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

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
Configurez
Diagramme du réseau
Configurez l'authentification ouverte
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurez le SSID pour l'authentification ouverte
Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN
Configurez l'authentification 802.1x/EAP
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurez le serveur local de RAYON pour l'authentification EAP
Configurez le SSID pour l'authentification 802.1x/EAP
Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN
Gestion de clé WPA
Configurer le WPA-PSK
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurez le SSID pour l'authentification de WPA-PSK
Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN
Configurez l'authentification WPA (avec l'EAP)
Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
Configuration de l'interface virtuelle pontée (BVI)
Configurez le serveur local de RAYON pour l'authentification WPA
Configurez le SSID pour le WPA avec l'authentification EAP
Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN
Configurez le client sans fil pour l'authentification
Configurez le client sans fil pour l'authentification ouverte
Configurez le client sans fil pour l'authentification 802.1x/EAP
Configurez le client sans fil pour l'authentification de WPA-PSK
Configurez le client sans fil pour l'authentification WPA (avec l'EAP)

Dépannez
Dépannage des commandes
Informations connexes

Introduction

Ce document fournit l'exemple de configuration qui explique 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 des commandes CLI.

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)
- 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®
- 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

Les Routeurs de configuration fixe de Services intégrés de Cisco prennent en charge une solution LAN Sans fil sécurisée, abordable, et facile à utiliser qui combine la mobilité et la flexibilité avec les configurations de classe entreprise exigées par des professionnels de réseau. Le système de gestion étant basé sur le logiciel de Cisco IOS, les Routeurs de Cisco agissent en tant que Points d'accès et sont WiFi certifié, les émetteurs-récepteurs Sans fil de RÉSEAU LOCAL d'IEEE 802.11a/b/g-compliant.

Vous pouvez configurer et surveiller les Routeurs avec l'interface de ligne de commande (CLI), le système de gestion basé sur navigateur, ou le Protocole SNMP (Simple Network Management Protocol). Ce document décrit comment configurer l'ISR pour la connexion sans fil avec les commandes CLI.

Configurez

Cet exemple affiche comment configurer ces types d'authentification sur un routeur de configuration fixe intégré par radio de Cisco avec des commandes CLI.

- Ouvrez l'authentification
- authentification 802.1x/EAP (Extensible Authentication Protocol)
- Authentification principale pré-partagée d'accès protégé par Wi-Fi (WPA-PSK)
- Authentification WPA (avec l'EAP)

Remarque: Ce document ne se concentre pas sur l'authentification partagée puisque c'est un type moins sécurisé d'authentification.

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 avec l'authentification de 802.1x.

Configurez l'authentification ouverte

L'authentification ouverte est un algorithme nul d'authentification. Le Point d'accès accorde 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 du Point d'accès peut accéder au réseau. Le cryptage WEP étant activé sur un Point d'accès, 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 peut pas transmettre des données par le Point d'accès. Ni l'un ni l'autre ne peuvent il déchiffrer des données transmises du Point d'accès.

Cet exemple de configuration explique juste une authentification ouverte simple. La clé WEP peut être rendue obligatoire ou facultative. Cet exemple configure la clé WEP comme facultative de sorte que n'importe quel périphérique qui n'utilise pas le WEP puisse également authentifier et s'associer avec cet AP.

Référez-vous au pour en savoir plus ouvert d'authentification.

Cet exemple emploie cette installation de configuration pour configurer l'authentification ouverte sur l'ISR.

- Nom SSID : « **ouvrez-vous** »
- VLAN 1
- Chaîne interne de serveur DHCP : **10.1.0.0/16**

Remarque: Dans l'intérêt de la simplicité, cet exemple n'utilise aucune technique de cryptage pour les clients authentifiés.

Terminez-vous ces actions sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurez le SSID pour l'authentification ouverte
4. Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Terminez-vous ces actions :

1. **Enable IRB dans le routeur.irb de** router<configure>#bridge**Remarque:** Si tous les types de Sécurité doivent être configurés sur un routeur unique, il est assez pour activer IRB seulement une fois globalement sur le routeur. Il n'a pas besoin d'être activé pour chaque type individuel d'authentification.
2. **Définissez un groupe de passerelle.**Cet exemple utilise le groupe de pontage numéro 1.router<configure>#bridge *1*
3. **Choisissez le Protocole Spanning Tree pour le groupe de passerelle.**Ici, l'IEEE Spanning-Tree Protocol est configuré pour ce groupe de passerelle.**protocol ieee du** router<configure>#bridge *1*
4. **Permettez à une BVI d'accepter et d'acheminer les paquets routables reçus de son groupe de pontage correspondant.**Cet exemple permet au BVI de recevoir et conduire le paquet IP.*IP d'***artère du** router<configure>#bridge *1*

Configuration de l'interface virtuelle pontée (BVI)

Terminez-vous ces actions :

1. **Configurez le BVI.**Configurez le BVI quand vous affectez le nombre correspondant du groupe de passerelle au BVI. Chaque groupe de passerelle peut seulement avoir un BVI correspondant. Cet exemple attribue le groupe de pontage numéro 1 à la BVI.router<configure>#interface **BVI** *<1>*
2. **Assignez une adresse IP au BVI.router<config-if>#ip address** *10.1.1.1 255.255.0.0*router<config-if>#no **fermé**

Référez-vous configurent la transition pour des informations détaillées sur la transition.

Configurez le SSID pour l'authentification ouverte

Terminez-vous ces actions :

1. **Activez l'interface par radio**Afin d'activer l'interface par radio, allez au mode de configuration d'interface de la radio DOT11 et assignez un SSID à l'interface.router<config>#interface

dot11radio0arrêt de router<config-if>#norouter<config-if>#ssid *ouvert*Le type ouvert d'authentification peut être configuré en combination avec l'authentification d'adresse MAC. Dans ce cas, le Point d'accès force tous les périphériques de client pour exécuter l'authentification de mac-address avant qu'on leur permette pour joindre le réseau.L'authentification ouverte peut également être configurée avec l'authentification EAP. Le Point d'accès force tous les périphériques de client pour exécuter l'authentification EAP avant qu'on leur permette pour joindre le réseau. Pour le nom de liste, spécifiez la liste de méthode d'authentification.Un Point d'accès configuré pour l'authentification EAP force tous les périphériques de client qui s'associent pour exécuter l'authentification EAP. Les périphériques de client qui n'utilisent pas l'EAP ne peuvent pas utiliser le Point d'accès.

2. **Grippage SSID à un VLAN.**Afin d'activer le SSID sur cette interface, liez le SSID au VLAN dans le mode de configuration SSID.*1* router<config-ssid>vlan
3. **Configurez le SSID avec l'authentification ouverte.**router<config-ssid>#authentication **ouvert**
4. **Configurez l'interface par radio pour la clé WEP facultative.VLAN de** router<config>#encryption *1* **mode WEP facultatif**
5. **Enable VLAN sur l'interface par radio.**router<config>#interface **Dot11Radio 0.1**router<config-subif>#encapsulation **dot1Q** *1*router<config-subif>#bridge-group *1*

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

Introduisez ces commandes en mode de configuration globale de configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- **ip dhcp excluded-address 10.1.1.1 10.1.1.5**
- **ip dhcp pool** *ouvert*

Dans le mode de configuration de pool DHCP, introduisez ces commandes :

- **réseau** *10.1.0.0 255.255.0.0*
- **default-router** *10.1.1.1*

Configurez l'authentification 802.1x/EAP

Ce type d'authentification fournit le de plus haut niveau de la Sécurité pour votre réseau Sans fil. Le Protocole EAP (Extensible Authentication Protocol) étant utilisé pour interagir avec un serveur Eap-compatible de RAYON, le Point d'accès 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 au Point d'accès, qui l'utilise pour tous les signaux de données d'unicast qu'elle envoie à ou reçoit du client.

Référez-vous au pour en savoir plus d'authentification EAP.

Cet exemple utilise cette configuration installée :

- Nom SSID : **LEAP**
- VLAN 2
- Chaîne interne de serveur DHCP : **10.2.0.0/16**

Cet exemple emploie l'authentification de LEAP comme mécanisme pour authentifier le client sans fil.

Remarque: Référez-vous au Cisco Secure ACS pour Windows v3.2 avec l'authentification de machine d'EAP-TLS pour configurer l'EAP-TLS.

Remarque: Référez-vous à configurer le Cisco Secure ACS pour Windows v3.2 avec l'authentification de machine PEAP-MS-CHAPv2 pour configurer PEAP-MS-CHAPv2.

Remarque: Comprenez que toute la configuration de ces types d'EAP implique principalement les modifications de configuration au côté client et au côté serveur d'authentification. La configuration au routeur Sans fil ou au Point d'accès plus ou moins demeure la même pour tous ces types d'authentification.

Remarque: Comme mentionné au commencement, cette installation utilise le serveur local de RAYON sur la radio ISR pour authentifier des clients sans fil avec l'authentification de 802.1x.

Terminez-vous ces actions sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurez le serveur local de RAYON pour l'authentification EAP
4. Configurez le SSID pour l'authentification 802.1x/EAP
5. Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Terminez-vous ces actions :

1. **Enable IRB dans le routeur.irb de** router<configure>#bridge**Remarque:** Si tous les types de Sécurité doivent être configurés sur un routeur unique, il est assez pour activer IRB seulement une fois globalement sur le routeur. Il n'a pas besoin d'être activé pour chaque type individuel d'authentification.
2. **Définissez un groupe de passerelle.**Cet exemple utilise le passerelle-groupe le numéro 2.router<configure>#bridge *2*
3. **Choisissez le Protocole Spanning Tree pour le groupe de passerelle.**Ici, l'IEEE Spanning-Tree Protocol est configuré pour ce groupe de passerelle.**protocol ieee du** router<configure>#bridge *2*
4. **Choisissez le Protocole Spanning Tree pour le groupe de passerelle.**Ici, l'IEEE Spanning-Tree Protocol est configuré pour ce groupe de passerelle.**protocol ieee du** router<configure>#bridge *2*
5. **Permettez à un BVI de recevoir et conduire les paquets routable qui sont reçus de son groupe correspondant de passerelle.**Cet exemple permet au BVI de recevoir et conduire des paquets IP.*IP d'***artère du** router<configure>#bridge *2*

Configuration de l'interface virtuelle pontée (BVI)

Terminez-vous ces actions :

1. **Configurez le BVI.**Configurez le BVI quand vous affectez le nombre correspondant du groupe de passerelle au BVI. Chaque groupe de passerelle peut seulement avoir un BVI correspondant. Cet exemple assigne le groupe le numéro 2 de passerelle au

BVI.router<configure>#interface **BVI** *<2>*
2. **Assignez une adresse IP au BVI.router<config-if>#ip address** *10.2.1.1 255.255.0.0*router<config-if>#no **fermé**

Configurez le serveur local de RAYON pour l'authentification EAP

Comme indiqué précédemment, ce document utilise le serveur local de RAYON sur le routeur averti Sans fil pour l'authentification EAP.

1. **Activez le modèle de contrôle d'accès d'Authentification, autorisation et comptabilité (AAA).nouveau-modèle de** router<configure>#aaa
2. **Créez un rad-eap de groupe de serveurs pour le serveur de RAYON.acct-port** *1813 du l'authentique*-**port** *1812 de 10.2.1.1 de* **serveur de rad-***eap de* **rayon de serveur de groupe de** router<configure>#aaa
3. **Créez les eap_methods d'une liste de méthode qui répertorie la méthode d'authentification utilisée pour authentifier l'utilisateur de connexion d'AAA. Assignez la liste de méthode à ce groupe de serveurs.***rad-eap de* **groupe d'***eap_methods d'***authentication login de** router<configure>#aaa
4. **Activez le routeur en tant que serveur d'authentification locale et entrez dans le mode de configuration pour l'authentificateur.gens du pays de** router<configure>#radius-server
5. **En mode de configuration du serveur RADIUS, ajoutez le routeur en tant que client d'AAA du serveur d'authentification locale.clé** *Cisco de 10.2.1.1 de* router<config-radsrv>#nas
6. **Configurez l'utilisateur *user1* sur le serveur local de rayon.***rad-eap de* **groupe du mot de passe** *user1 du* router<config-radsrv>#user *user1*
7. **Spécifiez l'hôte de serveur de RAYON.acct-port** *1813 Cisco* **principal du l'authentique-port** *1812 de 10.2.1.1 d'***hôte de** router<config-radsrv>#radius-server**Remarque:** Cette clé devrait être identique que celle a spécifiée dans le **nas** commandent sous le mode de configuration du serveur RADIUS.

Configurez le SSID pour l'authentification 802.1x/EAP

La configuration de l'interface par radio et du SSID associé pour 802.1x/EAP implique la configuration de divers paramètres Sans fil sur le routeur, qui inclut le SSID, le mode de chiffrement, et le type d'authentification. Cet exemple utilise le *LEAP* appelé par SSID.

1. **Activez l'interface par radio.**Afin d'activer l'interface par radio, allez au mode de configuration d'interface de la radio DOT11 et assignez un SSID à l'interface.router<config>#interface **dot11radio0arrêt de** router<config-if>#no*LEAP de* router<config-if>#ssid
2. **Grippage SSID à un VLAN.**Afin d'activer le SSID sur cette interface, liez le SSID au VLAN dans le mode de configuration SSID.*2* router<config-ssid>#vlan
3. **Configurez le SSID avec l'authentification 802.1x/LEAP.***eap_methods de réseau*-**eap de** router<config-ssid>#authentication
4. **Configurez l'interface par radio pour la gestion dynamique des clés.VLAN de** router<config>#encryption *2* **chiffrements wep40 de mode**
5. **Enable VLAN sur l'interface par radio.**router<config>#interface **Dot11Radio 0.2**router<config-subif>#encapsulation **dot1Q** *2*router<config-subif>#bridge-group *2*

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

Introduisez ces commandes en mode de configuration globale de configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- **ip dhcp excluded-address 10.2.1.1 10.2.1.5**
- *leapauth d'***ip dhcp pool**

Dans le mode de configuration de pool DHCP, introduisez ces commandes :

- **réseau** *10.2.0.0 255.255.0.0*
- **default-router** *10.2.1.1*

Gestion de clé WPA

L'accès protégé par Wi-Fi 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 les systèmes LAN Sans fil actuels et futurs.

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

Prises en charge de la gestion deux de clé WPA mutuellement - la Gestion exclusive tape : Le WPA-Pré-Sshared introduisent (WPA-PSK) et WPA (avec l'EAP).

Configurer le WPA-PSK

Le WPA-PSK est utilisé comme type de gestion des clés sur un RÉSEAU LOCAL Sans fil où l'authentification 802.1x-based n'est pas disponible. Dans de tels réseaux, vous devez configurer une clé pré-partagée sur le Point d'accès. 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 le Point d'accès développe la clé avec 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 cette configuration installée :

- Nom SSID : **WPA-partagé**
- VLAN 3
- Chaîne interne de serveur DHCP : **10.3.0.0/16**

Terminez-vous ces actions sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurez le SSID pour l'authentification de WPA-PSK
4. Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Terminez-vous ces actions :

1. **Enable IRB dans le routeur.irb de** router<configure>#bridge**Remarque:** Si tous les types de Sécurité doivent être configurés sur un routeur unique, il est assez pour activer IRB

seulement une fois globalement sur le routeur. Il n'a pas besoin d'être activé pour chaque type individuel d'authentification.
2. **Définissez un groupe de passerelle.**Cet exemple utilise le passerelle-groupe le numéro **3.**router<configure>#bridge *3*
3. **Choisissez le Protocole Spanning Tree pour le groupe de passerelle.**L'IEEE Spanning-Tree Protocol est configuré pour ce groupe de passerelle.**protocol ieee du** router<configure>#bridge *3*
4. **Permettez à une BVI d'accepter et d'acheminer les paquets routables reçus de son groupe de pontage correspondant.**Cet exemple permet au BVI de recevoir et conduire des paquets IP.*IP d'***artère du** router<configure>#bridge *3*

Configuration de l'interface virtuelle pontée (BVI)

Terminez-vous ces actions :

1. **Configurez le BVI.**Configurez le BVI quand vous affectez le nombre correspondant du groupe de passerelle au BVI. Chaque groupe de passerelle peut seulement avoir un BVI correspondant. Cet exemple assigne le groupe le numéro 3 de passerelle au BVI.router<configure>#interface **BVI** *<2>*
2. **Assignez une adresse IP au BVI.router<config-if>#ip address** *10.3.1.1 255.255.0.0*router<config-if>#no **fermé**

Configurez le SSID pour l'authentification de WPA-PSK

Terminez-vous ces actions :

1. **Activez l'interface par radio.**Afin d'activer l'interface par radio, allez au mode de configuration d'interface de la radio DOT11 et assignez un SSID à l'interface.router<config>#interface **dot11radio0arrêt de** router<config-if>#norouter<config-if>#ssid WPA-*partagé*
2. **Afin d'activer la Gestion de clé WPA, configurez d'abord le chiffrement de chiffrement WPA pour l'interface VLAN. Cet exemple utilise le tkip comme chiffrement de cryptage**.Introduisez cette commande de spécifier le type de Gestion de clé WPA sur l'interface par radio.router<config>#interface **dot11radio0***tkip de* **chiffrements de mode du VLAN** *3 de* #encryption de routeur (config-si)
3. **Grippage SSID à un VLAN.**Afin d'activer le SSID sur cette interface, liez le SSID au VLAN dans le mode de configuration SSID.*3* router<config-ssid>vlan
4. **Configurez le SSID avec l'authentification de WPA-PSK.Vous devez configurer l'authentification EAP ouverte ou de réseau d'abord dans le mode de configuration SSID pour activer la Gestion de clé WPA. Cet exemple configure l'authentification ouverte.**router<config>#interface **dot11radio0**router<config-if>#ssid WPA-*partagé*router<config-ssid>#authentication **ouvertMaintenant, Gestion de clé WPA d'enable sur le SSID. Le tkip de chiffrement de gestion des clés est déjà configuré pour ce VLAN.wpa de gestion des clés de** #authentication de routeur (config-si-SSID)**Configurez l'authentification de WPA-PSK sur le SSID.**#wpa-psk **ASCII** *1234567890 de* routeur (config-si-SSID) *! ------ 1234567890 est la valeur principale pré-partagée pour ce SSID. Assurez-vous que la même clé est spécifiée pour ce SSID au côté client.*
5. **Enable VLAN sur l'interface par radio.**router<config>#interface **Dot11Radio 0.3**router<config-subif>#encapsulation **dot1Q** *3*router<config-subif>#bridge-group *3*

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

Introduisez ces commandes en mode de configuration globale de configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- **ip dhcp excluded-address 10.3.1.1 10.3.1.5**
- *wpa-psk d'***ip dhcp pool**

Dans le mode de configuration de pool DHCP, introduisez ces commandes :

- **réseau** *10.3.0.0 255.255.0.0*
- **default-router** *10.3.1.1*

Configurez l'authentification WPA (avec l'EAP)

C'est un autre type de Gestion de clé WPA. Ici, les clients et le serveur d'authentification authentifient entre eux avec une méthode d'authentification EAP, et le client et serveur génèrent par paires une clé principale (PMK). Avec le WPA, le serveur génère le PMK dynamiquement et le passe au Point d'accès, mais, avec le WPA-PSK, vous configurez une clé pré-partagée sur le client et le Point d'accès, et cette clé pré-partagée est utilisée comme PMK.

Référez-vous au WPA avec le pour en savoir plus d'authentification EAP.

Cet exemple utilise cette configuration installée :

- Nom SSID : **wpa-dot1x**
- VLAN 4
- Chaîne interne de serveur DHCP : **10.4.0.0/16**

Terminez-vous ces actions sur le routeur :

1. Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont
2. Configuration de l'interface virtuelle pontée (BVI)
3. Configurez le serveur local de RAYON pour l'authentification WPA.
4. Configurez le SSID pour le WPA avec l'authentification EAP
5. Configurez le serveur DHCP interne pour les clients sans fil de ce VLAN

Configurez le Routage et pontage intégrés (IRB) et installez le groupe de pont

Terminez-vous ces actions :

1. **Enable IRB dans le routeur.irb de** router<configure>#bridge**Remarque:** Si tous les types de Sécurité doivent être configurés sur un routeur unique, il est assez pour activer IRB seulement une fois globalement sur le routeur. Il n'a pas besoin d'être activé pour chaque type individuel d'authentification.
2. **Définissez un groupe de passerelle.**Cet exemple utilise le passerelle-groupe le numéro **4.**router<configure>#bridge *4*
3. **Sélectionnez le Protocole Spanning Tree pour le groupe de passerelle.**Ici, l'IEEE Spanning-Tree Protocol est configuré pour ce groupe de passerelle.**protocol ieee du** router<configure>#bridge *4*

4. **Permettez à un BVI de recevoir et conduire les paquets routable reçus de son groupe correspondant de passerelle.**Cet exemple permet au BVI de recevoir et conduire des paquets IP.*IP d'***artère du** router<configure>#bridge *4*

Configuration de l'interface virtuelle pontée (BVI)

Terminez-vous ces actions :

1. **Configurez le BVI.**Configurez le BVI quand vous affectez le nombre correspondant du groupe de passerelle au BVI. Chaque groupe de passerelle peut seulement avoir un BVI correspondant. Cet exemple assigne le groupe le numéro 4 de passerelle au BVI.router<configure>#interface **BVI** *<4>*
2. **Assignez une adresse IP au BVI.router<config-if>#ip address** *10.4.1.1 255.255.0.0*router<config-if>#no **fermé**

Configurez le serveur local de RAYON pour l'authentification WPA

Référez-vous à la section sous l'authentification 802.1x/EAP pour la procédure détaillée.

Configurez le SSID pour le WPA avec l'authentification EAP

Terminez-vous ces actions :

1. **Activez l'interface par radio.**Afin d'activer l'interface par radio, allez au mode de configuration d'interface de la radio DOT11 et assignez un SSID à l'interface.router<config>#interface **dot11radio0arrêt de** router<config-if>#norouter<config-if>#ssid *wpa-dot1x*
2. **Afin d'activer la Gestion de clé WPA, configurez d'abord le chiffrement de chiffrement WPA pour l'interface VLAN. Cet exemple utilise le tkip comme chiffrement de cryptage**.Introduisez cette commande de spécifier le type de Gestion de clé WPA sur l'interface par radio.router<config>#interface **dot11radio0***tkip de* **chiffrements de mode du VLAN** *4 de* #encryption de routeur (config-si)
3. **Grippage SSID à un VLAN.**Afin d'activer le SSID sur cette interface, liez le SSID au VLAN dans le mode de configuration SSID.**VLAN** *4*
4. **Configurez le SSID avec l'authentification de WPA-PSK.**Afin de configurer l'interface par radio pour le WPA avec l'authentification EAP, configurez d'abord le SSID associé pour l'EAP de réseau.router<config>#interface **dot11radio0**router<config-if>#ssid WPA-*partagéeap_methods d'***eap de réseau de** router<config-ssid>#authentication
5. **Maintenant, activez la Gestion de clé WPA sur le SSID. Le tkip de chiffrement de gestion des clés est déjà configuré pour ce VLAN.wpa de gestion des clés de** #authentication de routeur (config-si-SSID)
6. **Enable VLAN sur l'interface par radio.**router<config>#interface **Dot11Radio 0.4**router<config-subif>#encapsulation **dot1Q** *4*router<config-subif>#bridge-group *4*

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

Introduisez ces commandes en mode de configuration globale de configurer le serveur DHCP interne pour les clients sans fil de ce VLAN :

- **ip dhcp excluded-address 10.4.1.1 10.4.1.5**
- **ip dhcp pool** *wpa-dot1shared*

Dans le mode de configuration de pool DHCP, introduisez ces commandes :

- **réseau** *10.4.0.0 255.255.0.0*
- **default-router** *10.4.1.1*

Configurez le client sans fil pour l'authentification

Après que vous configuriez l'ISR, configurez le client sans fil pour différents types d'authentification comme expliqué de sorte que le routeur puisse authentifier ces clients sans fil et permettre d'accéder au réseau WLAN. Ce document utilise Cisco Aironet Desktop Utility (ADU) pour la configuration de côté client.

Configurez le client sans fil pour l'authentification ouverte

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. Sous l'**onglet Général**, écrivez le nom de profil et le SSID que l'adaptateur de client utilise.Dans cet exemple, le nom de profil et le SSID sont **ouverts**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification ouverte.
2. Cliquez sur l'**onglet Sécurité** et laissez l'option de Sécurité en tant qu'**aucun** pour le cryptage WEP. Puisque cet exemple utilise le WEP comme facultatif, l'établissement de cette option à aucun permettra au client avec succès pour s'associer et communiquer avec le réseau WLAN.Cliquez sur OK
3. Sélectionnez la **fenêtre avancée de l'**onglet de **Profile Management** et placez l'authentication mode de 802.11 comme **ouverte** pour l'authentification ouverte.

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

1. Après que le profil de client soit créé, le clic **lancent** sous l'onglet de Profile Management pour lancer le profil.
2. Vérifiez l'état ADU pour une authentification réussie.

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. Sous l'**onglet Général**, écrivez le nom de profil et le SSID que l'adaptateur de client utilise.Dans cet exemple, le nom de profil et le SSID sont **LEAP**.
2. 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. Maintenant, cliquez sur Configure pour configurer des configurations de nom d'utilisateur et mot de passe de LEAP.**Remarque:** Remarque: Le SSID

doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification 802.1x/EAP.
3. Sous des 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 entrer le nom d'utilisateur et le mot de passe corrects tandis que les essais de client pour se connecter au réseau. Cliquez sur **OK**.

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

- Après que le profil de client soit créé, le clic **lancent** sous l'onglet de **Profile Management** pour lancer le **LEAP de** profil. Vous êtes incité pour le nom d'utilisateur et le mot de passe de **LEAP**. Cet exemple utilise le nom d'utilisateur et mot de passe **user1**. Cliquez sur **OK**.
- Vous pouvez observer le client authentifier avec succès et être assigné une adresse IP du serveur DHCP configuré sur le routeur.

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. Sous l'**onglet Général**, écrivez le **nom de profil** et le **SSID** que l'adaptateur de client utilise.Dans cet exemple, le nom de profil et le SSID WPA-**sont partagés**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification de WPA-PSK.
2. Sous **Profile Management**, cliquez sur l'**onglet Sécurité** et placez l'option de Sécurité en tant que **phrase de passe WPA/WPA2**. Maintenant, cliquez sur Configure pour configurer la phrase de passe WPA.
3. Définissez une clé pré-partagée WPA. La clé doit être 8 à 63 caractères ASCII de longueur. Cliquez sur **OK**.

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

- Après que le profil de client soit créé, le clic **lancent** sous l'onglet de **Profile Management** pour lancer le profil WPA-**partagé**.
- Vérifiez l'ADU pour une authentification réussie.

Configurez le client sans fil pour l'authentification WPA (avec l'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. Sous l'**onglet Général**, écrivez le nom de profil et le SSID que l'adaptateur de client utilise.Dans cet exemple, le nom de profil et le SSID sont **wpa-dot1x**.**Remarque:** Le SSID doit apparier le SSID que vous avez configuré sur l'ISR pour l'authentification WPA (avec l'EAP).
2. Sous **Profile Management**, cliquez sur l'**onglet Sécurité**, placez l'option de Sécurité comme **WPA/WPA2/CCKM**, et et choisissez le type approprié d'EAP WPA/WPA2/CCKM. Ce document utilise le LEAP comme type d'EAP pour l'authentification. Maintenant, cliquez sur Configure pour configurer des configurations de nom d'utilisateur et mot de passe de LEAP.

3. Sous la région de 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 entrer le nom d'utilisateur et le mot de passe corrects tandis que les essais de client pour se connecter au réseau. Cliquez sur **OK**.

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

1. Après que le profil de client soit créé, le clic **lancent** sous l'onglet de Profile Management pour lancer le profil **wpa-dot1x**. Vous êtes incité pour le nom d'utilisateur et le mot de passe de LEAP. Cet exemple utilise le nom d'utilisateur et mot de passe comme **user1**. Cliquez sur **OK**.
2. Vous pouvez observer le client authentifier avec succès.

Le show dot11 associations de commande du routeur CLI affiche les détails complets sur l'état d'association de client. Voici un exemple.

Associations de Router#show **dot11**

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.0.2 CB21AG/PI21AG WCS self
EAP-Assoc SSID [open] : SSID [pre-shared] : DISABLED, not associated with a configured VLAN SSID
[wpa-dot1x] : SSID [wpa-shared] : Others: (not related to any ssid)
```

Dépannez

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 sur des Points d'accès
- 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
- Support et documentation techniques - Cisco Systems

- 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