Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP

Contenu

Introduction

Ce document explique comment configurer un Integrated Services Router de gamme Cisco 870 (ISR) pour la Connectivité Sans fil réseau local avec le chiffrement WEP et SAUTER l'authentification.

La même configuration applique à n'importe quelle autres gamme de Cisco ISR modèles Sans fil.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer les paramètres de base de la gamme Cisco 870 ISR.
- La connaissance de la façon configurer l'adaptateur client sans fil 802.11a/b/g utilisant Aironet Desktop Utility (ADU).

Référez-vous aux adaptateurs client LAN sans fil de Cisco Aironet 802.11a/b/g (CB21AG et PI21AG) guide d'installation et de configuration, version 2.5 pour les informations sur la façon dont configurer l'adaptateur du client 802.11a/b/g.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

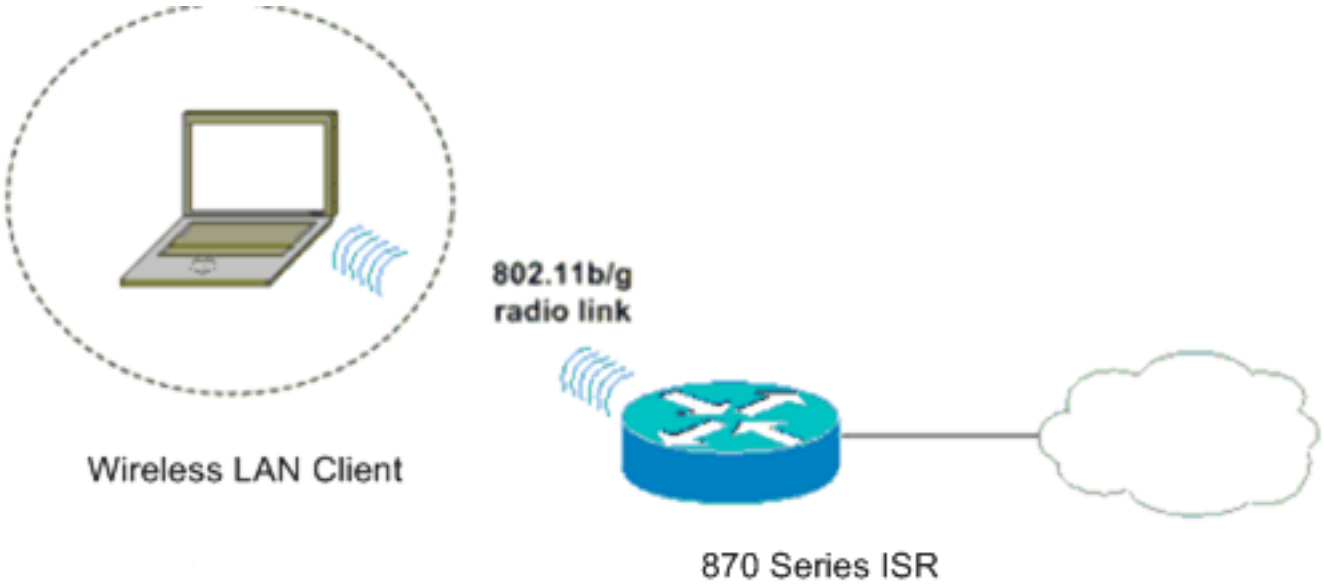
- Cisco 871W ISR qui exécute la version de logiciel 12.3(8)YI1 de Cisco IOS®
- Ordinateur portable avec la version 2.5 d'Aironet Desktop Utility
- adaptateur de client du 802.11 a/b/g qui exécute la version 2.5 de micrologiciels

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce document utilise cette configuration du réseau.

Dans cette installation, le client Sans fil de RÉSEAU LOCAL s'associe avec le routeur 870. Le serveur interne du protocole DHCP (DHCP) sur le routeur 870 est utilisé pour fournir une adresse IP aux clients sans fil. Le cryptage WEP est activé sur les 870 ISR et le client WLAN. L'authentification de LEAP est utilisée pour authentifier les utilisateurs de sans fil et la caractéristique locale de serveur de RAYON sur le routeur 870 est utilisée pour valider les qualifications.



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

configuration de routeur 871W

Terminez-vous ces étapes pour configurer le 871W ISR comme Point d'accès pour recevoir des demandes d'association des clients sans fil.

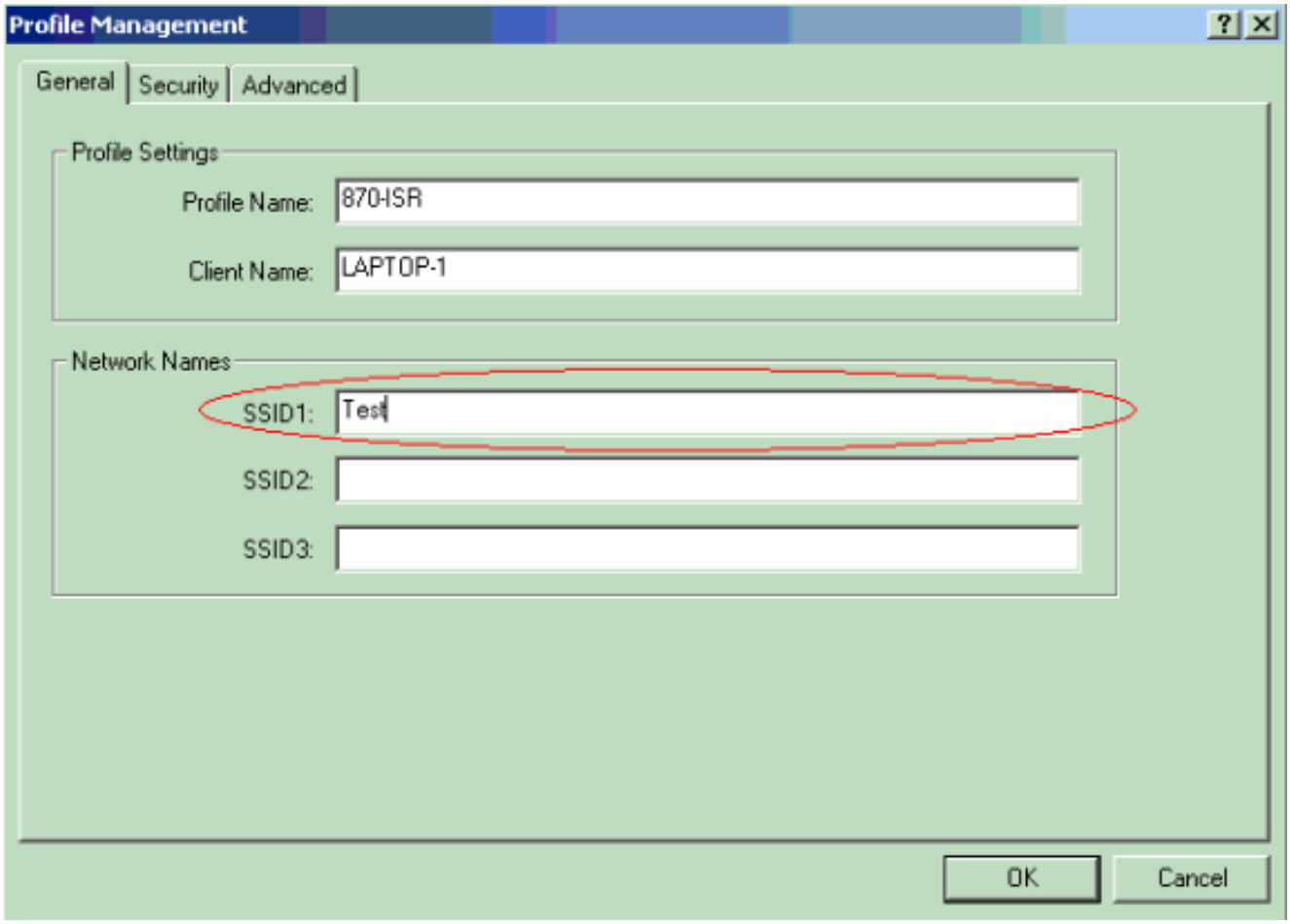
1. Configurez le Routage et mise en parallèle intégrés (IRB) et installez le groupe de passerelle.Introduisez ces commandes de mode de configuration globale afin d'activer IRB.`WirelessRouter<config>#bridge irb !--- Enables IRB. WirelessRouter<config>#bridge 1 protocol ieee !--- Defines the type of Spanning Tree Protocol as ieee. WirelessRouter<config>#bridge 1 route ip !--- Enables the routing of the specified protocol in a bridge group.`
2. Configurez l'interface virtuelle de pont (BVI).Assignez une adresse IP au BVI. Introduisez ces commandes de mode de configuration globale.`WirelessRouter<config>#interface bvi1 !--- Enter interface configuration mode for the BVI. WirelessRouter<config-if>#ip address 172.16.1.100 255.255.0.0` Référez-vous à la *configuration de groupe de passerelle sur la* section de *Points d'accès et de passerelles d'*utiliser des VLAN avec l'équipement sans fil de Cisco Aironet pour plus d'informations sur la fonctionnalité des groupes de passerelle aux Points d'accès.
3. Configurez la caractéristique interne de serveur DHCP sur le 871W ISR.La caractéristique interne de serveur DHCP sur le routeur peut être utilisée pour assigner des adresses IP aux clients sans fil qui s'associent au routeur. Terminez-vous ces commandes en mode de configuration globale.`WirelessRouter<config>#ip dhcp excluded-address 172.16.1.100 172.16.1.100 !--- Excludes IP addresses from the DHCP pool. !--- This address is used on the BVI interface, so it is excluded. WirelessRouter<config>#ip dhcp pool 870-ISR WirelessRouter<dhcp-config>#network 172.16.1.0 255.255.0.0` **Remarque:** L'adaptateur de client devrait également être configuré pour recevoir des adresses IP d'un serveur DHCP.
4. Configurez le 871W ISR en tant que serveur local de RAYON.En mode de configuration globale, introduisez ces commandes de configurer le 871W ISR en tant que serveur local de RAYON.`WirelessRouter<config>#aaa new-model !--- Enable the authentication, authorization, and accounting !--- (AAA) access control model. WirelessRouter<config>#radius-server local !--- Enables the 871 wireless-aware router as a local !--- authentication server and enters into configuration !--- mode for the authenticator. WirelessRouter<config-radsrv)#nas 172.16.1.100 key Cisco !--- Adds the 871 router to the list of devices that use !--- the local authentication server. WirelessRouter<config-radsrv>#user ABCD password ABCD WirelessRouter<config-radsrv)#user XYZ password XYZ !--- Configure two users ABCD and XYZ on the local RADIUS server. WirelessRouter<config-radsrv)#exit WirelessRouter<config>#radius-server host 172.16.1.100 auth-port 1812 acct-port 1813 key Cisco !--- Specifies the RADIUS server host.` **Remarque:** Utilisez les ports 1812 et 1813 pour l'authentification et expliquer le serveur local de RAYON.`WirelessRouter<config>#aaa group server radius rad_eap !--- Maps the RADIUS server to the group rad_eap . WirelessRouter<config-sg-radius>#server 172.16.1.100 auth-port 1812 acct-port 1813 !--- Define the server that falls in the group rad_eap. WirelessRouter<config>#aaa authentication login eap_methods group rad_eap !--- Enable AAA login authentication.`
5. Configurez l'interface par radio.La configuration de l'interface par radio implique la configuration de divers paramètres Sans fil sur le routeur comprenant le SSID, le mode de chiffrement, le type d'authentification, la vitesse, et le rôle du routeur Sans fil. Cet exemple utilise le **test** appelé par SSID.Introduisez ces commandes de configurer l'interface par radio en mode de configuration globale.`WirelessRouter<config>#interface dot11radio0 !--- Enter radio interface configuration mode. WirelessRouter<config-if>#ssid Test !--- Configure an SSID test. irelessRouter<config-ssid>#authentication open eap eap_methods WirelessRouter<config-ssid>#authentication network-eap eap_methods !--- Expect that users who attach to SSID 'Test' !--- are requesting authentication with the type 128 !--- Network Extensible Authentication Protocol (EAP) !--- authentication bit set in the headers of those requests. !--- Group these users into a group called 'eap_methods'. WirelessRouter<config-ssid>#exit !--- Exit interface configuration mode. WirelessRouter<config-if>#encryption mode wep mandatory !--- Enable WEP encryption. WirelessRouter<config-if>#encryption key 1 size 128 1234567890ABCDEF1234567890 !--- Define`

```
the 128-bit WEP encryption key. WirelessRouter<config-if>#bridge-group 1
WirelessRouter<config-if>#no shut !--- Enables the radio interface.
```
Le routeur 870 reçoit des demandes d'association des clients sans fil une fois que cette procédure est faite.Quand vous configurez le type d'authentification EAP sur le routeur, il est recommandé de choisir le **Network-EAP et de s'ouvrir avec l'EAP** comme types d'authentification afin d'éviter toutes les questions d'authentification.`WirelessRouter<config-ssid>#authentication network-eap eap_methods WirelessRouter<config-ssid>#authentication open eap eap_methods` **Remarque:** Ce document suppose que le réseau a seulement des clients sans fil de Cisco.**Remarque:** Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Configuration d'adaptateur de client

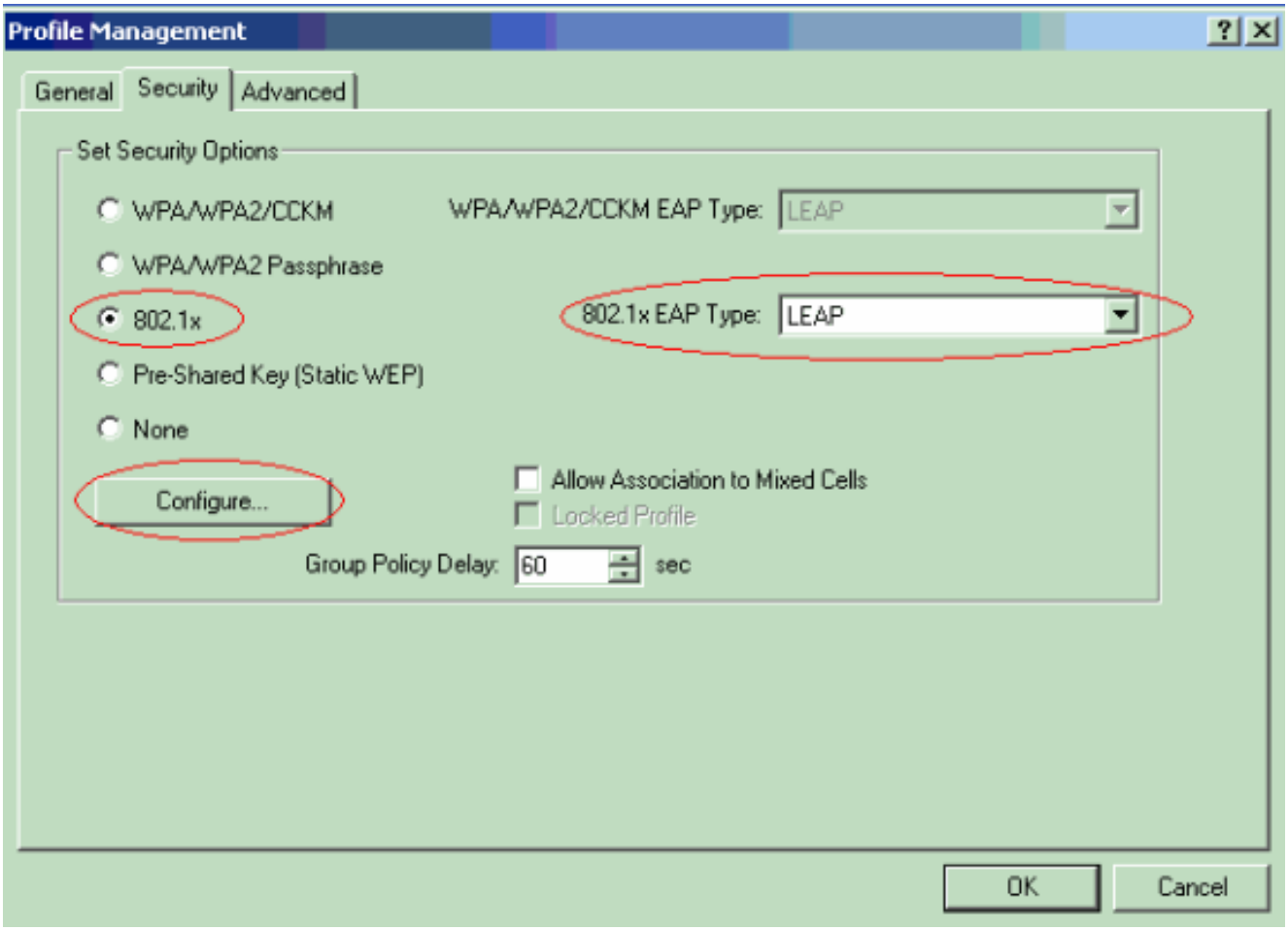
Terminez-vous ces étapes afin de configurer l'adaptateur de client. Cette procédure crée un nouveau profil appelé le **870-ISR** sur l'ADU, comme exemple. Cette procédure utilise également le test pendant que le SSID et les enables SAUTENT l'authentification sur l'adaptateur de client.

1. Cliquez sur New pour créer un nouveau profil dans la fenêtre Profile Management sur l'ADU. Écrivez le nom de profil et le SSID que l'adaptateur de client utilise sous l'onglet Général.Dans cet exemple, le nom de profil est **870-ISR** et le SSID est **test**.**Remarque:** Le SSID doit exactement apparier le SSID que vous avez configuré sur le 871W ISR. Le SSID distingue les majuscules et minuscules.

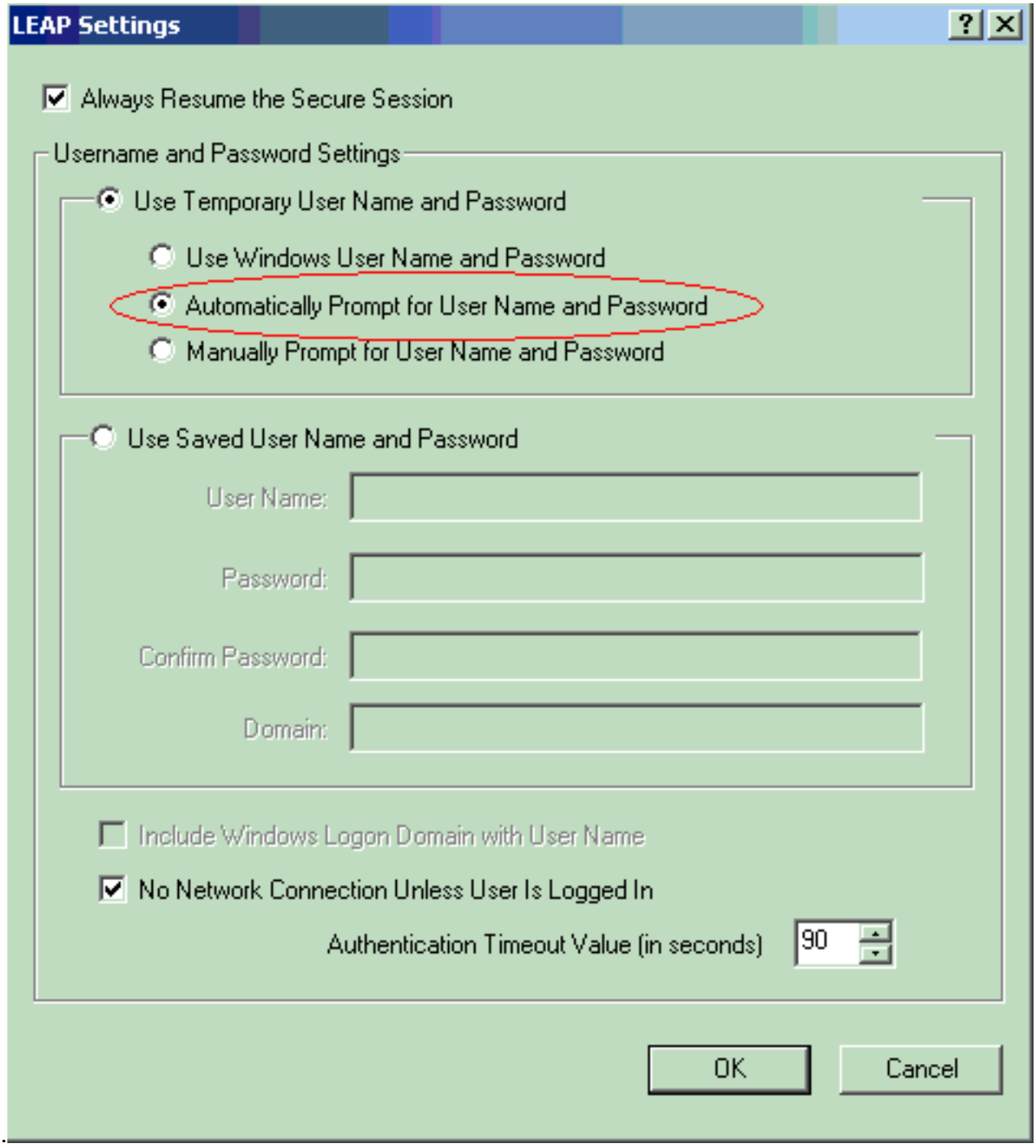


2. Allez à l'onglet Sécurité, sélectionnez le **802.1x** et choisissez le **LEAP du** menu Type d'EAP de 802.1x.Cette action active l'authentification de LEAP sur l'adaptateur de

client.

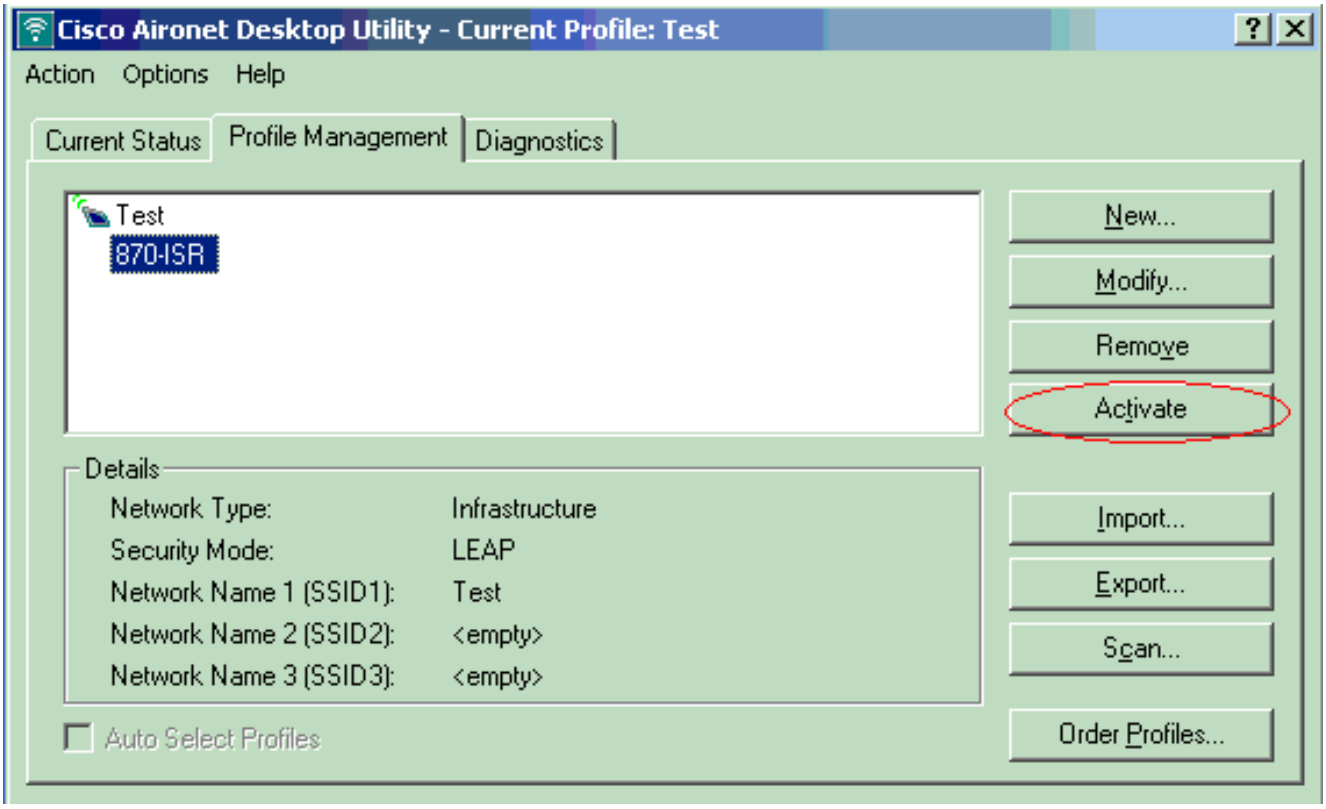


3. Cliquez sur Configure pour définir des configurations de LEAP.Cette configuration choisit l'**Automatically Prompt for Username and Password d'**option. Cette option vous permet de saisir manuellement le nom de l'utilisateur et le mot de passe quand l'authentification de LEAP a



lieu.

4. Cliquez sur OK pour quitter la fenêtre Profile Management.
5. Le clic **lancent** pour activer ce profil sur l'adaptateur de client.

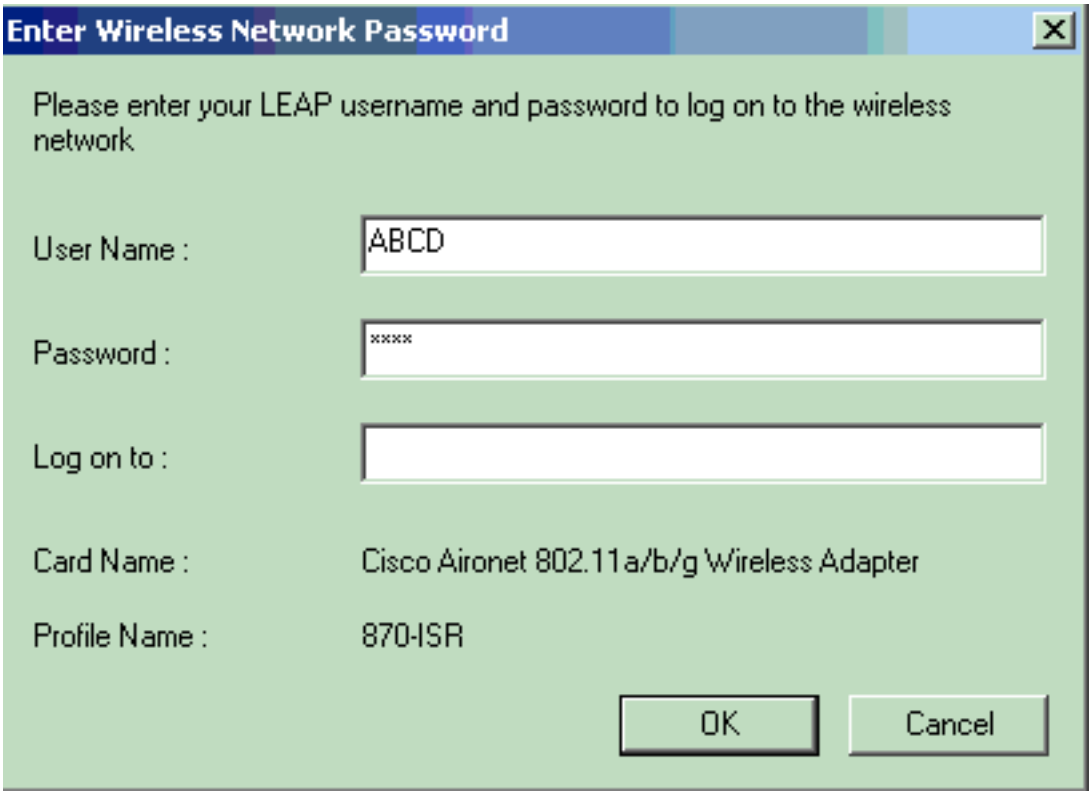


Vérifiez

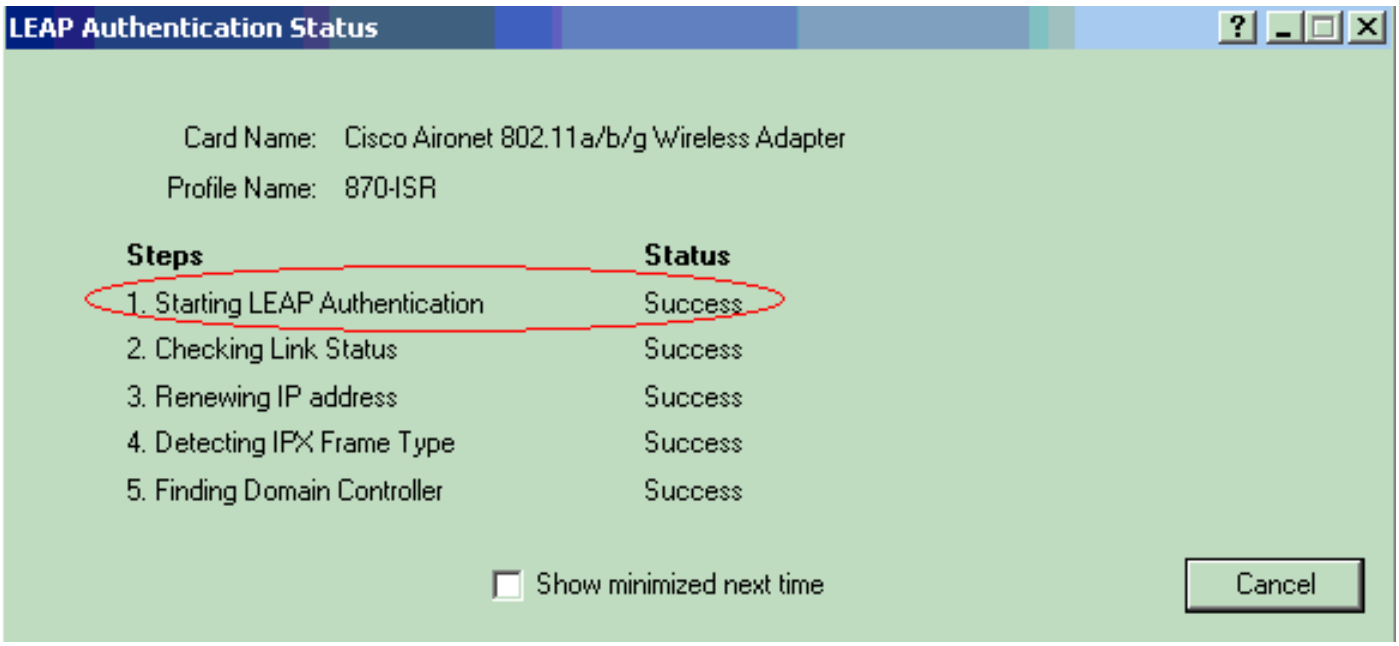
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Une fois l'adaptateur de client et le routeur 870 est configuré, lance le profil 870-ISR sur l'adaptateur de client pour vérifier la configuration.

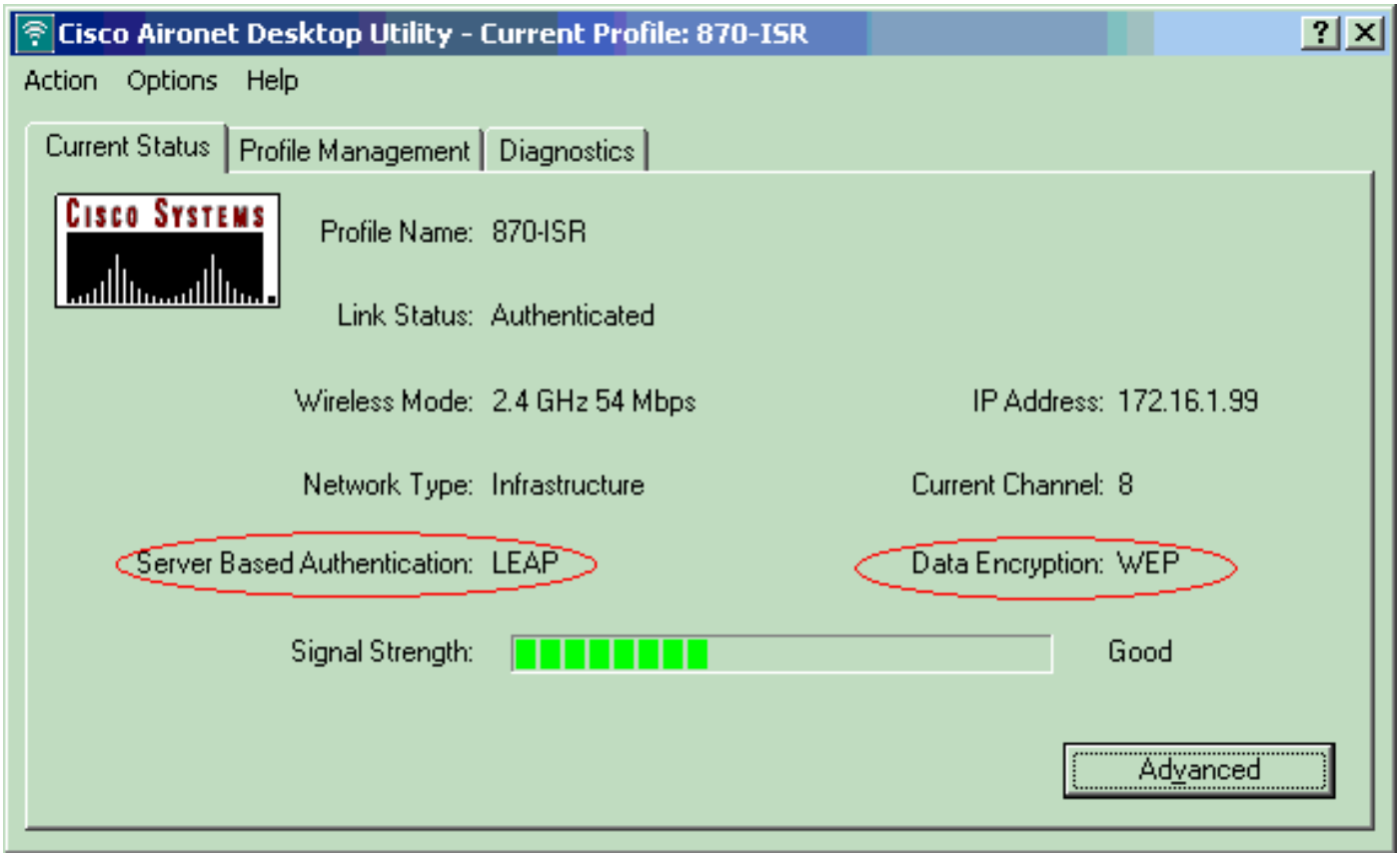
Entrez le nom d'utilisateur et le mot de passe quand les affichages de fenêtre d'Enter Wireless Network Password. Ceux-ci devraient correspondre à ceux configurés dans le 871W ISR. Un des profils utilisés dans cet exemple est le nom d'utilisateur **ABCD** et le mot de passe **ABCD**.



La fenêtre de LEAP Authentication Status apparaît. Cette fenêtre vérifie les identifiants utilisateurs contre le serveur local de RAYON.



Vérifiez l'état actuel ADU afin de vérifier que le client utilise le cryptage WEP et SAUTEZ l'authentification.



L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **affichez l'association dot11** — Vérifie la configuration sur le routeur 870.`WirelessRouter#`**`show dot11 association`** `802.11 Client Stations on Dot11Radio0: SSID [Test]: MAC Address IP Address Device Name Parent State 0040.96ac.dd05 172.16.1.99 CB21AG/PI21AG LAPTOP-1 self EAP-Associated Others: (not related to any ssid)`
- **show ip dhcp binding** — Vérifie que le client a une adresse IP par le serveur DHCP.`WirelessRouter#`**`show ip dhcp binding`** `Bindings from all pools not associated with VRF: IP address Client-ID/ Lease expiration Type Hardware address/ User name 172.16.1.99 0040.96ac.dd05 Feb 6 2006 10:11 PM Automatic`

Dépannez

Cette section fournit l'information de dépannage concernant cette configuration.

1. Placez la méthode sur le SSID **pour s'ouvrir** afin de désactiver temporairement l'authentification.Ceci élimine la possibilité de questions de Radiofréquence (RF) empêchant l'authentification réussie.N'utilisez l'**aucun eap_methods d'eap d'authentication open**, **aucun eap_methods d'authentication network-eap** et commandes d'**authentication open du** CLI.Si le client s'associe avec succès, alors le rf ne contribue pas au problème d'association
2. Vérifiez si les les clés WEP configurées sur le routeur Sans fil s'assortissent avec les clés WEP configurées sur les clients.S'il y a une non-concordance dans les clés WEP, les clients ne peuvent pas communiquer avec le routeur Sans fil.
3. Vérifiez que des mots de passe secret partagés sont synchronisés entre le routeur Sans fil et le serveur d'authentification.

Vous pouvez également utiliser ces commandes de débogage de dépanner votre configuration.

- **l'authentificateur de debug dot11 aaa** lance **entièrement l'**élimination des imperfections des paquets de MAC et d'authentification EAP.
- **authentification de debug radius** — Affiche les négociations de RAYON entre le serveur et le client.
- **paquets de debug radius local-server** — Affiche le contenu des paquets RADIUS qui sont envoyés et reçus.
- **client de debug radius local-server** — Affiche des messages d'erreur sur des authentifications client défectueuses.

Informations connexes

- Algorithmes de chiffrement et types d'authentification
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe via SDM
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe
- Cisco accèdent au guide de configuration de radio de routeur
- Exemple de configuration d'un routeur sans fil ISR 1800 avec DHCP interne et authentification ouverte
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems