Localisation des points d'accès sans fil non autorisés

Un point d'accès non autorisé peut compromettre la sécurité du réseau de l'entreprise en l'exposant au monde extérieur. Pour remédier à cette menace, l'administrateur réseau doit tout d'abord rechercher les points d'accès non autorisés présents sur le réseau pour les localiser ensuite.

Les deux méthodes de recherche les plus couramment utilisées pour identifier l'emplacement d'un point d'accès non autorisé sont la méthode par convergence et la méthode par vecteur. Chacune de ces méthodes requiert l'utilisation d'outils différents. Par ailleurs, elles présentent leurs avantages respectifs. La compréhension de leur fonctionnement permettra à l'administrateur réseau de garantir la sécurité de son réseau.

Table des matières

FLUKE networks

Localisation des points d'accès sans fil non autorisés

Un point d'accès non autorisé peut compromettre la sécurité d'un réseau sans fil. On qualifie un point d'accès de « non autorisé » lorsqu'il a été installé à l'insu de l'administrateur réseau de l'entreprise ou sans son approbation. Cette situation peut parfois être involontaire. En effet, un employé peut par exemple apporter son propre routeur sans fil au bureau pour fournir un accès sans fil temporaire dans le cadre d'une réunion. On peut également imaginer un scénario plus négatif, dans lequel une personne malintentionnée pourrait installer un point d'accès en dehors des locaux de l'entreprise pour pouvoir bénéficier d'un accès Internet gratuit ou pirater le réseau. Dans les deux cas, la configuration des paramètres de sécurité du point d'accès non autorisé n'est pas appropriée, que la personne concernée ait agi volontairement ou non. Ce type de point d'accès expose le réseau de l'entreprise au monde extérieur.

Des solutions permettent à l'administrateur réseau de détecter la présence d'un point d'accès non autorisé sur le réseau. Détecter un point d'accès non autorisé sur le réseau ne suffit toutefois pas à résoudre le problème. En effet, l'administrateur réseau doit poursuivre par la localisation physique du point d'accès. Il peut ensuite supprimer l'accès au réseau ou reconfigurer le point d'accès avec ses propres paramètres de sécurité.

Les deux méthodes de recherche les plus couramment utilisées pour identifier l'emplacement d'un point d'accès non autorisé sont la méthode par convergence et la méthode par vecteur. La méthode de recherche que vous utiliserez dépendra des outils dont vous disposez.

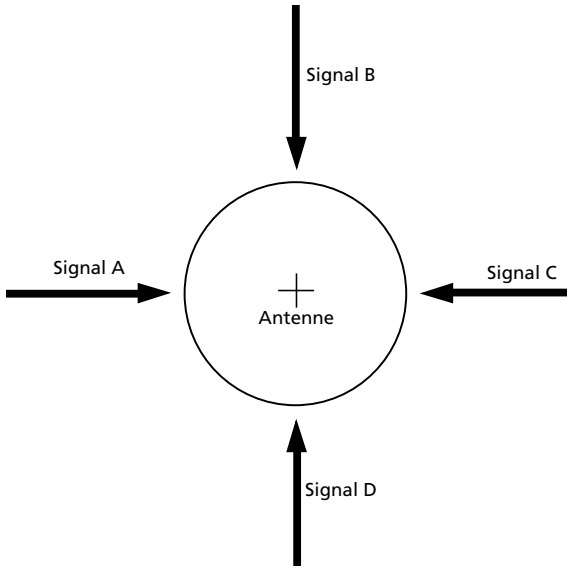

Figure 1 - Schéma d'une antenne omnidirectionnelle

Méthode par convergence

La méthode par convergence est la plus appropriée lorsque vous disposez d'une carte radio avec antenne omnidirectionnelle et d'un outil de mesure de l'intensité du signal. L'antenne omnidirectionnelle offre des taux d'émission et de réception équivalents dans toutes les directions. On l'appelle également antenne équidirective pour cette même raison. La figure 1 illustre le schéma d'une antenne omnidirectionnelle.

L'ordinateur portable utilise une carte radio standard pour réseau local (LAN) sans fil avec antenne omnidirectionnelle. Dans cette application, une antenne omnidirectionnelle convient car l'intensité du signal sera conservée, quelle que soit la position de l'ordinateur.

La méthode par convergence requiert également l'utilisation d'un outil de mesure de l'intensité du signal. Cet appareil permet de mesurer le signal RF émis par le point d'accès non autorisé. Plus l'intensité est élevée, plus le point d'accès est proche. Différents types d'appareils de mesure sont disponibles sur le marché. Il s'agit le plus souvent d'un utilitaire logiciel qui accompagne généralement la carte radio installée sur votre ordinateur portable. Si ces simples utilitaires varient selon le fabricant, ils ont en commun d'afficher l'intensité du signal de manière graphique. Seulement, ces utilitaires présentent l'inconvénient suivant : les petites variations d'intensité du signal ne sont pas clairement identifiables dans les graphiques simplistes proposés.

Figure 2 - Carte radio standard avec antenne omnidirectionnelle pour réseau local (LAN) sans fil

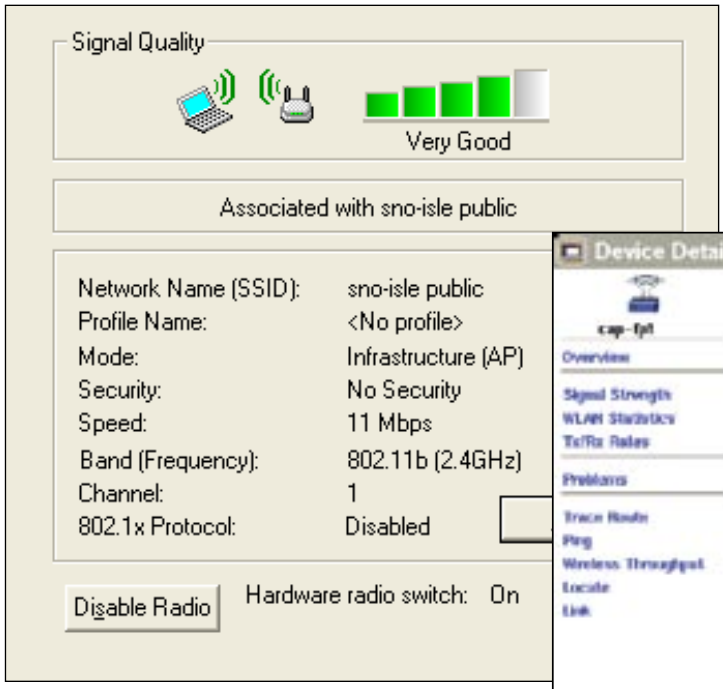

Figure 3 - Utilitaire de mesure de l'intensité du signal

Figure 4 - Graphique qui représente l'intensité du signal, optimisé pour la détection des points d'accès non autorisés

Le marché offre également un logiciel tiers pour ordinateur portable dont les capacités de mesure de l'intensité du signal sont plus élevées. Ces applications tierces offrent des mesures plus détaillées et des graphiques plus grands et plus efficaces. Si vous ne souhaitez pas utiliser un ordinateur portable, vous pouvez considérer l'utilisation d'un outil portatif de mesure de l'intensité du signal RF. Ce type d'instrument est généralement conçu pour la détection des points d'accès non autorisés et fournit des informations sur l'intensité du signal dans un format convivial qui vous permettra de les localiser plus rapidement.

Pour rechercher un point d'accès non autorisé à l'aide de la méthode par convergence, utilisez une carte radio avec antenne omnidirectionnelle et un outil de mesure de l'intensité du signal. Associez la carte radio au point d'accès cible. Parcourez le site tout en surveillant l'intensité du signal jusqu'à ce que vous puissiez déterminer l'emplacement de départ de votre recherche. Vous pouvez vous représenter mentalement la zone de recherche comme un grand rectangle segmenté en quatre. Reportez-vous à la figure 5. Mettez-vous dans un coin de votre zone de recherche. Enregistrez l'intensité du signal. Mettez-vous dans un autre coin de la zone de recherche. Enregistrez à nouveau l'intensité du signal. Mettez-vous dans le troisième coin et enregistrez l'intensité du signal. Mettez-vous dans le quatrième coin et enregistrez l'intensité du signal. Après comparaison des différentes données d'intensité du signal enregistrées, vous concluez que le point d'accès cible se trouve dans le quadrant dont l'intensité du signal est la plus élevée, le quadrant inférieur droit dans notre exemple. A présent, représentez-vous mentalement votre nouvelle zone de recherche comme le quadrant illustré, lui-même divisé en quatre quadrants. Répétez le même exercice de mesure pour cette zone de recherche plus petite, en passant d'un coin à un autre et en enregistrant les résultats à chaque fois comme expliqué plus haut. Dans notre exemple, le sous-quadrant de la partie supérieure droite présente l'intensité de signal la plus forte. Répétez la procédure, en segmentant la zone de recherche en quadrants encore plus petits. Dans notre exemple, trois segmentations – ou douze mesures – ont été nécessaires pour se rapprocher au maximum du point d'accès et le localiser avec précision. Il se peut toutefois que vous deviez ajouter des étapes de segmentation et de mesure si votre zone de recherche initiale est plus grande.

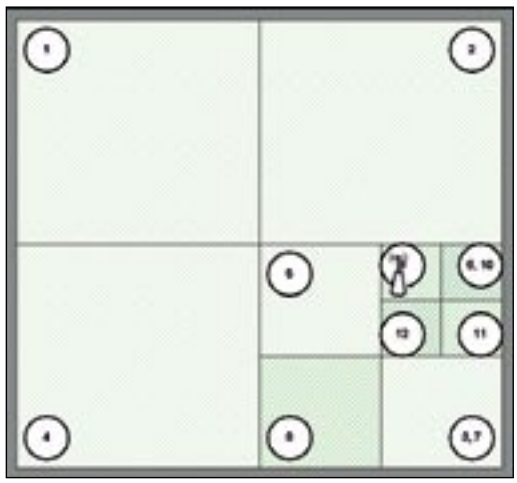

Figure 5 - Schéma de recherche de la méthode par convergence

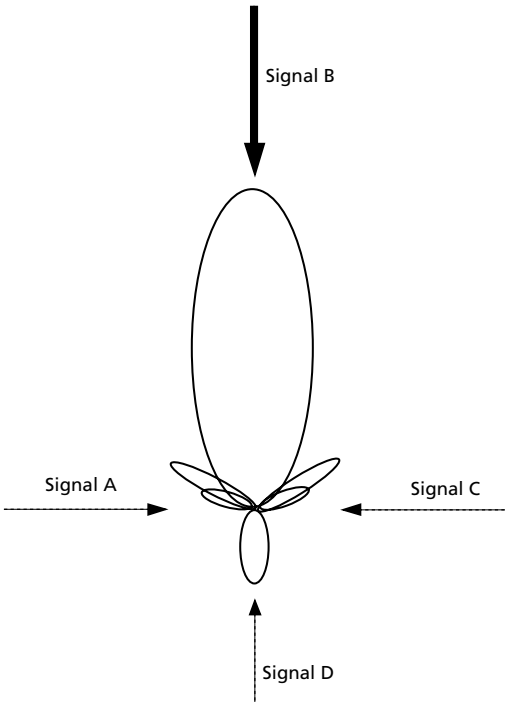

Figure 6 - Schéma d'une antenne unidirectionnelle

Figure 7 - Carte avec antenne unidirectionnelle externe

Méthode par vecteur

Il s'agit de l'autre méthode de recherche qui permet d'identifier l'emplacement physique d'un point d'accès non autorisé. La méthode par vecteur est la plus appropriée lorsque vous disposez d'une carte radio avec antenne unidirectionnelle et d'un outil de mesure de l'intensité du signal. Une antenne unidirectionnelle intensifie les signaux provenant d'une direction et ignore les signaux provenant d'autres directions. La figure 6 illustre le schéma d'une antenne unidirectionnelle.

Plusieurs configurations d'antennes unidirectionnelles sont disponibles. En l'occurrence, une antenne externe à la carte radio facilitera la tâche. Vous avez besoin d'une carte radio spécialement conçue pour ce type d'antenne. Ce type de carte comporte généralement un connecteur qui permettra de brancher la fiche de l'antenne. Par ailleurs, le branchement de l'antenne externe unidirectionnelle sur la carte aura pour effet de désactiver l'antenne omnidirectionnelle interne.

Tout comme la méthode par convergence, la méthode par vecteur requiert l'utilisation d'un outil de mesure de l'intensité du signal. Il conviendra d'utiliser un instrument portatif spécialement conçu à cet effet. Les deux méthodes de recherche diffèrent de par leurs algorithmes de recherche.

Pour rechercher un point d'accès non autorisé à l'aide de la méthode par vecteur, utilisez une antenne unidirectionnelle, une carte radio et un wattmètre. Associez la carte radio au point d'accès cible. Parcourez le site tout en surveillant l'intensité du signal jusqu'à ce que vous puissiez déterminer l'emplacement de départ de votre recherche. Comme expliqué plus haut, vous pouvez vous représenter mentalement la zone de recherche comme un grand rectangle segmenté en quatre parties. Reportez-vous à la figure 8. Positionnez-vous au centre de la zone de recherche et dirigez l'antenne vers l'un des coins de cette zone. Enregistrez l'intensité du signal. Restez au centre, tournez de 90° et dirigez l'antenne vers le deuxième coin. Enregistrez l'intensité du signal. Dirigez l'antenne vers le troisième coin et enregistrez l'intensité du signal. Dirigez l'antenne vers le dernier coin et enregistrez l'intensité du signal. Après comparaison des différentes données d'intensité du signal enregistrées, vous concluez que le point d'accès cible se trouve dans la zone dont l'intensité du signal est la plus élevée, la zone inférieure droite dans notre exemple.

A présent, représentez-vous mentalement cette zone comme votre nouvelle zone de recherche, elle-même divisée en quatre parties plus petites. Répétez l'exercice de mesure de l'intensité du signal dans cette zone plus petite, en son centre, et dirigez l'antenne vers chaque coin en n'oubliant pas d'enregistrer l'intensité du signal à chaque fois. Dans notre exemple, la sous-zone supérieure droite présente l'intensité de signal la plus élevée. Répétez la procédure, en segmentant la zone de recherche en zones encore plus petites. Dans notre exemple, trois segmentations – ou douze mesures – ont été nécessaires pour se rapprocher au maximum du point d'accès et le localiser avec précision. Il se peut toutefois que vous deviez ajouter des étapes de segmentation et de mesure si votre zone de recherche initiale est plus grande.

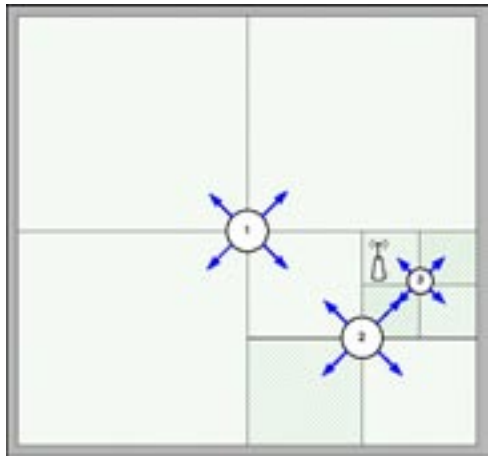

Figure 8 - Schéma de recherche de la méthode par vecteur

Comparaison des méthodes

Dans notre exemple, le nombre de segmentations et de mesures est identique pour chaque méthode. Il devrait vous apparaître évident que la méthode par convergence requiert davantage de déplacements. En effet, il vous faut parcourir la zone de recherche d'un coin à l'autre pour effectuer les mesures. Or, ces déplacements ralentissent la procédure de détection des points d'accès non autorisés. La différence entre les deux méthodes est encore plus marquée si vous effectuez la recherche dans une infrastructure répartie sur plusieurs étages. Par exemple, vous pensez qu'il y a un point d'accès au deuxième étage d'un immeuble qui en compte quatre. Vous utilisez la méthode de recherche par convergence et vous déduisez l'emplacement du point d'accès en fonction de l'intensité du signal la plus élevée. Cependant, vous ne trouvez pas le point d'accès. La faute aux résultats mesurés ? Non, le point d'accès se trouve peut-être à un autre étage. Par ailleurs, la méthode par vecteur vous permettrait de faire pivoter l'antenne de ± 180° à la verticale et d'identifier l'étage où se trouve le point d'accès non autorisé.

	Méthode de recherche par convergence	Méthode de recherche par vecteur
Outils requis	Carte radio pour réseau local (LAN) sans fil avec antenne omnidirectionnelle intégrée, outil de mesure de l'intensité du signal RF	Antenne unidirectionnelle (externe), carte radio pour réseau local (LAN) sans fil avec connecteur pour antenne, outil de mesure de l'intensité du signal RF
Avantages	Utilisation des types d'antenne et de carte radio les plus courants	Moins de déplacements, localisation plus rapide, recherche sur les axes vertical et horizontal, ce qui facilite les recherches en trois dimensions
Inconvénients	Plus de déplacements, durée de localisation plus longue, moins appropriée aux recherches sur plusieurs étages	Carte radio et antenne spéciales, généralement plus coûteuses

Considérations pratiques

Dans la pratique, il est fort probable que vous deviez modifier les zones de recherche pour prendre en compte les espaces qui se situent en dehors du rectangle et la présence des murs, des cloisons et autres obstacles. Veillez à maintenir l'antenne à une hauteur constante lors de vos mesures. Placez l'antenne au-dessus des cloisons pour favoriser l'homogénéité des mesures. Lorsque vous recherchez des points d'accès, vous devez réfléchir en trois dimensions. Si vous ne disposez que d'une antenne omnidirectionnelle, l'échantillonnage de l'intensité du signal sur plusieurs étages devrait vous permettre de déduire à quel étage se trouve le point d'accès non autorisé. Lorsque vous effectuez des mesures par vecteur, essayez de ne pas déplacer les autres objets à proximité (unité de test par exemple) et de ne pas trop bouger pendant que vous faites pivoter l'antenne. Nous conseillons de monter l'antenne directionnelle sur l'outil de mesure de l'intensité du signal (qu'il s'agisse d'un logiciel ou d'un instrument portatif) et de faire pivoter la plate-forme de mesure entière plutôt que de faire pivoter uniquement l'antenne. Vous pouvez vous exercer avec un point d'accès connu pour vous familiariser avec ces techniques de localisation et tester la sensibilité de votre outil aux changements de distance avec le point d'accès, de hauteur de l'antenne et d'orientation de l'antenne, s'il s'agit d'une antenne unidirectionnelle. Remarquez que les structures métalliques (cloisons en métal, postes de travail modulaires à ossature métallique, stores à enroulement automatique) peuvent altérer les mesures, particulièrement lorsque l'intensité du signal est faible. Cette prise de conscience des particularités de votre environnement devrait accélérer la détection des points d'accès le cas échéant.

Restez vigilants

Pour garantir la sécurité de votre réseau, formez vos employés sur les risques associés à l'installation de points d'accès non autorisés. Mettez à jour les stratégies de votre entreprise en ce sens. Utilisez un système d'accès réseau rigoureux tel qu'un système IEEE 802.1X. Effectuez des audits de sécurité à intervalles réguliers, aux endroits où vous recherchez des périphériques sans fil non autorisés et non protégés, pour identifier les menaces. Lorsque vous identifiez un point d'accès non autorisé, localisez-le rapidement pour vous débarrasser de cette faille de sécurité qui menace votre réseau. Par le respect des meilleures pratiques en termes de sécurité des réseaux sans fil, vous pouvez vraiment minimiser les risques.

A propos de Fluke Networks

Fluke Networks fournit des solutions novatrices destinées à l'installation et à la certification ainsi qu'au test, à l'analyse et au contrôle des réseaux cuivre, fibre optique et sans fil utilisés par des entreprises et des opérateurs de télécommunications. La gamme complète de solutions Network SuperVision™ de Fluke Networks propose aux propriétaires, aux installateurs et aux administrateurs de réseaux des solutions de qualité supérieure associant vitesse, précision et simplicité d'utilisation, pour des performances réseau optimales. Pour en savoir plus sur l'assistant réseau EtherScope Series II et ses fonctionnalités d'analyse des réseaux locaux (LAN) sans fil 802.11a/b/g et de détection des points d'accès non autorisés, rendez-vous sur notre site Web à la page **www.flukenetworks.com/etherscope**.

Références

CARR, Joseph J., Directional or Omnidirectional Antenna?, Universal Radio Research

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks est présent dans plus de 50 pays.
Pour connaître les coordonnées du bureau le plus proche, rendez-vous à l'adresse **www.flukenetworks.com/contact**.

Imprimé aux États-Unis. 6/2007 2804954 H-FRN-N Rév. B