Exemple de configuration d'un accès invité filaire à l'aide de contrôleurs de réseau local sans fil Cisco

Contenu

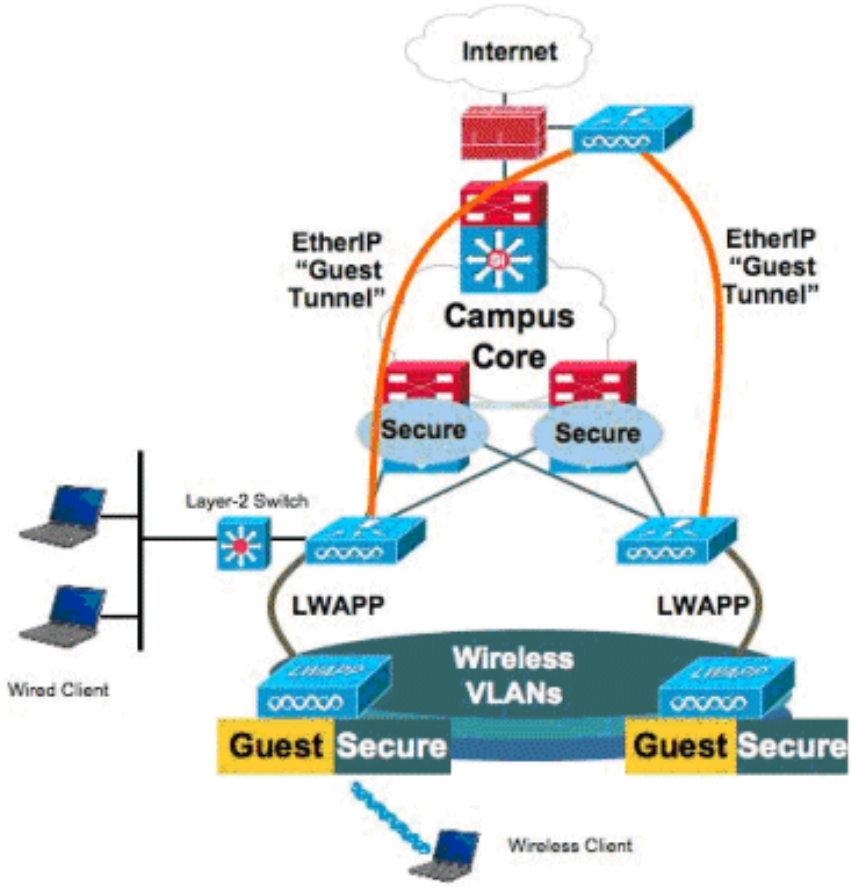
Introduction

Le présent document décrit comment configurer l’accès invité au moyen de la nouvelle fonctionnalité d’accès par câble pour invité sur les contrôleurs WLAN de Cisco qui utilisent la version 4.2.61.0 du logiciel sans fil unifié de Cisco ou une version ultérieure. Un nombre croissant d’entreprises reconnaissent l’importance de fournir un accès Internet à leurs clients, à leurs partenaires et à leurs consultants lorsqu’ils visitent leurs installations. Les gestionnaires des TI peuvent fournir un accès par câble ou sans fil, sécurisé et contrôlé, permettant aux invités d’accéder à Internet sur le même contrôleur de réseau local sans fil.

Les utilisateurs invités pourront se connecter aux ports Ethernet désignés et accéder au réseau invité configuré par l’administrateur après avoir franchi les mesures d’authentification configurées. Les utilisateurs invités sans fil peuvent facilement se connecter aux contrôleurs WLAN par l’intermédiaire des fonctions actuelles d’accès invité. De plus, le système de contrôle sans fil (WCS) ainsi que la configuration de base et la gestion des contrôleurs WLAN offrent une expérience améliorée aux utilisateurs invités. Les clients qui ont déjà déployé ou qui prévoient déployer des contrôleurs WLAN et le système WCS dans leur réseau peuvent utiliser la même infrastructure pour l’accès par câble pour invité. Ainsi, les utilisateurs finaux pourront profiter d’une expérience d’accès invité uniforme, qu’ils utilisent une connexion sans fil ou par câble.

Les ports câblés pour invité sont accessibles à un endroit désigné et sont branchés sur un commutateur d’accès. Selon la configuration du commutateur d’accès, ces ports sont associés à l’un des réseaux locaux virtuels (VLAN) de la couche 2 de l’accès invité par câble. Deux solutions s’offrent aux clients :

- Un seul contrôleur WLAN (mode « VLAN Translation ») – le commutateur d'accès relie le trafic de l'invité par câble sur le réseau VLAN d'invité au contrôleur WLAN qui assure la solution d'accès par câble pour invité. Ce contrôleur effectue la traduction VLAN du réseau VLAN d'entrée par câble pour invité vers le réseau VLAN de sortie.
- Deux contrôleurs WLAN (mode « Auto Anchor ») – le commutateur d'accès relie le trafic de l'invité par câble à un contrôleur WLAN local (le contrôleur le plus près du commutateur d'accès). Ce contrôleur WLAN local connecte le client à un contrôleur WLAN d'ancrage dans une zone démilitarisée (DMZ) qui est configuré pour prendre en charge un accès invité par câble et sans fil. Après avoir dirigé le client vers la zone démilitarisée du contrôleur d'ancrage, le système traite l'attribution de l'adresse IP au serveur DHCP, l'authentification du client et ainsi de suite. Lorsque le processus d'authentification est terminé, le client peut envoyer et recevoir du
  trafic.



Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

La fonctionnalité d'accès par câble pour invité sur les contrôleurs WLAN de Cisco est offerte dans la version 4.2.61.0 du logiciel sans fil unifié de Cisco et dans les versions ultérieures.

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.

Configuration

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

Configuration du commutateur d'accès au réseau

Afin d'assurer un accès par câble à l'invité, l'administrateur doit configurer les ports désignés du commutateur d'accès au réseau de la couche 2 sur le réseau VLAN pour invité. Le réseau VLAN pour invité doit être séparé de tous les autres réseaux VLAN configurés sur ce commutateur. Le trafic du réseau VLAN pour invité est acheminé au contrôleur WLAN local le plus près. Le contrôleur local achemine le trafic de l'invité par l'entremise d'un tunnel Ethernet sur IP (EoIP) vers un contrôleur d'ancrage de zone démilitarisée. Il faut au moins deux contrôleurs pour cette solution.

Par ailleurs, le commutateur d'accès relie le réseau VLAN pour invité au contrôleur, qui traduit ce réseau vers l'interface de sortie du contrôleur WLAN.

```
cat6506# show vlan id 49

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
49   VLAN0049                         active    Gi2/1, Gi2/2, Gi2/4, Gi2/35
                                                Gi2/39, Fa4/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
49   enet  100049     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------


cat6506#
interface FastEthernet4/24
 description Wired Guest Access
 switchport
 switchport access vlan 49
 no ip address
end
cat6506#
interface GigabitEthernet2/4
 description Trunk port to the WLC
 switchport
 switchport trunk native vlan 80
 switchport trunk allowed vlan 49,80,110
 switchport mode trunk
 no ip address
end
```

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Points importants pour un déploiement par câble pour invité

- Actuellement, cinq réseaux locaux pour invités sont pris en charge pour l'accès invité. Au total, 16 réseaux WLAN pour les utilisateurs sans fil et 5 réseaux WLAN pour les invités par câble peuvent être configurés sur le contrôleur WLAN d'ancrage. Il n'y a pas de tunnel distinct pour les réseaux WLAN. Tous les réseaux WLAN invités, y compris les réseaux WLAN à accès pour invité par câble, utilisent les mêmes tunnels EoIP connectés au contrôleur WLAN d'ancrage.
- Les administrateurs doivent créer des interfaces dynamiques dans le contrôleur WLAN, les marquer comme " LAN invité, les " et les associer aux WLAN créés en tant que LAN invité.
- Assurez-vous que les configurations WLAN, y compris le processus d'authentification, sont identiques sur les contrôleurs d'ancrage et sur les contrôleurs à distance afin d'assurer le transfert du trafic client.
- Les contrôleurs WLAN doivent avoir des versions logicielles compatibles. Assurez-vous qu'ils utilisent la même version principale.
- L'authentification Web est le mécanisme de sécurité par défaut disponible sur un réseau local invité par câble. Les options disponibles sont les suivantes : « Open » (ouvert), « Web Auth » (authentification Web) et « Web Passthrough » (intercommunication Web).
- En cas d'échec de connexion par tunnel EoIP entre le contrôleur WLAN d'ancrage et le contrôleur à distance, la base de données du client est effacée du contrôleur WLAN d'ancrage. Le client doit alors relancer les étapes d'association et d'authentification.
- Aucune sécurité pour la couche 2 n'est prise en charge.
- Le trafic de diffusion/multidiffusion du réseau local invité par câble est supprimé.
- Les paramètres du serveur mandataire DHCP doivent être identiques sur les contrôleurs d'ancrage et sur les contrôleurs à distance.

Avec un accès invité par câble, aucun délai d'inactivité n'est en fonction dans le contrôleur. Si aucun paquet n'est reçu pendant la période configurée par le client, ce dernier est retiré du contrôleur. Au prochain envoi d'une demande de protocole de résolution d'adresse (ARP) par le client, une nouvelle entrée de client est créée et l'état passe à « Web Auth/RUN », conformément à la configuration de sécurité.

Prise en charge de la plate-forme

L'accès par câble pour invité est pris en charge sur ces plateformes :

- Contrôleur WLAN 4402, 4404, WiSM, 3750G, 5508, WiSM2, contrôleur WLAN virtuel de Cisco

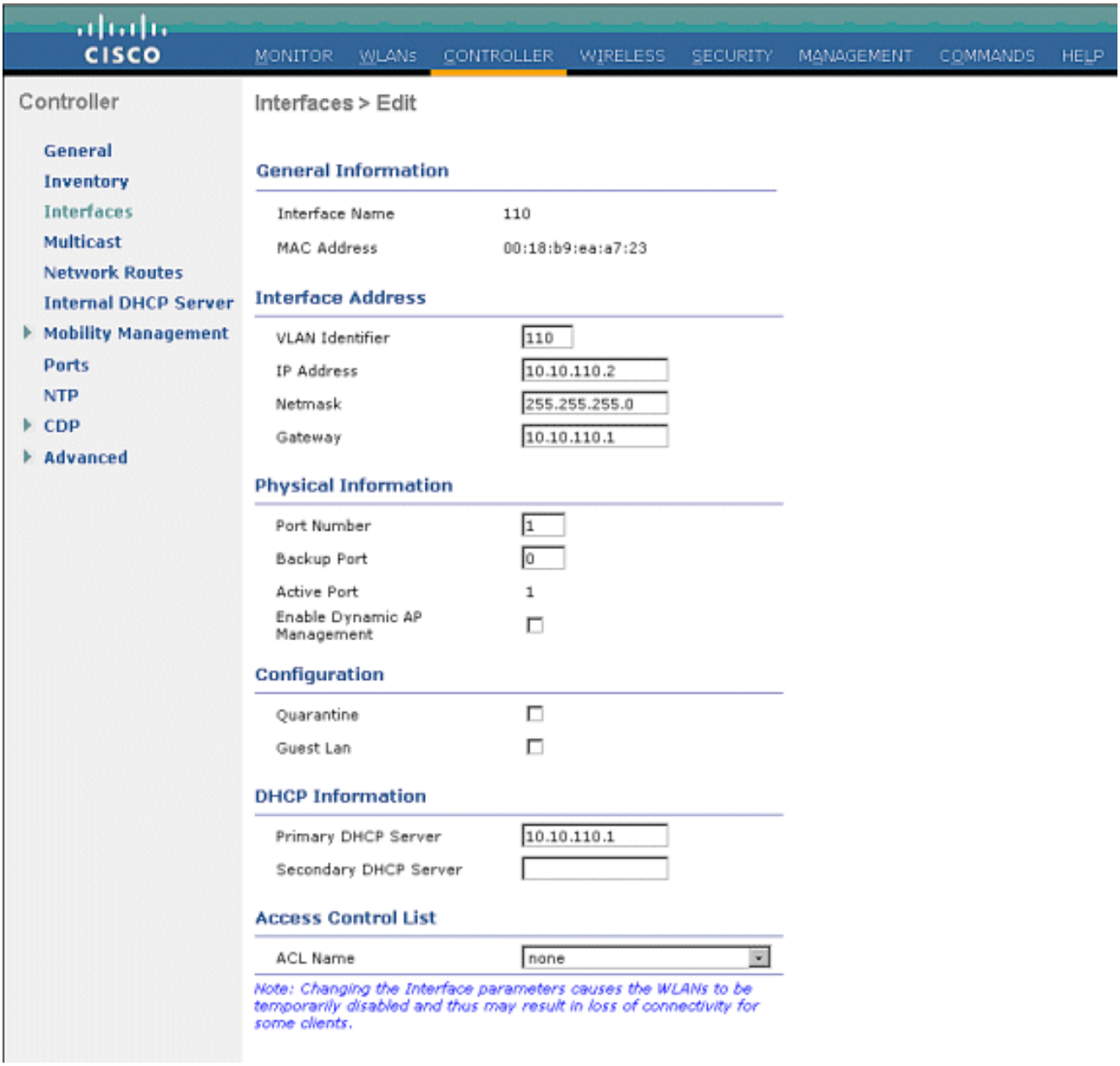
Configuration du réseau local sans fil (WLAN)

Dans l'exemple suivant, on emploie par défaut la configuration de base du contrôleur de réseau local sans fil. On se concentre sur la configuration supplémentaire requise pour mettre en œuvre l'accès par câble pour invité.

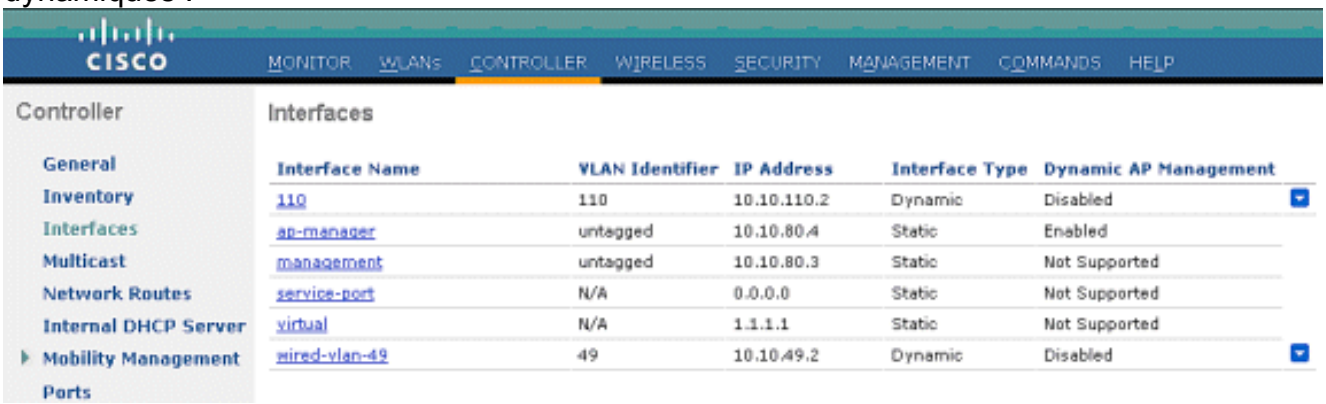
1. Créez une interface dynamique et marquez-la comme un réseau local invité ". " Dans la

version actuelle, lorsque vous créez une interface dynamique, vous devez fournir une adresse IP et une passerelle par défaut même s'il n'y en a pas, puisqu'il s'agit d'un réseau VLAN de la couche 2. Vous ne devez pas fournir n'importe quelle adresse DHCP. Les clients invités sont physiquement connectés par câble à ce réseau VLAN.

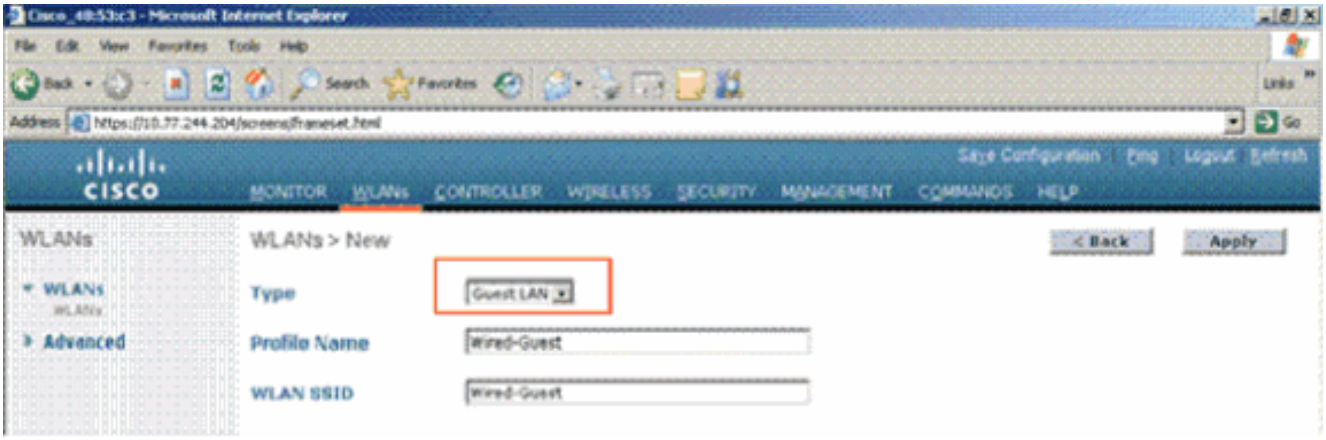
2. Créez une autre interface dynamique où les clients invités par câble reçoivent une adresse IP.**Note**: Vous devez fournir une adresse IP, une passerelle par défaut ou une adresse de serveur DHCP pour cette interface.



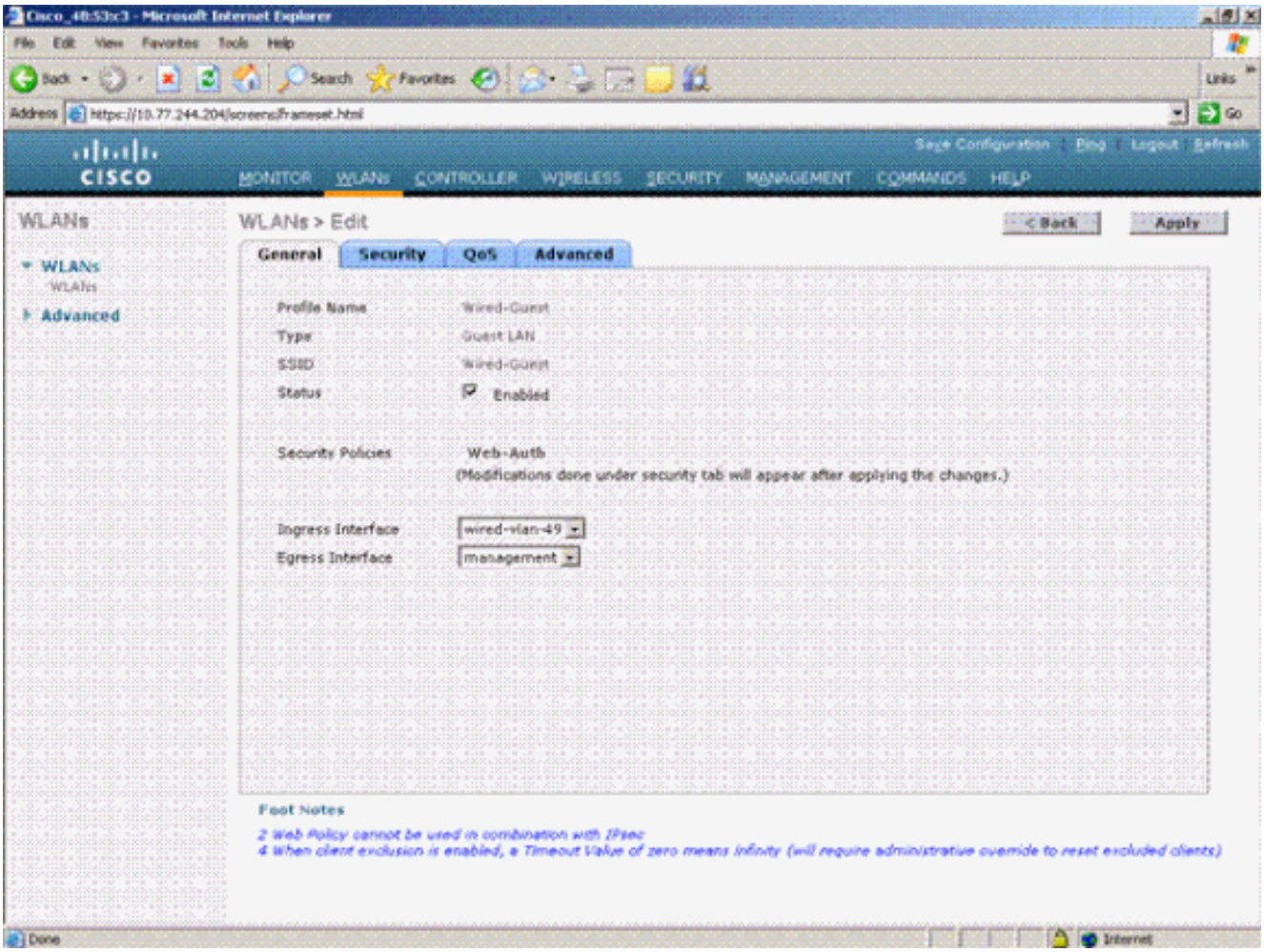
3. Voici les interfaces dynamiques :



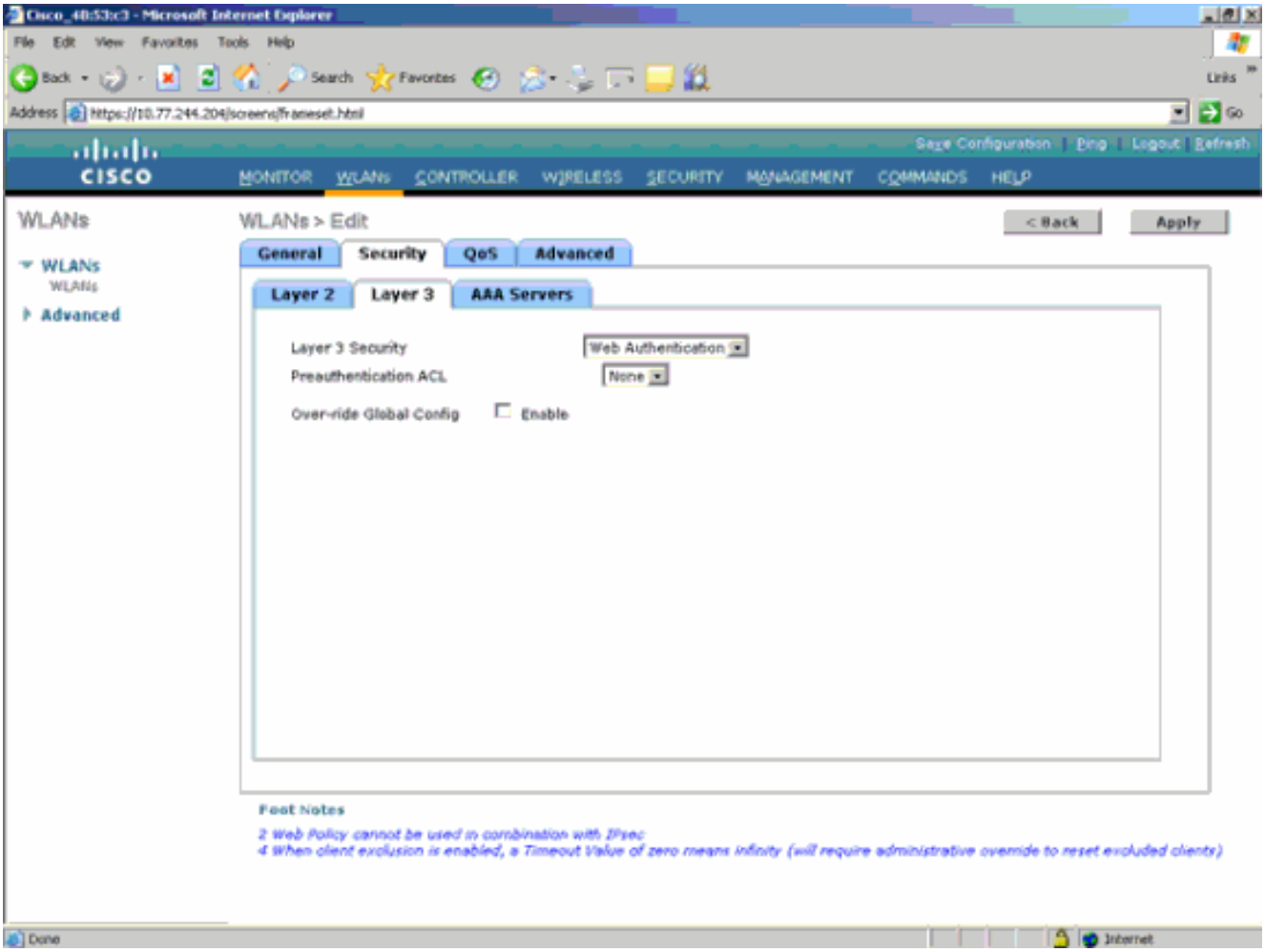
4. Ajoutez un nouveau réseau WLAN : Type = Guest LAN (réseau local pour invités).



5. Activez le réseau WLAN : mappez l'interface d'entrée à l'" de réseau local invité " créée à l'étape 1, et l'interface de sortie peut être une interface de gestion ou toute autre interface dynamique, bien que de préférence une interface dynamique telle que celle créée à l'étape 2.

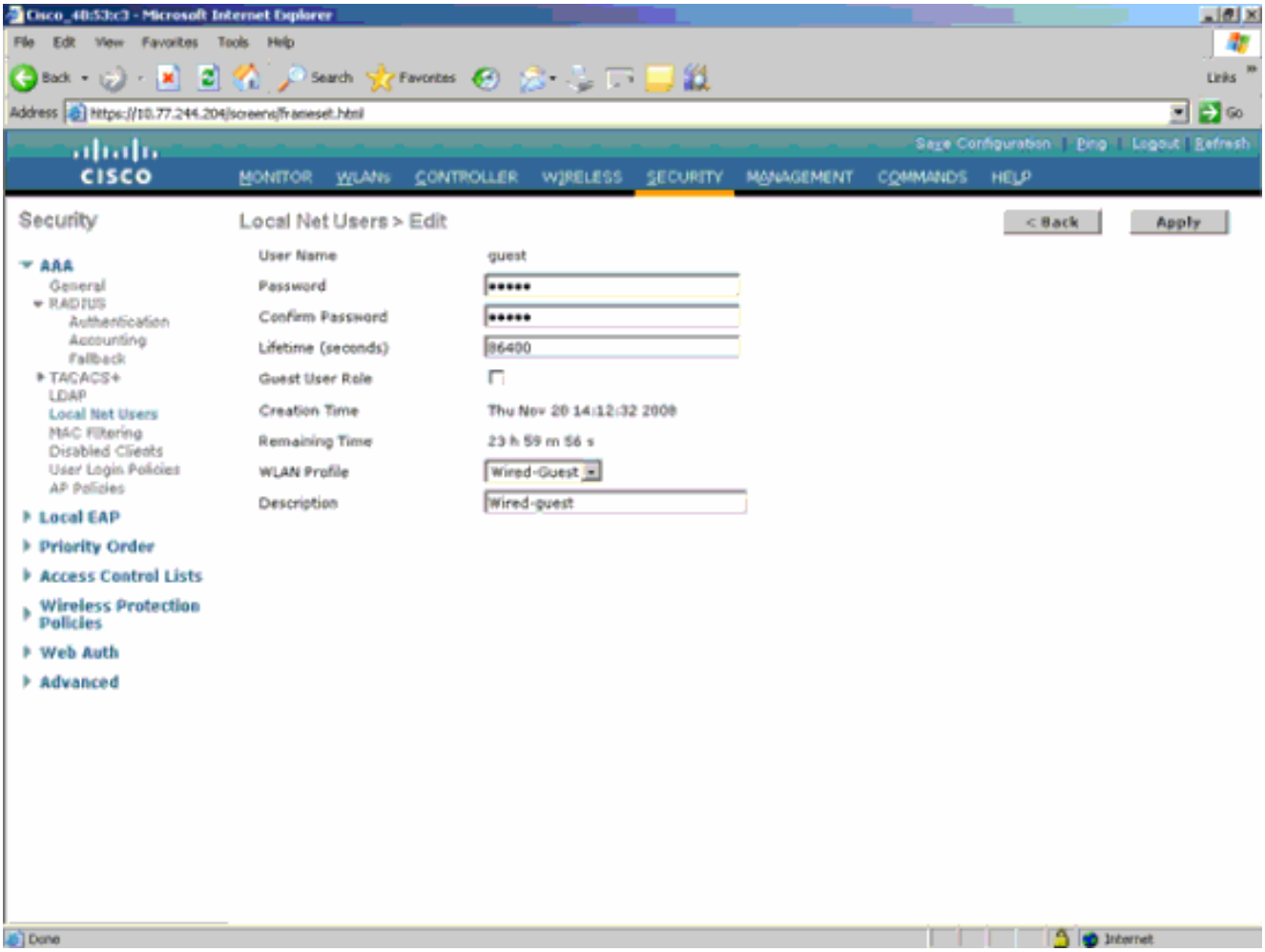


6. L'option « Web authentication » (authentification Web) est activée par défaut comme option de sécurité configurée sur le réseau local pour invités. Cette option peut être modifiée à *« None » (aucun) ou « Web Passthrough » (intercommunication Web)*.



7. Voici la configuration finale du réseau WLAN.

8. Ajoutez un utilisateur invité dans la base de données locale du contrôleur WLAN.

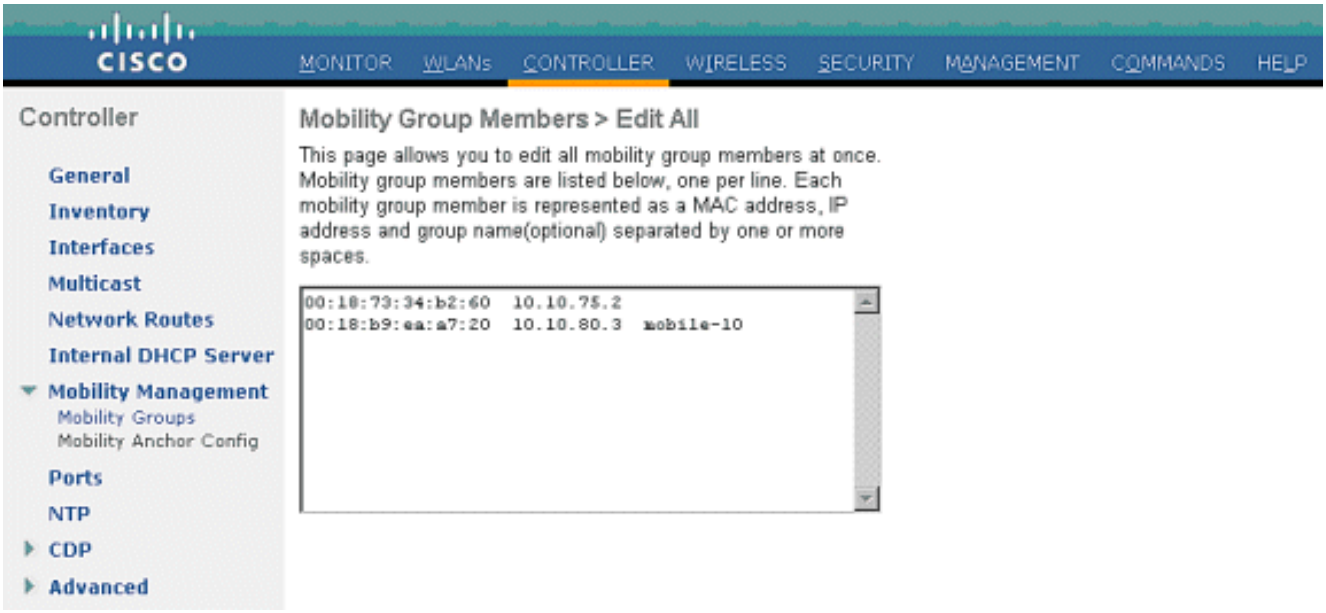


Sur l'Étranger, vous devez définir l'entrée en tant que réseau local invité “ configuré. ” Vous devez associer la sortie à certaines interfaces, possiblement l’interface de gestion. Cependant, une fois le tunnel EoIP mis en place, le trafic est acheminé automatiquement par le tunnel plutôt que par l’adresse de gestion.

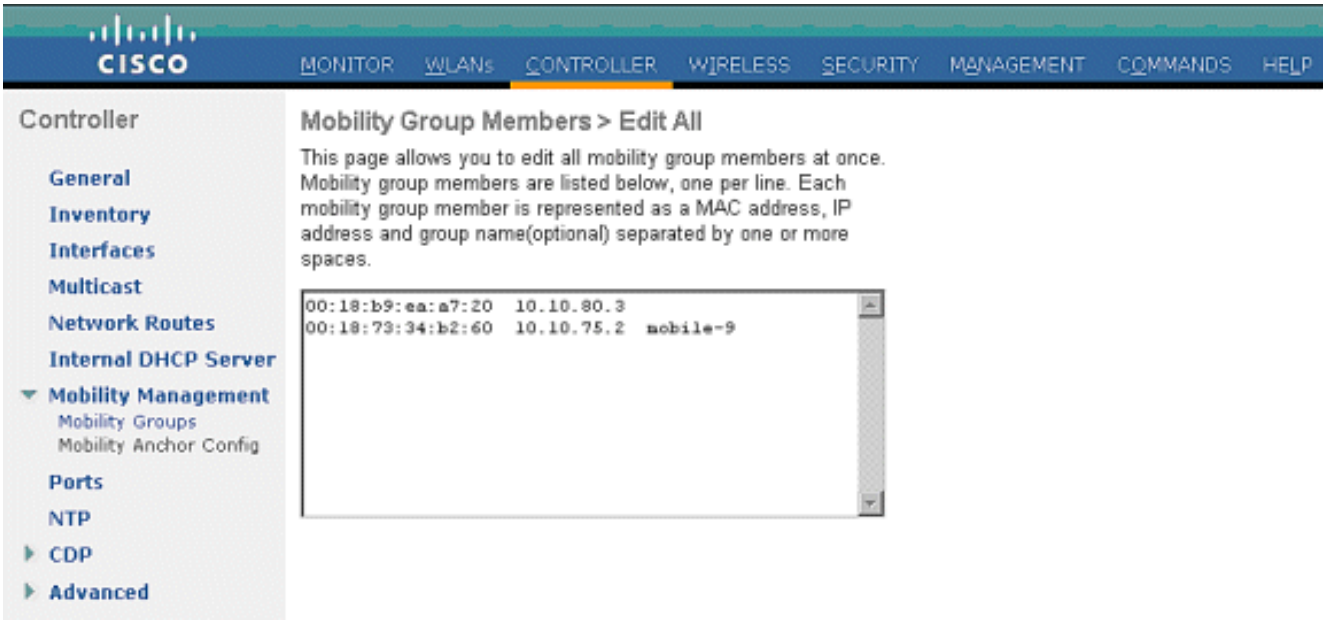
Accès par câble pour invité avec contrôleur d’ancrage WLAN

Dans cet exemple, l’adresse IP du contrôleur de réseau local sans fil à distance est 10.10.80.3 et l’adresse IP du contrôleur d’ancrage de zone démilitarisée (DMZ) est 10.10.75.2. Les deux font partie de groupes de mobilité différents.

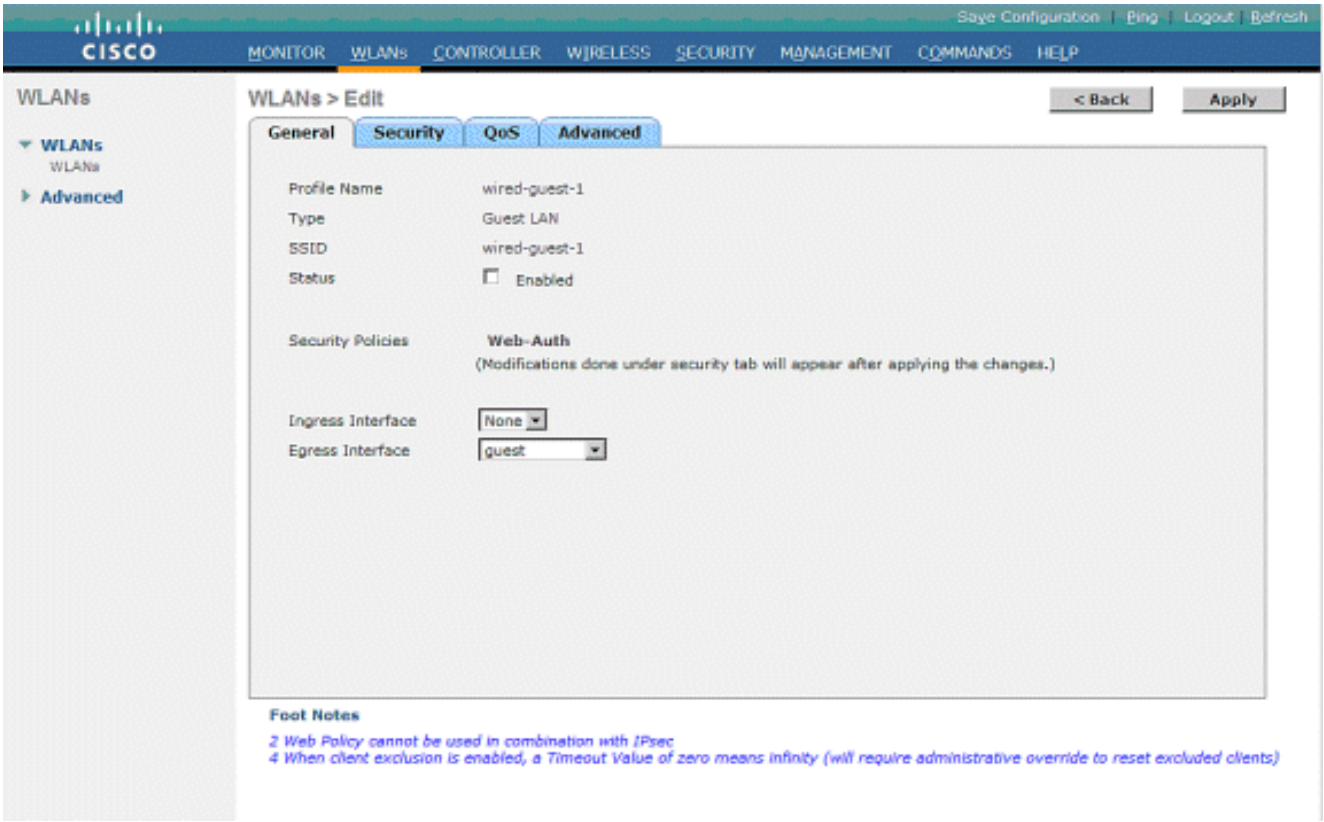
1. Configurez le groupe de mobilité du contrôleur d’ancrage DMZ lorsque vous entrez l’adresse MAC, l’adresse IP et le nom du groupe de mobilité du contrôleur à distance.



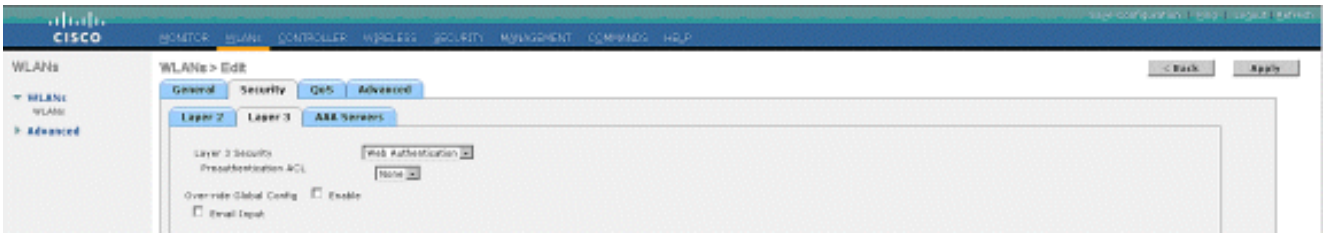
2. De même, configurez le groupe de mobilité du contrôleur à distance.



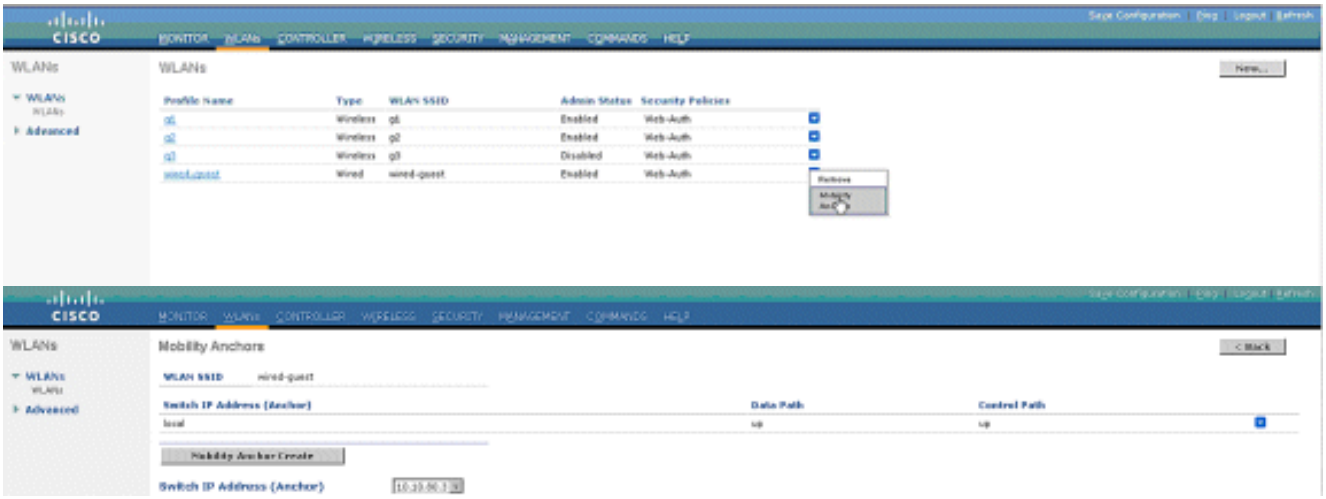
3. Créez le réseau WLAN câblé en lui donnant le même nom que le contrôleur WLAN d’ancrage. Dans ce cas, l'interface d'entrée n'est “ aucune ” car, logiquement, l'interface d'entrée est le tunnel EoIP à partir du contrôleur distant. L’interface de sortie est une interface différente, à laquelle les clients connectés par câble accèdent pour obtenir une adresse IP. Dans cet exemple, une interface dynamique appelée *« guest » (invité) est créée.* Cependant, à cette étape, vous ne pouvez pas activer le réseau WLAN puisqu’un message d’erreur s’affiche pour rappeler qu’une interface d’entrée ne peut pas indiquer *« none » (aucun)*.



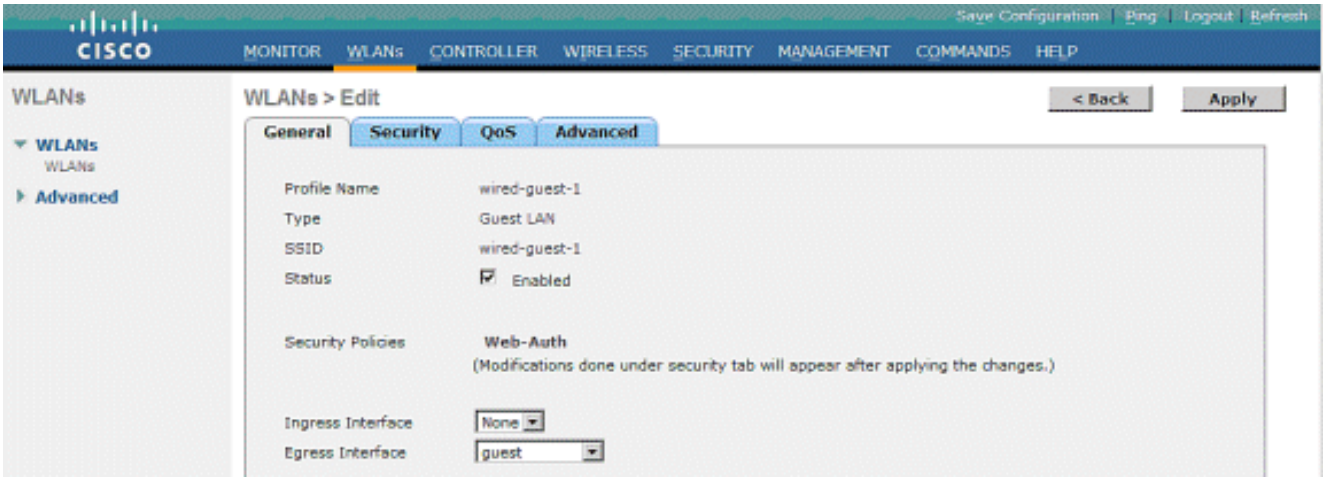
4. Sous « Security » (sécurité), configurez l'option « Layer 3 » (couche 3) selon le mode *web authentication* (authentification Web), de façon semblable au contrôleur à distance.



5. Créez l'ancrage de mobilité sur le contrôleur d'ancrage, puis associez-le à lui-même.



6. Après avoir créé l'ancrage de mobilité, retournez activer le réseau WLAN câblé.



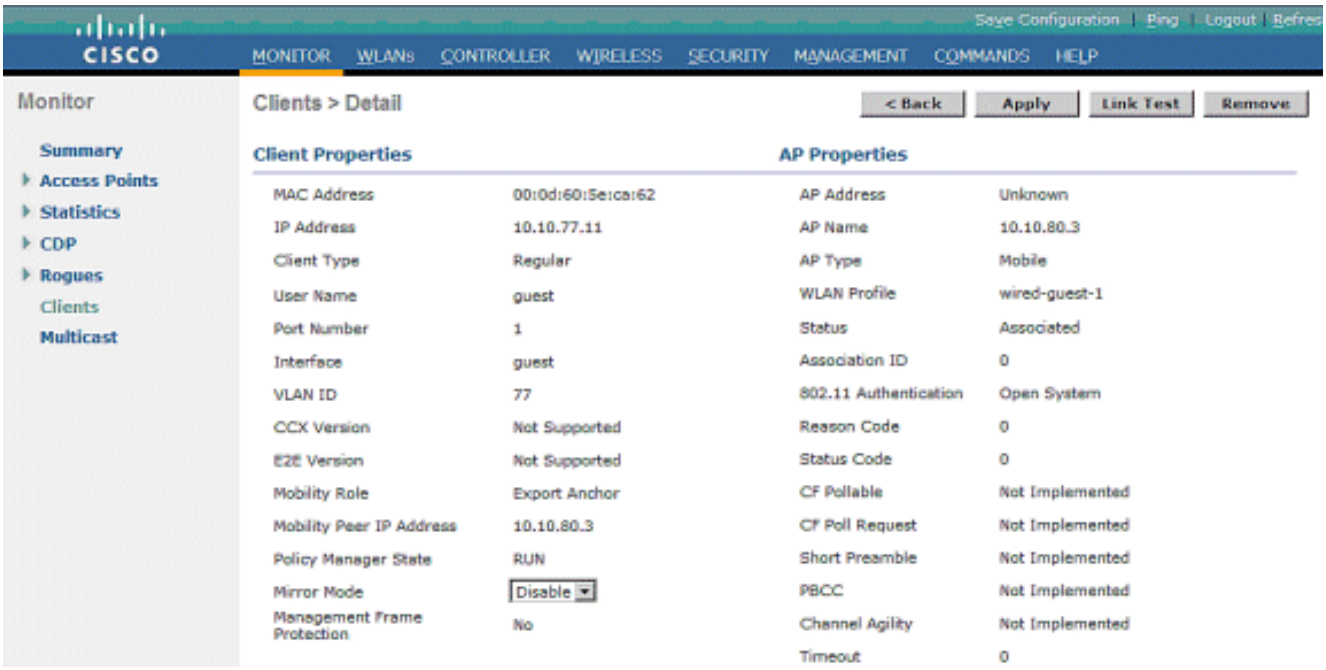
7. De même, créez l'ancrage de mobilité sur le contrôleur WLAN à distance pour le réseau WLAN par câble pour
invité.

Choisissez l'adresse IP du contrôleur WLAN d'ancrage, puis créez l'ancrage de mobilité.

Vérifiez si les données et la chaîne de commande sont opérationnelles. Si ce n'est pas le cas, assurez-vous que les ports suivants sont ouverts entre le contrôleur d'ancrage et le contrôleur de réseau local sans fil à distance : UDP 16666 ou IP 97.

8. Lorsque l'utilisateur invité est connecté par câble au commutateur et que l'authentification Web est terminée, le champ Policy Manager State (état du gestionnaire de politique) doit indiquer « RUN » et le champ Mobility Role (rôle de mobilité) doit indiquer « Export Foreign ».

De même, vérifiez l'état du contrôleur WLAN d'ancrage. Le champ Policy Manager State (état du gestionnaire de politique) doit indiquer « RUN » et le champ Mobility Role (rôle de mobilité) doit indiquer « Export
Anchor ».



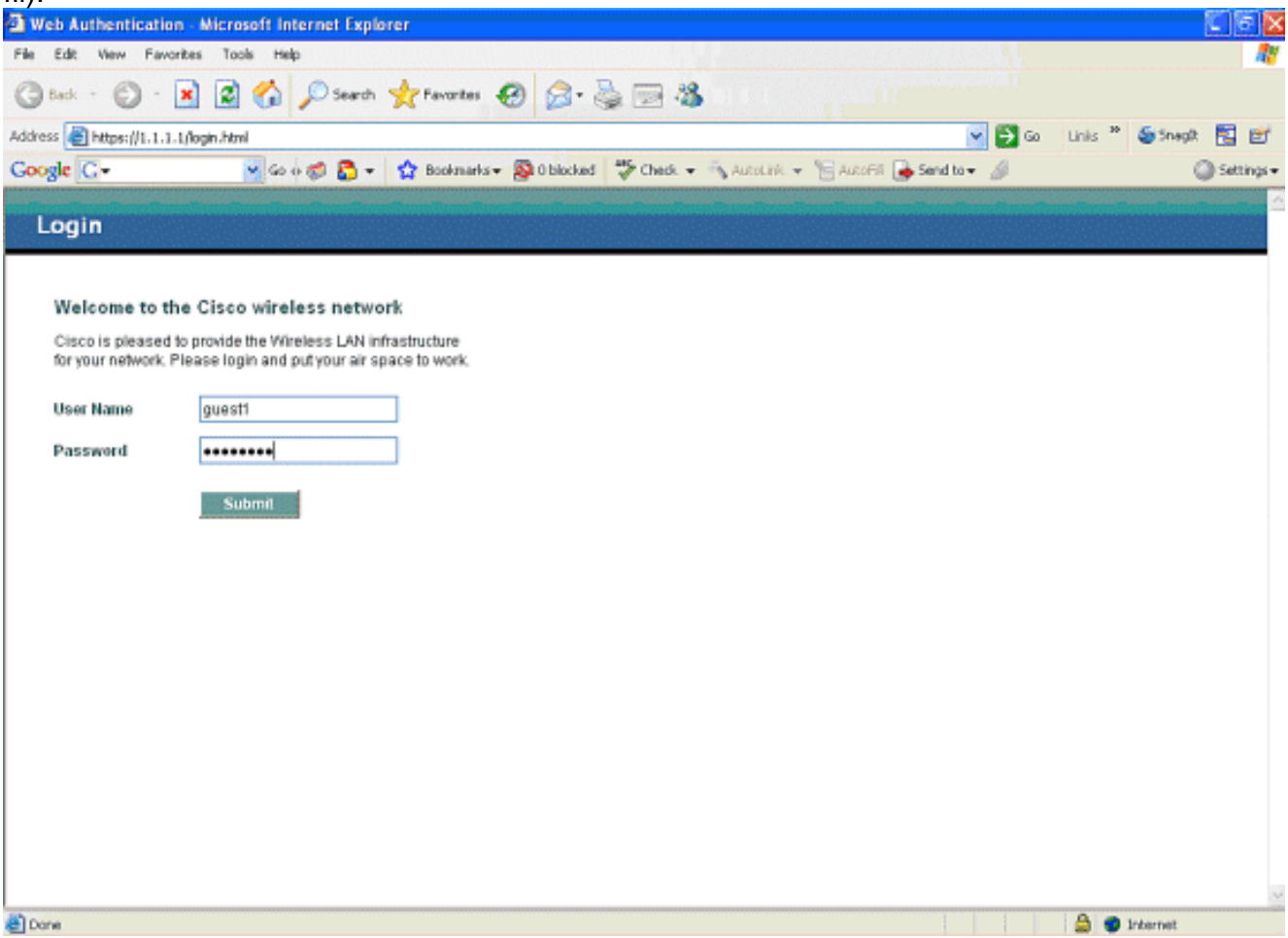
Configuration par câble du client invité

Le client invité par câble reçoit une adresse IP du réseau VLAN de sortie, mais n'a pas accès au trafic avant de terminer le processus d'authentification Web.

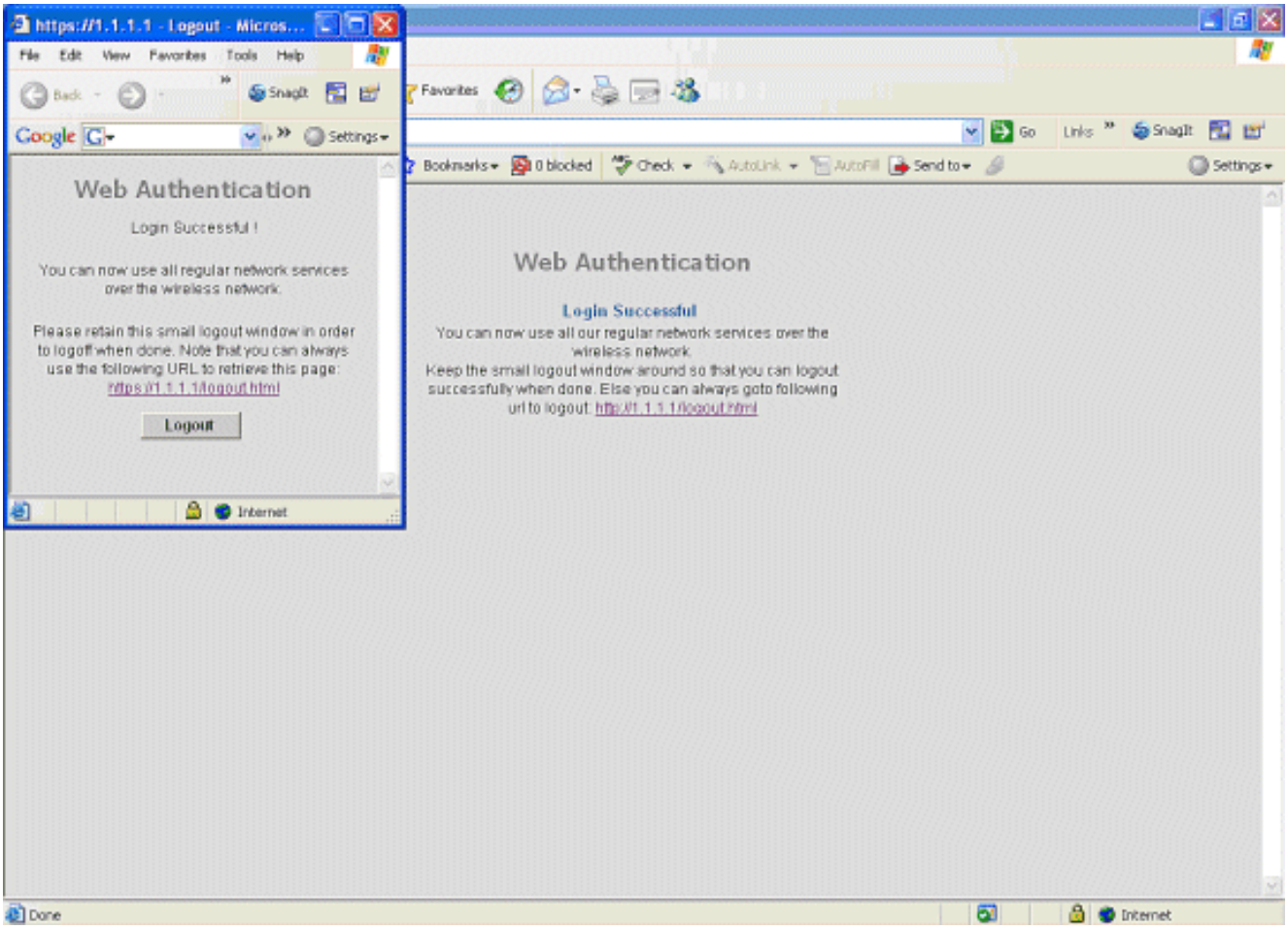
Afin de vous connecter tant qu'utilisateur invité, procédez comme suit :

1. Ouvrez une fenêtre du navigateur Web et entrez l'URL souhaitée (par exemple, www.cisco.com). Vous serez redirigé vers la page Web par défaut du contrôleur de réseau local sans fil si l'authentification Web est activée, et la résolution DNS sera alors lancée pour l'URL entrée. Autrement, entrez l'URL suivante : https://1.1.1.1/login.html (l'adresse IP 1.1.1.1 correspond à l'adresse IP virtuelle du contrôleur de réseau local sans

fil).



2. Entrez le nom d’utilisateur et le mot de passe fournis.
3. Lorsque la connexion est établie, une fenêtre s’affiche dans le navigateur Web.



Dépannage de la connexion par câble pour invité sur un contrôleur WLAN local

Ce processus de débogage contient tous les renseignements utiles concernant la connexion par câble d'un client invité.

debug client

```
 Cisco Controller) >show debug
MAC address ................................ 00:0d:60:5e:ca:62
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.

 (Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Adding mobile on Wired Guest 00:00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
```

```
   Initializing policy
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Change state to AUTHCHECK (2) last state AUTHCHECK (2)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)
   Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)
   Change state to DHCP_REQD (7) last state DHCP_REQD (7)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfPemAddUser2 (apf_policy.c:209) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:00:00:00 from Associated to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -
   not starting session timer for the mobile
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Stopping deletion of Mobile Station: (callerId: 48)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Orphan Packet from 10.10.80.252
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) State Update from Mobility-Incomplete
   to Mobility-Complete, mobility role=Local
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) pemAdvanceState2 3934, Adding TMP rule
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,
   slot 0, interface = 1, QOS = 0 ACL Id = 255,
   Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP_REQD
   (7) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Installing Orphan Pkt IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Unsuccessfully installed IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   0.0.0.0 Added NPU entry of type 9
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Sent an XID frame
Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
```

```
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip:10.10.80.252
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2
   VLAN: 110
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.80.252
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP setting server from OFFER
   (server 10.10.110.1, yiaddr 10.10.110.3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP OFFER (2)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
```

```
   DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1  rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP REQUEST (3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 10.10.110.1  rcvd server id: 1.1.1.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 -NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 DHCP_REQD (7) Change state to WEBAUTH_REQD
   (8) last state WEBAUTH_REQD (8)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) pemAdvanceState2
   4598, Adding TMP rule
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Successfully
   plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Plumbing web-auth redirect rule due to user logout
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Assigning Address 10.10.110.3 to mobile
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP ACK (5)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
```

```
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1  rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Setting guest session timeout for mobile
   00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Session Timeout is 79953 - starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Change state to
   WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_NOL3SEC (14) Change state to RUN
   (20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Replacing FastPath rule
type = Airespace AP Client
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
   Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
   ARP for 10.10.110.3, VLAN Id 110
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

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

Informations connexes

- Configuration de la mobilité d'ancrage automatique
- Exemple de configuration d'un WLAN invité et d'un WLAN interne à l'aide de contrôleurs de réseau local sans fil (WLC)
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil

- Guide de configuration du contrôleur de réseau local sans fil Cisco, version 4.2
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.