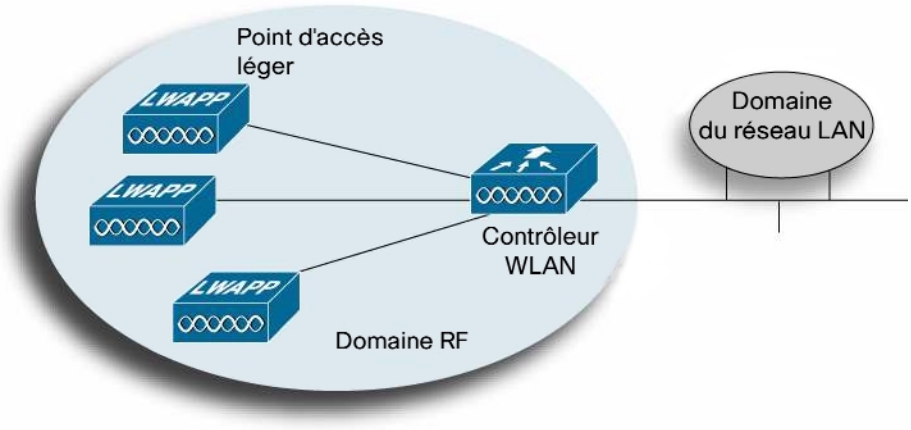
Bien comprendre le protocole LWAPP (LightWeight Access Point Protocol)

Dans la gestion des réseaux sans fil (WLAN – Wireless LAN), la tendance est à la centralisation de l'intelligence et du contrôle. Pour créer et appliquer les politiques sur un grand nombre de points d'accès différents, les nouvelles architectures font appel à un système de contrôleur WLAN. La centralisation de l'intelligence sur ces contrôleurs permet de gérer efficacement la sécurité, la mobilité, la qualité de service (QoS) et de nombreuses autres fonctions indispensables à l'exploitation des WLAN sur l'ensemble de l'entreprise. De plus, en répartissant diverses fonctions entre les points d'accès et le contrôleur, les responsables réseau simplifient les opérations de gestion, améliorent les performances et renforcent la sécurité des grands réseaux sans fil.

Figure 1. Les systèmes WLAN légers centralisent l'intelligence pour gérer la capacité RF et contrôler les politiques à l'échelle de l'entreprise



Un nombre croissant de constructeurs se mettent à proposer des architectures hiérarchiques tandis que la réalisation des grands réseaux sans fil fait intervenir de plus en plus souvent les points d'accès légers («lightweight»). Dans ce contexte, il devient indispensable de disposer d'un protocole normalisé capable de contrôler la manière dont les points d'accès légers communiquent avec les systèmes WLAN. Tel est le rôle du dernier projet de spécification de l'IETF (Internet Engineering Task Force) appelé LWAPP (Lightweight Access Point Protocol). Le protocole LWAPP permet de déployer de grands réseaux sans fil multiconstructeurs disposant d'un maximum de fonctionnalités et de souplesse.

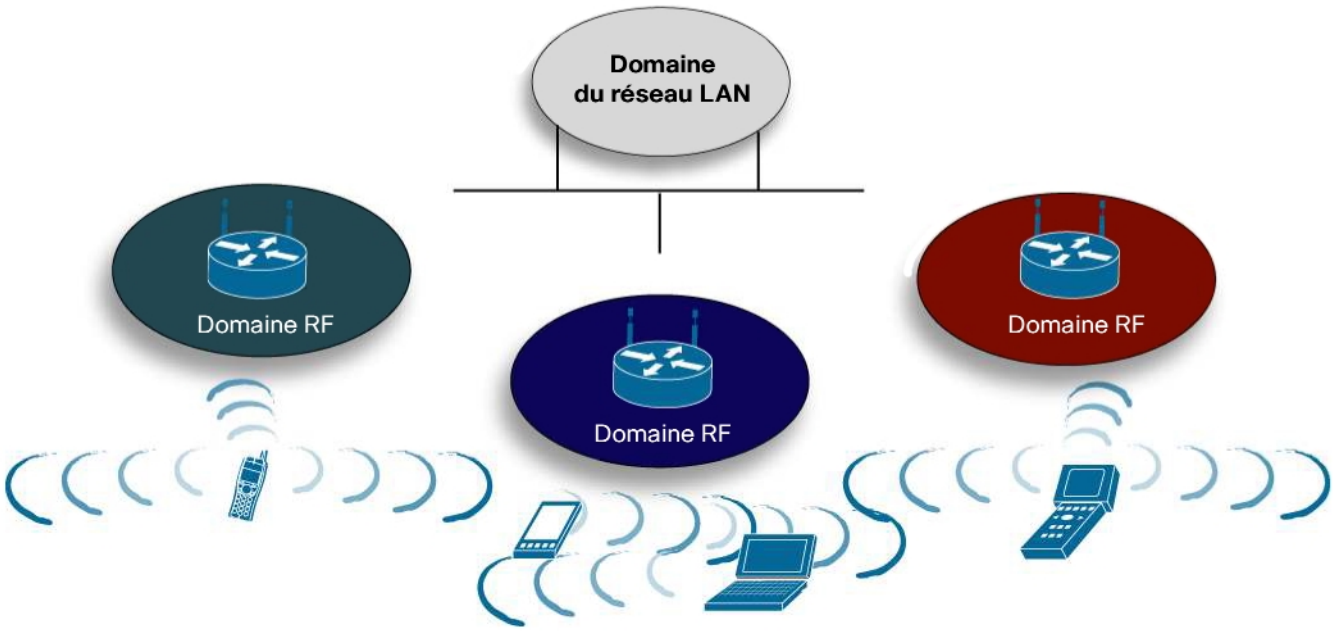
LES AVANTAGES DES POINTS D'ACCÈS LÉGERS

Les solutions WLAN traditionnelles attribuent l'ensemble des fonctions de gestion du trafic, de contrôle RF, de sécurité et de mobilité au point d'accès lui-même.

Malheureusement, ce type d'architecture limite la visibilité du trafic 802.11 à un seul point d'accès, avec les conséquences suivantes :

- les points d'accès individuels utilisés sans unité de gestion doivent être gérés un à un, ce qui augmente les frais d'exploitation et les besoins en personnel ;
- les attaques et les interférences sur l'ensemble du réseau ne sont pas détectables sur le système tout entier :
  - il n'existe qu'un seul point d'application des politiques de sécurité sur les couches 1, 2 et 3 ;
  - il est impossible de détecter et de contrer les attaques par saturation sur l'ensemble du réseau WLAN ;
- le système par lui-même est incapable d'effectuer des corrélations ou des prédictions d'activité sur l'ensemble de l'entreprise :
  - ceci limite la capacité à optimiser en temps réel l'équilibrage de charge ;
  - les clients ne peuvent pas effectuer de roaming rapides indispensables au support des applications temps réel comme la voix et la vidéo ;
- il existe un risque inhérent de sécurité en cas de vol ou de manipulation d'un point d'accès.

Figure 2. L'architecture WLAN «Peer-to-Peer» limite les performances, la capacité de gestion et la sécurité



De nombreux constructeurs d'équipements ont réagi devant les limitations de l'architecture «peer-to-peer» des réseaux WLAN (Figure 2) et ont proposé de nouvelles architectures capables de centraliser l'intelligence du réseau WLAN afin d'en améliorer les performances et la rentabilité.

LA NORMALISATION EST UNE NÉCESSITÉ

Alors qu'apparaissent de plus en plus de produits qui utilisent les points d'accès légers avec intelligence WLAN centralisée, il est nécessaire de mettre au point une norme industrielle capable de régir la manière dont ces appareils communiquent entre eux. Le protocole LWAPP est un projet de norme en cours d'homologation au sein du groupe de travail IETF et qui résoudra ce problème. Conçu à l'origine par Airespace (acquis en mars 2005 par Cisco Systems) et NTT DoCoMo, LWAPP normalise le protocole de communications entre les points d'accès et les systèmes WLAN (contrôleurs, commutateurs, routeurs, etc.). Tel qu'il est décrit dans la spécification IETF, l'initiative a les ambitions suivantes :

- réduire la quantité de traitement réalisée par un point d'accès pour permettre le recentrage des ressources de calcul limitées de ces appareils sur l'accès sans fil – par opposition au filtrage et à l'application des politiques ;
- élaborer un schéma permettant la centralisation à l'échelle du système WLAN des opérations de gestion de trafic, d'authentification, de cryptage et d'application des politiques (QoS, sécurité, etc.) ;
- définir un mécanisme générique d'encapsulation et de transport pour l'interopérabilité entre les points d'accès de différents constructeurs soit par l'intermédiaire d'une infrastructure de couche 2 ou du routage IP.

La spécification LWAPP atteint ces objectifs en définissant les types d'activités suivants :

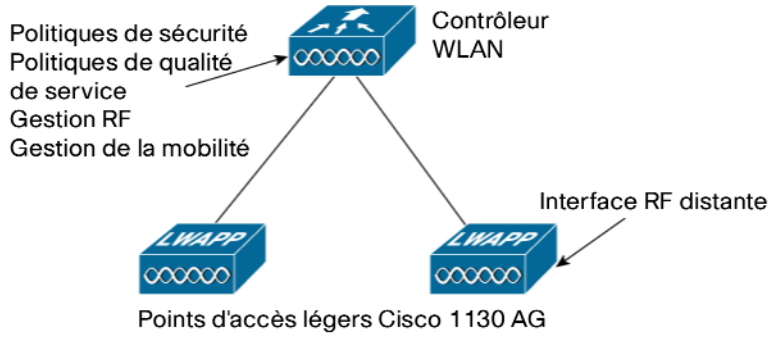
- la découverte et la configuration des points d'accès et l'échange d'informations avec eux ;
- la certification et le contrôle logiciel des points d'accès ;
- l'encapsulation, la fragmentation et le formatage des paquets ;
- le contrôle et la gestion des communications entre les points d'accès et les terminaux sans fil.

La généralisation du protocole LWAPP permettra aux entreprises de choisir des points d'accès et des unités systèmes sans fil multiconstructeurs et interopérables, sans se soucier de savoir si les différentes composantes peuvent travailler ensemble : les fonctionnalités proposées par les différents appareils deviendront le seul critère de décision. La généralisation industrielle du protocole LWAPP évitera aux entreprises de s'enfermer dans une relation avec un unique constructeur, autrement dit de ne pouvoir choisir que les points d'accès compatibles avec leur système WLAN propriétaire pour fonctionner de manière optimale. Le protocole LWAPP réalise également une solution à normes ouvertes pour la fourniture des services sécurisés des couches 2 et 3 sur des architectures centralisées de réseau WLAN multiconstructeur. Par ailleurs, avec LWAPP, les différents constructeurs bénéficieront d'une architecture commune pour le développement des applications.

LA MISE EN ŒUVRE DU PROTOCOLE LWAPP

Lorsque le protocole LWAPP a été introduit pour la première fois dans le secteur des réseaux locaux sans fil en 2002, il a révolutionné la gestion des déploiements de réseaux WLAN en présentant le concept de partage des adresses MAC ou «Split-MAC», autrement dit la capacité à distinguer l'aspect temps réel du protocole 802.11 de l'essentiel de ses caractéristiques de gestion (Figure 3). C'est ainsi, notamment, que l'échange de trames en temps réel et certaines parties de la gestion en temps réel des adresses MAC sont effectuées par le point d'accès, tandis que les fonctions d'authentification, de gestion de la sécurité et de la mobilité sont assurées par des contrôleurs WLAN. La solution de réseau sans fil centralisé Cisco, qui s'appuie sur le protocole LWAPP, est le premier système de WLAN centralisé à utiliser le concept «Split-MAC».

Figure 3. Les points d'accès légers Cisco 1130 AG



L'association du protocole LWAPP et des fonctionnalités intelligentes de gestion RF Cisco offre de nombreux avantages à l'utilisateur.

Gestion

- La gestion RF est dynamique et étendue à l'ensemble du système, et comprend un grand nombre de fonctionnalités pour une exploitation harmonieuse du réseau sans fil comme l'attribution dynamique des canaux, le contrôle de la puissance de transmission et l'équilibrage de charges.
- Une unique interface graphique permet l'application de toutes les politiques de l'entreprise, notamment en matière de VLAN, de sécurité et de qualité de service (QoS).

Sécurité

- Des politiques de sécurité applicables à l'échelle de l'entreprise couvrent toutes les couches du réseau sans fil, depuis la couche radio jusqu'à la couche MAC et la couche réseau. Cette particularité simplifie l'application uniforme des politiques de sécurité et de qualité de service utilisateurs qui peuvent ainsi englober les capacités spécifiques d'appareils aussi différents que les scanners à main, les PDA ou les ordinateurs portables.
- Le système peut identifier et contrer les attaques par saturation ou encore détecter les points d'accès non autorisés et leur refuser l'accès au réseau. Ces fonctions sont réalisables avec une solution complète de réseau WLAN léger Cisco.

Mobilité

- Les roaming d'un point d'accès à un autre sont rapides et analogues à ceux de la téléphonie cellulaire.
- Le système fournit un excellent support aux applications mobiles en temps réel comme la voix sur WLAN (VoWLAN).

Le protocole LWAPP est une composante essentielle des réseaux sans fil d'entreprise. Il jette les fondations sur lesquelles il sera possible de bâtir des WLAN hétérogènes à grande échelle. En offrant un concept normalisé de l'interconnexion réseau RF, il protège les investissements de l'entreprise dans son réseau WLAN, simplifie la gestion RF et optimise l'architecture sans fil pour les déploiements de réseaux WLAN quelle que soit leur taille.

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

205327.CX_ETMG_LS_9.05