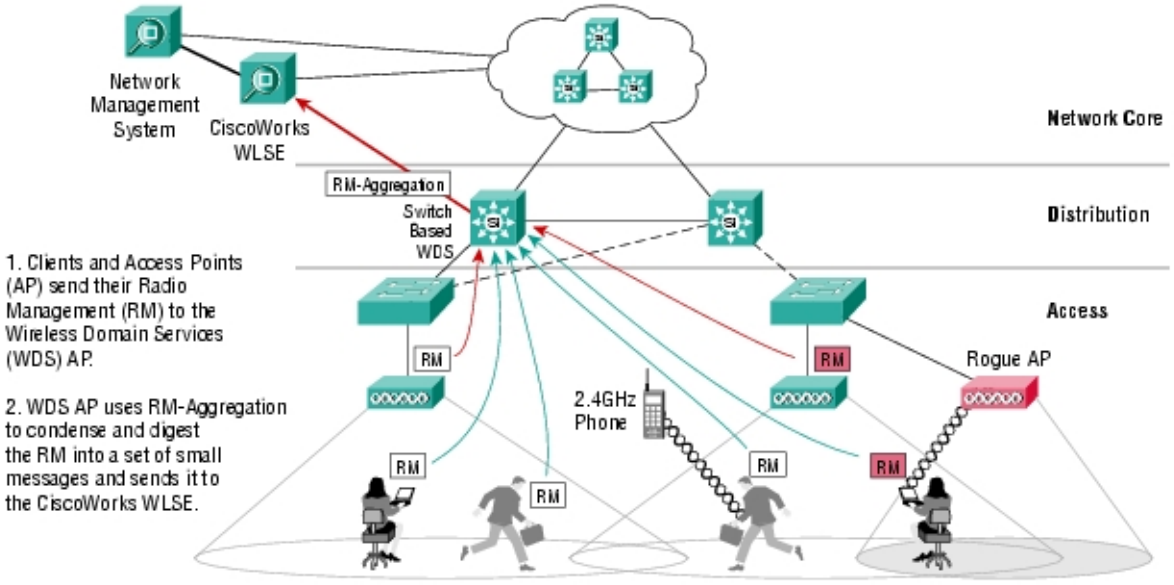
L'architecture Cisco SWAN renforce l'intégration des réseaux filaires et sans fil afin de simplifier la gestion et le contrôle des WLAN tout en dotant les produits d'infrastructure Cisco de fonctionnalités sans fil. Ces fonctionnalités seront dans un premier temps introduites sur les points d'accès de la gamme Cisco Aironet, les cartes client WLAN Cisco Aironet et les cartes clients compatibles Cisco. Dès 2004, elles deviendront disponibles sur certains commutateurs et routeurs LAN Cisco. Grâce à ce nouvel ensemble, les professionnels des technologies de l'information pourront déployer un réseau sans fil sans avoir à insérer de nouveaux éléments dans leurs locaux techniques.

L'ensemble de l'architecture Cisco SWAN exploite CiscoWorks WLSE (Wireless LAN Solution Engine) 2.x, une plate-forme d'administration clé en mains, évolutive et centralisée pour les réseaux sans fil qui permet aux entreprises de taille moyenne comme aux grandes sociétés de gérer des centaines, voire des milliers de points d'accès Cisco Aironet dans leurs déploiements de campus, verticaux ou de succursales. Son interface-utilisateur WEB/HTML légère et conviviale autorise la gestion et l'exploitation de l'ensemble de l'infrastructure sans fil Cisco Aironet.

WDS (Wireless Domain Services)

L'architecture Cisco SWAN fait appel à de nouveaux services appelés WDS (Wireless domain services). WDS regroupe des fonctions de la plate-forme Cisco IOS qui améliorent la mobilité des clients WLAN et simplifient le déploiement et la gestion des WLAN. Ils comprennent l'agrégation des mesures des fréquences radio (Figure 1).

Figure 1 Wireless Domain Services

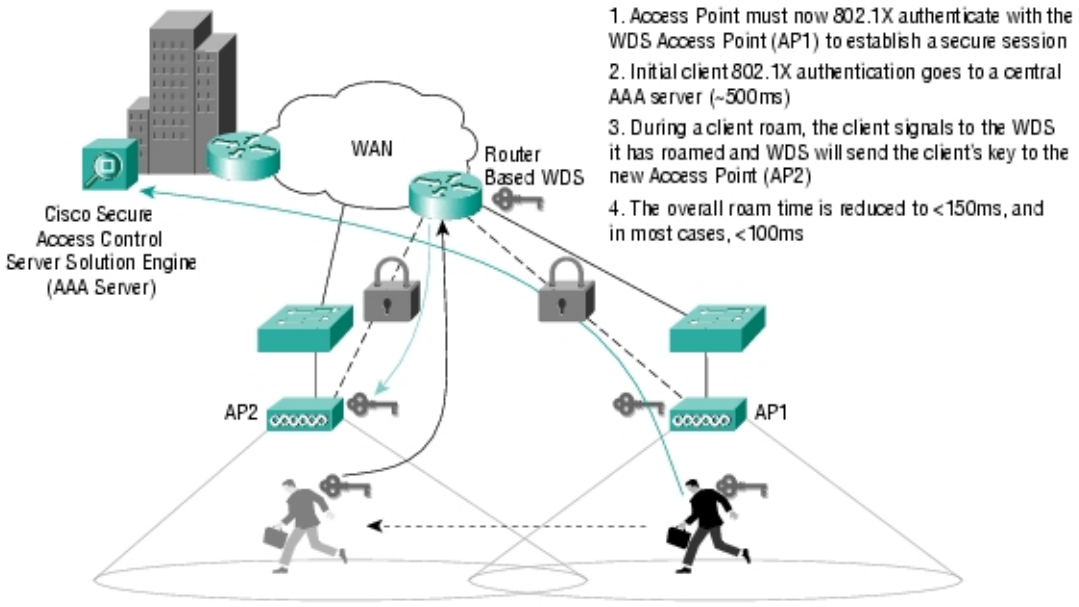


Tous les points d'accès d'un sous-réseau détectent et s'enregistrent de manière sécurisée – grâce au protocole IEEE 802.1X – auprès du WDS. Le WDS groupe les mesures RF des clients et des points d'accès à l'intention des services d'audit radio comme la détection des points d'accès illégaux, la détection des interférences (illustrée par le téléphone WiFi 2,4 GHz de la Figure 1), et l'assistance à l'analyse de site. L'ensemble des fonctionnalités WDS actuellement pris en charge comprend Fast Secure Roaming et l'authentification locale par le protocole IEEE 802.1X. Les futures versions logicielles offriront de nouvelles fonctionnalités WDS.

Fast Secure Roaming

Fast secure roaming permet aux cartes clientes authentifiées de transiter en toute sécurité d'un point d'accès à un autre sans délai perceptible au cours de la réassociation (Figure 2). Fast secure roaming prend en charge les applications sensibles aux temps de latence comme le VoIP (Voix sur IP) sans fil, les progiciels de gestion intégrés (PGI) ou les solutions sous Citrix, sans perte de connexion en cours de déplacement. Le WDS offre des services de transfert rapide et sécurisé vers les points d'accès avec un temps de latence des services itinérants inférieur à 150 ms au sein d'un même sous-réseau. Fast secure roaming de Cisco exige des cartes clientes Cisco ou compatibles qui supportent le protocole CCKM (Cisco Centralized Key Management) de gestion centralisé des clés.

Figure 2 Fast secure roaming



Note: Because the WDS handles roaming and reauthentication, the WAN link is not used

Fast Secure Roaming d'un sous-réseau à l'autre – mobilité de couche 3

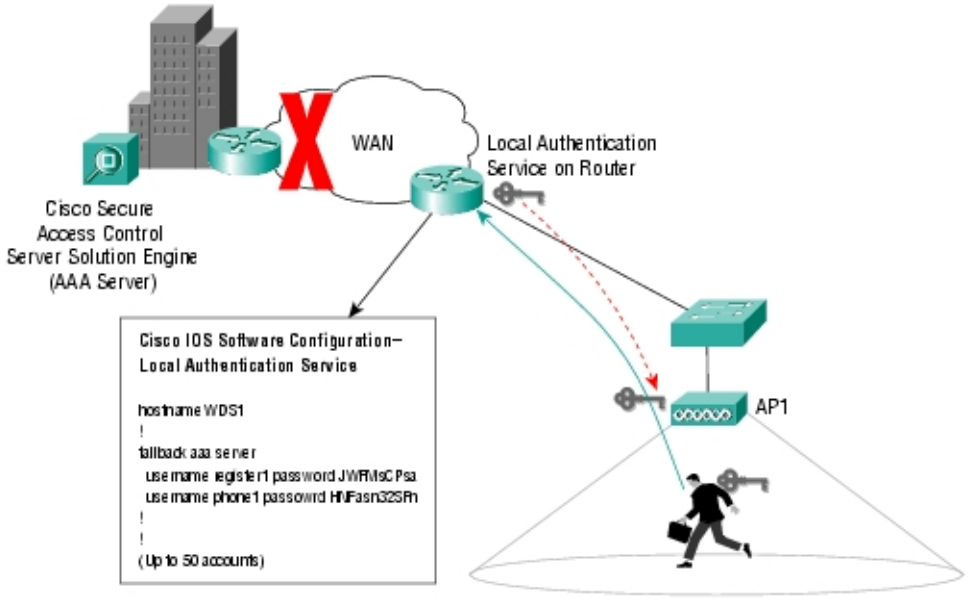
Pour les déploiements qui exigent une mobilité entre sous-réseaux IP (subnet), Cisco met au point une solution évolutive et facile à configurer qui s'appuie sur les bases solides de l'architecture Cisco SWAN. Cette solution sera supportée par de nombreux produits Cisco, notamment par les points d'accès Cisco Aironet et certains commutateurs LAN Cisco Catalyst® et des routeurs Cisco.

Service local d'authentification IEEE 802.1X

Le service local d'authentification IEEE 802.1X consiste à configurer les points d'accès Cisco Aironet pour qu'ils jouent le rôle de serveur RADIUS (Remote Authentication Dial-In User Service) local et qu'ils identifient ainsi les clients sans fil lorsque le serveur AAA (authentification, autorisation et administration) n'est pas disponible (Figure 3). Ce système permet d'assurer des services d'authentification sur les WLAN distants ou sur ceux des succursales d'entreprise qui ne disposent pas d'un serveur RADIUS, ou encore de suppléer à ces services en cas de défaillance du réseau distant (WAN) ou du serveur afin de fournir un accès à des ressources locales comme des serveurs de fichiers ou des imprimantes.

L'authentification locale IEEE 802.1X supporte l'authentification Cisco LEAP de 50 comptes au maximum par point d'accès. Un compte correspond à un nom d'utilisateur et à son mot de passe. La configuration de la base de données locale d'authentification IEEE 802.1X peut être gérée de manière centralisée grâce au système d'administration CiscoWorks WLSE 2.x. Le point d'accès offrant le service local d'authentification IEEE 802.1X n'a pas besoin d'être dédié au service local d'authentification IEEE 802.1X mais peut fonctionner comme un point d'accès classique tout en assurant ce service local d'authentification.

Figure 3 Service local d'authentification IEEE 802.1X



Le service local d'authentification IEEE 802.1X assuré par le point d'accès garantit la continuité du service. Le point d'accès utilise un serveur RADIUS avec le protocole IEEE 802.1X qui prend en charge les protocoles de type EAP (Extensible Authentication Protocol) exécutés sur la plate-forme Cisco IOS. Le service local d'authentification IEEE 802.1X Cisco supporte actuellement Cisco LEAP ainsi que le serveur ACS Cisco Secure Version 2.6 ou supérieure.

Détection et localisation des points d'accès illégaux

L'architecture Cisco SWAN (Structured Wireless-Aware Réseau) détecte, isole et désactive les points d'accès illégaux. Les points d'accès non autorisés installés par les employés pour leur propre compte ou pour celui de leur service représentent un grave problème de sécurité pour les administrateurs réseaux. Le plus souvent, ces employés établissent ces points d'accès parce qu'ils se trouvent dans des zones d'ombre ou parce qu'ils ne sont pas satisfaits de la capacité de leurs réseaux locaux filaires. Ces points d'accès illégaux créent une infrastructure parallèle de réseau LAN sans fil qui permet à n'importe quel utilisateur de se connecter au réseau moyennant une carte client et constituent autant de connexions WLAN non sécurisées qui mettent en danger l'ensemble du réseau d'information de l'entreprise.

Les points d'accès illégaux installés par les employés sont de plus en plus fréquents à mesure que la demande en réseau sans fil augmente, que le coût des points d'accès diminue et que leur installation devient plus simple. Aujourd'hui, il suffit de savoir se brancher sur un port Ethernet pour installer un point d'accès.

Il est clair que la plupart des entreprises – notamment celles qui n'ont pas déployé d'infrastructure sans fil administrée – sont actuellement parasitées par des points d'accès illégaux. Les employés qui possèdent les connaissances techniques nécessaires et qui connaissent les avantages d'un réseau sans fil sont susceptibles d'installer des LAN sans fil pour leur propre confort, sans chercher à obtenir l'accord des équipes réseau ou de l'entreprise. En revanche, il n'est pas surprenant de constater que dans les sociétés qui disposent d'infrastructures WLAN autorisées, le nombre des points d'accès installés par les employés se trouve fortement réduit.

Les réseaux d'entreprise doivent toutefois faire face à un second type de point d'accès illégal : les points d'accès malveillants installés par des intrus qui cherchent à pénétrer sans autorisation dans le site de l'entreprise. Ces points d'accès illégaux peuvent être placés à l'extérieur des locaux, contre un mur extérieur,

ou cachés à l'intérieur des installations elles-mêmes. Comme les signaux des points d'accès peuvent passer à travers les murs, ces installations dissimulées permettent à un pirate d'obtenir, sans être détecté, l'accès au réseau de l'entreprise. Bien qu'ils soient bien moins fréquents que les points d'accès illégaux installés par les employés, ils constituent un risque bien plus grand et sont beaucoup plus difficiles à déceler car ils sont volontairement cachés à la vue du personnel et du réseau.

Avant l'architecture Cisco SWAN (Structured Wireless-Aware Network), les administrateurs réseaux avaient beaucoup de peine à trouver et à désactiver ces points d'accès illégaux, car pour les localiser, ils devaient parcourir, à pied, l'intégralité de leur zone de réseau, armés d'un appareil de détection. De plus, pour déceler les points d'accès illégaux nouvellement installés, ils devaient répéter à intervalles réguliers cette tâche manuelle, fastidieuse et coûteuse. L'architecture Cisco SWAN automatise cette procédure et permet aux responsables réseaux de détecter, d'isoler et de désactiver facilement les points d'accès illégaux.

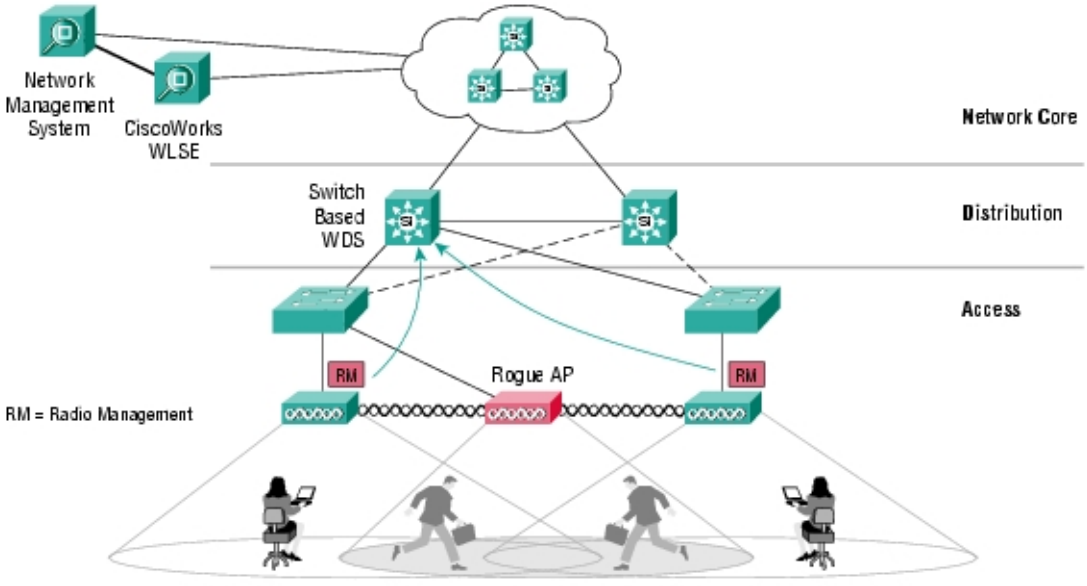
Balayage et contrôle des fréquences radio

L'architecture Cisco SWAN (Structured Wireless-Aware Network) permet aux responsables informatiques de détecter facilement les points d'accès illégaux et les ports de commutation auxquels ils sont connectés car les points d'accès comme les cartes clientes participent activement au balayage et au contrôle en continu de l'environnement radio. L'équipe IT peut ainsi gérer le médium radio par l'intermédiaire de la plate-forme CiscoWorks WLSE et de WDS (Figure 1).

Les points d'accès Cisco Aironet ainsi que les clients Cisco et compatibles Cisco travaillent ensemble pour réaliser des mesures RF à intervalles réguliers. Cette solution originale qui associe les points d'accès et les clients est bien plus efficace que le seul balayage par les points d'accès.

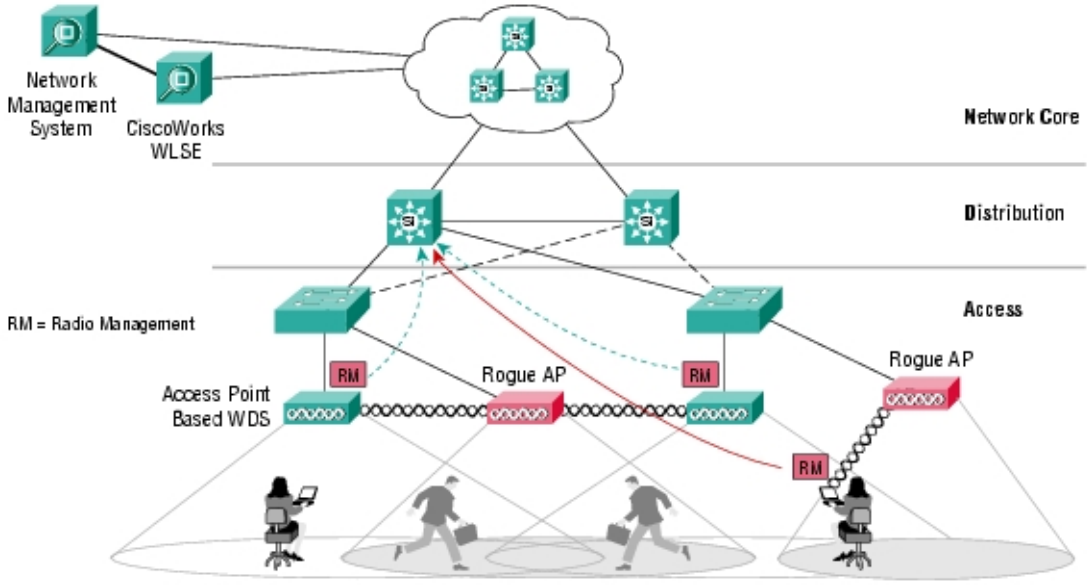
La Figure 4 illustre le balayage RF par des points d'accès seuls. Dans ce scénario, seuls les points d'accès illégaux qui se trouvent à l'intérieur de la zone RF couverte par les points d'accès déployés peuvent être détectés. Malheureusement, le balayage RF par les points d'accès seulement est loin de constituer une solution robuste car seuls les points d'accès balayent et contrôlent l'environnement RF.

Figure 4 Détection des points d'accès illégaux par balayage RF des points d'accès seulement



Grâce à l'architecture Cisco SWAN, les clients Cisco et compatibles Cisco détectent et signalent les zones obscures et les déploiements potentiellement dangereux en utilisant, comme sur la Figure 5, la détection des points d'accès illégaux assistée par les cartes clientes.

Figure 5 Détection des points d'accès illégaux assistée par les cartes clientes



Les clients WLAN ont la possibilité de se déplacer sur des zones physiques importantes : en ajoutant à l'ensemble le balayage et le contrôle des points d'accès illégaux par les clients, on augmente considérablement la zone de couverture RF. Cette gestion assistée client fournit de 10 à 20 fois plus de mesures RF que les points d'accès seuls. Elle permet donc d'élargir le contrôle RF aux zones les plus susceptibles de receler des points d'accès illégaux et de détecter avec plus de précision les installations non autorisées.

Toutes les données obtenues auprès des points d'accès et des cartes clientes sont compilées par WDS et transmises à CiscoWorks WLSE. Celui-ci traite les échantillons qu'il reçoit et signale ceux qui révèlent la présence d'un point d'accès illégal dans CiscoWorks WLSE Location Manager (Figure 6) et dans CiscoWorks WLSE Fault Summary (Figure 7).

Figure 6 CiscoWorks WLSE 2.5 Location Manager

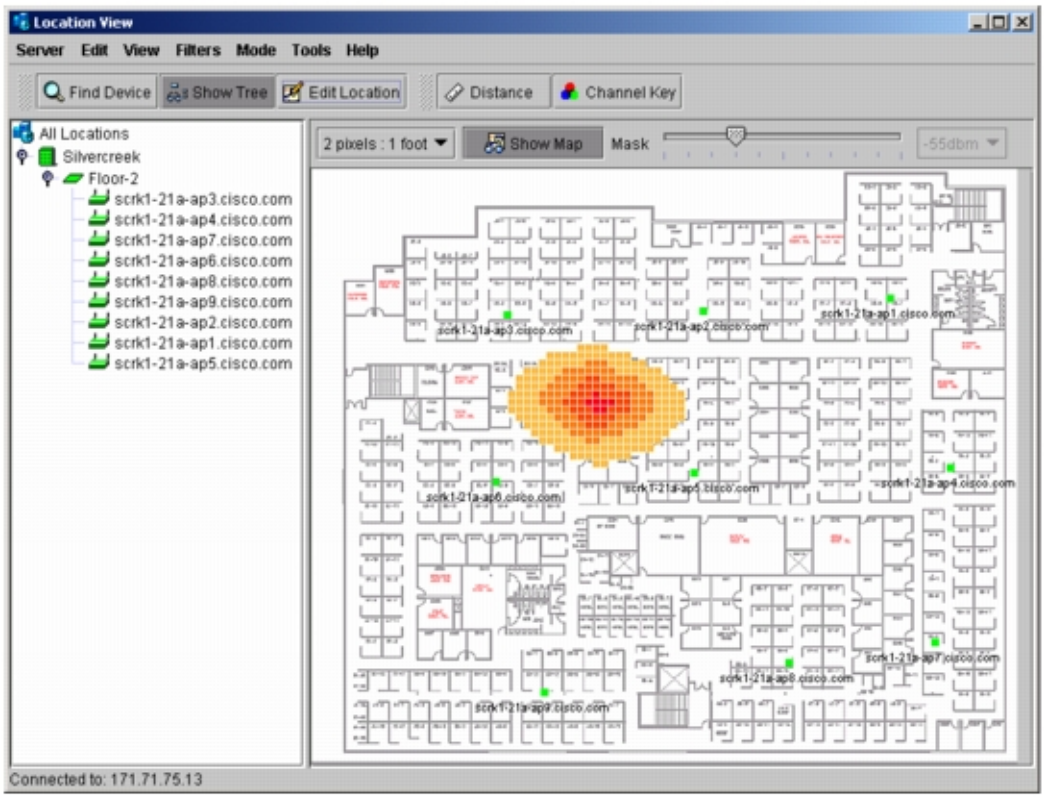
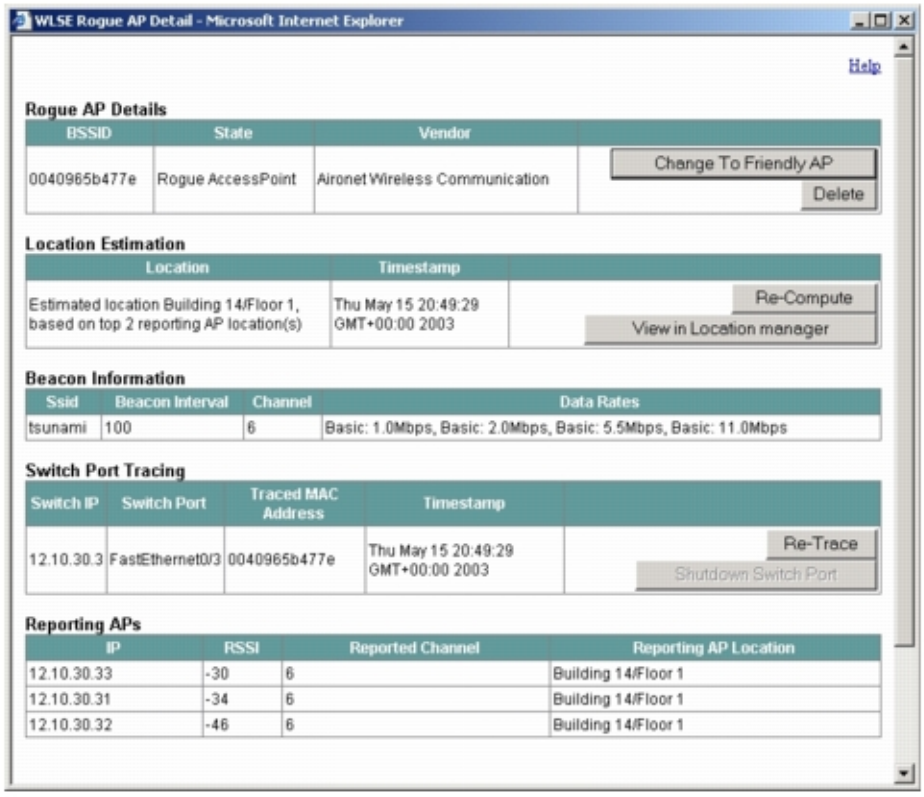


Figure 7 CiscoWorks WLSE 2.0 Fault Summary



Détection des interférences

L'architecture Cisco SWAN (Structured Wireless-Aware Network) réalise un catalogue de l'emplacement physique de tous les points d'accès gérés ainsi qu'une carte de l'installation WLAN. Le réseau supportant le sans fil peut ainsi déterminer les zones d'interférence RF qui réduisent les performances du réseau. Cette énergie RF indésirable peut être générée par point d'accès illégal ou par un appareil qui fonctionne dans la même gamme de fréquences – un téléphone sans fil à 2,4 GHz, par exemple, ou un four à micro-ondes mal isolé.

La détection et la localisation des interférences sont cruciales pour la fiabilité des réseaux WLAN. Les interférences IEEE 802.11 et non- IEEE 802.11 font partie des mesures RF envoyées à CiscoWorks WLSE. Si les interférences dépassent un seuil défini par l'administrateur, un message d'erreur est envoyé qui permet de localiser rapidement la source d'interférence et de la supprimer.

Processus simplifiés de déploiement de WLAN avec assistance à l'étude de site

L'étude de site est une composante indispensable du processus de déploiement d'un WLAN. Sans une étude détaillée réalisée sur le site lui-même, il est impossible de garantir une couverture WLAN exhaustive et fiable. Pour ce travail, la plupart des organisations font appel à des consultants. Malheureusement, dans le cas d'un déploiement à grande échelle et notamment lorsque la zone géographique est très étendue, le recours aux consultants est à la fois long et onéreux.

Malgré les honoraires élevés qu'ils demandent pour une étude de site, les consultants se servent encore d'outils rudimentaires. Leurs décisions pour le placement initial des points d'accès et le choix des canaux reposent sur des mesures RF, sur leur expérience et sur leur intuition. Après avoir effectué une installation provisoire des points d'accès, ils testent la zone de couverture et la qualité du signal en se déplaçant sur le site munis d'une carte client WLAN et d'un logiciel de contrôle. Ils procèdent ensuite aux réglages finaux – placement et orientation des points d'accès, et paramètres de transmission – en fonction des résultats de leurs tests. Former un membre de l'équipe réseau pour qu'il réalise ce type d'étude de site n'a pas d'intérêt économique : le plus souvent, ces études sont ponctuelles et doivent être effectuées site par site, parfois à des centaines de kilomètres de distance dans le cas de déploiements à grande échelle dans des succursales d'entreprise.

Grâce à l'architecture Cisco SWAN (Structured Wireless-Aware Network), les responsables informatiques peuvent réaliser en interne, sans consultant, des études de site économiques – un gain considérable de temps et d'argent pour leur entreprise. Les outils intégrés à CiscoWorks WLSE permettent aux administrateurs de réseaux, même s'ils ne possèdent pas de connaissances particulières en matière de propagation et de mesures RF, de mener à bien ce type d'étude.

L'utilitaire d'assistance à l'étude de site de CiscoWorks WLSE d'une architecture Cisco SWAN procède en cinq étapes simples :

1. L'opérateur commence par importer dans l'utilitaire un plan d'étage du site à étudier. Le logiciel reconnaît un grand nombre de formats de fichiers électroniques, notamment les formats .bmp, .jpg, et .gif. Si aucun fichier électronique n'est disponible, l'utilitaire permet de dresser un schéma approximatif du bâtiment.

2. Les positions initiales des points d'accès sont ajoutées au diagramme afin de déterminer le nombre approximatif des unités nécessaires.

3. Les points d'accès de la gamme Cisco Aironet doivent être installés aux emplacements indiqués par le diagramme.

4. Une fois installés, les points d'accès de la gamme Cisco Aironet sont placés en mode « étude de site » également appelé « AP Scan Mode » : ils transmettent tous sur la même fréquence et à leur puissance maximale. Dans ce mode, les points d'accès se détectent les uns les autres et sélectionnent automatiquement la puissance de transmission, la gamme de fréquence et les autres paramètres pour assurer une couverture exhaustive de la zone.

5. Pour finir, le réglage fin des paramètres RF des points d'accès s'effectue dans le mode « Client Walkabout » : un opérateur déambule dans les secteurs qui doivent être couverts, y compris dans la zone périmétrique, muni d'une carte cliente qui renvoie en continu les mesures RF aux points d'accès Cisco Aironet.

Rationalisation de la gestion et de l'exploitation de réseau WLAN

Le CiscoWorks WLSE 2.x de l'architecture Cisco SWAN (Structured Wireless-Aware Network) prend en charge de manière autonome les mises à niveaux des firmwares et les modifications de configuration de tous les points d'accès aussi bien sur le réseau local que sur le réseau étendu. Le déploiement et la gestion de centaines, voire de milliers de points d'accès sont ainsi administrés sans autre intervention. Les firmwares de tous les points d'accès Cisco Aironet peuvent être mis à jour avec CiscoWorks WLSE 2.x.

Les fonctionnalités de gestion et d'exploitation comprennent également :

- le contrôle proactif des défaillances et des performances en fonction de seuils définis par l'utilisateur,
- la configuration automatique centralisée des nouveaux points d'accès,

- la gestion d'archives de configuration des points d'accès Cisco,
- le contrôle de la politique de sécurité, des défaillances et des performances de l'infrastructure WLAN Cisco,
- l'intégration avec l'infrastructure existante d'administration de réseau (interface SOAP/XML, traps SNMP (Simple Network Management Protocol) et messages Syslog),
- une interface API XML pour l'exportation des données,
- l'intégration avec CiscoWorks LMS,
- la conversion en masse et centralisée des fichiers de configuration du système d'exploitation VxWorks pour les points d'accès de la gamme Cisco Aironet 1200 en fichiers de configuration Cisco IOS à l'aide d'une version élargie de l'utilitaire Cisco Aironet Conversion Tool pour la plate-forme Cisco IOS.

Outils améliorés de dépannage et de diagnostic

Les temps d'arrêt réseau coûtent très cher aux entreprises. Chaque fois qu'un utilisateur de réseau WLAN perd sa connectivité, il perd également en productivité. Il est par conséquent crucial de pouvoir optimiser les temps de fonctionnement et la fiabilité des réseaux WLAN. Le dépannage de ces réseaux est cependant plus complexe et prend davantage de temps en raison de la nature de l'infrastructure RF.

L'architecturee Cisco SWAN fournit des rapports intuitifs et complets qui facilitent le dépannage et la planification de capacité. Il permet de localiser plus précisément les problèmes liés aux utilisations et aux associations clients et contribue à maximiser les temps de fonctionnement réseau. Il offre également des fonctions de suivi client, des rapports de performances du réseau WLAN et le contrôle des défaillances qui simplifient le dépannage réseau.

Fourniture en continu de solutions améliorées de sécurité réseau

En plus des services locaux d'authentification IEEE 802.1X, l'architecture Cisco SWAN (Structured Wireless-Aware Network) offre des fonctionnalités complètes de gestion de sécurité développées autour de la solution de sécurité Cisco Wireless Security Suite, et notamment :

- *Le contrôle des politiques de sécurité* – Le contrôle des politiques de sécurité est assuré pour tous les points d'accès sur la base des paramètres prédéfinis sous Cisco Wireless Security Suite. Le système génère des alertes en cas de violation concernant les identificateurs SSID (Service Set Identifier), les transmissions, les paramètres 802.1X/EAP, le cryptage WEP (Wired Equivalent Privacy), etc. Ces alertes peuvent être envoyées par e-mail, par Syslog ou par des notifications SNMP.
- *La centralisation des paramètres de sécurité* – La gestion centralisée du réseau WLAN assure l'application des paramètres de sécurité comme 802.1X/EAP, WEP et WPA (Wi-Fi Protected Access) sur tous les points d'accès locaux et distants.
- *Le contrôle du serveur RADIUS 802.1X/EAP ou du serveur AAA* – Le système contrôle le serveur RADIUS ou AAA qui prend en charge les fonctions Cisco LEAP et PEAP (Protected-EAP) et vérifie la disponibilité des serveurs ACS Cisco Secure, ainsi que le temps de réponse EAP.
- *Le contrôle du temps de réponse des cartes clientes* – CiscoWorks WLSE simule une carte cliente qui permet de contrôler le temps de réponse des cartes clientes.
- *La notification des seuils de gestion des serveurs RADIUS 802.1X/EAP et AAA* – Les notifications des seuils définis par l'utilisateur sont gérées par e-mail, par Syslog et par notifications SNMP.
- *L'assistance au cryptage AES IEEE 802.11i* – Les futures versions prendront en charge l'assistance aux cryptage AES du protocole IEEE 802.11i.

En résumé

Si les WLAN offrent aux utilisateurs réseaux une liberté, une souplesse et des avantages concurrentiels inconnus jusqu'à présent, ils placent également les professionnels des technologies de l'information devant un ensemble de défis d'un genre nouveau. L'architecture Cisco SWAN (Structured Wireless-Aware Network) est conçue pour relever ces défis en intégrant les réseaux locaux sans fil et filaires et offrir des niveaux de sécurité, d'évolutivité et de facilité de gestion des réseaux WLAN identiques à ceux que nos clients attendent de leurs réseaux LAN filaires. Cette solution, qui s'appuie sur les outils bien connus de la plate-forme Cisco IOS, les points d'accès Cisco Aironet, des cartes clientes ainsi que des commutateurs et des routeurs Cisco, permet de structurer, de contrôler et maintenir une sécurité renforcée sur les réseaux locaux sans fil.

L'architecture Cisco SWAN est un ensemble complet pour réussir l'intégration des réseaux filaire et sans fil d'entreprise. Il apporte aux administrateurs réseaux les outils dont ils ont besoin pour sécuriser, contrôler et gérer leur réseau WLAN dans des déploiements de campus de taille moyenne ou de grande taille, ainsi que des déploiements distribués dans les succursales d'entreprise, les grands centres commerciaux, les centres de productions et les centres de soins de santé.

Pour en savoir plus sur ces produits et solutions Cisco :

Produits Cisco Aironet : http://www.cisco.com/go/aironet

CiscoWorks WLSE : http://www.cisco.com/go/wlse

Serveur ACS Cisco Secure : http://www.cisco.com/go/acs

Cisco Wireless Security Suite :
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a0080088829.html

Programme Cisco Compatible Extensions :
http://www.cisco.com/go/ciscocompatible/wireless

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe