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

Contenu

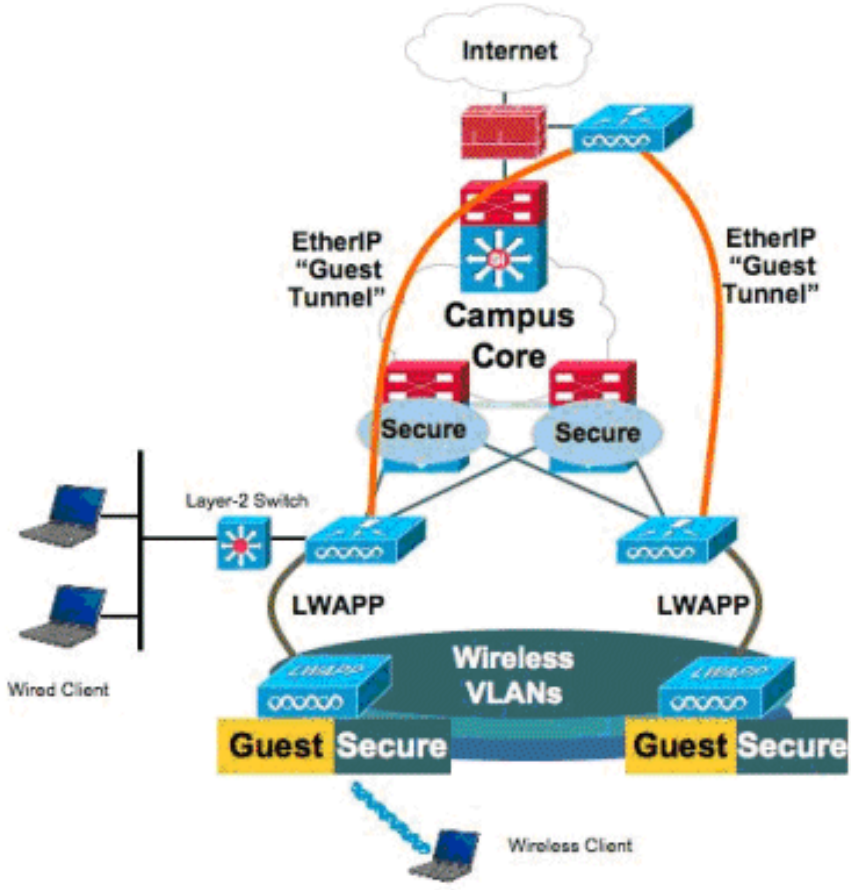
Introduction

Ce document décrit comment configurer l'accès invité avec la nouvelle prise en charge de fonctionnalité de câble d'accès invité sur les contrôleurs de WLAN Cisco (WLCs) cette version de logiciel 4.2.61.0 et ultérieures de Cisco Unified Wireless d'utilisation. Un nombre de plus en plus important de sociétés identifient la nécessité de permettre d'accéder l'accès Internet à ses clients, les Partenaires, et les consultants quand ils visitent leurs équipements. Les gestionnaires informatiques peuvent fournir de câble et radio sécurisé et accès contrôlé à l'Internet pour des invités sur le même contrôleur LAN Sans fil.

On doit permettre à des des utilisateurs d'invité pour se connecter aux ports Ethernet indiqués et pour accéder au réseau d'invité comme configurés par l'administrateur après qu'ils se terminent les méthodes d'authentification configurées. Les utilisateurs Sans fil d'invité peuvent facilement se connecter aux contrôleurs WLAN aux configurations en cours d'accès invité. En outre, le système de contrôle sans fil (WCS), avec la configuration de base et la Gestion des contrôleurs WLAN, fournit des services améliorés d'utilisateur d'invité. Pour les clients qui ont déjà déployé ou prévoient de déployer des contrôleurs WLAN et WCS dans leur réseau, ils peuvent accroître la même infrastructure pour l'accès invité de câble. Ceci fournit une expérience Sans fil et de câble unifiée d'accès invité aux utilisateurs finaux.

Des ports de câble d'invité sont fournis dans un emplacement indiqué et branchés à un commutateur d'accès. La configuration sur le commutateur d'accès met ces ports dans un de la couche de câble 2 VLAN d'invité. Deux solutions distinctes sont à la disposition des clients :

- Un contrôleur WLAN simple (VLAN à mode de traduction) - les joncteurs réseau de commutateur d'accès le trafic de câble d'invité dans le VLAN invité au contrôleur WLAN qui fournit la solution de câble d'accès invité. Ce contrôleur effectue la traduction VLAN du VLAN invité de câble par d'entrée au de sortie VLAN.
- Deux contrôleurs WLAN (mode automatique d'ancre) - les joncteurs réseau de commutateur d'accès le trafic de câble d'invité à un contrôleur WLAN local (le contrôleur le plus près au commutateur d'accès). Ce contrôleur WLAN de gens du pays ancre le client sur un contrôleur WLAN d'ancre de la zone démilitarisée (DMZ) qui est configuré pour de câble et accès invité sans fil. Après qu'un transfert réussi du client au contrôleur d'ancre DMZ, l'affectation d'adresse IP DHCP, authentification du client, et ainsi de suite soient manipulés dans le DMZ WLC. Après qu'il se termine l'authentification, on permet le client au trafic émetteur-récepteur.



Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

La prise en charge de fonctionnalité de câble d'accès invité sur les contrôleurs de WLAN Cisco est prise en charge par la version de logiciel 4.2.61.0 et ultérieures de Cisco Unified Wireless.

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.

Configurez

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

Configuration de commutateur de couche d'accès

Afin de fournir l'accès invité de câble, les ports désignés dans la couche le besoin de commutateur de 2 couches d'accès d'être configuré sur le VLAN invité par l'administrateur. Le VLAN invité doit être séparé de tous les autres VLAN qui sont configurés sur ce commutateur. Le trafic de VLAN invité est trunked au contrôleur de gens du pays WLAN le plus proche. Le contrôleur de gens du pays perce un tunnel le trafic d'invité à travers un Ethernet au-dessus de tunnel IP (EoIP) à un contrôleur d'ancre DMZ. Cette solution exige au moins deux contrôleurs.

Alternativement, les joncteurs réseau de commutateur d'accès le VLAN invité au contrôleur simple traduit le VLAN invité à 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 Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Points importants pour le déploiement de câble d'invité

- Actuellement, cinq réseaux locaux d'invité pour l'accès invité de câble sont pris en charge. Au total, 16 WLAN pour des utilisateurs de sans fil et 5 WLAN pour l'accès invité de câble peuvent être configurés sur l'ancre WLC. Tunnel distinct n'existe pas pour des WLAN. Tous les WLAN invités, qui incluent les WLAN pour l'accès invité de câble, utilisent les mêmes tunnels d'EoIP à l'ancre WLC.
- Les administrateurs doivent créer des interfaces dynamiques dans le contrôleur WLAN, les marquer en tant que « RÉSEAU LOCAL d'invité, » et les associer aux WLAN créés comme réseaux locaux d'invité.
- Assurez-vous que les configurations WLAN, y compris l'authentification, sont identiques sur l'ancre et des contrôleurs distants pour passer le trafic de client.
- WLCs devrait avoir les versions de logiciel compatibles. Assurez-vous qu'ils exécutent la même version majeure.
- L'authentification Web est le mécanisme de sécurité par défaut disponible sur un RÉSEAU LOCAL de câble d'invité. Les options en cours disponibles sont ceux-ci : Ouvrez-vous, Web authentique, et fonction émulation de Web.
- En cas de panne du tunnel d'EoIP entre le distant et l'ancre WLC, la base de données de client est nettoyée de l'ancre WLC. Le client doit rassocier et authentifier à nouveau.
- Aucun degré de sécurité de la couche 2 n'est pris en charge.
- Le trafic de Multidiffusion/émission sur les réseaux locaux de câble d'invité est abandonné.
- Les paramètres de proxy DHCP doivent être identiques sur l'ancre et des contrôleurs distants.

Pour l'invité de câble, il y a un délai d'attente de veille qui fonctionne dans le contrôleur. Si aucun paquet n'est reçu au cours de la période configurée du client, le client est retiré du contrôleur. Quand un client envoie une demande de Protocole ARP (Address Resolution Protocol) la prochaine fois, une nouvelle entrée de client est créée et déplacée au Web authentique/à état de passage convenablement selon la configuration de sécurité.

Prise en charge de la plate-forme

L'accès invité de câble est pris en charge sur ces Plateformes :

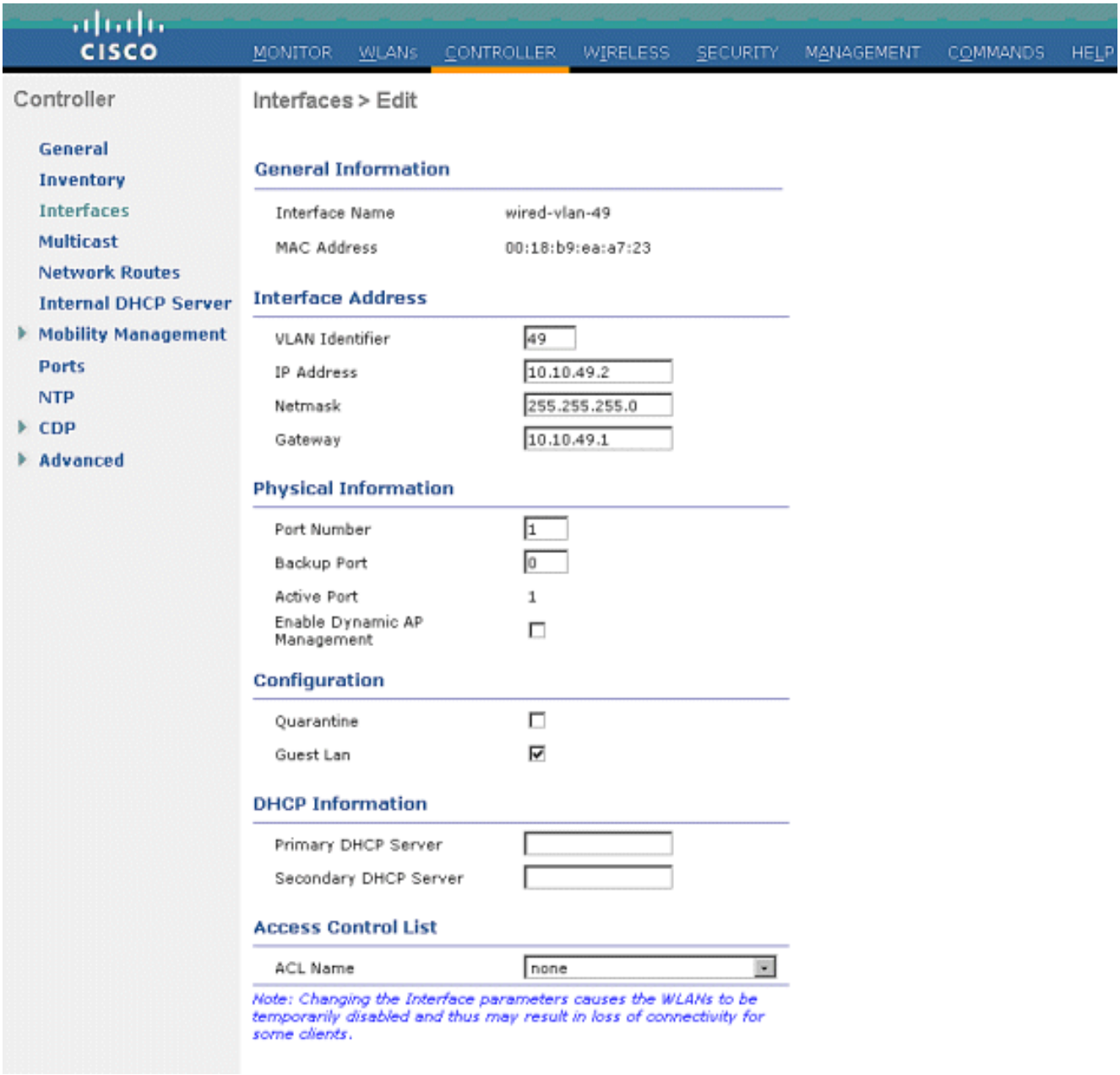
- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, WLC virtuel

Configuration LAN Sans fil

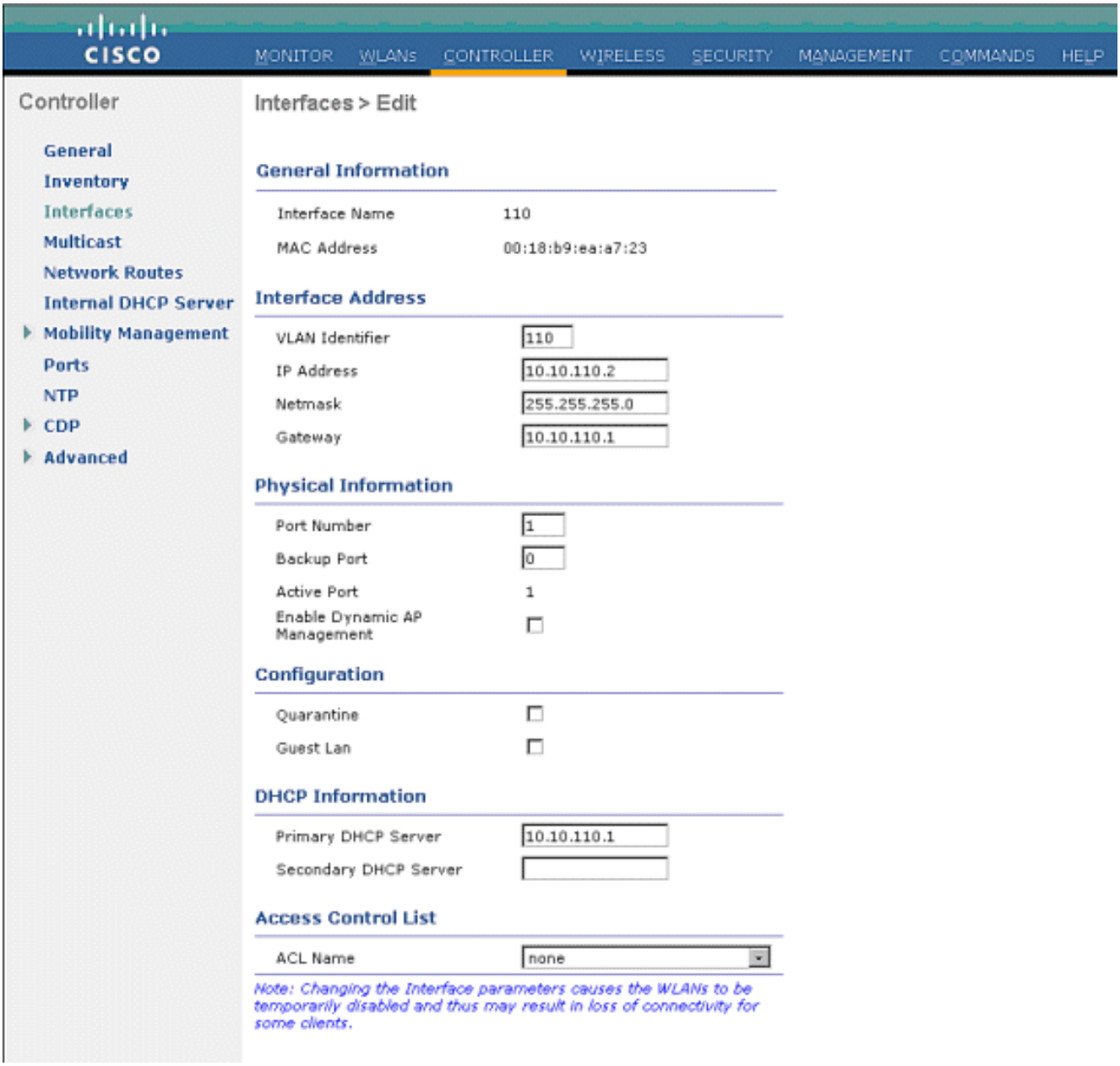
Dans cet exemple, la configuration de base du contrôleur LAN Sans fil est assumée. Le foyer est

sur la configuration supplémentaire exigée pour se terminer l'implémentation de câble d'accès invité.

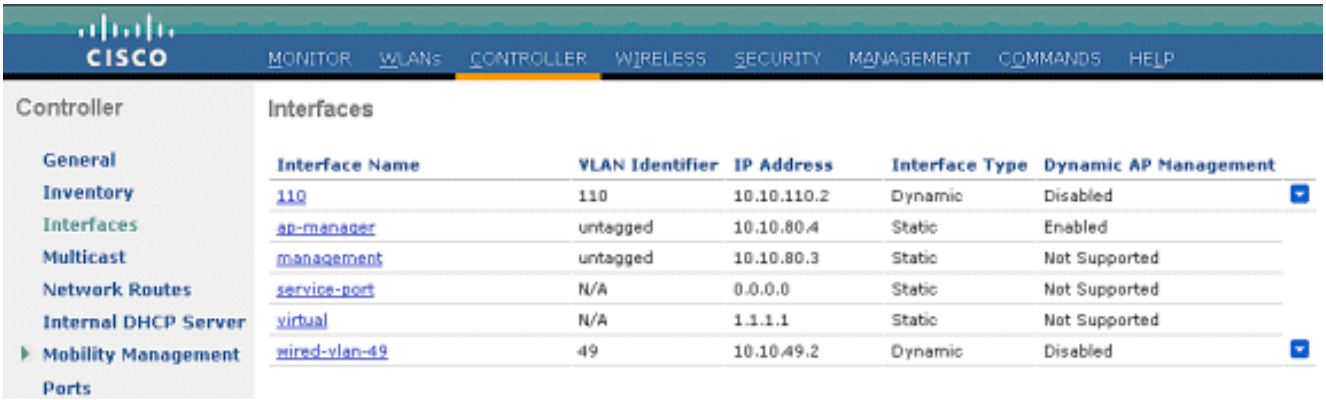
1. Créez une interface dynamique et marquez-la est comme « RÉSEAU LOCAL d'invité. » Quand vous créez cette interface dynamique dans la version en cours, vous devez fournir une adresse IP et une passerelle par défaut, quoiqu'elle n'existe pas puisque c'est une couche 2 VLAN ; vous n'avez pas besoin de ne fournir aucune adresse DHCP. Des clients de câble d'invité sont physiquement connectés à ce
VLAN.



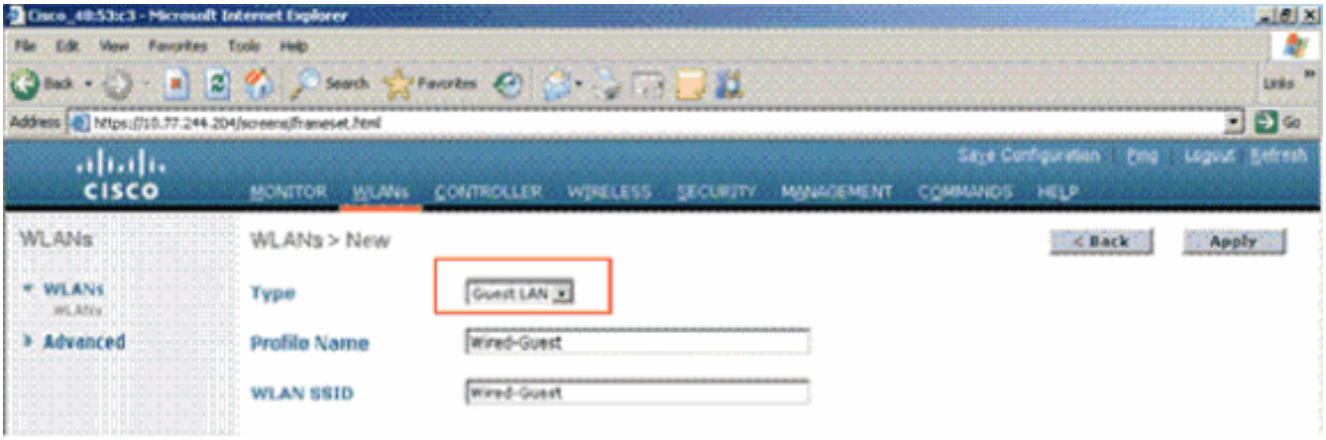
2. Créez une autre interface dynamique où les clients de câble d'invité reçoivent une adresse IP.Remarque: Vous devez fournir une adresse IP/passerelle par défaut/adresse de serveur DHCP dans cette
interface.



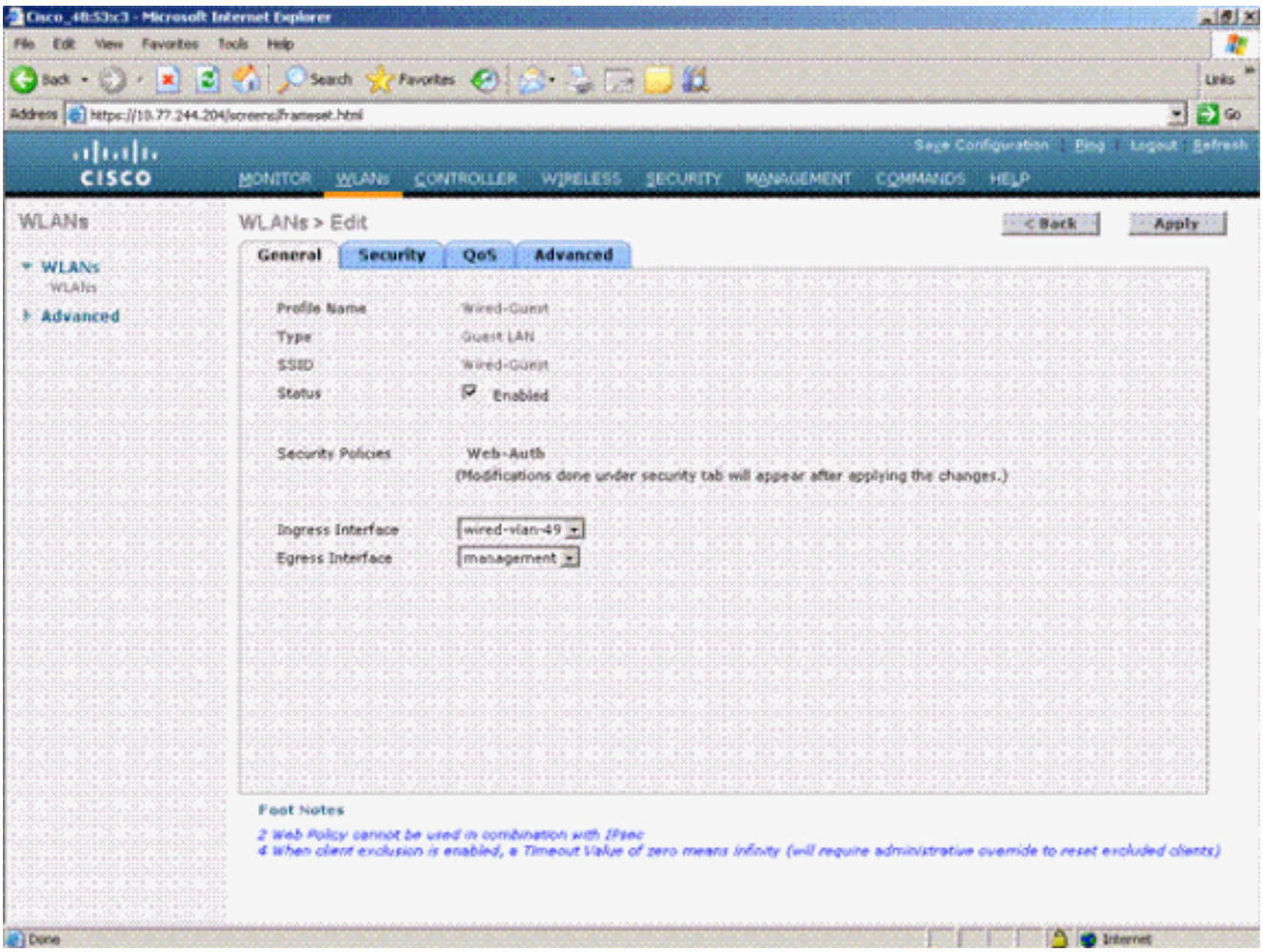
3. Ce sont les interfaces dynamiques
:



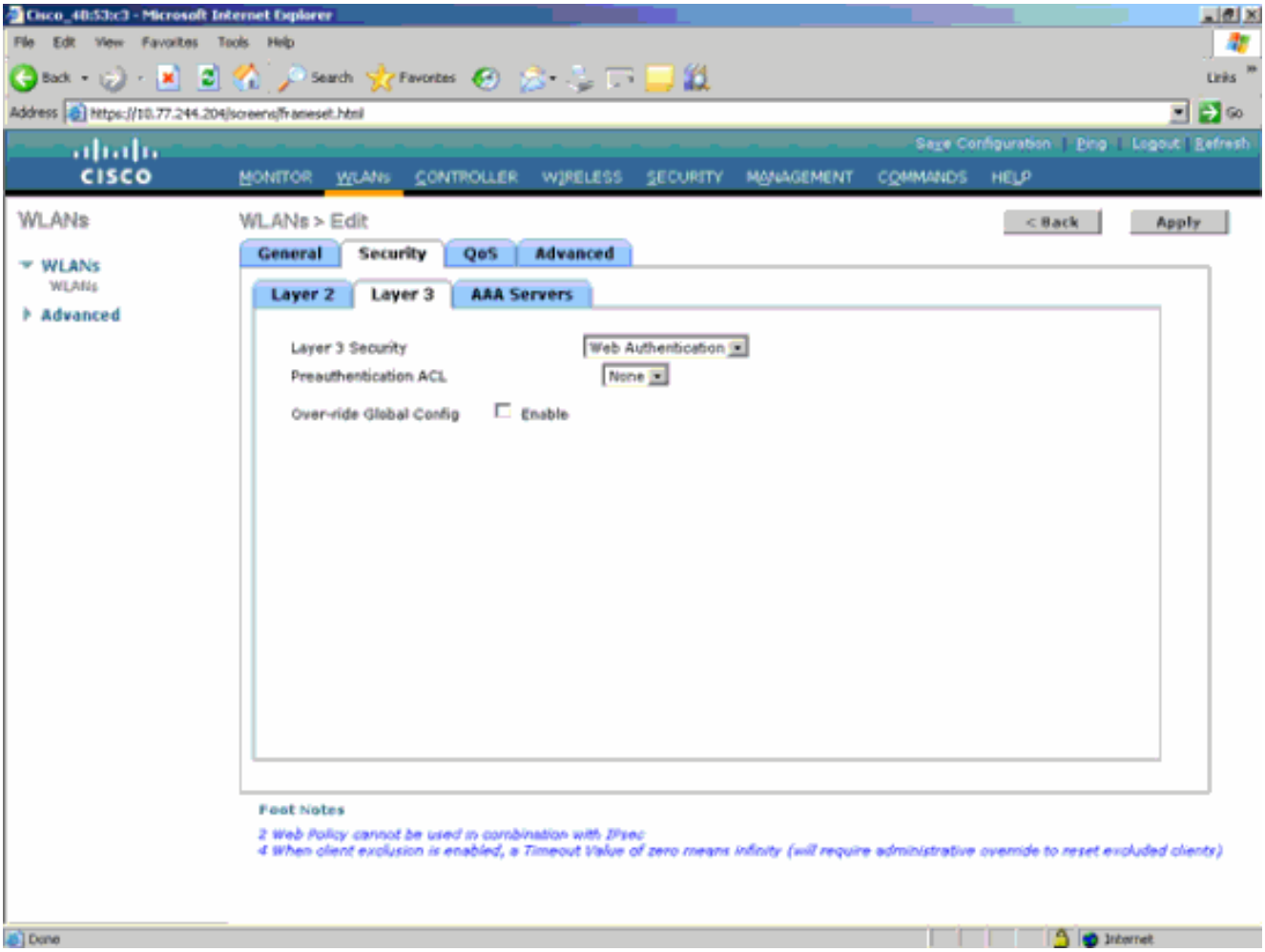
4. Ajoutez un nouveau WLAN : RÉSEAU LOCAL de Type=Guest.



5. Activez le WLAN ; tracez l'interface d'entrée au « RÉSEAU LOCAL d'invité » créé dans l'étape 1, et l'interface de sortie peut être une interface de gestion ou n'importe quelle autre interface dynamique, bien que de préférence une interface dynamique comme cela créé dans l'étape
2.

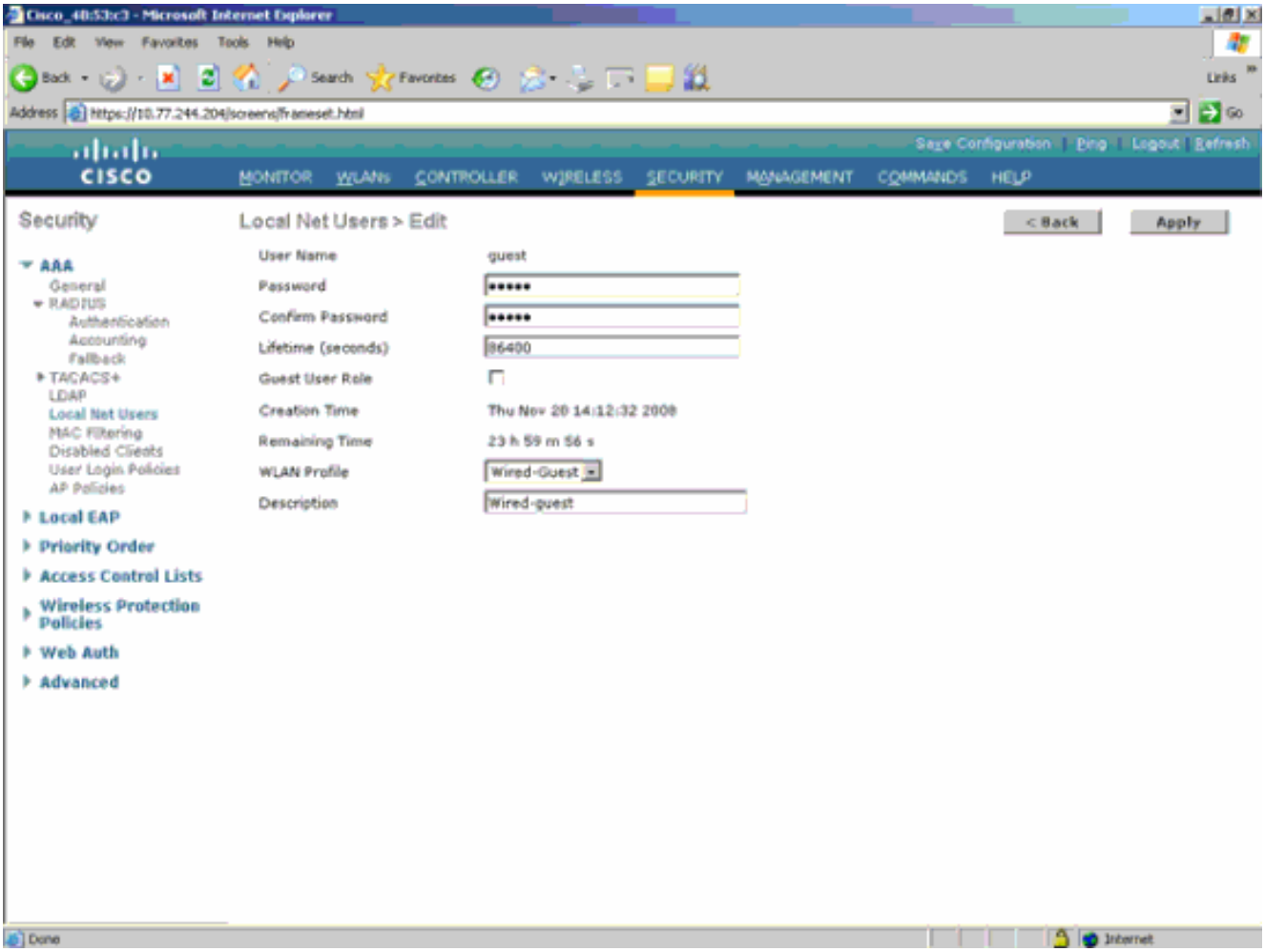


6. L'authentification Web est activée par défaut comme option de Sécurité configurée sur le RÉSEAU LOCAL d'invité. Il peut être changé à la *fonction émulation d'aucun* ou de *Web*.



7. C'est la configuration finale du WLAN.

8. Ajoutez un utilisateur d'invité dans la base de données locale du WLC.

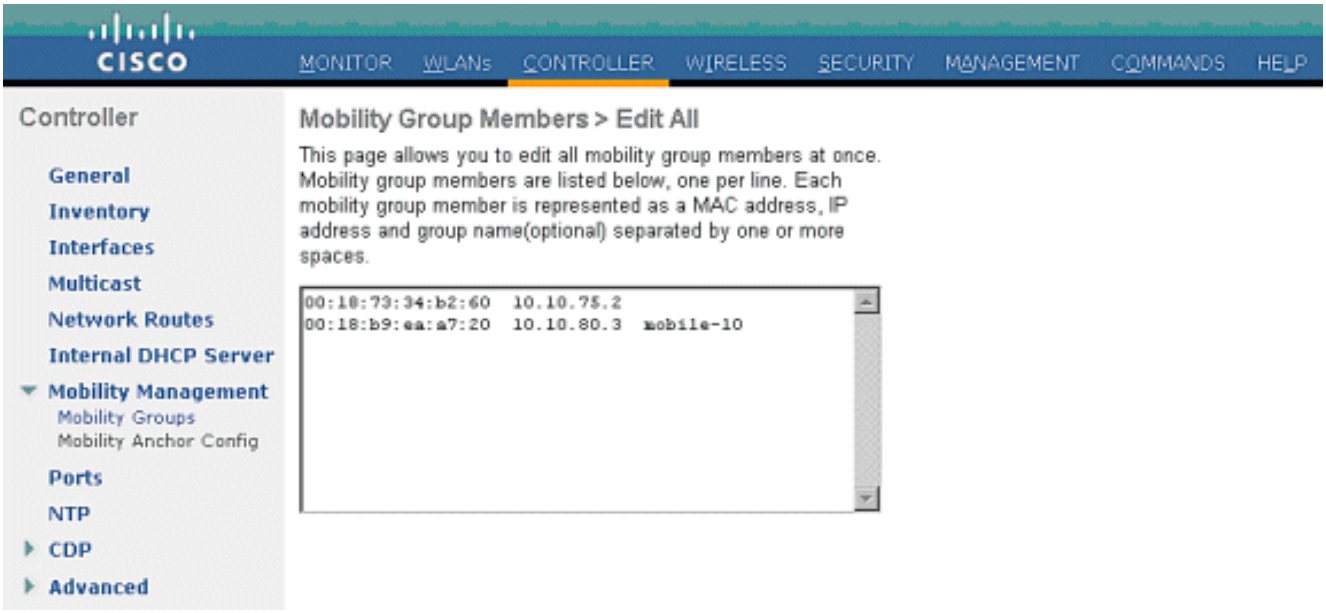


Sur l'étranger, vous devez placer le d'entrée comme « RÉSEAU LOCAL configuré d'invité. » Au de sortie, vous devez le placer à une certaine interface, probablement l'interface de gestion. Cependant, une fois que le tunnel d'EoIP est construit, il envoie le trafic automatiquement par le tunnel au lieu de l'adresse de gestion.

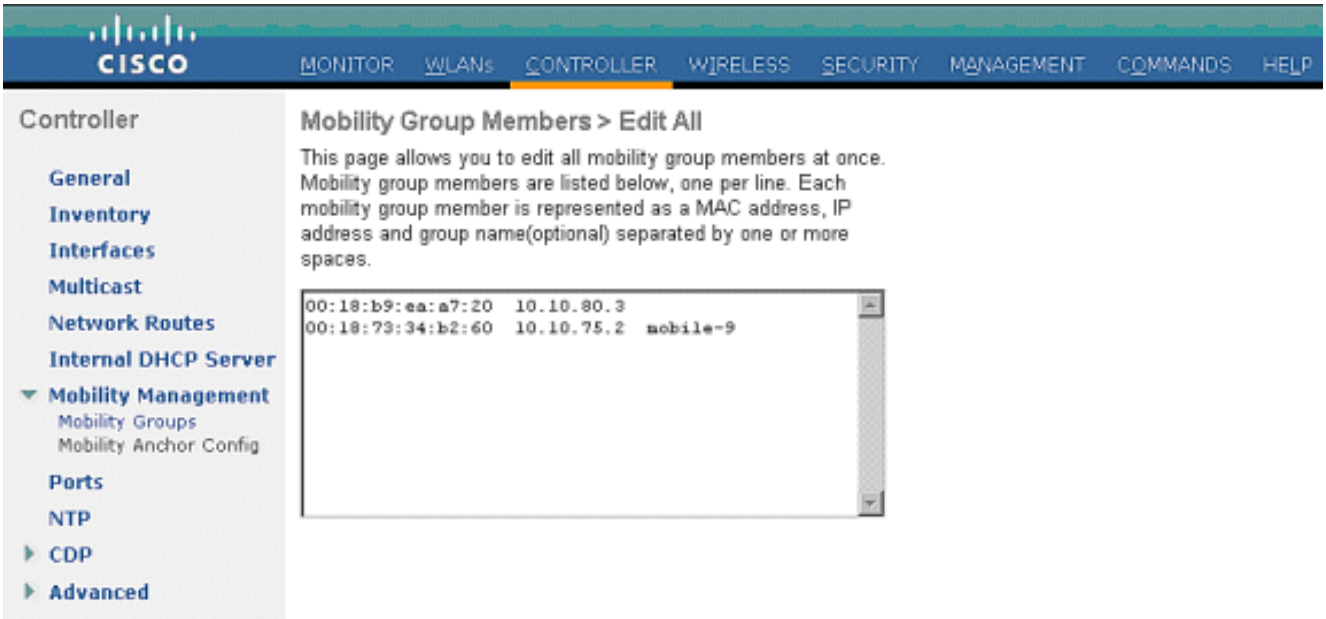
Accès invité de câble avec le contrôleur WLAN d'ancre

Dans cet exemple, l'adresse IP du contrôleur LAN Sans fil distant est 10.10.80.3, et l'adresse IP du contrôleur de l'ancre DMZ est 10.10.75.2. Chacun des deux font partie de deux Groupes de mobilité différents.

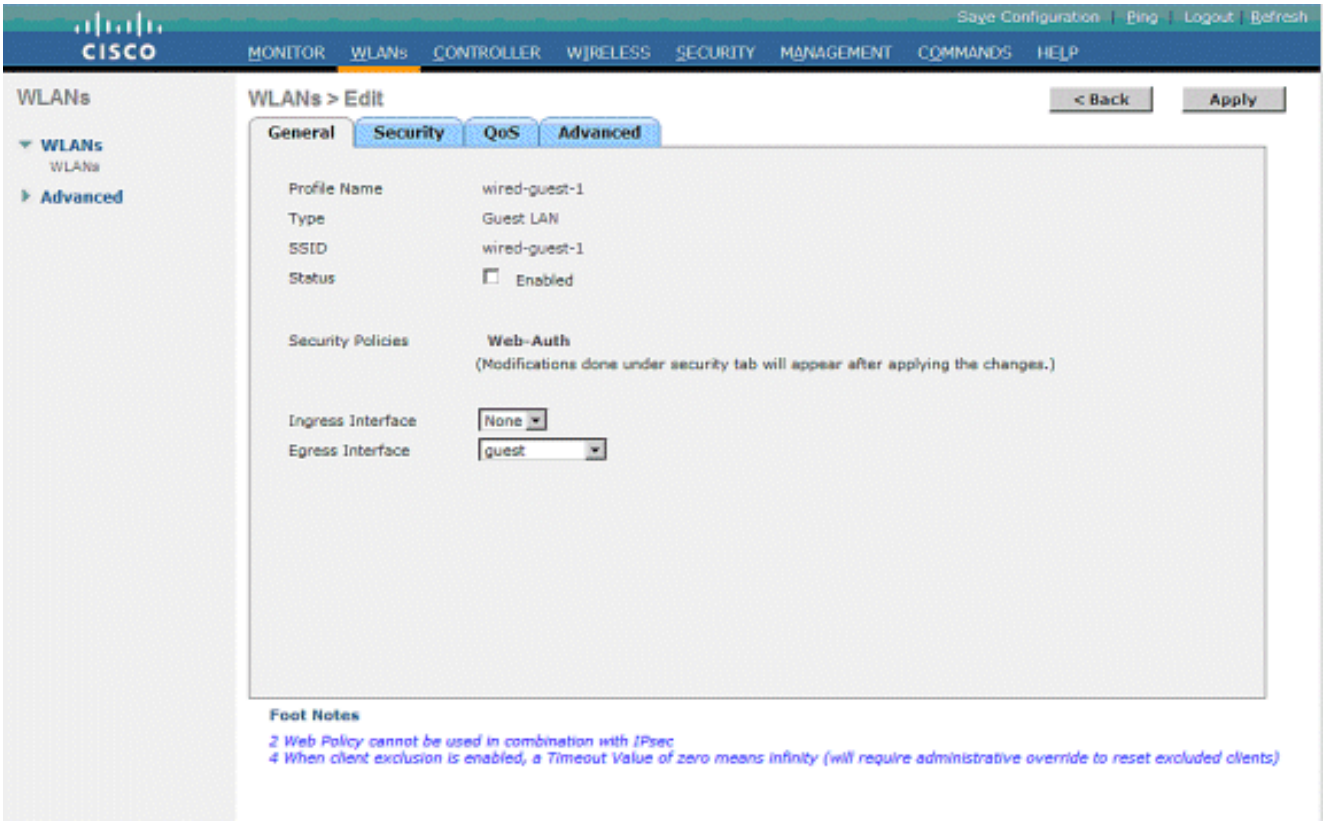
1. Configurez le groupe de mobilité du contrôleur de l'ancre DMZ quand vous ajoutez l'adresse MAC, l'adresse IP, et le nom de groupe de mobilité du contrôleur distant.



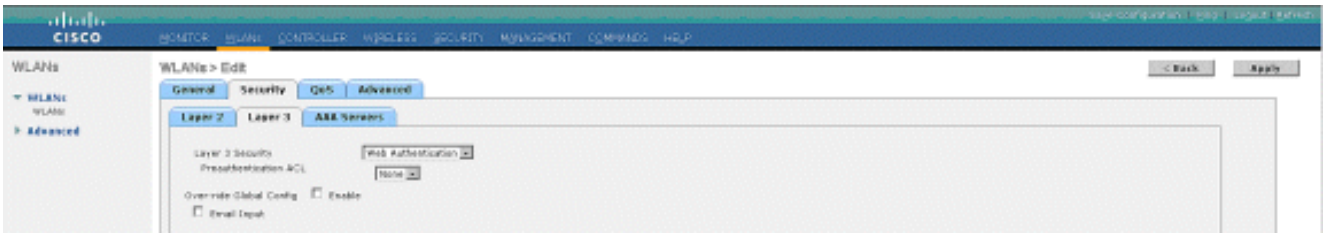
2. De même, configurez le groupe de mobilité dans le contrôleur distant.



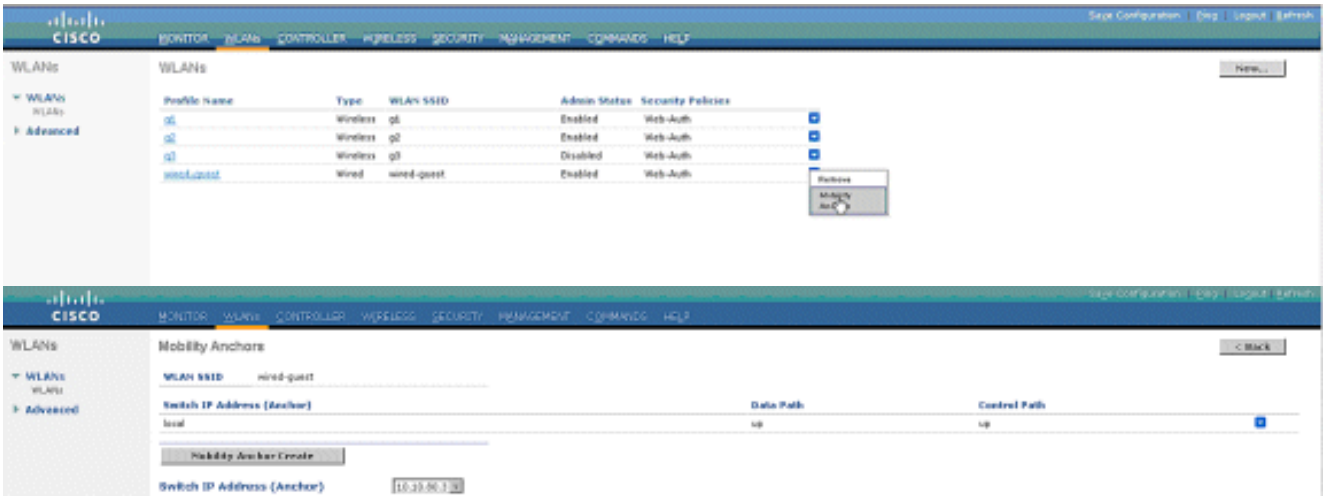
3. Créez le WLAN de câble avec le nom précis dans l'ancre WLC. L'interface d'entrée n'en est dans ce cas « aucune » parce que, logiquement, l'interface d'entrée est le tunnel d'EoIP du contrôleur distant. L'interface de sortie est une interface différente, où les clients câblés vont recevoir l'adresse IP. Dans cet exemple, une interface dynamique appelée l'*invité* est créée. Cependant, à ce stade vous ne pouvez pas activer le WLAN parce qu'il affiche un message d'erreur, qui lit qu'une interface d'entrée ne peut pas n'en être *aucune*.



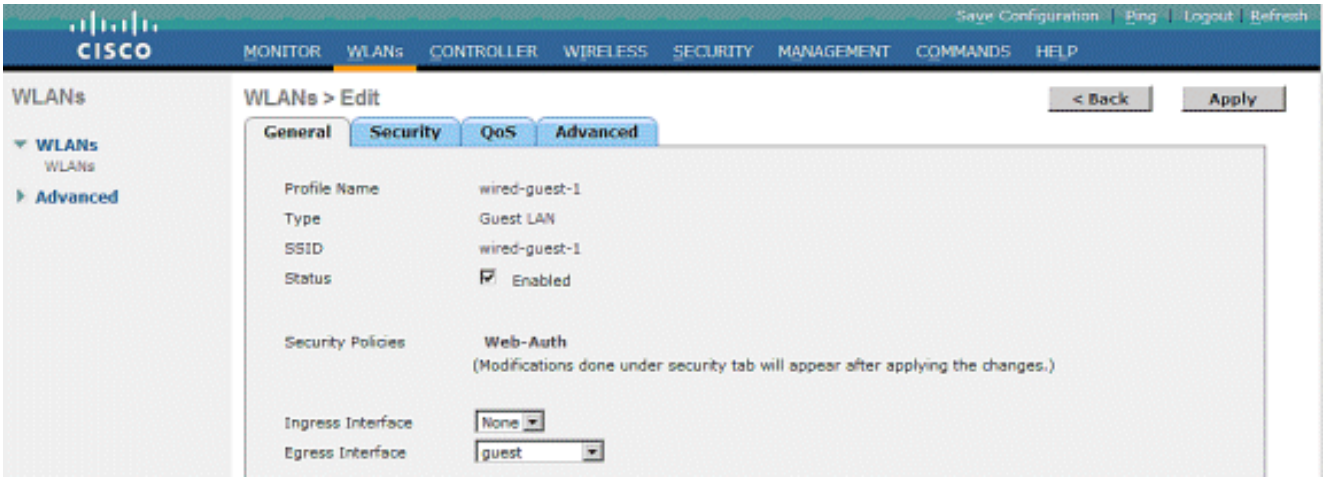
4. Configurez le degré de sécurité de la couche 3 comme *authentification Web*, semblable au contrôleur
distant.



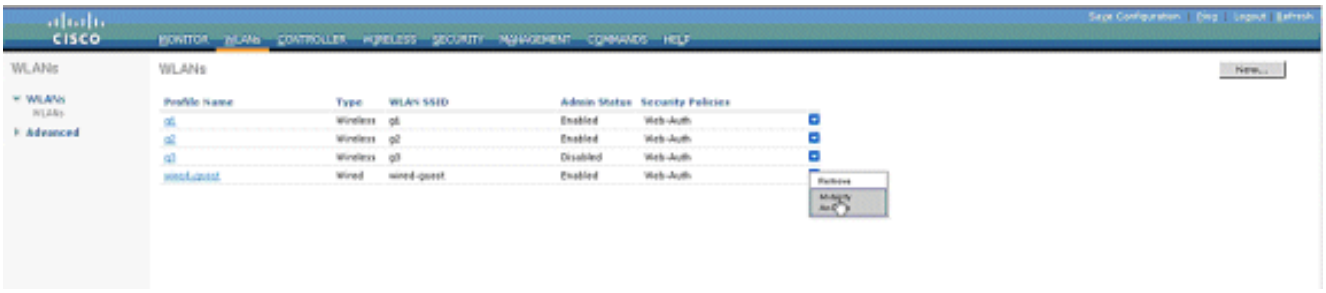
5. Créez l'ancre de mobilité sur le contrôleur d'ancre, et tracez-la à elle-même.



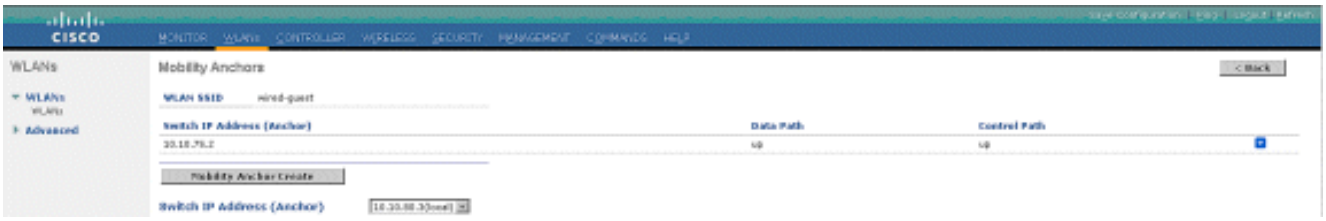
6. Une fois que l'ancre de mobilité est créée, retournez et activez le WLAN de câble.



7. De même, créez l'ancre de mobilité sur le distant WLC pour le WLAN invité de câble.



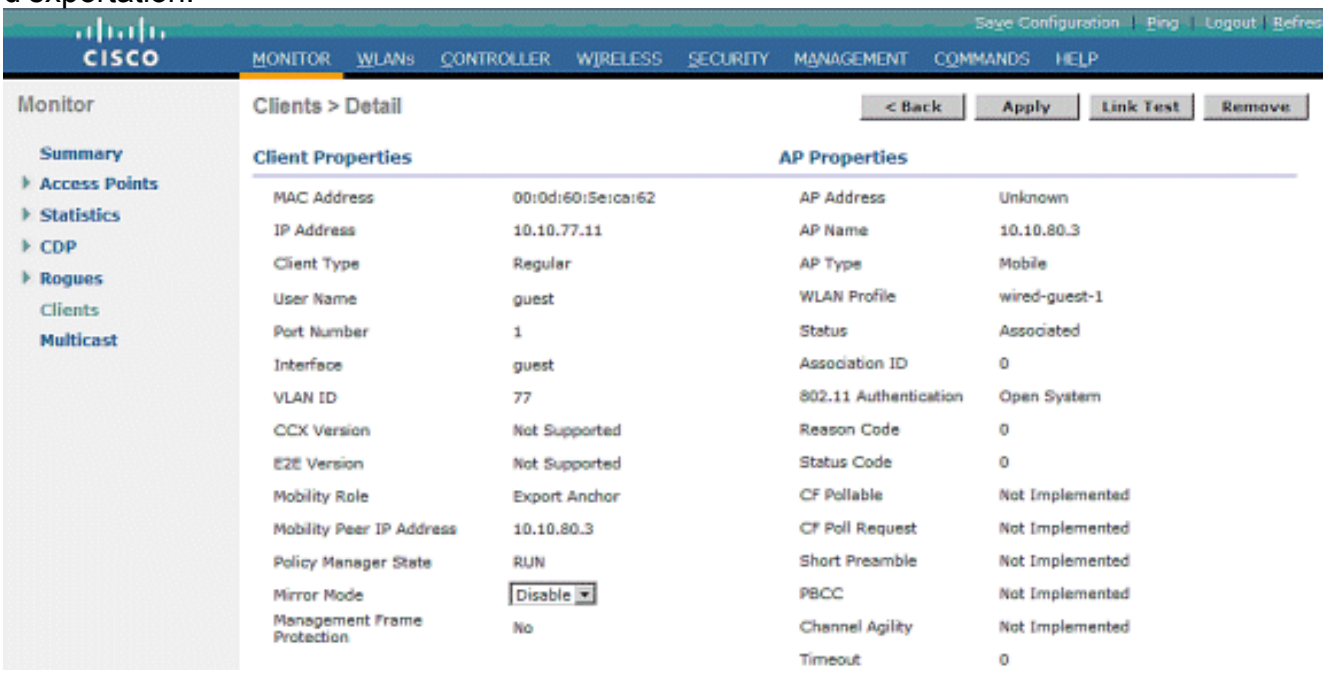
Choisissez l'adresse IP de l'ancre WLC et créez l'ancre de mobilité.



Vérifiez si le chemin de données et de contrôle est. Sinon, assurez que ces ports sont ouverts entre l'ancre et le contrôleur LAN Sans fil de distant : UDP 16666 ou IP 97.

8. Une fois qu'un utilisateur de câble d'invité est connecté au commutateur et s'est terminé l'authentification Web, l'état de Policy Manager doit ÊTRE EXÉCUTÉ, et le rôle de mobilité est exportation
étrangère.

De même, vérifiez l'état dans l'ancre WLC. L'état de Policy Manager doit ÊTRE EXÉCUTÉ, et le rôle de mobilité est ancre d'exportation.

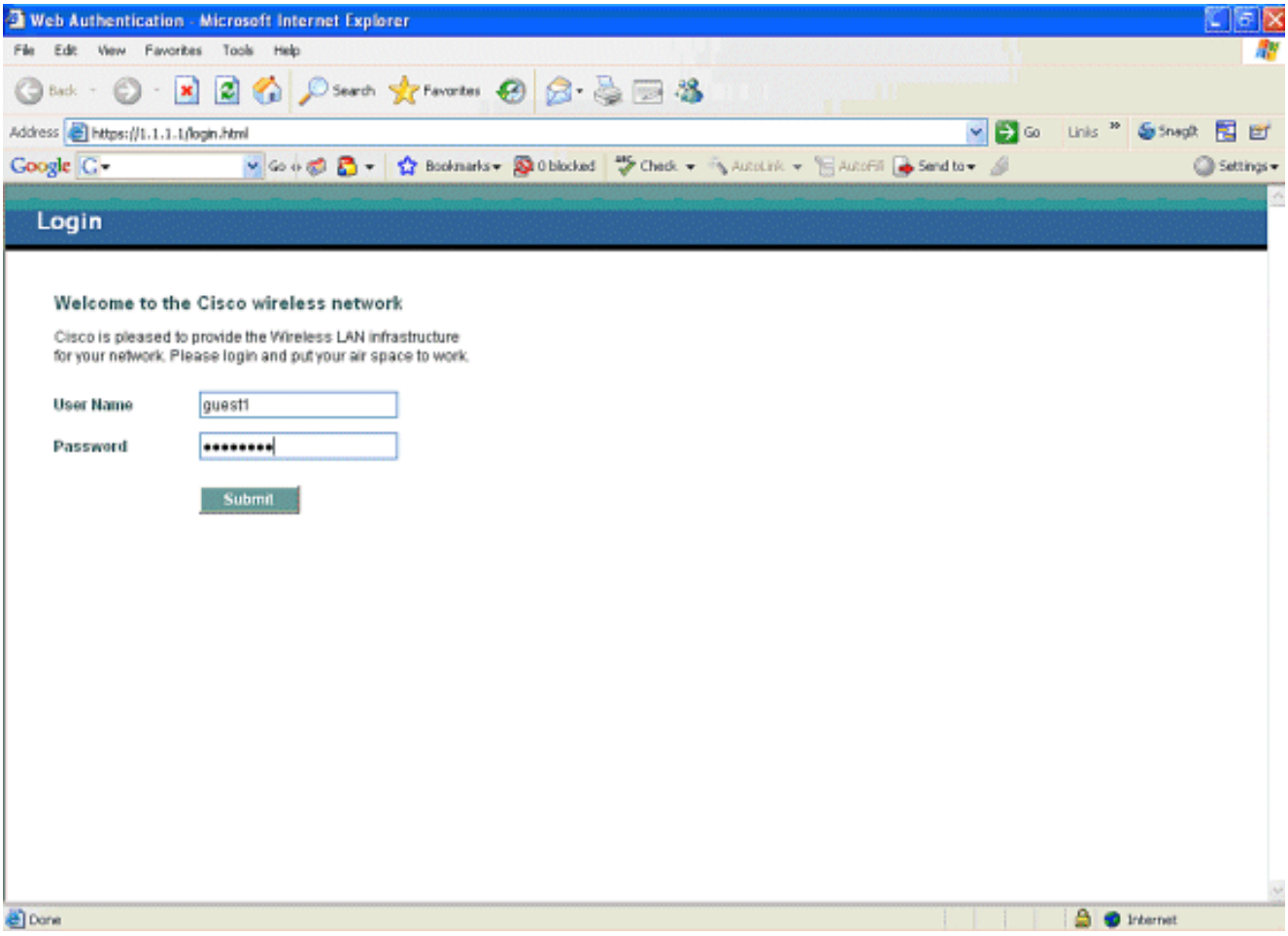


Configuration de client de câble d'invité

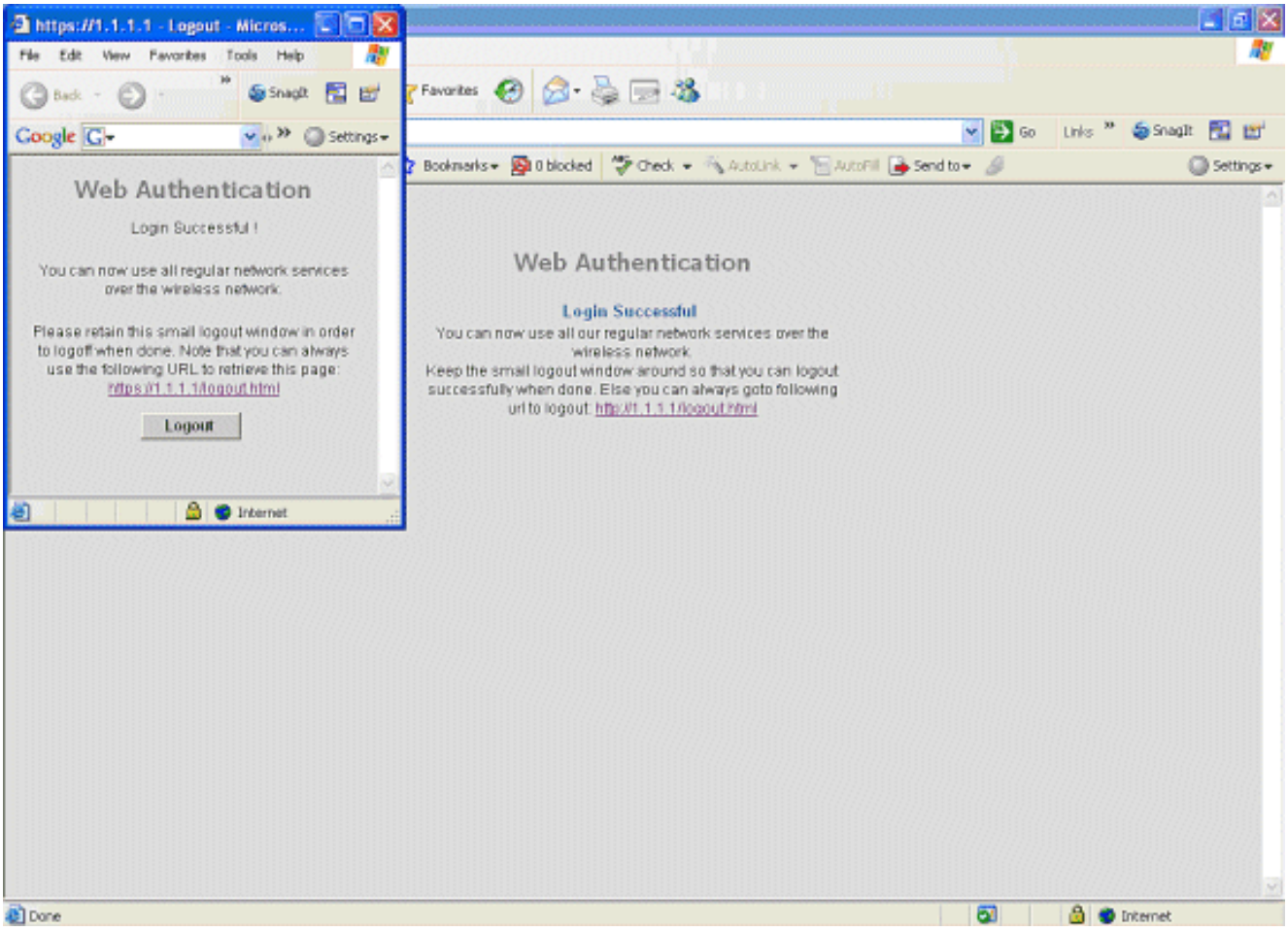
Le client de câble d'invité reçoit une adresse IP du de sortie VLAN mais ne peut passer aucun trafic jusqu'à ce qu'il complète le procédé d'authentification Web.

Afin d'ouvrir une session en tant qu'utilisateur d'invité, suivez ces étapes :

1. Ouvrez une fenêtre du navigateur et écrivez le nom désiré URL (par exemple, www.cisco.com). L'invité est réorienté à la page Web par défaut du contrôleur LAN Sans fil si l'authentification Web est activée, et une résolution de DN peut être terminée pour l'URL qui est écrit. Autrement, écrivez cet URL : https://1.1.1.1/login.html, où l'adresse IP 1.1.1.1 est l'adresse IP virtuelle du contrôleur LAN Sans fil.



2. Écrivez le nom d'utilisateur et mot de passe qui sont fournis.
3. Si la procédure de connexion est réussie, des notes en fenêtre du navigateur cela.



Debugs pour la connexion de câble d'invité sur les gens du pays WLC

Ceci mettent au point fournit tout le relatif à l'information au client de câble d'invité.

debug client <mac-address>

```
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 â 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
```

Vérifiez

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

Dépannez

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

Informations connexes

- Configurer la mobilité d'auto-ancrage
- 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 Sans fil de contrôleur LAN de Cisco, version 4.2
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems