# Exemple de configuration d'un WLAN invité et d'un WLAN interne à l'aide de contrôleurs de réseau local sans fil (WLC)

## Contenu



# Introduction

Ce document fournit un exemple de configuration pour un réseau local (WLAN) sans fil d'invité et un WLAN interne sécurisé qui utilise des contrôleurs WLAN (WLC) et des points d'accès léger (LAP). Dans la configuration dans ce document, le WLAN invité emploie l'authentification Web pour authentifier des utilisateurs et le WLAN interne sécurisé utilise l'authentification Extensible Authentication Protocol (EAP).

# Conditions préalables

## Conditions requises

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

- La connaissance de la façon configurer le WLC avec des paramètres de base
- La connaissance de la façon installer un DHCP et un serveur de Système de noms de domaine (DNS)

## Composants utilisés

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

- Cisco 2006 WLC qui exécute la version de microprogramme 4.0
- RECOUVREMENT de gamme Cisco 1000
- Adaptateur client sans fil Cisco 802.11a/b/g exécutant la version de microprogramme 2.6
- Routeur de Cisco 2811 qui exécute la version 12.4(2)XA de Cisco IOS®
- Cisco 3500 gammes XL commutent que version 12.0(5)WC3b de Cisco IOS de passages
- Serveur DNS qui fonctionne sur un serveur de Microsoft Windows 2000

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.

# Configuration du réseau

L'exemple de configuration dans ce document utilise l'installation affichée dans ce diagramme. Le RECOUVREMENT est enregistré au WLC. Le WLC est connecté au commutateur de la couche 2. Le routeur qui connecte les utilisateurs au WAN également se connecte au commutateur de la couche 2. Vous devez créer deux WLAN, un pour les utilisateurs d'invité et l'autre pour les utilisateurs internes de RÉSEAU LOCAL. Vous avez besoin également d'un serveur DHCP pour fournir des adresses IP pour l'invité et les clients sans fil internes. Les utilisateurs d'invité emploient l'authentification Web afin d'accéder au réseau. L'authentification EAP d'utilisation d'utilisateurs internes. Le routeur 2811 agit également en tant que serveur DHCP pour les clients sans fil.

**Remarque:** Ce document suppose que le WLC est configuré avec les paramètres de base et le RECOUVREMENT est enregistré au WLC. Référez-vous à l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC) pour les informations sur la façon dont configurer les paramètres de base sur un WLC et la façon enregistrer le RECOUVREMENT à WLC.

Une fois configurés comme serveur DHCP, certains des Pare-feu ne prennent en charge pas des requêtes DHCP d'un agent de relais. Le WLC est un agent de relais pour le client. Le Pare-feu configuré comme serveur DHCP ignore ces demandes. Des clients doivent être directement connectés au Pare-feu et ne peuvent pas envoyer des demandes par un agent ou un routeur différent de relais. Le Pare-feu peut fonctionner comme serveur DHCP simple pour les hôtes internes qui sont directement connectés à lui. Ceci permet au Pare-feu pour mettre à jour sa table basée sur les adresses MAC qui sont directement connectées et qui elle peut voir. C'est pourquoi une tentative d'assigner des adresses d'un relais DHCP ne sont pas disponible et les paquets sont jetés. Le Pare-feu PIX a cette limite.

# Configurez

Terminez-vous ces étapes afin de configurer les périphériques pour cette configuration réseau :

1. Configurez les interfaces dynamiques sur le WLC pour l'invité et les utilisateurs internes
2. Créez les WLAN pour l'invité et les utilisateurs internes
3. Configurez le port de commutateur de la couche 2 qui se connecte au WLC comme port de joncteur réseau
4. Configurez le routeur pour les deux VLAN

## Configurez les interfaces dynamiques sur le WLC pour l'invité et les utilisateurs internes

La première étape est de créer deux interfaces dynamiques sur le WLC, un pour les utilisateurs d'invité et l'autre pour des utilisateurs internes.

L'exemple dans ce document utilise ces paramètres et valeurs pour les interfaces dynamiques :

```
Guest-WLAN                                                    Internal-WLAN
VLAN Id : 10                              VLAN Id : 20
IP address: 10.0.0.10                            IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                               Gateway: 20.0.0.50
Physical port on WLC: 1                               Physical port on WLC: 1
DHCP server: 172.16.1.60                                DHCP server: 172.16.1.60
```

Procédez comme suit :

1. Du GUI WLC, choisissez les **contrôleurs > les interfaces**.La fenêtre Interfaces apparaît. Cette fenêtre liste les interfaces qui sont configurées sur le contrôleur. Ceci inclut les interfaces par défaut, qui sont l'interface de gestion, interface d'AP-gestionnaire, l'interface virtuelle et l'interface de port de service, et les interfaces dynamiques définies par l'utilisateur.
2. Afin de créer une nouvelle interface dynamique, cliquez sur **New**.
3. Dans les interfaces > la nouvelle fenêtre, écrivent le nom d'interface et l'ID de VLAN. Cliquez ensuite sur **Apply**.Dans cet exemple, l'interface dynamique est nommée Invité-WLAN et l'ID de VLAN est assigné 10.
4. Dans la fenêtre d'Interfaces > Edit, pour l'interface dynamique, entrez dans l'adresse IP, le masque de sous-réseau, et la passerelle par défaut. Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur **Apply**.C'est l'exemple :La même procédure doit être terminée afin de créer une interface dynamique pour le WLAN interne.
5. Dans les interfaces > la nouvelle fenêtre, écrivent l'Interne-**WLAN** pour l'interface dynamique pour les utilisateurs internes, et écrivent **20** pour l'ID de VLAN. Cliquez ensuite sur **Apply**.
6. Dans la fenêtre d'Interfaces > Edit, pour l'interface dynamique, entrez dans l'adresse IP, le masque de sous-réseau, et la passerelle par défaut. Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur **Apply**.Maintenant que deux interfaces dynamiques sont créées, la fenêtre d'interfaces récapitule la liste d'interfaces configurée sur le contrôleur.

## Créez les WLAN pour l'invité et les utilisateurs internes

L'étape suivante est de créer des WLAN pour les utilisateurs d'invité et les utilisateurs internes, et trace l'interface dynamique aux WLAN. En outre, les méthodes de Sécurité qui sont utilisées pour

authentifier l'invité et les utilisateurs de sans fil doivent être définies. Procédez comme suit :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.Dans cet exemple, le WLAN est nommé *Guest* et l'ID de WLAN est 2.
3. Cliquez sur Apply dans le coin haut droit.
4. L'écran de WLAN > Edit apparaît, qui contient de divers onglets.Sous l'**onglet Général** pour le WLAN invité, choisissez invité-**WLAN du** champ Interface Name. Ceci trace l'interface dynamique invité-**WLAN** qui a été précédemment créée à l'**invité** WLAN.Assurez-vous que l'état du WLAN est activé.Cliquez sur l'onglet **Security**. Pour ce WLAN, l'authentification Web un mécanisme de sécurité de la couche 3 est utilisée pour authentifier des clients. , N'en choisissez par conséquent **aucun** sous le champ de degré de sécurité de la *couche 2*. Dans le domaine de degré de sécurité de la *couche 3*, cochez la case de **stratégie de Web** et choisissez l'option d'**authentification**.**Remarque:** Pour plus d'informations sur l'authentification Web, référez-vous à l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN.Cliquez sur **Apply**.
5. Créez un WLAN pour les utilisateurs internes. Dans la fenêtre de WLANs > New, entrez dans **interne** et choisissez **3** afin de créer un WLAN pour les utilisateurs internes. Cliquez ensuite sur **Apply**.
6. La fenêtre de WLANs > Edit apparaît. Sous l'*onglet Général*, choisissez interne-**WLAN du** champ Interface Name.Ceci trace l'interface dynamique interne-**WLAN** qui a été précédemment créée au WLAN **interne**. Assurez-vous que le WLAN est activé.Laissez l'option de degré de sécurité de la couche 2 au 802.1x de valeur par défaut parce que l'authentification EAP est utilisée pour les utilisateurs internes WLAN.
7. Cliquez sur **Apply**.La fenêtre WLAN apparaît et elle affiche la liste de WLAN qui sont créés.**Remarque:** Référez-vous à l'authentification EAP avec l'exemple de configuration des contrôleurs WLAN (WLC) pour plus d'informations détaillées sur la façon configurer un WLAN basé sur eap avec WLCs.
8. Sur le GUI WLC, la **save configuration de** clic, cliquent sur alors des **commandes du** GUI de contrôleur. Ensuite, choisissez l'option de **réinitialisation** de redémarrer le WLC afin de permettre à l'authentification Web pour prendre effet.**Remarque:** Cliquez sur la **save configuration** afin de sauvegarder la configuration à travers des réinitialisations.

## Configurez le port de commutateur de la couche 2 qui se connecte au WLC comme port de joncteur réseau

Vous devez configurer le port de commutateur pour prendre en charge les VLAN multiples configurés sur le WLC parce que le WLC est connecté à un commutateur de la couche 2. Vous devez configurer le port de commutateur comme port de joncteur réseau de 802.1Q.

Chaque connexion de port de contrôleur est un joncteur réseau de 802.1Q et devrait être configurée en tant que ceci sur le commutateur voisin. Sur des Commutateurs de Cisco, le VLAN indigène d'un joncteur réseau de 802.1Q, par exemple **VLAN 1**, est laissé non-marqué. Par conséquent, si vous configurez l'interface d'un contrôleur pour utiliser le VLAN indigène sur un commutateur voisin de Cisco, veillez-vous pour configurer l'interface sur le contrôleur comme non-marqué.

Une valeur zéro pour l'identifiant **VLAN** (sur la fenêtre de Controller > Interfaces) signifie que l'interface est non-marquée. Dans l'exemple dans ce document, l'AP-gestionnaire et les interfaces de gestion sont configurés dans le VLAN non balisé par défaut.

Quand une interface de contrôleur est placée à une valeur différente de zéro, elle ne devrait pas être étiquetée au VLAN indigène du commutateur et on doit permettre le VLAN sur le commutateur. Dans cet exemple, VLAN 60 est configuré comme VLAN indigène sur le port de commutateur qui se connecte au contrôleur.

C'est la configuration pour le port de commutateur qui se connecte au WLC :

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

C'est la configuration pour le port de commutateur qui se connecte au routeur comme port de joncteur réseau :

```
interface f0/10
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

C'est la configuration pour le port de commutateur qui se connecte au RECOUVREMENT. Ce port est configuré comme port d'accès :

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

## Configurez le routeur pour les deux WLAN

Dans l'exemple dans ce document, le routeur 2811 connecte les utilisateurs d'invité à l'Internet et connecte également les utilisateurs de câble internes aux utilisateurs de sans fil internes. Vous devez également configurer le routeur pour fournir des services DHCP.

Sur le routeur, créez les sous-interfaces sous l'interface FastEthernet qui se connecte au port de joncteur réseau sur le commutateur pour chaque VLAN. Assignez les sous-interfaces aux VLAN correspondants, et configurez une adresse IP des sous-réseaux respectifs.

**Remarque:** Seulement des parties appropriées de la configuration de routeur ne sont indiquées, et pas la configuration complète.

C'est la configuration exigée sur le routeur pour accomplir ceci.

Ce sont les commandes qui doivent être émises afin de configurer des services DHCP sur le routeur :

```
!
ip dhcp excluded-address 10.0.0.10
```

```
!--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC.
ip dhcp excluded-address 10.0.0.50 !--- IP excluded because this IP is assigned to the !--- sub-
interface on the router. ip dhcp excluded-address 20.0.0.10 !--- IP excluded because this IP is
assigned to the dynamic !--- interface created on the WLC. ip dhcp excluded-address 20.0.0.50 !-
-- IP excluded because this IP is assigned to the sub-interface on the router. ! ip dhcp pool
Guest !--- Creates a DHCP pool for the guest users. network 10.0.0.0 255.0.0.0 default-router
10.0.0.50 dns-server 172.16.1.1 !--- Defines the DNS server. ! ip dhcp pool Internal network
20.0.0.0 255.0.0.0 default-router 20.0.0.50 !--- Creates a DHCP pool for the internal users. !
```

Ces commandes doivent être émises sur l'interface FastEthernet pour l'exemple installé :

```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest
VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN
encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the internal VLAN. !
```

# Vérifiez

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

Connectez deux clients sans fil, un utilisateur d'invité (à l'**invité de l'**identifiant d'ensemble de services [SSID]) et un utilisateur interne (avec le SSID **interne**), afin de vérifier la configuration travaille comme prévu.

Souvenez-vous que le WLAN invité a été configuré pour l'authentification Web. Quand le client sans fil d'invité monte, écrivez n'importe quel URL sur le navigateur Web. La page d'authentification de web par défaut s'affiche et vous incite à écrire le nom d'utilisateur et mot de passe. Une fois que l'utilisateur d'invité entre un nom d'utilisateur valide/mot de passe, le WLC authentifie l'utilisateur d'invité et permet l'accès au réseau (probablement l'Internet). Cet exemple affiche la fenêtre d'authentification Web que l'utilisateur reçoit et la sortie sur une authentification réussie :

Le WLAN interne dans cet exemple est configuré pour l'authentification de 802.1x. Quand le client WLAN interne monte, le client utilise l'authentification EAP. Pour plus d'informations sur la façon configurer le client pour l'authentification EAP, référez-vous à la section de utilisation d'authentification EAP du guide d'installation et de configuration d'adaptateurs client LAN sans fil de Cisco Aironet 802.11a/b/g (CB21AG et PI21AG). Après l'authentification réussie, l'utilisateur peut accéder au réseau interne. Cet exemple affiche un client sans fil interne qui utilise l'authentification de Lightweight Extensible Authentication Protocol (LEAP) :

# Dépannez

## Procédure de dépannage

Utilisez cette section pour dépanner votre configuration.

Si la configuration ne fonctionne pas comme prévu, terminez-vous ces étapes :

1. Assurez-vous qu'on permet tous les VLAN configurés sur le WLC sur le port de commutateur connecté au WLC.
2. Assurez que ce port de commutateur qui se connecte au WLC et au routeur est configuré comme port de joncteur réseau.
3. Assurez-vous que les IDs de VLAN utilisés sont identiques sur le WLC et le routeur.
4. Vérifiez si les clients reçoivent des adresses DHCP du serveur DHCP. Sinon, vérifiez si le serveur DHCP est configuré correctement. Pour plus d'informations sur des questions de client de dépannage, référez-vous aux questions de client de dépannage dans le réseau sans fil unifié Cisco.

Une des questions fréquentes qui se produit avec l'authentification Web est quand le redirect to que la page d'authentification Web ne fonctionne pas. L'utilisateur ne voit pas la fenêtre d'authentification Web quand le navigateur est ouvert. Au lieu de cela, l'utilisateur doit manuellement entrer dans **https://1.1.1.1/login.html** afin d'obtenir à la fenêtre d'authentification Web. Ceci doit faire avec la consultation de DN, que les besoins de fonctionner avant le redirect to la page d'authentification Web se produit. Si la page d'accueil de navigateur sur le client sans fil indique un nom de domaine, vous devez exécuter le nslookup avec succès une fois que les associés de client afin du redirect to travaillent.

En outre, pour un WLC qui exécute une version plus tôt que 3.2.150.10, la manière dont les travaux d'authentification Web est quand un utilisateur dans ce SSID tente d'accéder à l'Internet, l'interface de gestion du contrôleur fait une requête DNS pour voir si l'URL est valide. S'il est valide, l'URL affiche la page d'autorisation avec l'adresse IP d'interfaces virtuelles. Après d'utilisateur les logins avec succès, on permet la demande d'origine de passer de nouveau au client. C'est en raison de l'ID de bogue Cisco CSCsc68105 (clients enregistrés seulement). Le pour en savoir plus, se rapportent à l'authentification Web de dépannage sur un contrôleur LAN Sans fil (WLC).

## Dépannage des commandes

**Remarque:** Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Vous pouvez employer ces commandes de débogage afin de dépanner la configuration :

- **debug mac addr <adresse-MAC-client xx: xx : xx : xx : xx : xx>** — Configure le débogage d'adresse MAC pour le client.
- **le debug aaa tout activent** — Configures mettent au point de tous les messages d'AAA.
- **debug pem state enable** — Configure le débogage de l'ordinateur d'état de gestionnaire des stratégies.
- **debug pem events enable** — Configure le débogage des événements de gestionnaire des stratégies.
- **enable de message de debug dhcp** — Employez cette commande afin d'afficher les informations de débogage au sujet des activités de DHCP Client et surveiller l'état des paquets DHCP.
- **debug dhcp packet enable** — Employez cette commande afin d'afficher les informations de niveau de paquet DHCP.
- **debug pm ssh-appgw enable** — Configure le débogage des passerelles d'application.
- **enable de ssh-TCP de debug pm** — Configures mettent au point de la manipulation de TCP de gestionnaire de stratégie.

Voici les sorties témoin de certaines de ces commandes de **débogage** :

**Remarque:** Quelques lignes de sortie ont été enveloppées à une deuxième ligne due aux raisons spatiales.

**(Cisco Controller) >debug dhcp message enable** Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: **requested ip = 10.0.0.1** Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8) Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet (332 octets)from 00:40:96:ac:e6:57 -- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64

**(Cisco Controller) >debug dhcp packet enable** Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1, encap: 0xec03 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request, client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb port number: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57 dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50, dhcpRelay: 10.0.0.10 VLAN: 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57 Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50, VLAN: 30, port: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREQUEST, htype: Ethernet,hlen: 6, hops: 1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50, len 350,switchport 2, vlan 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2, encap: 0xec00 Fri Mar 2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412, switchport 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1 rcvd server id: 10.0.0.50

**(Cisco Controller) >debug aaa all enable** Fri Mar 2 16:22:40 2007: **User user1 authenticated** Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 **Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57** Fri Mar 2 16:22:40 2007: AuthorizationResponse: 0xbadff97c Fri Mar 2 16:22:40 2007: structureSize.....70 Fri Mar 2 16:22:40 2007: resultCode.....0 Fri Mar 2 16:22:40 2007: protocolUsed.....0x00000008 Fri Mar 2 16:22:40 2007: proxyState.....00:40:96:AC:E6:57-00:00 Fri Mar 2 16:22:40 2007: Packet contains 2 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] Service-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override policy for station 00:40:96:ac:e6:57 -

VapAllowRadiusOverride is FALSE Fri Mar 2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c Fri Mar 2 16:22:40 2007: Packet contains 13 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:22:40 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:22:40 2007: AVP[11] Acct-Status-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[12] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:22:40 2007: AVP[13] Called-Station-Id.....10.77.244.210 (13 bytes) when web authentication is closed by user: (Cisco Controller) >Fri Mar 2 16:25:47 2007: AccountingMessage Accounting Stop: 0xa627c78 Fri Mar 2 16:25:47 2007: Packet contains 20 AVPs: Fri Mar 2 16:25:47 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:25:47 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:25:47 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:25:47 2007: AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:25:47 2007: AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes)
**(Cisco Controller) >debug pem state enable** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **WEBAUTH_REQD (8) Change state to START (0)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_NOL3SEC (14) Change state to RUN (20) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1 DHCP_REQD (7) Change stateto RUN (20) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2 DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)
**(Cisco Controller) >debug pem events enable** Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57

```
10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Replacing Fast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot
0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2
16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL
ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Deleting mobile
policy rule 27 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for mobile
00:40:96:ac:e6:57 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding
TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) ReplacingFast Path
rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo
Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57
10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007:
00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry. Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57
10.0.0.1 Added NPU entry of type 8 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU
entry of type 8
```

# Informations connexes

- Accès invité sans fil - Forum Aux Questions
- Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco
- Authentification sur l'exemple Sans fil de configuration de contrôleurs LAN
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems