Détection de systèmes indésirables sous des réseaux sans fil unifiés

Contenu

Introduction

Les réseaux sans fil étendent les réseaux filaires et augmentent la productivité des travailleurs et l'accès aux informations. Cependant, un réseau sans fil non autorisé représente un souci supplémentaire de couche de sécurité. La sécurité du port sur les réseaux filaires est moins mise de l'avant, et les réseaux sans fil sont une extension facile aux réseaux filaires. Par conséquent, un employé qui amène son propre point d'accès Cisco (AP) dans une infrastructure sans fil bien-sécurisée ou une infrastructure filaire et permet l'accès d'utilisateurs non autorisés à ce réseau autrement sécurisé peut facilement compromettre un réseau sécurisé.

La détection escroc permet à l'administrateur réseau pour surveiller et éliminer ce problème de sécurité. Le Network Architecture de Cisco Unified fournit deux méthodes de détection escroc qui activent une solution escroc complète d'identification et de retenue sans besoin de cher et dur-à-justifient des réseaux et des outils de substitution.

Vue d'ensemble des fonctionnalités

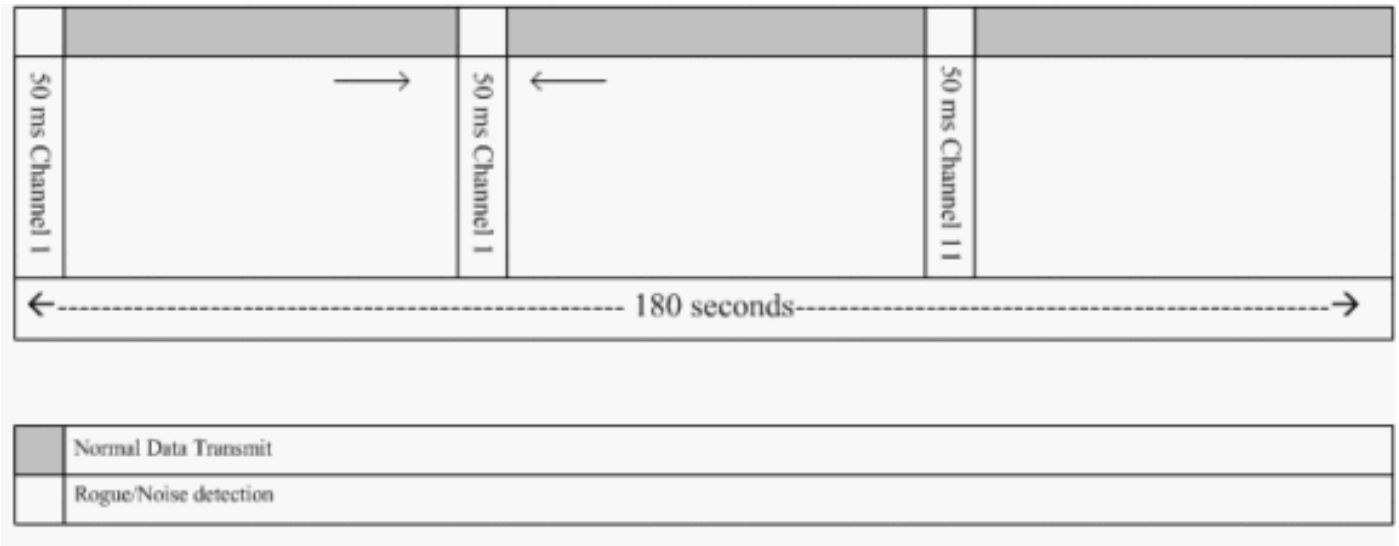
La détection escroc n'est liée par aucune réglementation et aucun respect juridique n'est exigé pour son exécution. Cependant, la retenue escroc introduit habituellement les questions juridiques qui peuvent mettre le fournisseur d'infrastructure dans une position inconfortable si parti pour fonctionner automatiquement. Cisco est extrêmement sensible à de telles questions et fournit ces solutions. Chaque contrôleur est configuré avec un nom de groupe rf. Une fois qu'AP léger s'inscrit à un contrôleur, il inclut un **élément d'informations d'authentification (IE)** qui est spécifique au groupe configuré rf sur le contrôleur dans toutes ses balises/trames réponse de sonde. Quand AP léger entend des balises sonder des trames de réponse d'AP sans cet **IE** ou avec l'**IE faux**, alors les états légers AP qu'AP en tant qu'escroc, enregistre son BSSID dans une table escroc, et envoie la table au contrôleur. Il y a deux méthodes, à savoir le Discovery Protocol escroc

d'emplacement (RLDP) et l'exécution passive, qui sont expliquées en détail ; voyez la section active d'escrocs de détermination.

Détection escroc d'infrastructure

La détection escroc dans un environnement sans fil actif peut être coûteuse. Ce processus demande à AP en service (ou le mode local) de cesser le service, d'écouter le bruit, et d'exécuter la détection escroc. L'administrateur réseau configure les canaux pour balayer, et configure le délai prévu l'où toutes les stations sont balayées. AP écoute 50 ms pour les balises escrocs de client, puis revient au canal configuré afin d'entretenir des clients de nouveau. Cette lecture active, combinée avec les messages voisins, identifie quels aps sont des escrocs et quels aps sont valides et une partie du réseau. Afin de configurer les canaux balayés et le délai prévu de lecture, parcourez à la **radio > au réseau 802.11b/g** (« **b/g** » ou « **a** » selon la spécification du réseau) et sélectionnez le bouton d'**Auto RF** dans le coin droit supérieur de la fenêtre du navigateur.

Vous pouvez faire descendre l'écran pour **ébruiter/des canaux de surveillance d'interférence/escroc** afin de configurer les canaux à balayer pour des escrocs et le bruit. Les choix disponibles sont : Tout le) des canaux (1 à 14, les canaux de pays (1 à 11) ou les canaux dynamiques de l'association de la Manche (DCA) (par défaut 1, 6 et 11). Le délai prévu de lecture par ces canaux peut être configuré dans la même fenêtre, sous des **intervalles de moniteur (60 à 3600 sec)** avec l'intervalle de mesure de bruit. Par défaut, l'intervalle de écoute pour le bruit de hors fonction-canal et les escrocs est de 180 secondes. Ceci signifie que chaque canal est balayé toutes les 180 secondes. C'est un exemple des canaux DCA qui sont balayés toutes les 180 secondes :



Comme illustré, un nombre élevé de canaux configurés pour être balayé a combiné avec les intervalles courts de lecture, laisse moins d'heure pour les clients de manuel de base AP réellement.

Les attentes légères AP afin d'étiqueter des clients et des aps comme escrocs parce que ces escrocs ne sont pas probablement signalés par un autre AP jusqu'à ce qu'un autre cycle soit terminé. Même AP se déplace au même canal de nouveau afin de surveiller pour l'escroc aps et les clients, aussi bien que le bruit et l'interférence. Si les mêmes clients et/ou aps sont détectés, ils sont répertoriés comme escrocs sur le contrôleur de nouveau. Le contrôleur commence maintenant à déterminer si ces escrocs sont reliés au réseau local ou simplement à AP voisin. Dans l'un ou l'autre de cas, AP qui n'est pas une partie du réseau Sans fil local géré est considéré un escroc.

Détails escrocs

AP léger va le hors fonction-canal pour 50 ms afin d'écouter les clients escrocs, le moniteur pour le bruit, et l'interférence de canal. Tous les clients ou aps escrocs détectés sont envoyés au contrôleur, qui recueille ces informations :

- L'adresse MAC de l'escroc AP
- Le nom de l'escroc AP
- L'adresse MAC de clients connectée par escroc
- Si les trames sont protégées avec le WPA ou le WEP
- Le préambule
- Le rapport signal/bruit (SNR)
- L'indicateur de force du signal de récepteur (RSSI)

Point d'accès escroc de détecteur

Vous pouvez faire AP opérer comme détecteur escroc, qui le permet à placer sur un port de joncteur réseau de sorte qu'il puisse entendre tous les VLAN connectés parside. Il poursuit pour trouver le client sur le sous-réseau de câble sur tous les VLAN. Le détecteur escroc AP écoute des paquets de Protocole ARP (Address Resolution Protocol) afin de déterminer les adresses de la couche 2 des clients ou de l'escroc escrocs identifiés aps envoyés par le contrôleur. Si une adresse de la couche 2 qui s'assortit est trouvée, le contrôleur génère une alarme qui identifie l'escroc AP ou le client comme menace. Cette alarme indique que l'escroc a été vu sur le réseau câblé.

Déterminez les escrocs actifs

Des aps escrocs doivent « être vus » deux fois avant qu'ils soient ajoutés en tant qu'escroc par le contrôleur. Des aps escrocs ne sont pas considérés une menace s'ils ne sont pas connectés au segment de câble du réseau d'entreprise. Afin de déterminer si l'escroc est des approches actives et diverses sont utilisés. Ces approches incluent RLDP.

Discovery Protocol escroc d'emplacement (RLDP)

RLDP est une approche active, qui est utilisée quand AP escroc n'a aucune authentification (authentification ouverte) configurée. Ce mode, qui est désactivé par défaut, demande à AP actif pour se déplacer au canal escroc et pour se connecter à l'escroc en tant que client. Pendant ce temps, AP actif envoie des messages de deauthentication à tous les clients connectés et a puis arrêté l'interface par radio. Puis, il s'associera à l'escroc AP en tant que client.

Les essais AP puis pour obtenir une adresse IP de l'escroc AP et en avant d'un paquet de Protocole UDP (User Datagram Protocol) (port 6352) qui contient les gens du pays AP et les informations de connexion escrocs au contrôleur par l'escroc AP. Si le contrôleur reçoit ce paquet, l'alarme est placée pour informer l'administrateur réseau qu'un escroc AP a été découvert sur le réseau câblé avec la configuration RLDP.

Remarque: Employez la commande d'**enable de rldp de debug dot11** afin de vérifier si AP léger associe et reçoit une adresse DHCP de l'escroc AP. Cette commande affiche également le paquet UDP envoyé par AP léger au contrôleur.

Un échantillon d'un paquet d'UDP (destination port 6352) envoyé par AP léger est affiché ici :

```
0020 0a 01 01 0d 0a 01 ....... (. * ..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
..... x ......... 0040 00 00 00 00 00 00 00 00 00 00
```

Les 5 premiers octets des données contiennent l'adresse DHCP indiquée au mode local AP par l'escroc AP. Les 5 prochains octets sont l'adresse IP du contrôleur, suivie de 6 octets qui représentent l'adresse MAC de l'escroc AP. Puis, il y a 18 octets de zéros.

Exécution passive :

Cette approche est utilisée quand AP escroc a une certaine forme d'authentification, WEP ou WPA. Quand une forme d'authentification est configurée sur l'escroc AP, AP léger ne peut pas s'associer parce qu'il ne connaît pas le clé configuré sur l'escroc AP. Le processus commence par le contrôleur quand il transmet la liste d'adresses MAC escrocs de client à AP qui est configuré comme détecteur escroc. Le détecteur escroc balaye tous les sous-réseaux connectés et configurés pour des demandes d'ARP, et l'ARP recherche une adresse assortie de la couche 2. Si une correspondance est découverte, le contrôleur informe l'administrateur réseau qu'un escroc est détecté sur le sous-réseau de câble.

Retenue escroc d'Active

Une fois un client escroc est détecté sur le réseau câblé, l'administrateur réseau peut contenir l'escroc AP et les clients escrocs. Ceci peut être réalisé parce que des paquets de désauthentification de 802.11 sont envoyés aux clients qui sont associés pour débarrasser des plants peu vigoureux des aps de sorte que la menace qu'un tel trou crée soit atténuée. Chaque fois que il y a une tentative de contenir l'escroc AP, presque 15% de la ressource d'AP léger est utilisé. Par conséquent, on lui suggère physiquement de localiser et retirer l'escroc AP une fois qu'il est contenu.

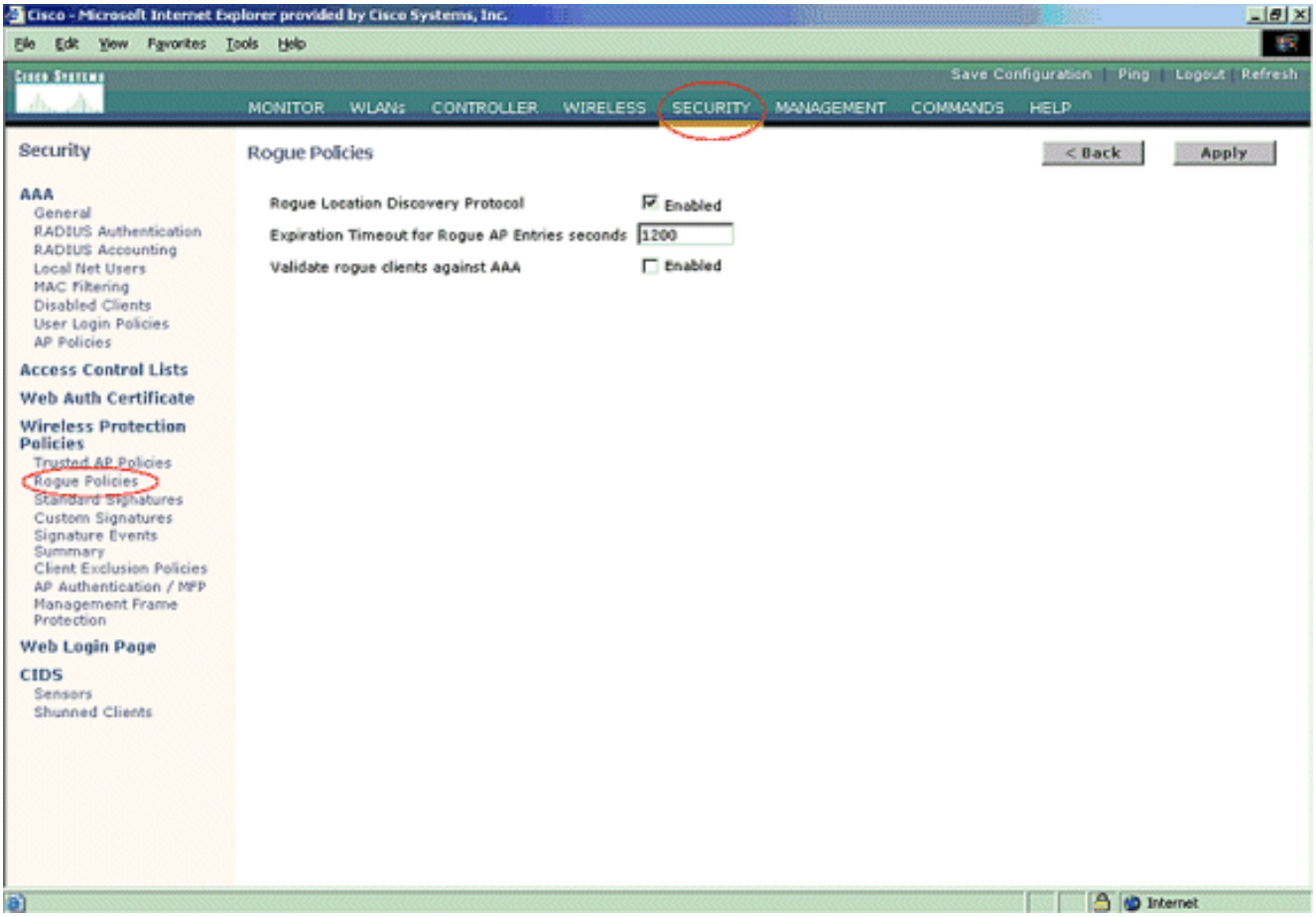
Remarque: Du WLC libérez 5.2.157.0, une fois que le fard à joues t'est détecté peut maintenant choisir contenir à manuellement ou automatiquement l'escroc détecté. Dans des versions de logiciel de logiciel contrôleur avant 5.2.157.0, la retenue manuelle est la seule option.

Détection escroc – Étapes de configuration

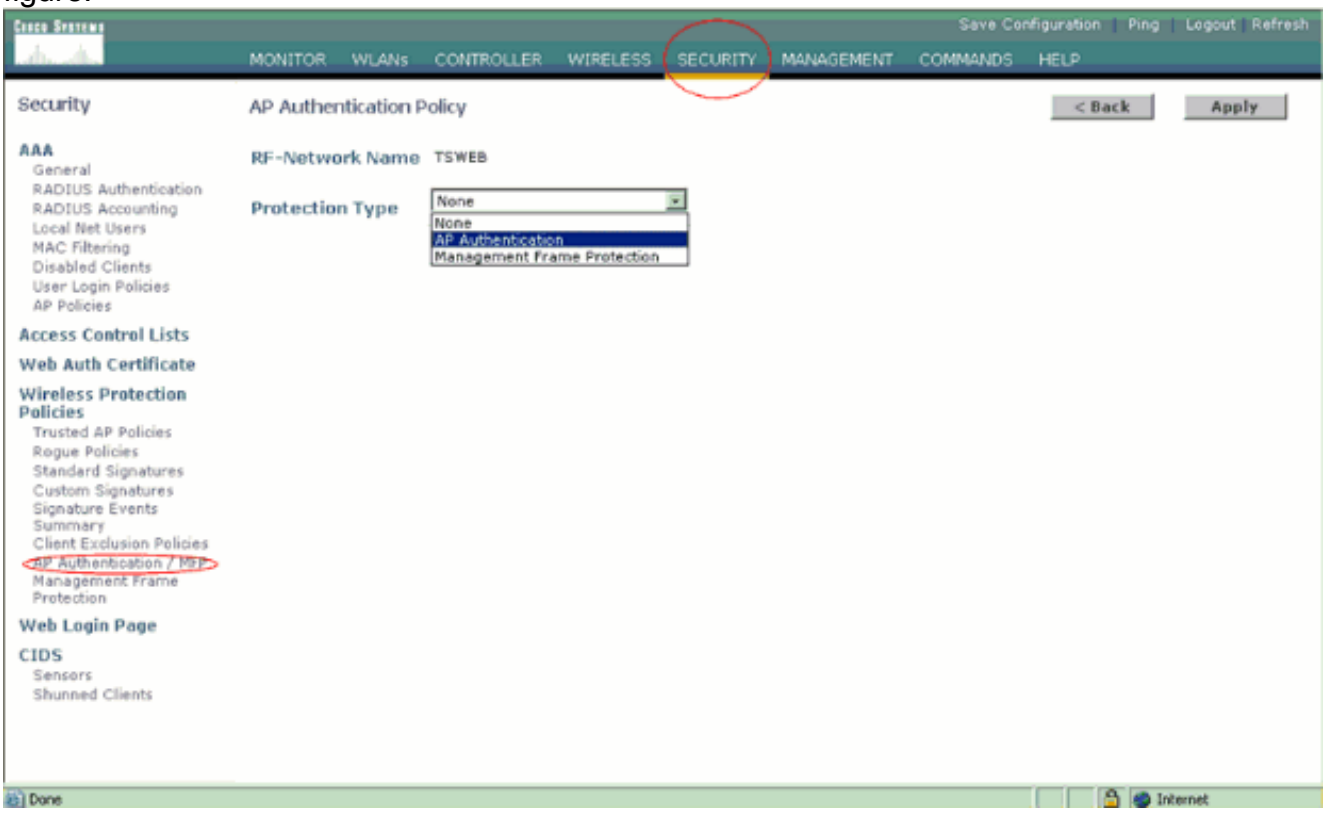
Presque la configuration escroc entière de détection est activée par défaut tenir compte de maximiser, sécurité des réseaux de sortie de la boîte. Ces étapes de configuration supposent qu'aucune détection escroc n'est installée sur le contrôleur afin de clarifier les importantes informations escrocs de détection.

Afin d'installer la détection escroc, terminez-vous ces étapes :

1. Assurez-vous que le protocole de détection d'emplacement d'escroc est activé. Afin de l'allumer, choisir la **Sécurité > les stratégies d'escroc** et cliquer sur **a activé** sur le **Discovery Protocol escroc d'emplacement** suivant les indications de la figure.**Remarque:** Si un escroc AP n'est pas entendu pendant une heure, c'est forme retirée le contrôleur. C'est le **délai d'attente d'expiration** pour un escroc AP, qui est configuré au-dessous de l'option RLDP.

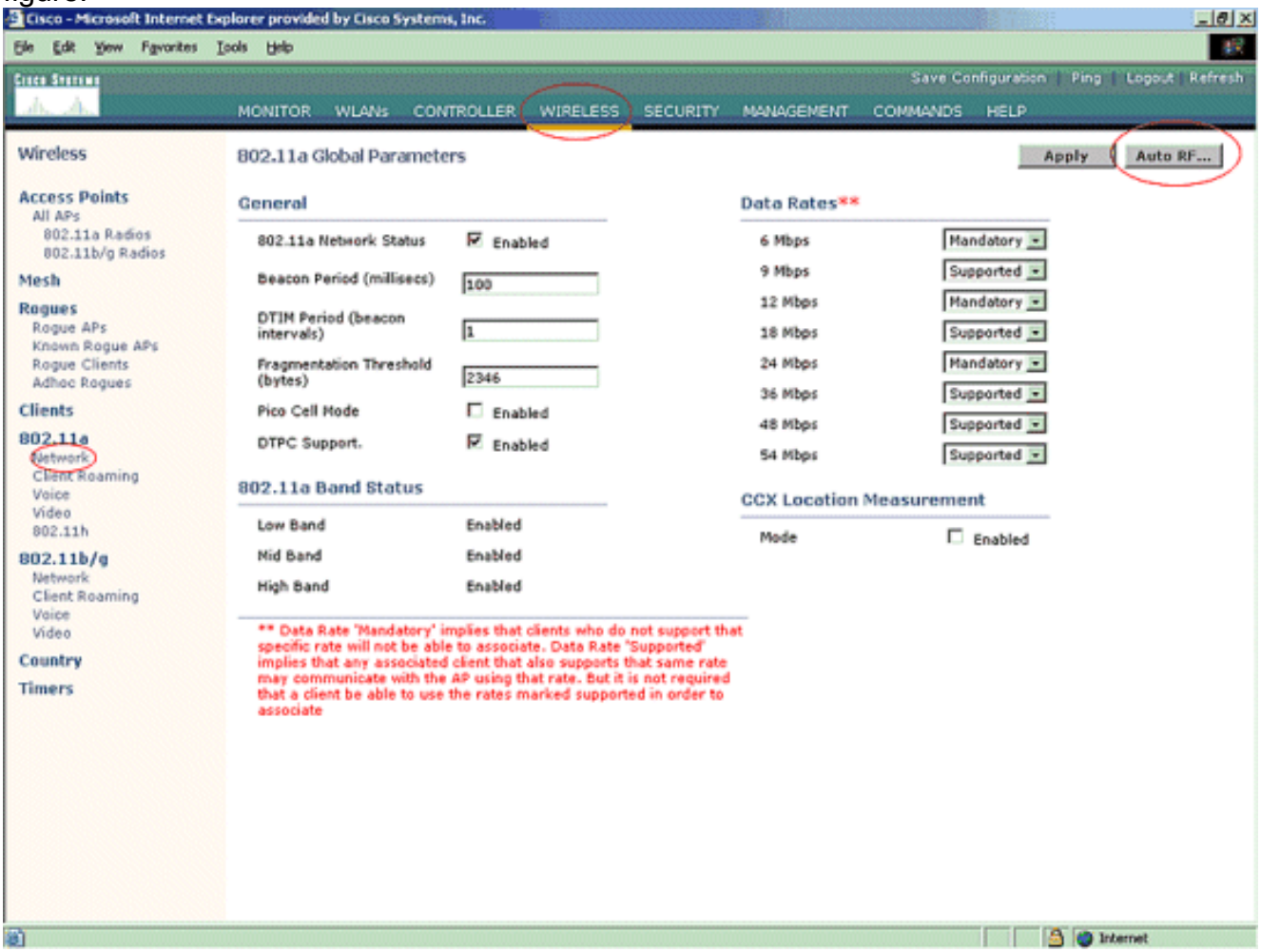


2. C'est une étape facultative. Quand cette caractéristique est activée, les aps envoyant à RRM les paquets voisins avec différents noms de **groupe rf** sont signalés comme escrocs. Ce sera utile en étudiant votre environnement rf. Afin de l'activer, choisissez l'**authentification de Security-> AP**. Puis, choisissez l'**authentification AP** comme type de protection suivant les indications de la
figure.

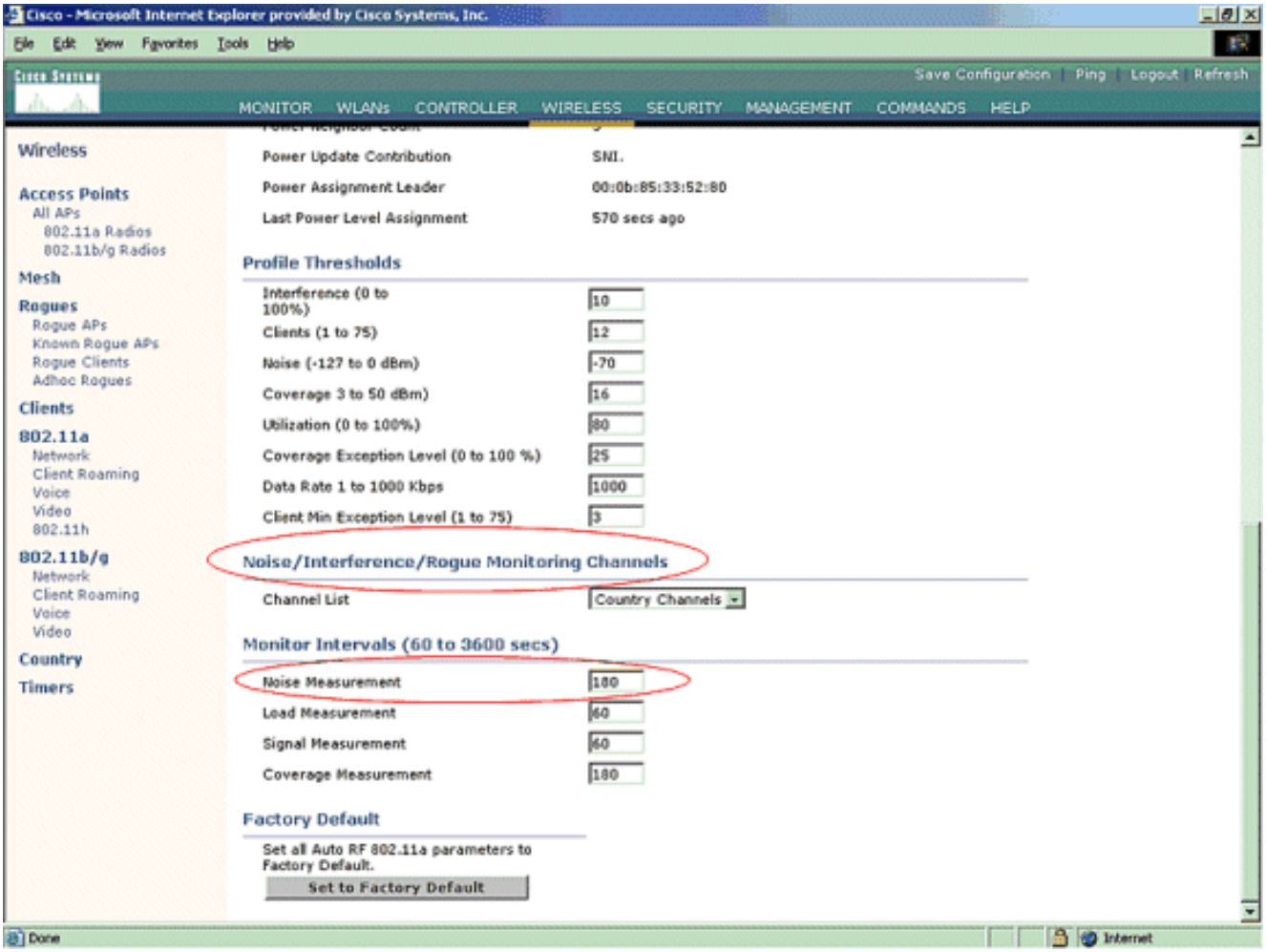


3. Vérifiez les canaux à balayer dans ces étapes :**Radio > réseau 802.11a** choisis, puis **Auto**

RF dans le côté droit suivant les indications de la figure.



Àla page d'**Auto RF**, faites descendre l'écran et choisissez les **canaux de surveillance de bruit/interférence/escroc**.



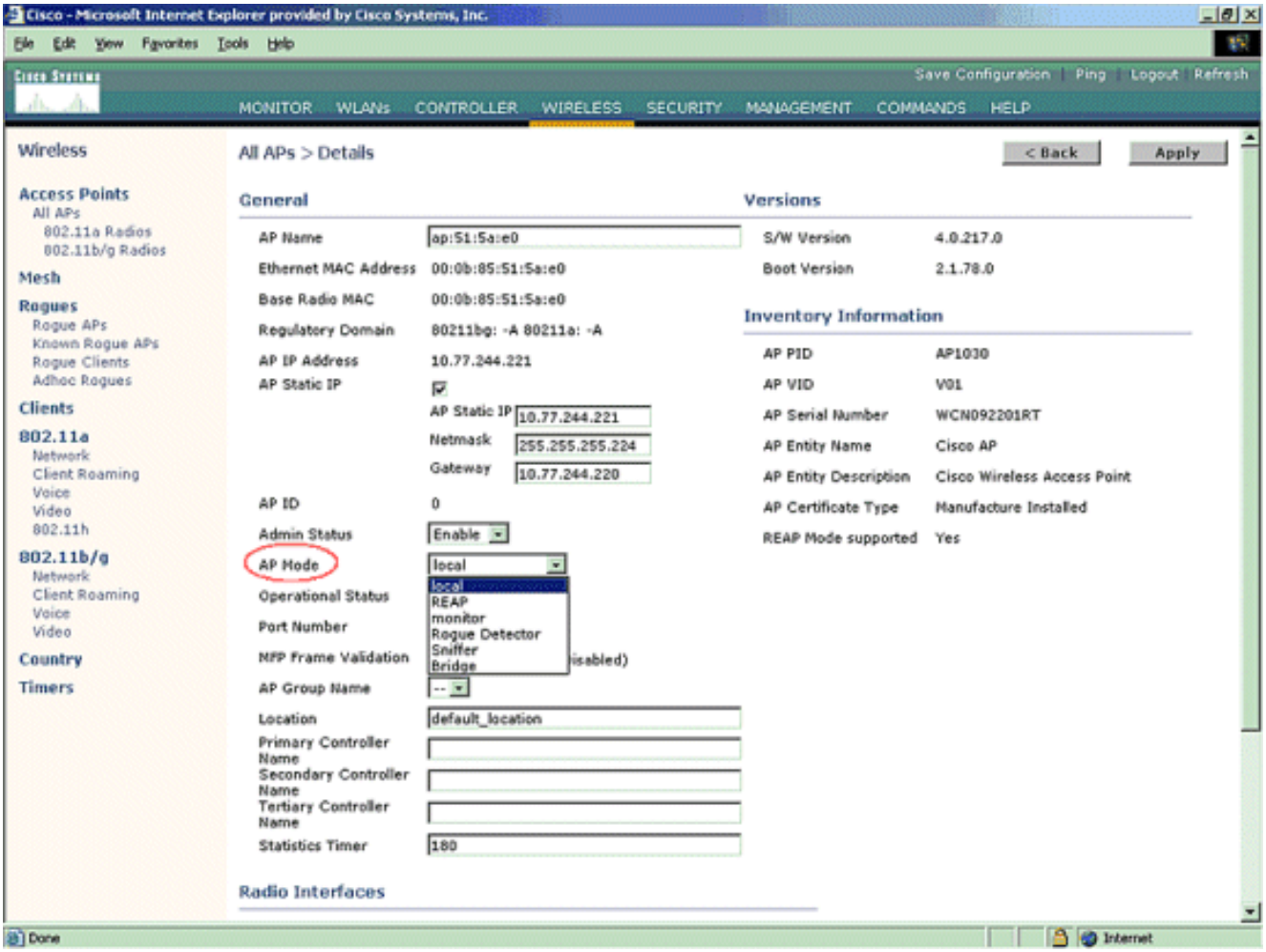
La liste de la Manche détaille les canaux à balayer pour la surveillance escroc, en plus de l'autre contrôleur et des fonctions AP. Référez-vous à la Foire aux questions de point d'accès léger pour plus d'informations sur des aps légers, et le contrôleur LAN Sans fil (WLC) dépannent la Foire aux questions pour plus d'informations sur des contrôleurs sans-fil.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Fixez le délai prévu pour balayer les canaux sélectionnés :La durée de lecture du groupe défini de canaux est configurée sous des **intervalles de moniteur > la mesure de bruit**, et la plage permise est de 60 à 3600 secondes. Si parti au par défaut de 180 secondes, les aps balayent chaque canal au groupe de canaux une fois, pour 50 ms, toutes les 180 secondes. Au cours de cette période, les modifications de radio AP de son canal de service au canal spécifié, écoute et enregistre des valeurs pendant une période de 50 ms, et puis revient au canal d'origine. Le temps de saut plus le temps de pause de 50 ms prend le hors fonction-canal AP pour approximativement 60 ms chaque fois. Ceci signifie que chaque AP passe approximativement 840 ms du total 180 secondes écoutant des escrocs.« Écoutez » ou le

temps de « angle de saturation » ne peut pas être modifié et n'est pas changé avec un réglage de la valeur de mesure de bruit. Si le temporisateur de mesure de bruit est diminué, le processus de découverte escroc est susceptible de trouver plus d'escrocs et de les trouver plus rapidement. Cependant, cette amélioration est livré aux dépens de l'intégrité des données et du service clientèle. Une valeur supérieure, d'autre part, tient compte d'une meilleure intégrité des données mais diminue la capacité de trouver des escrocs rapidement.

5. Configurez le mode de fonctionnement AP :Un mode de fonctionnement léger AP définit le rôle d'AP. Les modes liés aux informations présentées dans ce document sont :**Gens du pays** — C'est le fonctionnement normal d'AP. Ce mode permet des clients de données à entretenir tandis que des canaux configurés sont balayés pour le bruit et les escrocs. Dans ce mode de fonctionnement, AP disparaît le hors fonction-canal pour 50 ms et écoute des escrocs. Il fait un cycle par chaque canal, un par un, pour la période spécifiée sous la configuration d'Auto RF.**Moniteur** — C'est le mode uniquement récepteur par radio, et permet à AP pour balayer le tout configuré creuse des rigoles toutes les 12 secondes. Seulement des paquets de désauthentification sont introduits l'air avec AP ont configuré de cette façon. Un mode moniteur AP peut détecter des escrocs, mais il ne peut pas se connecter à un escroc méfiant car un client afin d'envoyer les paquets RLDP.**Remarque:** Le DCA se rapporte aux canaux non-recouverts qui sont configurables avec les modes par défaut.**Détecteur escroc** — En ce mode, la radio AP est arrêtée, et AP écoute le trafic de câble seulement. Le contrôleur passe les aps configurés en tant que les détecteurs escrocs aussi bien que listes de clients escrocs suspectés et d'adresses MAC AP. Le détecteur escroc écoute des paquets d'ARP seulement, et peut être connecté à tous les domaines d'émission par une liaison agrégée si désiré.Vous pouvez configurer un mode individuel AP simplement, une fois qu'AP léger est connecté au contrôleur. Afin de changer le mode AP, connectez à l'interface web de contrôleur et naviguez vers la **radio**. Cliquez sur en fonction les **détails** à côté d'AP désiré à afin d'afficher un écran semblable à celui-ci
:



Employez le menu déroulant de mode AP afin de sélectionner le mode de fonctionnement désiré AP.

Dépannage des commandes

Vous pouvez également employer ces commandes afin de dépanner votre configuration sur AP :

- **show rogue ap summary** — Cette commande affiche la liste de l'escroc aps détecté par les aps légers.
- **show rogue ap detailed** *< adresse MAC de l'ap> escroc* — employez cette commande afin de visualiser des détails au sujet d'un escroc individuel AP. C'est la commande qui aide à déterminer si l'escroc AP est branché sur le réseau câblé.

Conclusion

La détection escroc et la retenue dans la solution de contrôleur centralisée par Cisco est la méthode la plus efficace et moins la plus intrusive dans le secteur. La flexibilité fournie à l'administrateur réseau tient compte d'une adaptation plus personnalisée qui peut faciliter toutes les spécifications du réseau.

Informations connexes

- Aperçu des groupes rf

- Support et documentation techniques - Cisco Systems