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 :

- Savoir configurer le WLC avec les paramètres de base
- Savoir configurer un serveur DHCP et DNS (Domain Name System)

Components Used

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

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

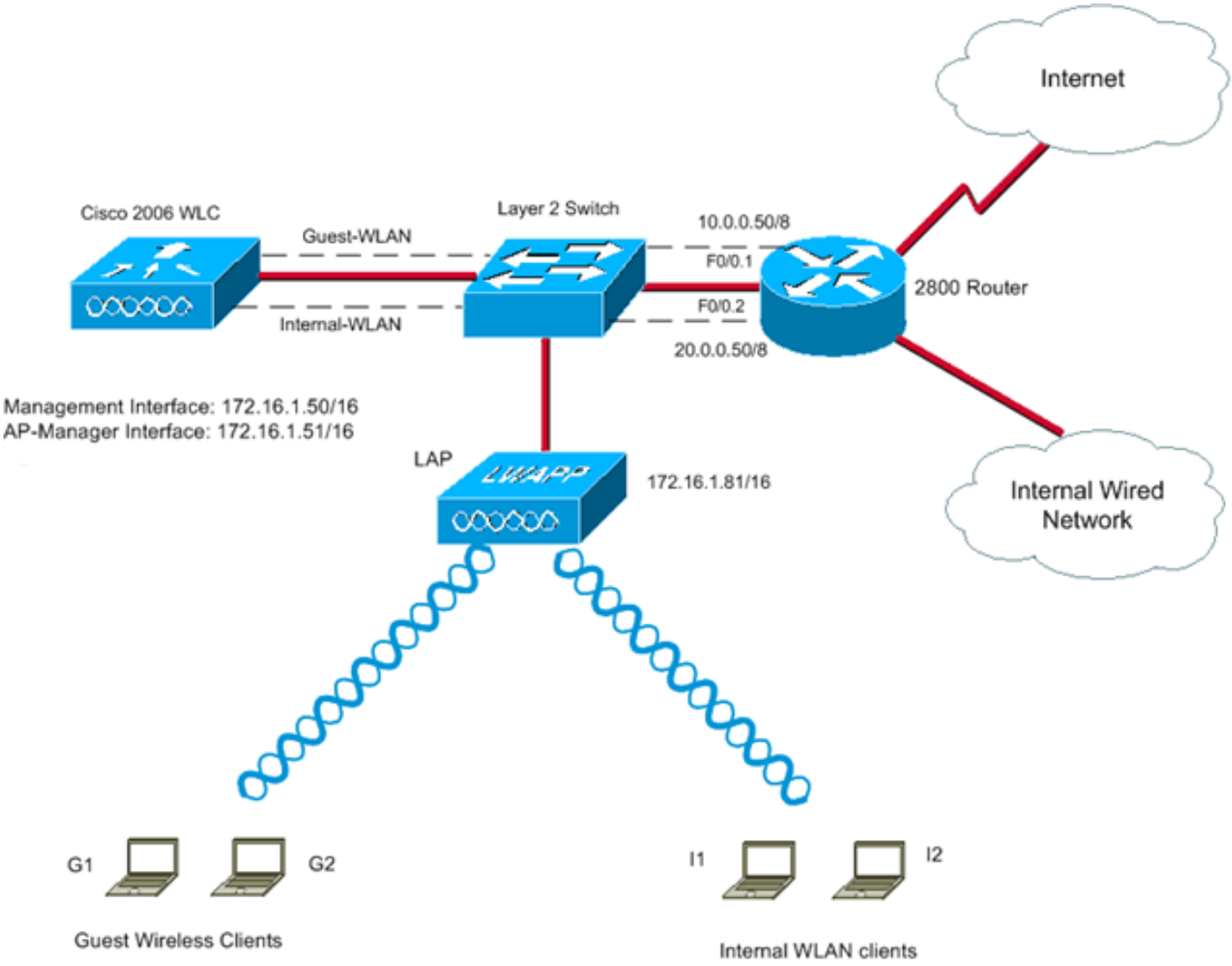
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Configuration du réseau

La configuration donnée en exemple dans le présent document utilise la configuration affichée dans ce diagramme. Le LAP est enregistré sur le WLC. Le WLC est connecté au commutateur de couche 2. Le routeur qui connecte les utilisateurs au réseau WAN se connecte également au commutateur de couche 2. Vous devez créer deux réseaux WLAN, un pour les utilisateurs invités et l'autre pour les utilisateurs du réseau LAN. Vous avez également besoin d'un serveur DHCP pour fournir les adresses IP des clients invités et internes sans fil. Les utilisateurs invités utilisent l'authentification Web pour accéder au réseau. Les utilisateurs internes emploient l'authentification EAP. Le routeur 2811 sert également de serveur DHCP pour les clients sans fil.



Remarque : Le présent document suppose que le WLC est configuré selon les paramètres de base et que le LAP est enregistré sur le WLC. Consulter la section Enregistrer un point d'accès léger (LAP) sur un contrôleur réseau local sans fil (WLC) pour en savoir plus sur la configuration des paramètres de base d'un WLC et l'enregistrement du LAP sur le WLC.

Lorsqu'ils sont configurés comme serveur DHCP, certains pare-feu ne prennent pas en charge les demandes DHCP provenant d'un agent de relais. Le WLC est un agent de relais pour le client. Le pare-feu configuré en tant que serveur DHCP ignore ces demandes. Les clients doivent être connectés directement au pare-feu et ne peuvent pas envoyer de demandes par l'intermédiaire d'un autre agent de relais ou routeur. Le pare-feu peut fonctionner comme un simple serveur DHCP pour les hôtes internes qui y sont directement connectés. Ainsi, le pare-feu peut maintenir sa table en fonction des adresses MAC qui y sont connectées directement et qu'il peut détecter. Pour cette raison, il est impossible d'attribuer des adresses à partir d'un relais DHCP, et les paquets sont rejetés. Par ailleurs, le pare-feu PIX a cette limitation.

Configuration

Effectuer les étapes suivantes pour configurer les périphériques en fonction de cette configuration réseau :

1. Configurer les interfaces dynamiques sur le WLC pour les utilisateurs invités et internes
2. Créer des réseaux WLAN pour les utilisateurs invités et internes

3. Configurer le port de commutation de couche 2 qui se connecte au WLC comme port de liaison
4. Configurer le routeur pour les deux réseaux VLAN

Configurer les interfaces dynamiques sur le WLC pour les utilisateurs invités et internes

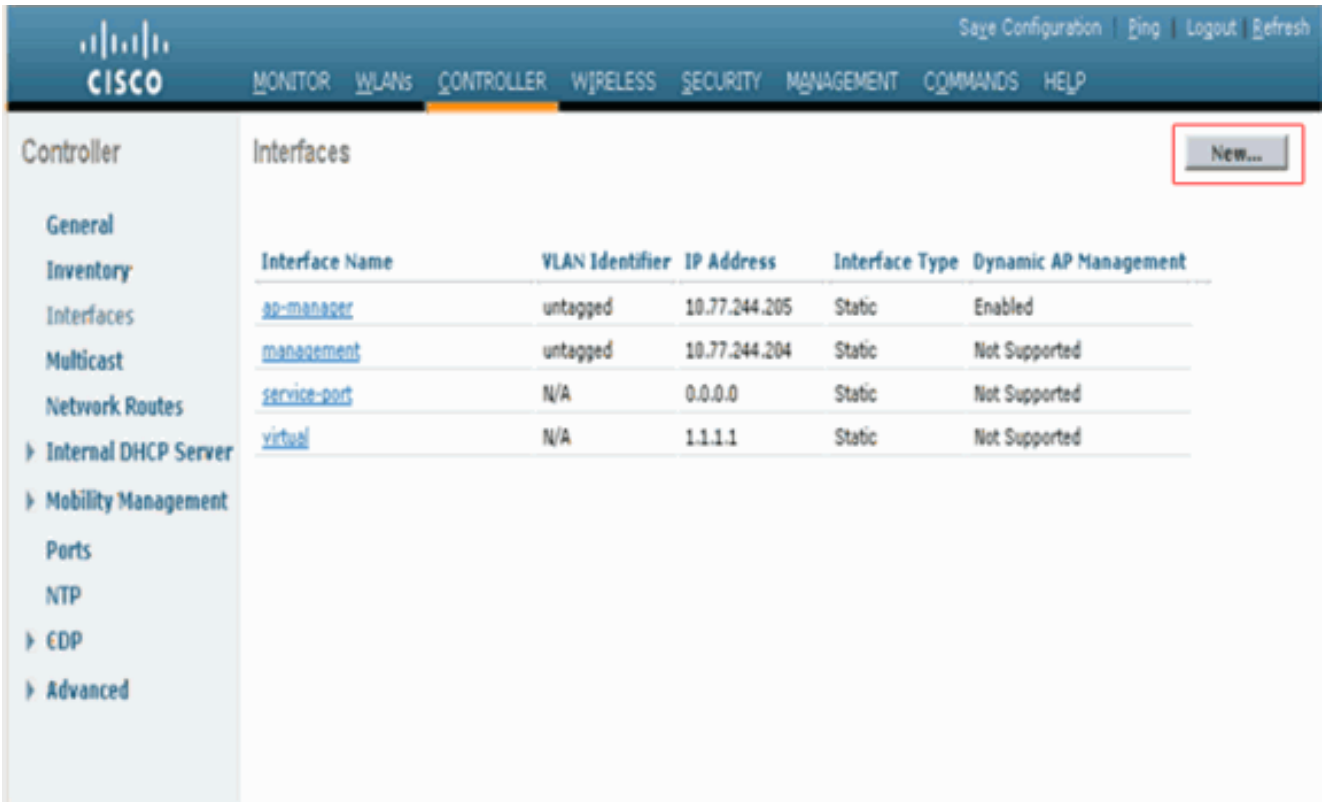
La première étape consiste à créer deux interfaces dynamiques sur le WLC, une pour les utilisateurs invités et l'autre pour les utilisateurs internes.

L'exemple fourni dans le présent document utilise ces paramètres et ces 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 :

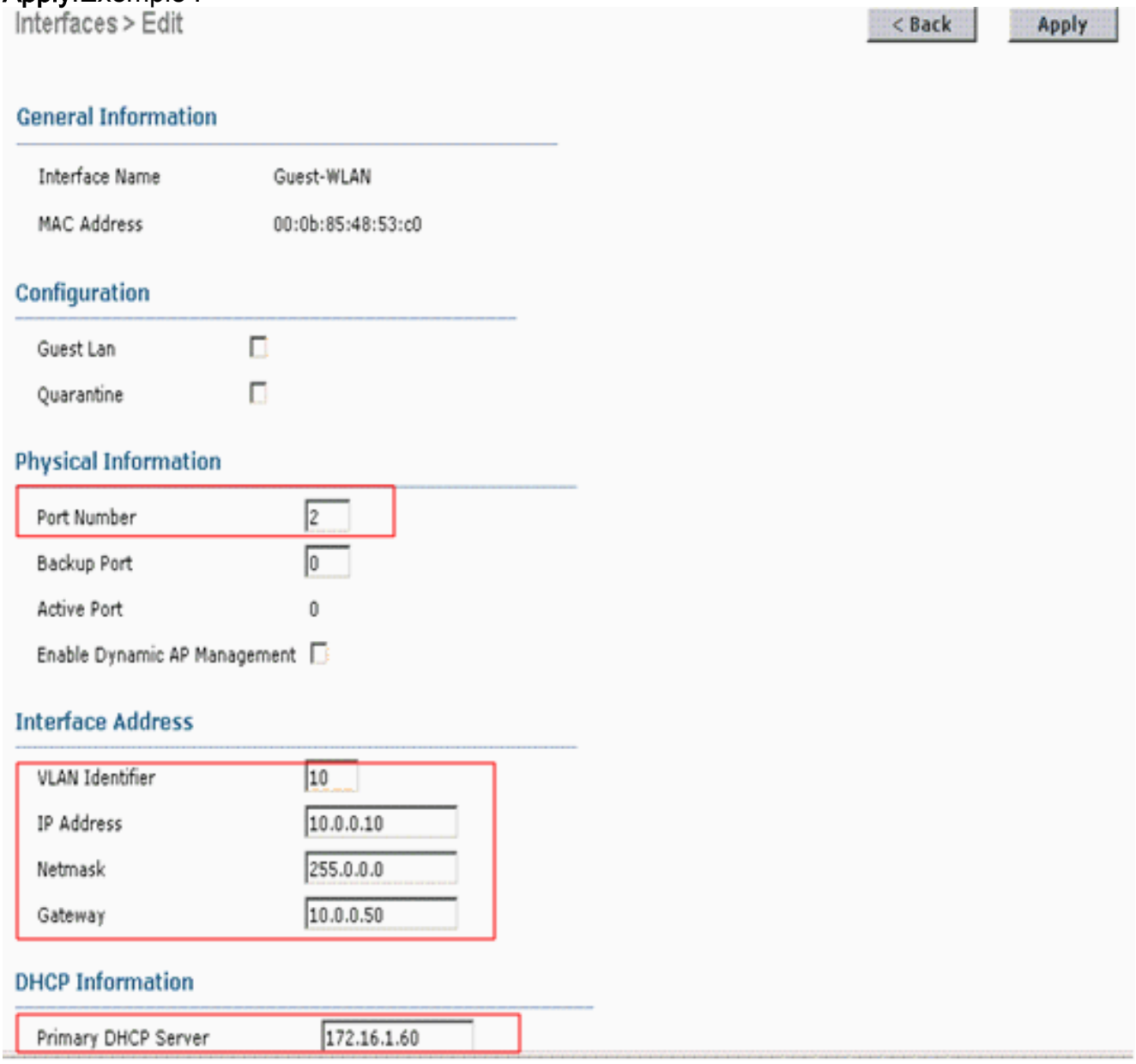
1. Àpartir de l'interface graphique utilisateur du WLC, choisir **Controller > Interfaces** [contrôleur > interfaces].La fenêtre Interfaces apparaît. Cette fenêtre liste les interfaces qui sont configurées sur le contrôleur. Les interfaces par défaut sont comprises, soit l'interface de gestion, l'interface de gestionnaire du point d'accès, l'interface virtuelle, l'interface du port de service et les interfaces dynamiques définies par l'utilisateur.



2. Afin de créer une nouvelle interface dynamique, cliquez sur **New.**
3. Dans la fenêtre Interfaces > New [interfaces > nouveau], entrer le nom de l'interface et

l'identifiant du réseau VLAN. Cliquer ensuite sur **Apply** [appliquer].Dans l'exemple donné, l'interface dynamique s'intitule Guest-WLAN, et l'identifiant du réseau VLAN est 10.

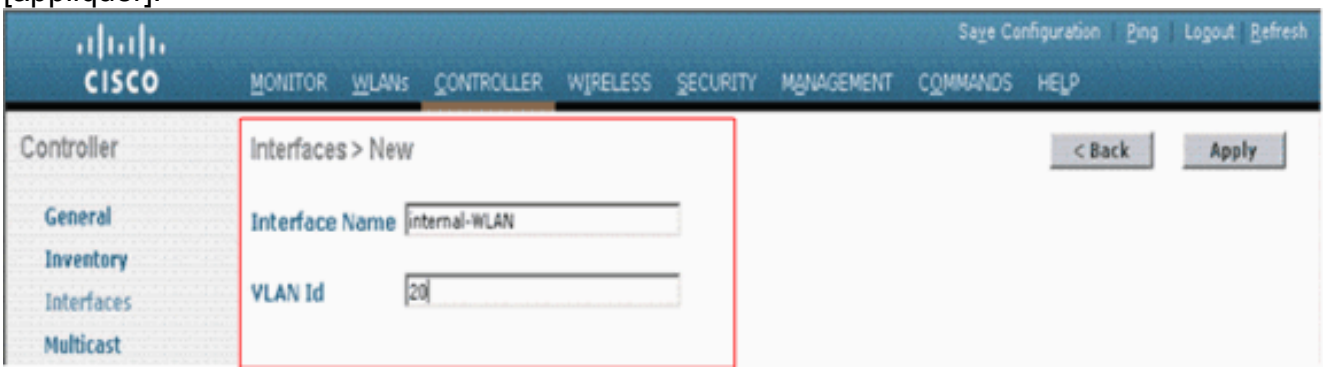
4. Dans la fenêtre Interfaces > Edit [interfaces > modifier], pour l'interface dynamique, saisir l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur **Apply**.Exemple :



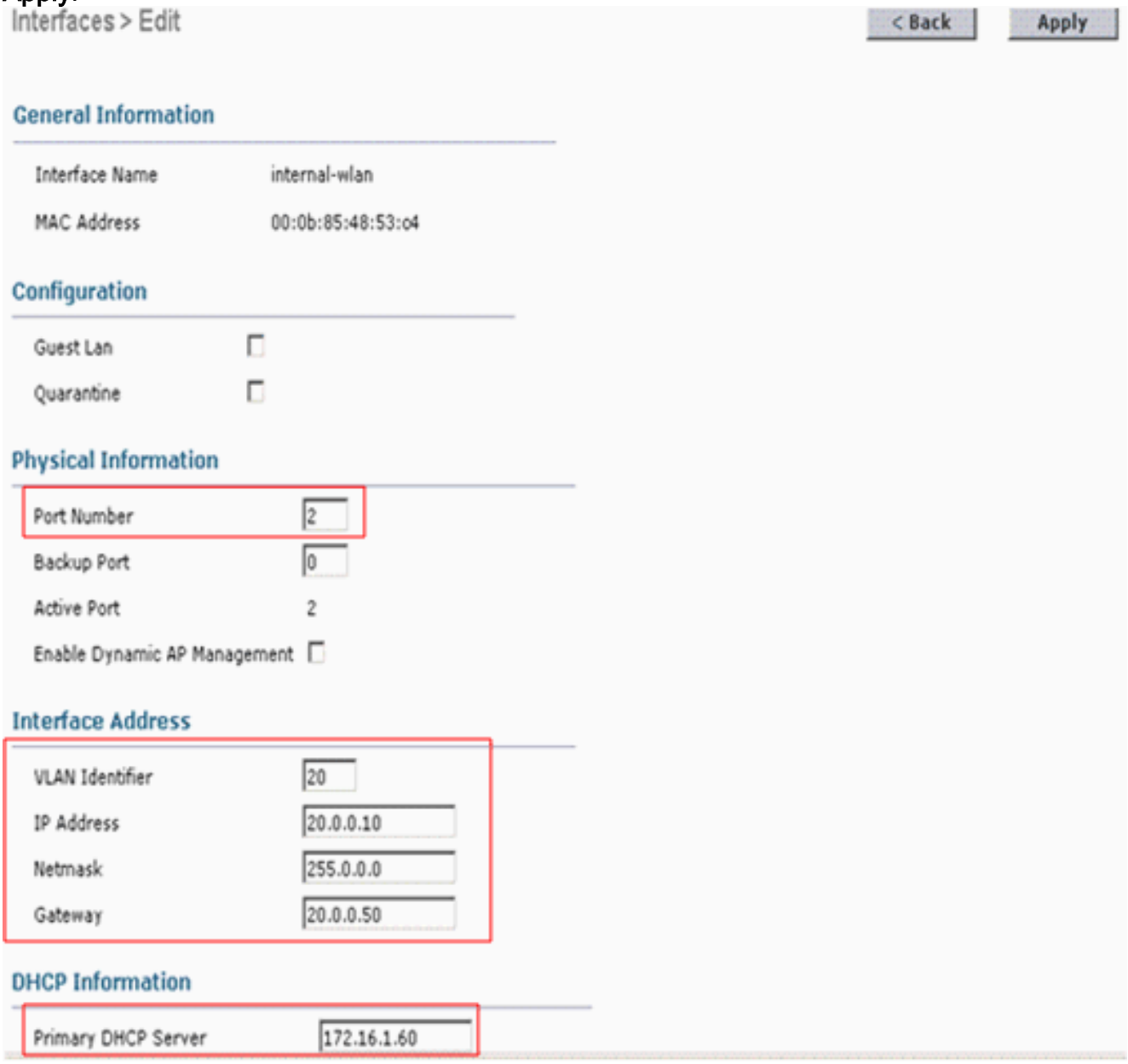
Il faut suivre la même procédure pour créer une interface dynamique sur le réseau WLAN interne.

5. Dans la fenêtre Interfaces > New [interfaces > nouveau], saisir **Internal-WLAN** pour l'interface dynamique des utilisateurs internes, puis **20** comme identifiant du réseau VLAN.

Cliquer ensuite sur **Apply** [appliquer].



6. Dans la fenêtre Interfaces > Edit [interfaces > modifier], pour l'interface dynamique, saisir 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**.



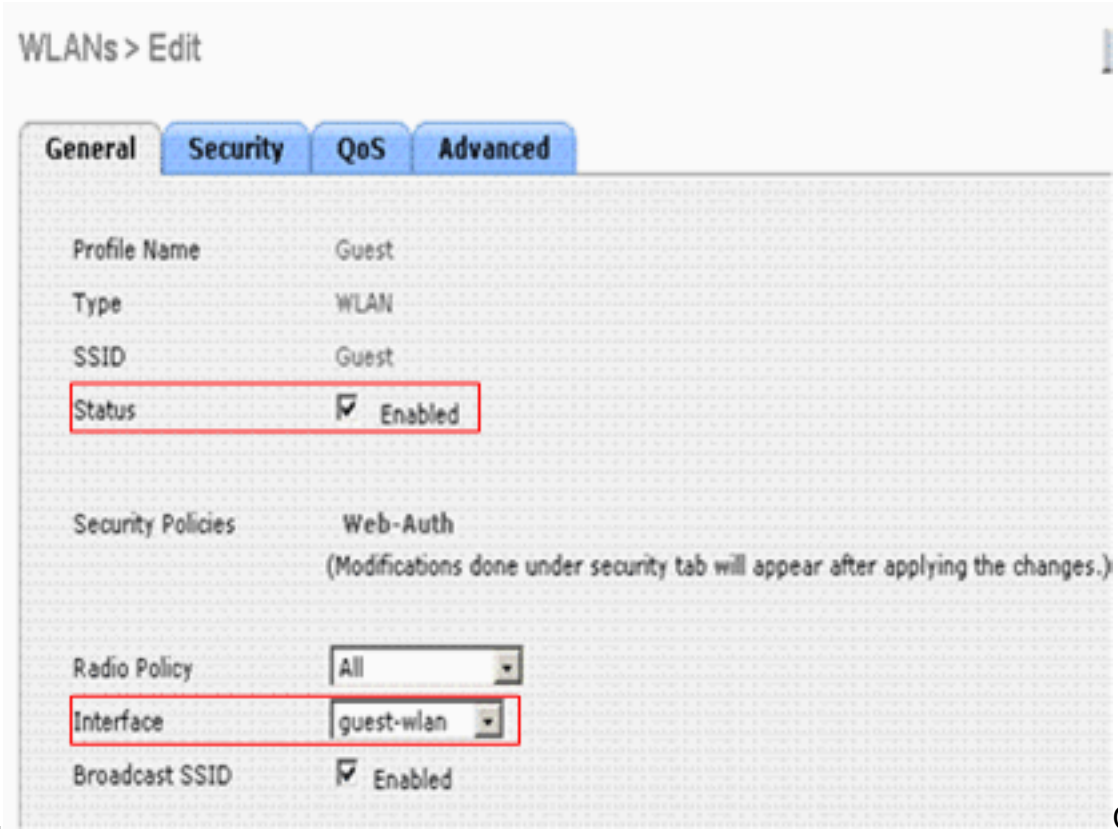
Puisque deux interfaces dynamiques sont maintenant créées, la fenêtre Interfaces résume la liste des interfaces configurées sur le contrôleur.

Créer des réseaux WLAN pour les utilisateurs invités et internes

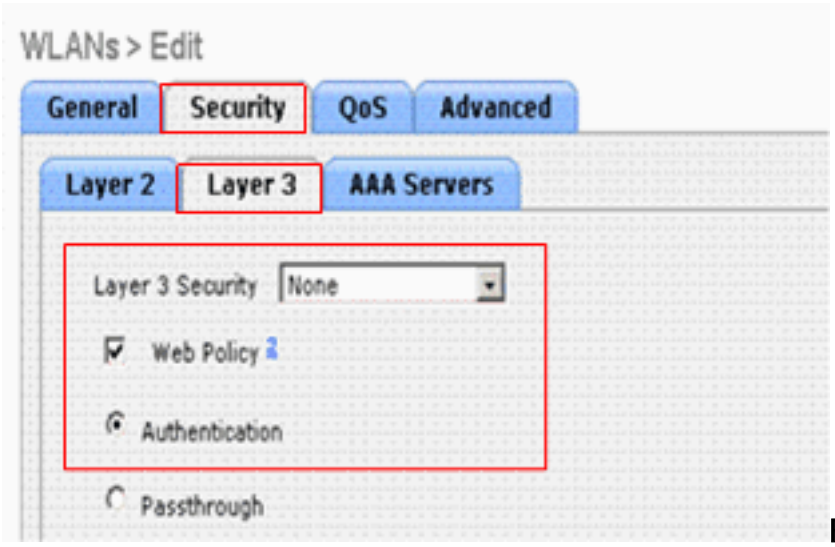
L'étape suivante consiste à créer des réseaux WLAN pour les utilisateurs invités et les utilisateurs internes et à mapper l'interface dynamique avec les réseaux WLAN. En outre, les méthodes de sécurité utilisées pour authentifier les utilisateurs invités et sans fil doivent être définies. Procédez comme 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 l'exemple-ci, le WLAN est désigné *invité* et son identifiant est 2.

3. Cliquer sur **Apply** [appliquer] dans le coin supérieur droit.
4. La page WLAN > Edit [WLAN > modifier], qui contient divers onglets, apparaît.Sous l'onglet **General** [général] du réseau WLAN invité, choisir **guest-wlan** dans le champ « Interface Name » [nom de l'interface]. Cette procédure vient mapper, avec **l'invité WLAN**, l'interface dynamique **guest-wlan** qui a été créée précédemment.Il faut s'assurer que l'état du réseau WLAN est

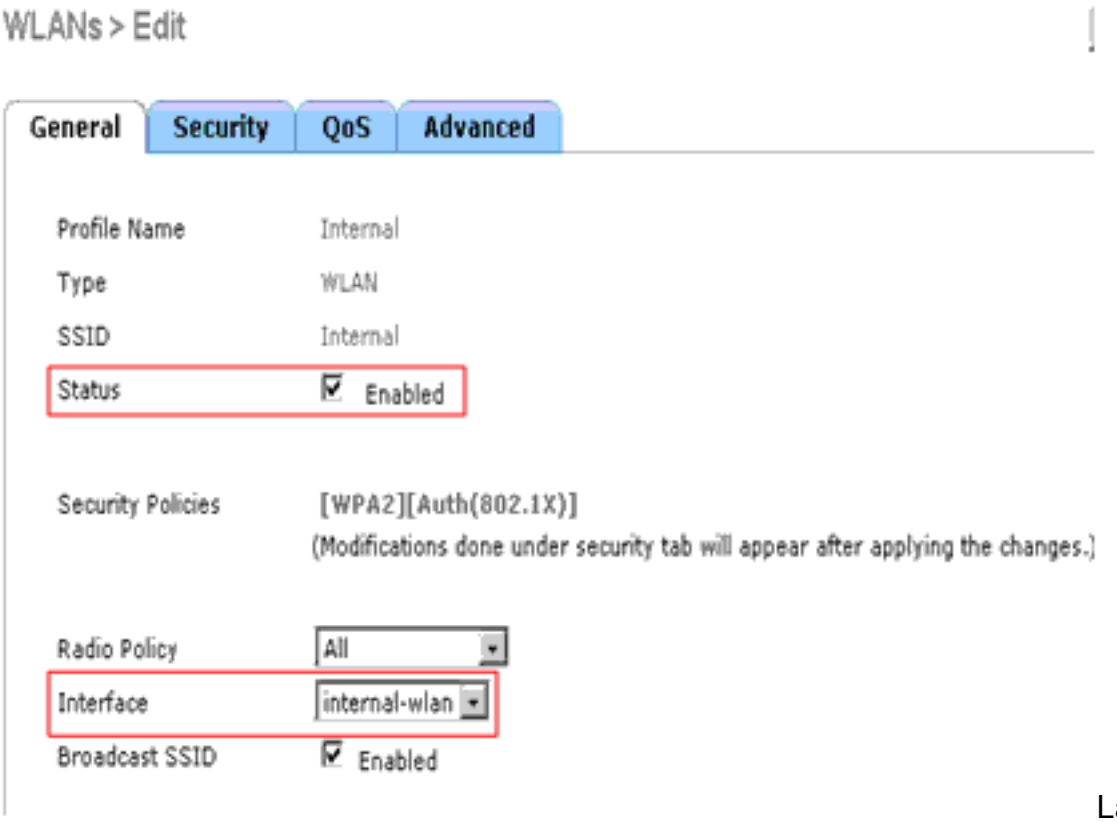


activé. Cliquez sur l'onglet **Security.** Pour ce réseau WLAN, l'authentification Web utilise un mécanisme de sécurité de couche 3 pour authentifier les clients. Choisir, par conséquent, **None** [aucun] dans le champ *Layer 2* Security [sécurité de couche 2]. Dans le champ *Layer 3* Security [sécurité de couche 3], cocher la case **Web Policy** [politique Web] et choisir l'option **Authentication**

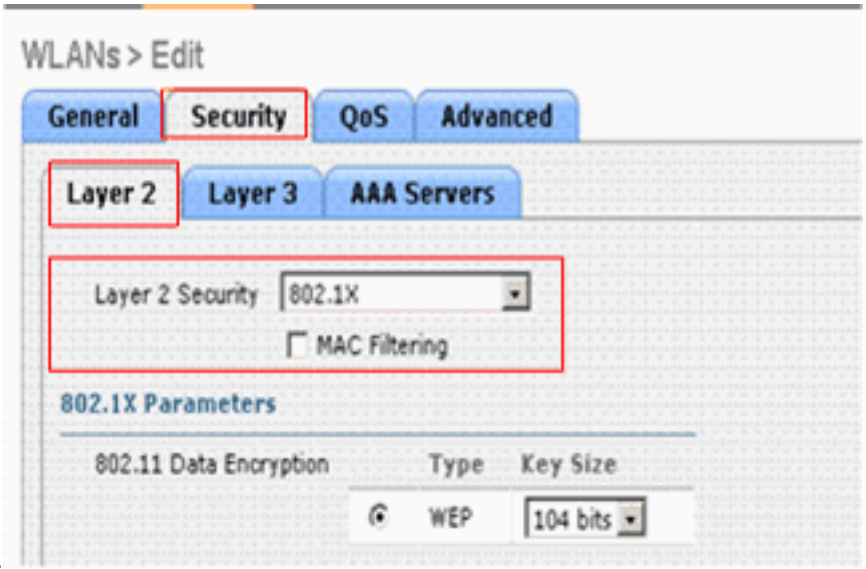


[authentification]. **Remarque :** Pour en savoir plus sur l'authentification Web, consulter [l'exemple de configuration d'authentification Web du contrôleur LAN sans fil](#).Cliquez sur Apply.

5. Créer un réseau WLAN pour les utilisateurs internes. Dans la fenêtre WLAN > New [WLAN > nouveau], saisir **Internal** [interne], puis choisir **3** afin de créer un WLAN pour les utilisateurs internes. Cliquez ensuite sur **Apply**.
6. La fenêtre WLAN > Edit [WLAN > Modifier] s'affiche. Sous l'onglet *General* [général], sélectionner **internal-wlan** dans le champ Interface Name [nom de l'interface].Ainsi, l'interface dynamique **internal-wlan** précédemment créée est mappée avec le WLAN **interne**. Il faut s'assurer que le WLAN est



activé. Laisser l'option de sécurité de couche 2 à la valeur par défaut 802.1x, car l'authentification EAP est utilisée pour les utilisateurs WLAN



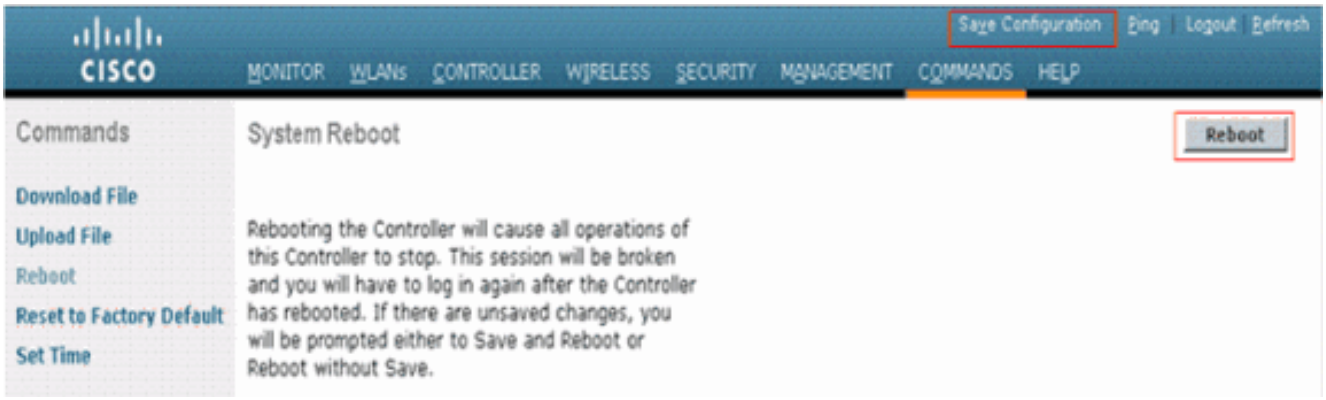
internes.

7. Cliquez sur Apply.La fenêtre WLAN apparaît, affichant la liste des réseaux WLAN créés.

Remarque : Consulter [l'exemple de configuration de l'authentification EAP avec les contrôleurs WLAN (WLC)] pour savoir comment configurer un réseau WLAN basé sur EAP

avec des WLC.

8. Sur la GUI WLC, cliquer sur **Save Configuration** [enregistrer la configuration], puis sur **Commands** [commandes] à partir de la GUI du contrôleur. Ensuite, choisir l'option **Reboot** [redémarrer] pour redémarrer le WLC et appliquer l'authentification Web.



Remarque : Cliquer sur **Save Configuration** [enregistrer la configuration] afin d'enregistrer la configuration après un redémarrage.

Configurer le port de commutation de couche 2 qui se connecte au WLC comme port de liaison

Il faut configurer le port de commutation pour prendre en charge les multiples réseaux VLAN configurés sur le WLC, car ce dernier est connecté à un commutateur de couche 2. Il faut également configurer le port de commutation en tant que port de liaison 802.1Q.

Chaque connexion du port du contrôleur constitue une liaison 802.1Q et devrait être configurée comme tel sur le commutateur voisin. Sur les commutateurs Cisco, le VLAN natif d'une liaison 802.1Q, par exemple **VLAN 1**, n'est pas étiqueté. Par conséquent, lors de la configuration de l'interface d'un contrôleur en vue de l'utilisation du VLAN natif sur un commutateur Cisco voisin, il faut alors configurer l'interface sur le contrôleur comme non étiqueté.

Si la valeur pour l'identifiant **VLAN** est zéro (dans la fenêtre Controller > Interfaces [contrôleur > interfaces]), l'interface n'est donc pas étiquetée. Dans l'exemple présenté ici, le gestionnaire AP et les interfaces de gestion sont configurés dans le réseau VLAN non étiqueté par défaut.

Lorsqu'une interface de contrôleur est réglée à une autre valeur que zéro, elle ne devrait pas être étiquetée sur le VLAN natif du commutateur, et le VLAN doit alors être autorisé sur le commutateur. Dans cet exemple, le VLAN 60 est configuré comme VLAN natif sur le port de commutation qui se connecte au contrôleur.

Voici la configuration du port de commutation 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
```

Voici la configuration du port de commutation qui se connecte au routeur en tant que port de liaison :

```
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
```

Voici la configuration du port de commutation qui se connecte au LAP. Ce port est configuré comme un port d'accès :

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

Configurer le routeur pour les deux réseaux WLAN

Dans l'exemple du présent document, le routeur 2811 connecte les utilisateurs invités à Internet et connecte les utilisateurs filaires internes aux utilisateurs sans fil internes. Il faut également configurer le routeur pour fournir des services DHCP.

Sur le routeur, créer des sous-interfaces sous l'interface FastEthernet qui se connecte au port de liaison du commutateur pour chaque VLAN. Affecter les sous-interfaces aux réseaux VLAN correspondants, puis configurer une adresse IP à partir des sous-réseaux respectifs.

Remarque : Seules les parties pertinentes de la configuration du routeur sont fournies, et non la configuration complète.

Voici la configuration requise sur le routeur pour y parvenir.

Voici les commandes qui doivent être saisies pour configurer les 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 saisies sur l'interface FastEthernet pour la configuration de l'exemple :

```
!
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
```

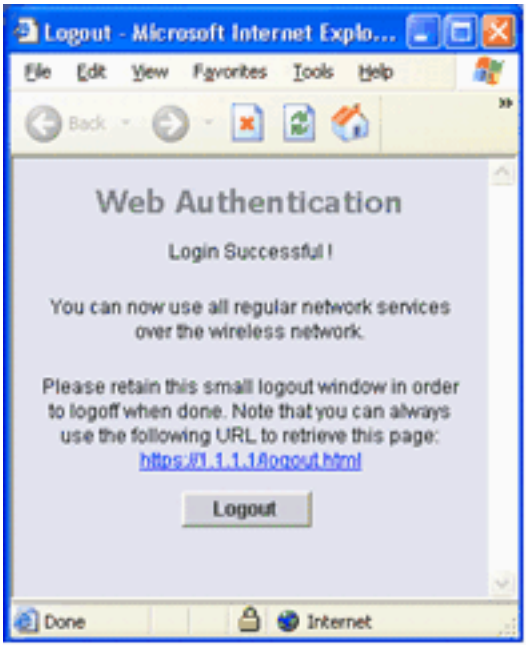
```
FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN
encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under
FastEthernet0/0 for the internal VLAN. !
```

Vérification

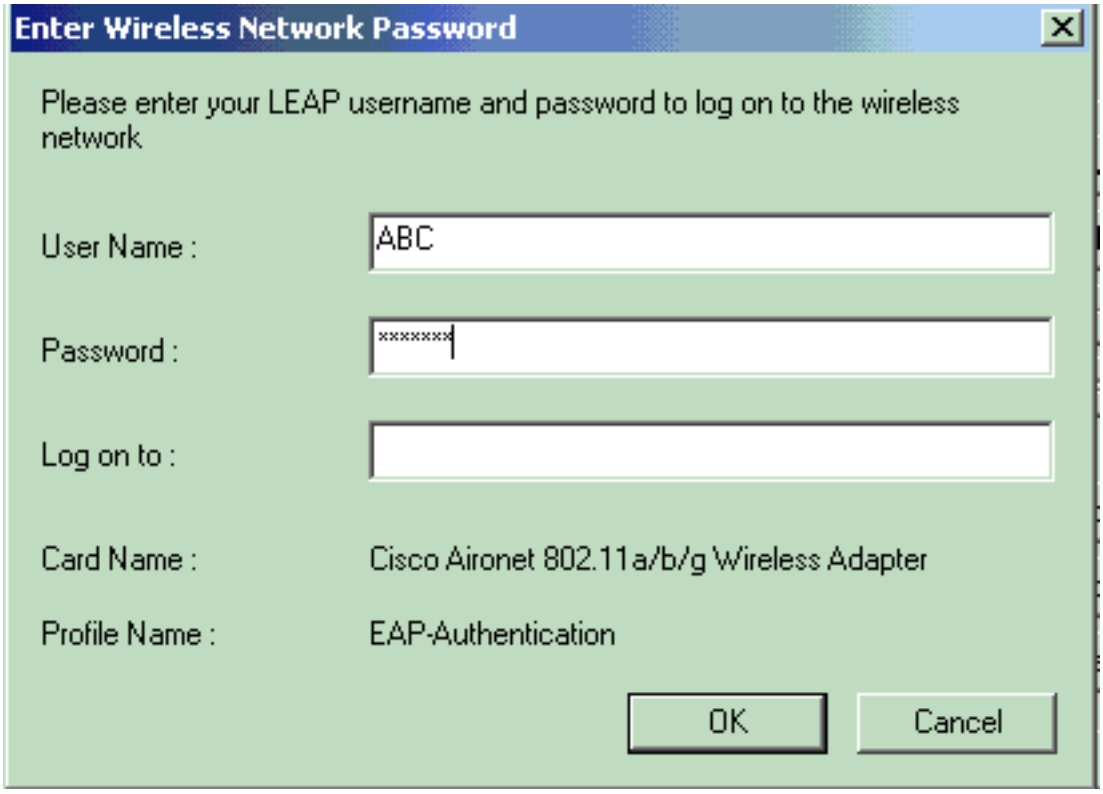
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

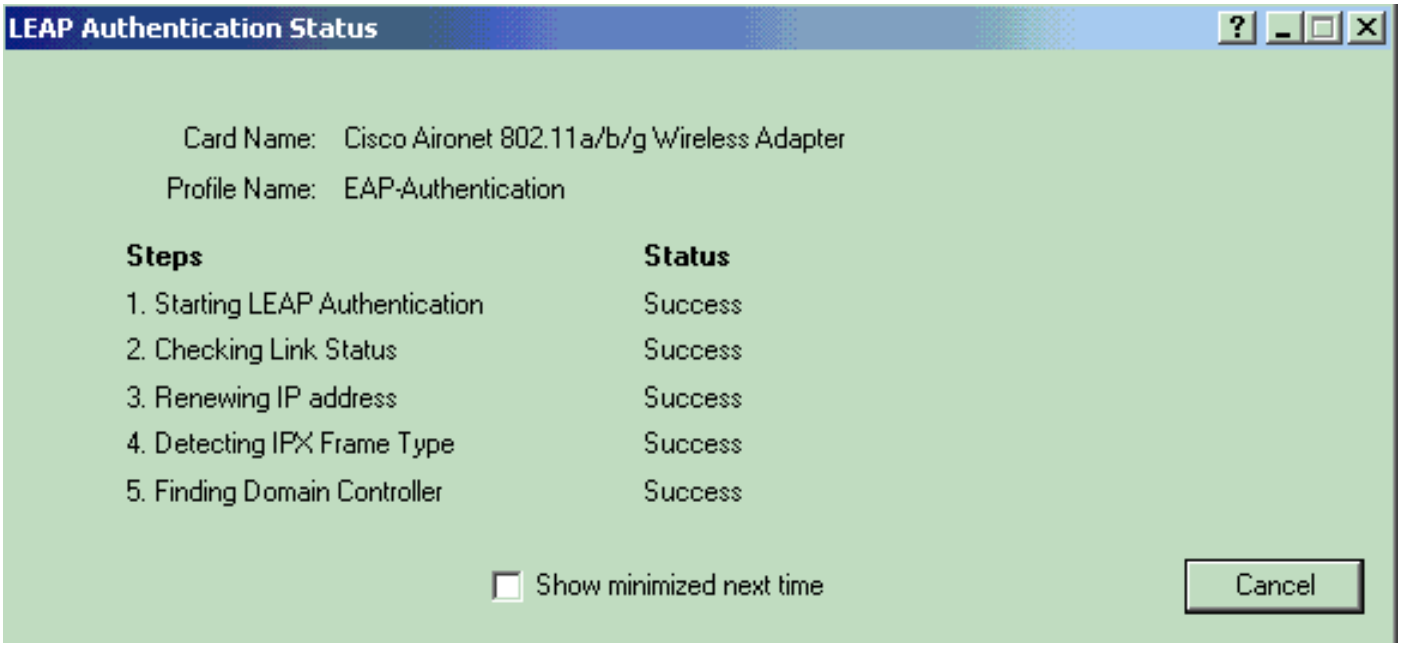
Connecter deux clients sans fil, soit un utilisateur invité (avec l'identifiant SSID **invité**) et un utilisateur interne (avec l'identifiant SSID **interne**), pour vérifier que la configuration fonctionne comme prévu.

Il faut se rappeler que le WLAN invité a été configuré pour l'authentification Web. Lorsque le client sans fil invité s'affiche, saisir une URL dans le navigateur Web. La page d'authentification Web par défaut apparaît et vous invite à entrer le nom d'utilisateur et le mot de passe. Une fois que l'utilisateur invité saisit un nom d'utilisateur et un mot de passe valides, le WLC l'authentifie et le laisse accéder au réseau (éventuellement à Internet). Cet exemple montre la fenêtre d'authentification Web que reçoit l'utilisateur ainsi que le résultat d'une authentification réussie :



Le réseau WLAN interne du présent exemple est configuré pour l'authentification 802.1x. Lorsque le client WLAN interne se manifeste, le client utilise l'authentification EAP. Pour savoir comment configurer le client pour l'authentification EAP, consulter la section Utilisation de l'authentification EAP du Guide de configuration et d'installation des adaptateurs client pour réseau LAN sans fil 802.11a/b/g Cisco Aironet (CB21AG et PI21AG). Une fois l'authentification réussie, l'utilisateur peut accéder au réseau interne. Cet exemple montre un client sans fil interne qui utilise l'authentification LEAP (Lightweight Extensible Authentication Protocol) :





Dépannage

Procédure de dépannage

Utilisez cette section pour dépanner votre configuration.

Voici quoi faire si la configuration ne fonctionne pas comme prévu :

1. Il faut s'assurer que tous les réseaux VLAN configurés sur le WLC sont autorisés sur le port de commutation connecté au WLC.
2. Il faut s'assurer que le port de commutation qui se connecte au WLC et au routeur est configuré comme un port de liaison.
3. Il faut s'assurer que les identifiants des VLAN utilisés sont les mêmes sur le WLC et le routeur.
4. Vérifier si les clients reçoivent des adresses DHCP du serveur DHCP. Sinon, il faut s'assurer que le serveur DHCP est configuré correctement. Pour en savoir plus sur le dépannage des problèmes des clients, consulter la section Dépannage des problèmes des clients dans Cisco Unified Wireless Network.

Un problème fréquent de l'authentification Web, c'est lorsque la redirection vers la page d'authentification Web ne fonctionne pas. L'utilisateur ne voit pas la fenêtre d'authentification Web lorsque le navigateur est ouvert. Plutôt, l'utilisateur est contraint d'entrer manuellement l'adresse **https://1.1.1.1/login.html** pour accéder à la fenêtre d'authentification Web. Il est ici question de la recherche DNS, qui doit fonctionner avant la redirection vers la page d'authentification Web. Si la page d'accueil du navigateur sur le client sans fil pointe vers un nom de domaine, il faut effectuer nslookup avec succès lorsque le client s'associe pour que la redirection fonctionne.

En outre, concernant un WLC qui exécute une version antérieure à 3.2.150.10, l'authentification Web fonctionne lorsqu'un utilisateur du SSID tente d'accéder à Internet. L'interface de gestion du contrôleur effectue alors une requête DNS pour déterminer si l'URL est valide. Si c'est le cas, l'URL affiche la page d'autorisation avec l'adresse IP des interfaces virtuelles. Une fois que l'utilisateur a réussi à se connecter, la demande initiale est réacheminée au client. Cela est causé par l'ID de bogue Cisco CSCsh68105 (clients inscrits seulement). Pour en savoir plus, consulter la section Dépannage de l'authentification Web sur un contrôleur LAN sans fil (WLC).

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Il est également possible d'utiliser ces commandes de débogage pour corriger la configuration :

- **debug mac addr<client-MAC-address xx:xx:xx:xx:xx:xx>** : configure le débogage des adresses MAC pour le client.
- **debug aaa all enable** : configure le débogage de tous les messages 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.**
- **debug dhcp message enable** : cette commande sert à afficher les renseignements sur le débogage des activités du client DHCP et à 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.**
- **debug pm ssh-tcp enable** : configure le débogage du traitement TCP du gestionnaire de politiques.

Voici des exemples de résultats de certaines commandes de **débogage** :

Remarque : Certaines lignes de sortie ont été intégrées à une deuxième ligne pour des 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
- Exemple de configuration de l’authentification sur des contrôleurs LAN sans fil
- 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