Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe via SDM

Contenu

Introduction

Ce document fournit les exemples de configuration qui expliquent comment configurer de divers types d'authentification de la couche 2 sur un routeur de configuration fixe intégré par radio de Cisco pour la connexion sans fil avec le Security Device Manager (SDM).

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 l'Integrated Services Router de Cisco (ISR) avec SDM
- La connaissance de la façon configurer l'adaptateur client sans fil 802.11a/b/g avec Aironet Desktop Utility (ADU)

Composants utilisés

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

- Cisco 877W ISR qui exécute la version de logiciel 12.3(8)YI1 de Cisco IOS®
- Version 2.4.1 de Cisco SDM installée sur l'ISR
- Ordinateur portable avec la version 3.6 d'Aironet Desktop Utility
- adaptateur de client du 802.11 a/b/g qui exécute la version 3.6 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.

Conventions

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

Informations générales

Le Cisco SDM est un outil de Gestion de périphériques intuitif et basé sur le WEB pour les Routeurs articulés autour d'un logiciel de Cisco IOS. Le Cisco SDM simplifie le routeur et la configuration de sécurité par les assistants intelligents, qui aident des clients rapidement et se déploient facilement, configurent, et surveillent des Routeurs de Cisco Systems® sans exiger la connaissance de l'interface de ligne de commande de logiciel de Cisco IOS (CLI).

SDM peut être gratuit téléchargé du centre de logiciel sur Cisco.com.

SDM peut être installé indépendamment pendant qu'une copie distincte sur le chaque des routeurs individuels, ou lui peut également être installée sur un PC. Le Cisco SDM installé sur un PC te permet pour employer SDM pour gérer d'autres Routeurs qui exécutent des images appropriées IOS sur le réseau. Cependant, SDM sur un PC ne prend en charge pas la remise de la configuration de routeur pour fabriquer le par défaut.

Ce document utilise le SDM installé sur le routeur Sans fil pour configurer le routeur pour l'authentification Sans fil.

Le Cisco SDM communique avec des Routeurs pour deux buts :

- Accédez aux fichiers d'application de Cisco SDM pour le téléchargement au PC
- Lisez et écrivez la configuration de routeur et l'état

Le Cisco SDM emploie des HTTPS pour télécharger les fichiers d'application (sdm.tar, home.tar) au PC. Une combinaison des HTTPS et du Telnet/SSH est utilisée pour lire et écrire la configuration de routeur.

Référez-vous au Cisco Router and Security Device Manager Q&A pour les dernières informations concernant les Routeurs et les versions logicielles IOS qui prennent en charge SDM.

Référez-vous configurent votre routeur pour prendre en charge SDM pour plus d'informations sur la façon utiliser le Cisco SDM sur un routeur.

Référez-vous installent les fichiers SDM pour que les instructions installent et de téléchargent des fichiers SDM sur le routeur ou sur le PC.

Configurez

Le document explique comment configurer ces types d'authentification par SDM :

- Ouvrez l'authentification avec le cryptage WEP
- Ouvrez-vous avec l'authentification MAC
- Authentification partagée
- authentification de Protocol d'authentification 802.1x/Extensible (EAP)
- Protocole WPA (Wi-Fi Protected Access) - Authentification (PSK) principale pré partagée
- Authentification WPA

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Cette installation utilise le serveur local de RAYON sur la radio ISR pour authentifier des clients sans fil utilisant l'authentification de 802.1x.

Configurez le routeur pour SDM Access

Terminez-vous ces étapes afin de permettre le routeur à accéder à par SDM :

1. Configurez le routeur pour le HTTP/https que l'accès suivant la procédure expliquée dedans configurent votre routeur pour prendre en charge SDM.
2. Assignez une adresse IP au routeur avec ces étapes :`Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface fastEthernet 0 Router(config-if)#ip address 10.77.244.197 255.255.255.224 % IP addresses cannot be configured on L2 links.` Dans le routeur 871W, vous pourriez rencontrer un tel

message d'erreur. Ce message d'erreur prouve que l'Ethernet rapide 0 est un lien de la couche 2 sur lequel vous ne pouvez configurer aucune adresse IP.

3. Afin de surmonter cette question, créez une interface Layer-3 (VLAN) et assignez une adresse IP sur la même chose avec ces étapes :`Router(config)#interface Vlan1 Router(config-if)#ip address 10.77.244.197 255.255.255.224`
4. Permettez à ce VLAN sur les Ethernets Layer-2 rapides 0 interfaces avec ces étapes. Ce document configure l'interface rapide d'Ethernets comme interface de joncteur réseau pour permettre VLAN1. Vous pouvez également le configurer comme interface d'accès et permettre VLAN1 sur l'interface par votre configuration réseau.`Router(config)#interface fastEthernet 0 Router(config-if)#switchport trunk encapsulation dot1q Router(config-if)#switchport trunk allowed vlan add vlan1 !--- This command allows VLAN1 through the fast ethernet interface. !--- In order to allow all VLANs through this interface, issue the !--- switchport trunk allowed vlan add all command on this interface.` **Remarque:** Cet exemple suppose que des configurations de base de routeur et de radio sont déjà exécutées sur le routeur. Par conséquent, l'étape suivante est immédiatement de lancer l'application Sans fil sur le routeur pour configurer des paramètres d'authentification.

Lancez l'application Sans fil SDM sur le routeur

Terminez-vous ces étapes afin de lancer l'application Sans fil :

1. Commencez SDM ouvrir un navigateur et en écrivant l'adresse IP de votre routeur.Vous êtes incité à recevoir ou refuser une fenêtre d'alerte sécurité de navigateur Web qui ressemble à ceci :
2. Cliquez sur **oui** pour poursuivre.
3. Sur la fenêtre qui apparaît, écrivez le nom d'utilisateur et mot de passe du privilège level_15 afin d'accéder au routeur.Cet exemple utilise l'**admin** comme nom d'utilisateur et mot de passe :
4. Cliquez sur **OK** pour continuer. Écrivez les mêmes informations partout où on l'exige.
5. Clic **oui** et **CORRECT** comme approprié dans les pages résultantes afin de lancer l'application SDM.Pendant que l'application SDM s'ouvre, vous êtes incité par une fenêtre d'alerte sécurité à recevoir un Security Certificate signé.
6. Cliquez sur **oui** pour recevoir le certificat signé.Le routeur résultant de Cisco et la page principale SDM ressemblent à ceci :
7. Àcette page, cliquez sur Configure au supérieur afin de lancer le routeur configurent la fenêtre de mode.
8. Dans la fenêtre de mode de configurer, les **interfaces** choisies **et les connexions de la** colonne de tâches qui apparaît au côté gauche de cette page.
9. Dans la fenêtre d'interfaces et de connexions, cliquez sur l'**onglet Connection de création**.Ceci répertorie toutes les interfaces disponibles pour être configuré sur le routeur.
10. Afin de lancer l'application Sans fil, choisissez la **radio de la** liste d'interfaces. Puis, **lancement d'application sans fil de** clic.Ce tir d'écran explique les étapes 8, 9 et 10 :Ceci lance l'application Sans fil SDM dans une fenêtre séparée où de divers types d'authentification peuvent être configurés.La page d'accueil Sans fil d'application SDM ressemble à ceci :Observez que l'état du logiciel **est désactivé** et le statut de matériel de l'interface (Sans fil) par radio est **en baisse** parce qu'aucun SSID n'est configuré sur l'interface. Ensuite, vous configurez le SSID et l'authentification tape sur cette interface par radio de sorte que les clients sans fil puissent communiquer par cette interface.

Configurez l'authentification ouverte avec le cryptage WEP

L'authentification ouverte est un algorithme nul d'authentification. Le Point d'accès (AP) accordera n'importe quelle demande de l'authentification. L'authentification ouverte permet n'importe quel accès au réseau de périphérique. Si aucun cryptage n'est activé sur le réseau, n'importe quel périphérique qui connaît le SSID d'AP peut accéder au réseau. Le cryptage WEP étant activé sur AP, la clé WEP elle-même devient des moyens de contrôle d'accès. Si un périphérique n'a pas la clé WEP correcte, quoique l'authentification soit réussie, le périphérique ne pourra pas transmettre des données par AP. En outre, il ne peut pas déchiffrer des données transmises d'AP.

Référez-vous à l'authentification ouverte au pour en savoir plus de Point d'accès.

Cet exemple utilise ces paramètres de configuration pour l'authentification ouverte avec le cryptage WEP :

- Nom SSID : **openwep**
- Id VLAN : **1**
- Adresse IP VLAN : **10.1.1.1/16**
- Plage d'adresses DHCP pour les clients sans fil de ce VLAN/SSID : **10.1.1.5/16 - 10.1.1.10/16**

Terminez-vous ces étapes afin de configurer l'authentification ouverte avec le WEP :

1. Sur la page d'accueil Sans fil d'application, **Services sans fil de** clic > **VLAN** afin de configurer un VLAN.
2. **Routage** choisi des services : **VLAN** .
3. Sur les services : La page de choix VLAN, créent le VLAN et l'assignent à l'interface par radio.C'est la fenêtre de configuration de VLAN1 sur l'interface par radio. VLAN1 est le VLAN indigène ici :
4. Sur la page d'accueil Sans fil d'application, la **sécurité sans fil** choisie > le **gestionnaire SSID** afin de configurer le SSID et l'authentification tapent.
5. Sur la Sécurité : La page de gestionnaire SSID, configurent le SSID et assignent le SSID au VLAN créé dans step1 afin d'activer le SSID sur l'interface par radio.
6. Sous la section de configurations d'authentification de cette page, choisissez l'**authentification ouverte**.Voici la fenêtre de configuration qui explique ces étapes :
7. Cliquez sur **Apply**.**Remarque:** La liste déroulante qui correspond dans la case à cocher Open Authentication implique cela l'authentification qu'ouverte peut être configurée en outre avec plusieurs types supplémentaires d'authentification, tels que l'EAP ou l'authentification MAC. Cette section discute seulement l'authentification ouverte sans l'AJOUT (sans type supplémentaire d'authentification).
8. Configurez le cryptage WEP pour ce SSID/VLAN. Sur la page d'accueil Sans fil, **gestionnaire** choisi de **sécurité sans fil** > de **cryptage** afin de configurer les configurations de cryptage.Sur la Sécurité : La page de gestionnaire de cryptage, a placé le mode de chiffrement et les clés pour **VLAN1**.Choisissez le **cryptage WEP : Obligatoire** comme mode de chiffrement.Placez la clé de chiffrement pour ce VLAN.Cette section utilise ces configurations de clé de chiffrement :Emplacement 1 de clé de chiffrement : utilisé comme touche de transmissionTaille de clé de chiffrement : bit 40Clé de chiffrement en valeur hexadécimale : 1234567890**Remarque:** Le même emplacement de clé de chiffrement (1, dans ce cas) devrait être utilisé comme touche de transmission au client sans fil. En outre, le client sans fil devrait être configuré avec la même valeur principale (1234567890 dans ce cas) pour que le client sans fil communique avec ce réseau WLAN.Cette fenêtre de configuration explique ces étapes :Cette page de

sécurité sans fil représente la configuration entière :

Configurez le serveur DHCP interne pour des clients sans fil de ce VLAN

Terminez-vous ces étapes afin de configurer un serveur DHCP interne sur le routeur. C'est un facultatif, bien que recommandé, méthode pour assigner l'adresse IP aux clients sans fil.

1. Sur le SDM configurez la fenêtre de mode, des **tâches supplémentaires** choisies sous la colonne de tâches qui est du côté gauche de la fenêtre.
2. Sur les **tâches supplémentaires** paginez, développez l'arborescence **DHCP** et choisissez les **pools DHCP** suivant les indications de cet exemple. Dans la colonne de pools DHCP affichée du côté droit de cette page, cliquez sur Add pour créer un nouveau pool DHCP.
3. Àla page de pool DHCP d'ajouter, spécifiez le nom de pool DHCP, réseau de pool DHCP, masque de sous-réseau, en commençant l'adresse IP, en finissant des paramètres de routeur d'adresse IP et de par défaut suivant les indications de cet exemple :
4. Cliquez sur **OK**.Le serveur DHCP interne est configuré sur le routeur.

Configurez ouvert avec l'authentification MAC

Dans ce type d'authentification, on permettra au le client sans fil pour accéder au réseau WLAN seulement si l'adresse MAC du client est sous la liste d'adresses MAC permises dans le serveur d'authentification. AP transmet par relais l'adresse MAC du périphérique de client sans fil à un serveur d'authentification RADIUS sur votre réseau, et le serveur vérifie l'adresse contre une liste d'adresses MAC permises. l'authentification basée sur MAC fournit une méthode d'authentification alternative pour les périphériques de client qui n'ont pas la capacité d'EAP.

Référez-vous à l'authentification d'adresse MAC au pour en savoir plus de réseau.

Remarque: Le document entier utilise le serveur local de RAYON pour l'authentification MAC, le 802.1x/EAP, aussi bien que l'authentification WPA.

Cet exemple utilise ces paramètres de configuration pour ouvert avec l'authentification MAC :

- Nom SSID : **openmac**
- Id VLAN : **2**
- Adresse IP VLAN : **10.2.1.1/16**
- Plage d'adresses DHCP pour les clients sans fil de ce VLAN/SSID : **10.2.1.5/16 - 10.2.1.10/16**

Terminez-vous ces étapes afin de configurer ouvert avec l'authentification MAC :

1. Sur la page d'accueil Sans fil d'application, **Services sans fil de** clic **> VLAN** afin de configurer un VLAN.
2. **Routage** choisi des services : **VLAN** . Sur les services : La page de choix VLAN, créent le VLAN et l'assignent à l'interface par radio.Voici la fenêtre de configuration du **VLAN 2** sur l'interface par radio :
3. Configurez le serveur local de RAYON pour l'authentification MAC. Ce serveur local de RAYON tiendra l'adresse MAC du client sans fil dans sa base de données et permettra ou refusera le client dans le réseau WLAN selon le résultat de l'authentification.Sur la page d'accueil Sans fil, **gestionnaire du serveur** choisi de **sécurité sans fil >** afin de configurer le serveur local de RAYON.Àla page de gestionnaire du serveur, configurez l'adresse IP, le

secret partagé, et l'authentification et les ports de traçabilité du serveur de RAYON.Puisque c'est un serveur local de RAYON, l'adresse IP spécifiée est l'adresse de cette interface Sans fil. La clé secrète partagée utilisée devrait être identique sur la configuration de client d'AAA.Dans cet exemple, le secret partagé est **Cisco**.Cliquez sur **Apply**.Faites descendre l'écran la page pour rechercher la section de Default Server Priorities. Dans cette section, choisissez ce serveur de RAYON (**10.2.1.1**) en tant que serveur prioritaire par défaut pour l'authentification MAC suivant les indications de cet exemple :Afin de configurer le client et les identifiants utilisateurs d'AAA, **sécurité sans fil** choisie > **serveur local de RAYON de la** page d'accueil Sans fil.Àla page locale de serveur de RAYON, **CONFIGURATION GÉNÉRALE de** clic.Àla page de CONFIGURATION GÉNÉRALE, configurez le client d'AAA et la clé secrète partagée comme affichée.Avec une configuration du serveur RADIUS locale, l'adresse IP du serveur et le client d'AAA seront identique.Faites descendre l'écran la page de CONFIGURATION GÉNÉRALE pour rechercher la section de configuration d'**utilisateurs individuels**. Dans les utilisateurs individuels sectionnez, configurez l'adresse MAC du client sans fil comme nom d'utilisateur et mot de passe.Activez la case d'**authentification MAC seulement**, puis cliquez sur Apply.Afin d'éviter le client de l'échec d'authentification parfois, spécifiez l'adresse MAC du client dans un format continu sans n'importe quelle séparation suivant les indications de cet exemple.

4. Sur la page d'accueil Sans fil d'application, la **sécurité sans fil** choisie > le **gestionnaire SSID** afin de configurer le SSID et l'authentification tapent.Sur la Sécurité : La page de gestionnaire SSID, configurent le SSID et assignent le SSID au VLAN créé dans step1 afin d'activer le SSID sur l'interface par radio.Sous la section de configurations d'authentification de cette page, choisissez l'**authentification ouverte** et de la liste déroulante correspondante, choisissent **avec l'authentification MAC**.Afin de configurer des priorités de serveur, choisissez **personnalisent** sous le MAC authentifient des serveurs et choisissent l'adresse IP du serveur local **10.2.1.1 de** RAYON.C'est un exemple qui explique cette étape :
5. Afin de configurer le serveur DHCP interne pour des clients sans fil de ce VLAN, terminez-vous les mêmes étapes expliquées dans le serveur DHCP interne de configurer pour des clients sans fil de cette partie VLAN de ce document avec ces paramètres de configuration :Nom de pool DHCP : VLAN 2Réseau de pool DHCP : 10.2.0.0**Subnet Mask**: 255.255.0.0Commencer l'IP : 10.2.1.5Finir l'IP : 10.2.1.10Routeur par défaut : 10.2.1.1

Configurez l'authentification 802.1x/EAP

Ce type d'authentification fournit le de plus haut niveau de la Sécurité pour votre réseau Sans fil. À l'aide de l'EAP à interagir avec un serveur Eap-compatible de RAYON, AP aide un périphérique de client sans fil et le serveur de RAYON à exécuter l'authentification mutuelle et à dériver une clé WEP dynamique d'unicast. Le serveur de RAYON envoie la clé WEP à AP qui l'utilise pour tous les signaux de données d'unicast aux lesquels elle envoie, ou la reçoit, du client.

Référez-vous à l'authentification EAP au pour en savoir plus de réseau.

Remarque: Il y a plusieurs méthodes d'authentification EAP disponibles. Dans tout ce document, il explique comment configurer le Lightweight Extensible Authentication Protocol (LEAP) comme authentification EAP. Le LEAP utilise le nom d'utilisateur et mot de passe comme identifiants utilisateurs pour l'authentification.

Remarque: Afin de configurer l'EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) comme type d'authentification EAP, référez-vous au guide de configuration de version 1.02 d'EAP-

FAST pour la procédure.

Cet exemple utilise ces paramètres de configuration pour l'authentification EAP :

- Nom SSID : **LEAP**
- Id VLAN : **3**
- Adresse IP VLAN : **10.3.1.1/16**
- Plage d'adresses DHCP pour les clients sans fil de ce VLAN/SSID : **10.3.1.5/16 - 10.3.1.10/16**

Terminez-vous ces étapes afin de configurer l'authentification EAP :

1. Répétez les étapes 1 et 2 Configure ouvert avec l'authentification MAC afin de créer et configurer le VLAN avec ces paramètres de configuration :Id VLAN : 3Adresse IP par radio d'interface : 10.3.1.1masque de sous-réseau : 255.255.0.0
2. Puis, configurez le serveur local de RAYON pour l'authentification client. Afin d'exécuter ceci, répétez les étapes 3a à 3c Configure ouvert avec l'authentification MAC avec ces paramètres de configuration :Adresse IP de serveur de RAYON : 10.3.1.1Secret partagé : CiscoVoici l'écran de configuration qui explique l'étape 2 de l'authentification EAP :
3. Faites descendre l'écran la page pour rechercher la section de Default Server Priorities. Dans cette section, choisissez ce serveur de RAYON (**10.3.1.1**) en tant que serveur prioritaire par défaut pour l'authentification EAP suivant les indications de cet exemple.
4. Répétez les étapes 3e et 3f Configure s'ouvrent avec l'authentification MAC.
5. Répétez les étapes 3g et 3h Configure s'ouvrent avec l'authentification MAC avec ces paramètres de configuration pour l'authentification EAP :Adresse IP de client d'AAA : 10.3.1.1Secret partagé : CiscoSous les utilisateurs individuels sectionnez, configurez le nom d'utilisateur et mot de passe comme **user1**.
6. Sur la page d'accueil Sans fil d'application, la **sécurité sans fil** choisie > le **gestionnaire SSID** afin de configurer le SSID et l'authentification tapent.Sur la Sécurité : La page de gestionnaire SSID, configurent le SSID et assignent le SSID au VLAN créé dans l'étape 1 afin d'activer le SSID sur l'interface par radio.Sous la section de configurations d'authentification de cette page, choisissez l'**authentification ouverte** et de la liste déroulante correspondante, choisissent l'**authentification EAP**. En outre, sélectionnez le type d'**authentification EAP de réseau**.Afin de configurer les priorités de serveur, choisissez **personnalisent** sous l'EAP authentifient des serveurs et choisissent l'adresse IP du serveur local **10.3.1.1 de** RAYON.Voici un exemple qui explique ces étapes :
7. Afin de configurer le serveur DHCP interne pour des clients sans fil de ce VLAN, terminez-vous les mêmes étapes expliquées dans le serveur DHCP interne de configurer pour des clients sans fil de cette partie VLAN de ce document avec ces paramètres de configuration :Nom de pool DHCP : VLAN 3Réseau de pool DHCP : 10.3.0.0**Subnet Mask**: 255.255.0.0Commencer l'IP : 10.3.1.5Finir l'IP : 10.3.1.10Routeur par défaut : 10.3.1.1
8. Configurez le chiffrement à utiliser pour la gestion dynamique des clés sur l'authentification réussie du client sans fil.Sur la page d'accueil Sans fil, **gestionnaire** choisi de **sécurité sans fil** > de **cryptage** afin de configurer les configurations de cryptage.Sur l'écran de gestionnaire de sécurité sans fil > de cryptage sur la Sécurité : La page de gestionnaire de cryptage, écrivent **3** pour le mode de chiffrement et les clés de positionnement pour le VLAN.Choisissez le **chiffrement** comme mode de chiffrement, et choisissez un algorithme de chiffrement de chiffrement de la liste déroulante.Cet exemple utilise le **TKIP** comme algorithme de chiffrement :**Remarque:** Tout en configurant la plusieurs authentification tape sur un routeur Sans fil par SDM, parfois il ne pourrait pas être possible pour configurer deux

l'authentification que différente tape chacun des deux utilisant le mode de chiffrement de chiffrement sur le même routeur. En pareil cas, la configuration de cryptage configurée par SDM ne pourrait pas être appliquée sur le routeur. Afin de surmonter ceci, configurez ces types d'authentification par le CLI.

Configurez l'authentification partagée

Cisco fournit l'authentification principale partagée pour être conforme à la norme d'IEEE 802.11b.

Pendant l'authentification principale partagée, AP envoie une chaîne de texte de défi décryptée à n'importe quel périphérique qui tente de communiquer avec AP. Le périphérique qui demande l'authentification chiffre le texte de défi et l'envoie de nouveau à AP. Si le texte de défi est chiffré correctement, AP permet au périphérique demandeur pour authentifier. Le défi décrypté et le défi chiffré peuvent être surveillés. Cependant, ceci laisse AP ouvert pour attaquer d'un intrus qui calcule la clé WEP en comparant les chaînes de texte décryptées et chiffrées.

Référez-vous à l'authentification principale partagée au pour en savoir plus de Point d'accès.

Cet exemple utilise ces paramètres de configuration pour l'authentification partagée :

- Nom SSID : **partagé**
- Id VLAN : **4**
- Adresse IP VLAN : **10.4.1.1/16**
- Plage d'adresses DHCP pour les clients sans fil de ce VLAN/SSID : **10.4.1.5/16 - 10.4.1.10/16**

Terminez-vous ces étapes afin de configurer l'authentification partagée :

1. Répétez les étapes 1 et 2 Configure ouvert avec l'authentification MAC afin de créer et configurer le VLAN avec ces paramètres de configuration :Id VLAN : 4Adresse IP par radio d'interface : 10.4.1.1masque de sous-réseau : 255.255.0.0
2. Sur la page d'accueil Sans fil d'application, la **sécurité sans fil** choisie > le **gestionnaire SSID** afin de configurer le SSID et l'authentification tapent.Sur la Sécurité : La page de gestionnaire SSID, configurent le SSID et assignent le SSID au VLAN créé dans step1 afin d'activer le SSID sur l'interface par radio.Sous la section de configurations d'authentification de cette page, choisissez l'**authentification partagée**.Voici l'écran de configuration qui explique ces étapes :Cliquez sur **Apply**.
3. Configurez le cryptage WEP pour ce SSID/VLAN. Puisque c'est l'authentification principale partagée, la même clé est aussi bien utilisée pour l'authentification. Sur la page d'accueil Sans fil, **gestionnaire** choisi de **sécurité sans fil** > de **cryptage** afin de configurer les configurations de cryptage.Sur la Sécurité : La page de gestionnaire de cryptage, écrivent **4** pour le mode de chiffrement et les clés de positionnement pour le VLAN.Choisissez le **cryptage WEP : Obligatoire** comme mode de chiffrement.Placez la clé de chiffrement pour ce VLAN.Cette section utilise ces configurations de clé de chiffrement :Emplacement 1 de clé de chiffrement : utilisé comme touche de transmissionTaille de clé de chiffrement : bit 40Clé de chiffrement en valeur hexadécimale : 1234567890**Remarque:** Le même emplacement de clé de chiffrement (1, dans ce cas) devrait être utilisé comme touche de transmission au client sans fil. En outre, le client sans fil devrait être configuré avec la même valeur principale (1234567890 dans ce cas) pour que le client sans fil communique avec ce réseau WLAN.Cet écran de configuration explique ces étapes :
4. Afin de configurer le serveur DHCP interne pour des clients sans fil de ce VLAN, terminez-

vous les mêmes étapes expliquées dedans configurent le serveur DHCP interne pour des clients sans fil de cette partie VLAN de ce document avec ces paramètres de configuration :Nom de pool DHCP : VLAN 4Réseau de pool DHCP : 10.4.0.0**Subnet Mask**: 255.255.0.0Commencer l'IP : 10.4.1.5Finir l'IP : 10.4.1.10Routeur par défaut : 10.4.1.1

Configurez l'authentification WPA

Le WPA est une amélioration de la sécurité basée sur des standards et interopérable qui augmente fortement le niveau de la protection des données et du contrôle d'accès pour exister et de futurs systèmes LAN Sans fil. Prises en charge de la gestion deux de clé WPA mutuellement - la Gestion exclusive tape : WPA et WPA-PSK.

Référez-vous en utilisant le pour en savoir plus de Gestion de clé WPA.

Utilisant la Gestion de clé WPA, les clients et le serveur d'authentification authentifient entre eux suivre une méthode d'authentification EAP, et le client et serveur génèrent par paires une clé principale (PMK). Utilisant le WPA, le serveur génère le PMK dynamiquement et le passe à AP.

Cet exemple utilise ces paramètres de configuration pour l'authentification WPA :

- Nom SSID : **wpa**
- Id VLAN : **5**
- Adresse IP VLAN : **10.5.1.1/16**
- Plage d'adresses DHCP pour les clients sans fil de ce VLAN/SSID : **10.5.1.5/16 - 10.5.1.10/16**

Terminez-vous ces étapes afin de configurer l'authentification WPA :

1. Répétez les étapes 1 et 2 Configure ouvert avec l'authentification MAC afin de créer et configurer le VLAN avec ces paramètres de configuration :Id VLAN : 5Adresse IP par radio d'interface : 10.5.1.1masque de sous-réseau : 255.255.0.0
2. Puisque le WPA est une norme de gestion des clés, configurez le chiffrement à utiliser pour la Gestion de clé WPA.Sur la page d'accueil Sans fil, **gestionnaire** choisi de **sécurité sans fil** > de **cryptage** afin de configurer les configurations de cryptage.Sur l'écran de gestionnaire de sécurité sans fil > de cryptage sur la Sécurité : La page de gestionnaire de cryptage, écrivent **5** pour le mode de chiffrement et les clés de positionnement pour le VLAN.Choisissez le **chiffrement** comme mode de chiffrement, et choisissez un algorithme de chiffrement de chiffrement de la liste déroulante.Cet exemple utilise le **TKIP** comme algorithme de chiffrement :**Remarque:** Tout en configurant la plusieurs authentification tape sur un routeur Sans fil par SDM, parfois il ne pourrait pas être possible pour configurer deux l'authentification que différente tape chacun des deux utilisant le mode de chiffrement de chiffrement sur le même routeur. En pareil cas, la configuration de cryptage configurée par SDM ne pourrait pas être appliquée sur le routeur. Afin de surmonter ceci, configurez ces types d'authentification par le CLI.
3. L'étape suivante est de configurer le serveur local de RAYON pour l'authentification client. Afin d'exécuter ceci, répétez les étapes 3a à 3c Configure ouvert avec l'authentification MAC avec ces paramètres de configuration :Adresse IP de serveur de RAYON : 10.5.1.1Secret partagé : CiscoFaites descendre l'écran la page de **gestionnaire du serveur** pour rechercher la section de Default Server Priorities. Dans cette section, choisissez ce serveur de RAYON (**10.5.1.1**) en tant que serveur prioritaire par défaut pour l'authentification EAP suivant les indications de cet exemple :Répétez les étapes 3e et 3f Configure s'ouvrent avec

l'authentification MAC.Répétez les étapes 3g et 3h Configure s'ouvrent avec l'authentification MAC avec ces paramètres de configuration pour l'authentification EAP :Adresse IP de client d'AAA : 10.5.1.1Secret partagé : CiscoSous les utilisateurs individuels sectionnez, configurez le nom d'utilisateur et mot de passe comme **user2**.

4. Afin d'activer le WPA pour un SSID, vous devez activer ouvert avec l'EAP ou l'EAP de réseau sur le SSID. Afin d'activer l'EAP de réseau, sur la page d'accueil Sans fil d'application, la **sécurité sans fil** choisie > le **gestionnaire SSID** pour configurer le SSID et l'authentification tapent.Sur la Sécurité : La page de gestionnaire SSID, configurent le SSID et assignent le SSID au VLAN créé dans step1 afin d'activer le SSID sur l'interface par radio.Sous la section de configurations d'authentification de cette page, choisissez l'**authentification ouverte** et de la liste déroulante correspondante, choisissent l'**authentification EAP**. En outre, sélectionnez le type d'**authentification EAP de réseau**.Afin de configurer des priorités de serveur, choisissez **personnalisent** sous l'EAP authentifient des serveurs et choisissent l'adresse IP du serveur local **10.5.1.1 de** RAYON.Voici un exemple qui explique ces étapes :
5. Faites descendre l'écran la page de gestionnaire SSID pour rechercher la section d'**Authenticated Key Management**.
6. Dans cette section, choisissez **obligatoire de la** liste déroulante de gestion des clés, et activez la case **WPA**.Voici la fenêtre de configuration qui explique ces étapes :
7. Cliquez sur **Apply**.
8. Afin de configurer le serveur DHCP interne pour des clients sans fil de ce VLAN, terminez-vous les mêmes étapes expliquées dedans configurent le serveur DHCP interne pour des clients sans fil de cette partie VLAN de ce document avec ces paramètres de configuration :Nom de pool DHCP : VLAN 5Réseau de pool DHCP : 10.5.0.0**Subnet Mask**: 255.255.0.0Commencer l'IP : 10.5.1.5Finir l'IP : 10.5.1.10Routeur par défaut : 10.5.1.1

Configurez l'authentification de WPA-PSK

L'autre type de Gestion de clé WPA s'appelle le WPA-PSK. Le WPA-PSK est utilisé pour prendre en charge le WPA sur un RÉSEAU LOCAL Sans fil où l'authentification 802.1x-based n'est pas disponible. Avec ce type, vous devez configurer une clé pré-partagée sur AP. Vous pouvez introduire la clé pré-partagée comme ASCII ou caractères hexadécimaux. Si vous introduisez la clé comme caractères ASCII, vous entrez entre 8 et 63 caractères, et AP développe la clé utilisant le processus décrit dans la norme basée sur mot de passe de chiffrement (RFC2898). Si vous introduisez la clé comme caractères hexadécimaux, vous devez écrire 64 caractères hexadécimaux.

Cet exemple utilise ces paramètres de configuration pour l'authentification de WPA-PSK :

- Nom SSID : **wpa-psk**
- Id VLAN : **6**
- Adresse IP VLAN : **10.6.1.1/16**
- Plage d'adresses HCP pour les clients sans fil de ce VLAN/SSID : **10.6.1.5/16 - 10.6.1.10/16**

Terminez-vous ces étapes afin de configurer le WPA-PSK :

1. Répétez les étapes 1 et 2 Configure ouvert avec l'authentification MAC afin de créer et configurer le VLAN avec ces paramètres de configuration :Id VLAN : 6Adresse IP par radio d'interface : 10.6.1.1masque de sous-réseau : 255.255.0.0
2. Puisque le WPA-PSK est une norme de gestion des clés, configurez le chiffrement à utiliser

pour la Gestion de clé WPA.Sur la page d'accueil Sans fil, **gestionnaire** choisi de **sécurité sans fil** > de **cryptage** afin de configurer les configurations de cryptage.Sur la fenêtre de **gestionnaire de sécurité sans fil** > de **cryptage** sur la Sécurité : La page de gestionnaire de cryptage, écrivent **6** pour le mode de chiffrement et les clés de positionnement pour le VLAN.Choisissez le **chiffrement** comme mode de chiffrement, et choisissez un algorithme de chiffrement de chiffrement de la liste déroulante.Cet exemple utilise **TKIP+WEP 128bit** comme algorithme de chiffrement.**Remarque:** Tout en configurant la plusieurs authentification tape sur un routeur Sans fil par SDM, parfois il ne pourrait pas être possible pour configurer deux l'authentification que différente tape chacun des deux utilisant le mode de chiffrement de chiffrement sur le même routeur. En pareil cas, la configuration de cryptage configurée par SDM ne pourrait pas être appliquée sur le routeur. Afin de surmonter ceci, configurez ces types d'authentification par le CLI.

3. Afin d'activer le WPA-PSK pour un SSID, vous devez activer l'authentification ouverte sur le SSID. Afin d'activer l'authentification ouverte, répétez l'étape 6 de l'authentification ouverte Configure avec le cryptage WEP.Voici la fenêtre de configuration du WPA-PSK :
4. Faites descendre l'écran la page de gestionnaire SSID pour rechercher la section d'**Authenticated Key Management**.
5. Dans cette section, choisissez **obligatoire de la** liste déroulante de gestion des clés, activez la case **WPA** et introduisez la clé pré-partagée WPA dans l'ASCII ou le format hexadécimal.Cet exemple utilise le format ASCII. Le même format devrait être utilisé à la configuration de côté client. Voici la fenêtre de configuration qui explique l'étape 5 :La clé pré-partagée WPA utilisée dans cette configuration est 1234567890.
6. Cliquez sur **Apply**.
7. Afin de configurer le serveur DHCP interne pour des clients sans fil de ce VLAN, terminez-vous les mêmes étapes expliquées dedans configurent le serveur DHCP interne pour des clients sans fil de cette partie VLAN de ce document avec ces paramètres de configuration :Nom de pool DHCP : VLAN 6Réseau de pool DHCP : 10.6.0.0**Subnet Mask**: 255.255.0.0Commencer l'IP : 10.6.1.5Finir l'IP : 10.6.1.10Routeur par défaut : 10.6.1.1

Configuration de client sans fil

Après que vous configuriez l'ISR par SDM, vous devez configurer le client sans fil pour les différents types d'authentification de sorte que le routeur puisse authentifier ces clients sans fil et permettre d'accéder au réseau WLAN. Ce document utilise l'ADU pour la configuration de côté client.

Configurez le client sans fil pour l'authentification ouverte avec le cryptage WEP

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont **openwep**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification ouverte.
3. Cliquez sur l'**onglet Sécurité** et laissez l'option de Sécurité en tant que clé pré-partagée

(WEP statique) pour le cryptage WEP.
4. Cliquez sur Configure et définissez la clé pré-partagée suivant les indications de cet exemple :
5. Cliquez sur l'**onglet Avancé à la** page de Profile Management et placez l'authentication mode de 802.11 comme **ouverte** pour l'authentification ouverte.
6. Afin de vérifier ouvert avec l'authentification WEP, lancez l'**openwep** SSID configuré.
7. Vérifiez le client sans fil est associé avec succès avec le routeur. Ceci peut être vérifié en détail du routeur Sans fil utilisant la commande de **show dot11 associations**.Voici un exemple :

```
Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openwep] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.1.1.5 CB21AG/PI21AG client self Assoc Others: (not related to any ssid)
```

Configurez le client sans fil pour ouvert avec l'authentification MAC

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont **openmac**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification ouverte.
3. Cliquez sur l'**onglet Sécurité** et laissez l'option de Sécurité en tant qu'**aucun** pour ouvert avec l'authentification MAC. Puis, cliquez sur OK.
4. Afin de vérifier ouvert avec l'authentification MAC, lancez l'**openmac** SSID configuré.
5. Vérifiez le client sans fil est associé avec succès avec le routeur. Ceci peut être vérifié en détail du routeur Sans fil utilisant la commande de **show dot11 associations**.Voici un exemple :

```
Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openmac] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.2.1.5 CB21AG/PI21AG client1 self MAC-Assoc SSID [openwep] : Others: (not related to any ssid)
```

Configurez le client sans fil pour l'authentification 802.1x/EAP

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont **LEAP**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification 802.1x/EAP.
3. Sous Profile Management, cliquez sur l'**onglet Sécurité**, placez l'option de Sécurité comme **802.1x** et choisissez le type approprié d'EAP.Ce document utilise le **LEAP** comme type d'EAP pour l'authentification.
4. Cliquez sur Configure afin de configurer les configurations de nom d'utilisateur et mot de passe de LEAP.Sous les configurations de nom d'utilisateur et mot de passe, cet exemple choisit **d'inciter manuellement pour le nom d'utilisateur et le mot de passe** de sorte que le client soit incité à écrire le nom d'utilisateur et mot de passe correct tout en essayant de se connecter au réseau.

5. Cliquez sur **OK**.
6. Afin de vérifier l'authentification EAP, lancez le **LEAP** SSID configuré. Vous êtes incité à écrire un nom d'utilisateur et mot de passe de LEAP. Entrez dans les les deux les qualifications comme **user1** et cliquez sur OK.
7. Vérifiez le client sans fil est authentifié avec succès et assigné avec une adresse IP. Ceci peut être vérifié clairement de la fenêtre d'état ADU.Voici la sortie équivalente du CLI du routeur :`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [leap] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.1.5 CB21AG/PI21AG client2 self EAP-Assoc SSID [openmac] : SSID [openwep] : Others: (not related to any ssid)`

Configurez le client sans fil pour l'authentification partagée

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID **sont partagés**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification ouverte.
3. Cliquez sur l'**onglet Sécurité** et laissez l'option de Sécurité en tant que clé pré-partagée (WEP statique) pour le cryptage WEP. Puis, cliquez sur Configure.
4. Définissez la clé pré-partagée suivant les indications de cet exemple :
5. Cliquez sur **OK**.
6. Sous Profile Management, cliquez sur l'authentication mode de 802.11 d'**onglet Avancé** et de positionnement comme **partagé** pour l'authentification partagée.
7. Afin de vérifier a partagé l'authentification, lancent le SSID **partagé** configuré.
8. Vérifiez le client sans fil est associé avec succès avec le routeur. Ceci peut être vérifié en détail du routeur Sans fil utilisant la commande de **show dot11 associations**.Voici un exemple :`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [shared] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.4.1.5 CB21AG/PI21AG WCS self Assoc`

Configurez le client sans fil pour l'authentification WPA

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont **wpa**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification WPA (avec l'EAP).
3. Sous Profile Management, cliquez sur l'**onglet Sécurité**, placez l'option de Sécurité comme **WPA/WPA2/CCKM** et choisissez le type approprié d'EAP WPA/WPA2/CCKM.Ce document utilise le **LEAP** comme type d'EAP pour l'authentification.
4. Cliquez sur Configure afin de configurer les configurations de nom d'utilisateur et mot de passe de LEAP.Sous les configurations de nom d'utilisateur et mot de passe, cet exemple choisit **d'inciter manuellement pour le nom d'utilisateur et le mot de passe** de sorte que le

client soit incité à écrire le nom d'utilisateur et mot de passe correct tout en essayant de se connecter au réseau.
5. Cliquez sur **OK**.
6. Afin de vérifier l'authentification EAP, lancez le LEAP SSID configuré. Vous êtes incité à écrire un nom d'utilisateur et mot de passe de LEAP. Entrez dans les les deux les qualifications comme **user2**, puis cliquez sur OK.
7. Vérifiez le client sans fil est authentifié avec succès et assigné avec une adresse IP. Ceci peut être vérifié clairement de la fenêtre d'état ADU.

Configurez le client sans fil pour l'authentification de WPA-PSK

Procédez comme suit :

1. Dans la fenêtre Profile Management sur l'ADU, cliquez sur **New** afin de créer un nouveau profil.D'une nouvelle affichages fenêtre où vous pouvez placer la configuration pour l'authentification ouverte.
2. Sous l'onglet General, entrez le nom de profil et le SSID que l'adaptateur client utilisera.Dans cet exemple, le nom de profil et le SSID sont **wpa-psk**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification de WPA-PSK.
3. Sous Profile Management, cliquez sur l'**onglet Sécurité** et placez l'option de Sécurité en tant que **phrase de passe WPA/WPA2**. Puis, cliquez sur Configure afin de configurer la phrase de passe WPA.
4. Définissez une clé pré-partagée WPA. La clé devrait être 8 à 63 caractères ASCII de longueur. Puis, cliquez sur OK.
5. Afin de vérifier le WPA-PSK, lancez le **wpa-psk** SSID configuré.
6. Vérifiez le client sans fil est associé avec succès avec le routeur. Ceci peut être vérifié en détail du routeur Sans fil utilisant la commande de **show dot11 associations**.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Dépannage des commandes

Vous pouvez utiliser ces commandes **debug** pour 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

- Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil
- Configurer des VLAN
- Exemple de configuration d'un routeur sans fil ISR 1800 avec DHCP interne et authentification ouverte
- Radio ISR de Cisco et guide de configuration de Point d'accès HWIC
- Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP
- Configuration des types d'authentification
- Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP
- Support et documentation techniques - Cisco Systems