Groupe de tavail Réseau
Request for Comments : 3990
Catégorie : Informationnel

Février 2005

B. O'Hara
P. Calhoun
Airespace
J. Kempf
Docomo Labs USA

Configuration et approvisionnement pour les Points d'accès sans fil (CAPWAP) Etat des problèmes

RésuméLe présent document décrit l'état des problèmes de la Configuration et approvisionnement pour les point d'accès sans fil (CAPWAP, Configuration and Provisioning for Wireless Access Points).

1. Introduction

Avec l'approbation de la norme 802.11 par l'IEEE en 1997, les LAN sans fil (WLAN) ont commencé doucement à entrer dans les réseaux d'entreprise. Les débits de données limités de la norme 802.11 d'origine, seulement 1 et 2 Mbit/s, empêchaient l'adoption généralisée de cette technologie. La norme 802.11 a trouvé un large développement dans des applications verticales, telles que la gestion d'inventaire, la gestion de point de vente, et la gestion des transports. Les entreprises pionnières ont commencé à mettre en œuvre 802.11, principalement aux fins d'expérimentation.
En 1999, l'IEEE a approuvé les amendements 802.11a et 802.11b à la norme de base, augmentant le débit de données disponible respectivement à 54 et 11 Mbit/s, et qui occupent une nouvelle bande radioélectrique. Cela a supprimé un des facteurs de blocage les plus significatifs à l'adoption de 802.11 dans les grands réseaux d'entreprise. Ces grands développements étaient limités par la définition et les fonctionnalités d'un point d'accès (AP, *Access Point*) de 802.11, tel que décrit dans la norme 802.11. Les techniques exigent une large utilisation du pontage de couche 2 et des VLAN pour assurer le bon fonctionnement des protocoles de couches supérieures. On a décrit des développements de WLAN 802.11 de plusieurs milliers de points d'accès.
Les grands développements de WLAN 802.11 ont posé plusieurs problèmes qui réclament des solutions. Les limitations à l'extensibilité du pontage ne devraient pas causer de surprise dans le monde du réseautage, car des limitations similaires sont apparues au début des années 1980 pour les pontages de réseau filaire durant la phase d'expansion et d'interconnexion des réseaux filaires de zone locale. Le présent document va décrire les problèmes introduits par le développement à grande échelle de WLAN 802.11 dans les réseaux d'entreprise.

2. Etat des problèmes

Le développement de grands WLAN pose plusieurs problèmes.
D'abord, chaque AP est un appareil IP adressable qui exige de la gestion, de la surveillance et du

contrôle. Le développement d’un grand WLAN va normalement doubler le nombre des appareils d’infrastructure de réseau à gérer. Cela représente un fardeau supplémentaire significatif pour les ressources d’administration du réseau et est souvent un obstacle à l’adoption des technologies sans fil, particulièrement à cause de la configuration de chaque point d’accès qui est presque identique à celle du suivant. Cette proche similitude conduit souvent à des erreurs de configuration et à un mauvais fonctionnement du WLAN.
Ensuite, la distribution et la maintenance d’une configuration cohérente à travers tout l’ensemble des points d’accès du WLAN est problématique. La configuration de points d’accès consiste à la fois en informations statiques à long terme (telles que l’adressage et les réglages matériels) et en informations d’approvisionnement plus dynamiques (telles que les réglages individuels de WLAN et les paramètres de sécurité). Les grandes installations de WLAN qui ont à mettre à jour les informations d’approvisionnement dynamique dans tous les points d’accès du WLAN exigent un délai prolongé de mise hors circuit. Comme chaque point d’accès est à mettre à jour, le WLAN n’aura pas une configuration unitaire et cohérente.

Troisièmement, il est difficile de s’accomoder de façon efficace de la nature dynamique du support WLAN lui-même. Du fait de la nature partagée du support sans fil (partagé avec les points d’accès dans le même WLAN, avec les points d’accès dans les autres WLAN, et avec des appareils qui ne sont pas du tout des points d’accès), les paramètres qui contrôlent le support sans fil sur chaque AP doivent être surveillés fréquemment et modifiés de façon coordonnée pour maximiser les performances du WLAN. Cela doit être coordonné parmi tous les points d’accès, pour minimiser les interférences d’un point d’accès avec ses voisins. La surveillance manuelle de ces paramètres et la détermination d’une configuration optimale nouvelle pour les paramètres qui se rapportent au support sans fil est une tâche qui coûte du temps et des efforts significatifs.
Quatrièmement, relever le défi de la sécurisation de l’accès au réseau et empêcher l’installation de points d’accès non autorisés. Il est souvent difficile de sécuriser les localisations physiques des points d’accès dans la mesure où ces localisations doivent souvent être en dehors d’un local réseau fermé ou d’une chambre de serveur. Le vol d’un point d’accès, avec ses secrets incorporés, permet au voleur d’obtenir l’accès aux ressources gardées par ces secrets.
Récemment, pour s’attaquer à certains, ou à la totalité, des problèmes ci-dessus, plusieurs fabricants ont commencé à offrir des solutions personnelles qui combinent des aspects de commutation réseau, de commande et gestion centralisée, et d’accès sans fil distribué, dans diverses nouvelles architectures. Dans la mesure où des solutions interopérables permettent aux entreprises et fournisseurs de service un plus large choix, une interface interopérable normalisée entre les points d’accès et un contrôleur centralisé qui s’occupe des problèmes semble souhaitable.
Dans les appareils mis actuellement sur le marché, les portions physiques de ce système réseau sont un ou plusieurs points d’accès (AP) 802.11 et un ou plusieurs appareils de commande central, aussi décrits comme des contrôleurs (ou des controleurs d’accès, AC). Théoriquement, un concepteur de réseau devrait être capable de choisir un ou plusieurs fabricants pour les AP et un ou plusieurs fabricants pour les appareils de commande centrale en nombre suffisant pour concevoir un réseau avec un accès sans fil 802.11 qui satisfasse aux exigences du concepteur.
Les mises en œuvre existantes ne sont ni normalisées ni interopérables. Cela est dû à un certain nombre de facteurs, y compris les choix architecturaux disparates faits par les divers fabricants. Une taxonomie des architectures employées dans les produits existants sur le marché va fournir une base à un document qui sera produit au groupe de travail IEEE 802.11. Cette taxonomie sera utilisée par le groupe de travail 802.11 comme apport à la définition de l’architecture fonctionnelle de point d’accès. L’architecture fonctionnelle, y compris les descriptions des blocs fonctionnels détaillés, des interfaces, et des flux d’information, seront revus par CAPWAP pour déterminer si des travaux ultérieurs sont nécessaires pour appliquer ou développer des protocoles normalisés permettant des mises en œuvre interopérables de WLAN d’origine de fabrication multiples construits à partir d’appareils qui adhèrent à la nouvelle architecture hiérachisée qui émerge en utilisant une

séparation fonctionnelle entre point d'accès et contôleur d'accès.

3. Considérations sur la sécurité

Les appareils utilisés dans les WLAN contrôlent l'accès réseau et participent à la livraison des paquets entre les hôtes utilisant le WLAN et d'autres hôtes sur le WLAN ou ailleurs sur l'Internet. Donc, les fonctions de commande et d'approvisionnement des points d'accès sans fil, exigent une protection pour empêcher le mauvais usage de ces appareils.
Les exigences de confidentialité, d'intégrité, et d'authenticité devraient examiner la gestion centralisée, la surveillance et le contrôle des points d'accès sans fil qui devraient être visés. Une fois qu'un AP et un AC ont été authentifiés l'un à l'autre, un seul niveau d'autorisation permettant la surveillance, le contrôle et l'approvisionnement peut n'être pas suffisant. L'exigence de plus d'un seul niveau d'autorisation devrait être évaluée. La sécurité physique devrait aussi être examinée pour les appareils qui contiennent des paramètres sensibles de sécurité qui pourraient compromettre la sécurité du système, si ces paramètres devaient tomber entre les mains d'un agresseur.
Pour fournir une couverture radio complète, les AP sont souvent installés dans des localisations qu'il est difficile de sécuriser. L'architecture CAPWAP peut réduire les conséquences d'un AP volé. Si des secrets de grande valeur, comme un secret partagé RADIUS, sont conservés dans l'AC, la perte physique d'un AP ne compromet alors pas ces secrets. De plus, l'AC peut facilement être localisé dans une installation physiquement sécurisée. Bien sûr, concentrer tous les secrets de grande valeur dans un seul endroit fait de l'AC une cible attrayante, et des contrôle physiques, procéduraux, et techniques stricts sont nécessaires pour protéger les secrets.

Adresse des auteurs

Bob O'Hara Airespace 110 Nortech Parkway San Jose, CA 95134 Phone: +1 408-635-2025 email: bob@airespace.com	Pat R. Calhoun Airespace 110 Nortech Parkway San Jose, CA 95134 Phone: +1 408-635-2000 email: pcalhoun@airespace.com	James Kempf Docomo Labs USA 181 Metro Drive, Suite 300 San Jose, CA 95110 Phone: +1 408 451 4711 email: kempf@docomolabs-usa.com

Déclaration de Copyright

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels

droits pourrait être ou n’être pas disponible ; pas plus qu’elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l’IETF au sujet des droits dans les documents de l’IETF figurent dans les BCP 78 et BCP 79.
Des copies des dépôts d’IPR faites au secrétariat de l’IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d’utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l’IETF à http://www.ietf.org/ipr.
L’IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d’adresser les informations à l’IETF à ietf- ipr@ietf.org.

RemerciementLe financement de la fonction d’édition des RFC est actuellement fourni par Internet Society.