Contenu

Introduction

Ce document décrit pourquoi le client ne peut pas s'associer à un Point d'accès (AP) dans ces conditions :

- Serveur de communication de Lightweight Extensible Authentication Protocol de passages (LEAP) /asynchronous (ACS).
- Le micrologiciel sur AP est mis à jour à 11.06 ou plus tard.
- Le micrologiciel sur le client est amélioré à la version 4.25.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version 4.25.5 version 11.06 des micrologiciels AP340, et des micrologiciels PC340.
- AP AIR-AP342E2R et adaptateur AIR-PCM342 de client.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Problème 1

Les versions 11.06 de micrologiciels et plus tard AP se conforment aux normes de l'ébauche 10 de 802.1X d'IEEE. La norme de l'ébauche 8 a été utilisée avant cette release. La version 4.25 de micrologiciels sur les clients se conforme pour dessiner 10. Sur AP qui exécute le micrologiciel 11.06, vous pouvez utiliser l'un ou l'autre d'ébauche. Si vous voulez que les clients qui exécutent le micrologiciel 4.23 et plus tôt pour s'associer, l'ébauche 8. d'utilisation. Un client 4.25 ne travaille pas avec des 11.06 AP qui utilise la configuration de l'ébauche 8, et un client 4.25 ne travaille pas avec des 11.05 AP.

Version de micrologiciel d'AP	Version de microprogramme de client	Ébauche de 802.1X d'IEEE
11.06 (et plus tard)	4.25	10
	4.23 ou plus tôt	8
11.03--11.05	4.25 (ne fonctionne pas avec 11.05)	AP exige 8, mais le client ne travaille pas avec 8
	4.23 ou plus tôt	8

Solution 1

Il y a deux options de résoudre ce problème :

1. Utilisez l'ébauche 10 (11.06) sur AP et améliorez le micrologiciel des cartes client à 4.25.
2. Utilisez l'ébauche 8 sur AP et utilisez AP avec un micrologiciel plus tôt sur les clients.

Cette table affiche les projets de norme de 802.1X d'IEEE auxquels les différentes versions du micrologiciel d'adaptateur de client (et du microprogramme d'un pont de groupe de travail) se conforment.

Version de microprogramme de client	Ébauche 8	Ébauche 10
4.13	X	-
4.16	X	-
4.23	X	-
4.25 ou plus tard	-	X
WGB340/350 8.58	X	-
WGB340/350 8.61	-	X

Problème 2

L'authentification MAC avec le serveur de RAYON est utilisée. Quelques uns de l'Aironet 1231G aps (les aps du Cisco IOS® libèrent 12.3(7)JA1 à 12.3(7)JA3,) ont des problèmes pour

l'authentification de l'utilisateur.

C'est un problème courant si vous améliorez d'une version ultérieure de Cisco IOS à 12.3(7)JA3.

Solution 2

La première étape pour résoudre ce problème est de tester avec la configuration. Procédez comme suit :

1. Retirez la clé de chiffrement au Security > Encryption Manager.
2. N'en cliquez sur **aucun** et puis appliquez.
3. Allez au gestionnaire SSID, mettez en valeur le SSID **SSID_Name**, et choisissez **<NO ADDITION>**.
4. Du menu ouvert d'authentification, faites descendre l'écran et cliquez sur Apply.Une fois que vous avez appliqué ces modifications, vous pouvez tester avec l'adaptateur de client.S'il échoue toujours, même sans configuration de cryptage et d'authentification, il vaut mieux de remettre à l'état initial AP de nouveau aux par défaut et de modifier le à partir de zéro.
5. Terminez-vous ces étapes afin de remettre à l'état initial AP de nouveau au par défaut :Choisissez le **System Software > System Configuration**.**Reset to Defaults de** clic (excepté l'IP).Une fois qu'il redémarre, vous pouvez le modifier de nouveau et tester avec l'adaptateur de client.
6. Vérifiez la configuration d'authentification MAC sous la Sécurité anticipée et placez-la au serveur seulement. Procédez comme suit :Choisissez la **Sécurité > la Sécurité > l'authentification MAC à l'avance**.**Serveur de** clic seulement.Cliquez sur la configuration de **sauvegarde**.

Informations connexes

- Conseils techniques sur le LAN Sans fil
- Support et documentation techniques - Cisco Systems