Wiens Guest Access met Cisco WLAN-controllers - configuratievoorbeeld

Inhoud

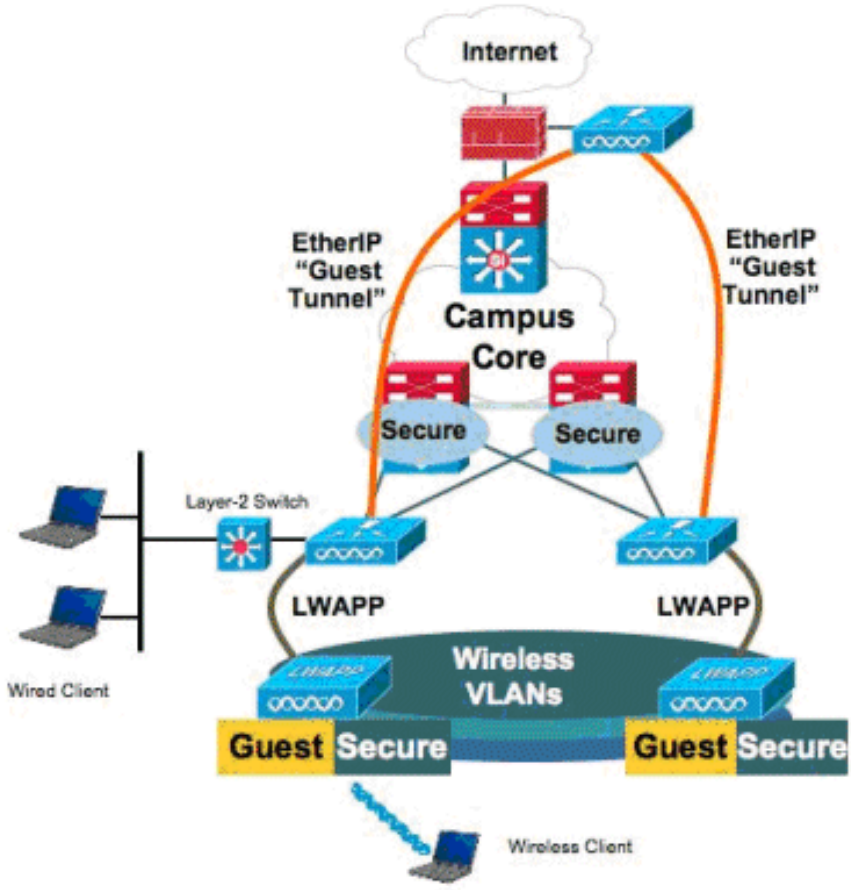
Inleiding

Dit document beschrijft hoe u de toegang tot uw workflow kunt configureren met de nieuwe ondersteuning voor bekabelde toegang voor Cisco WLAN-controllers (WLC's) die Cisco Unified Wireless-softwarerelease 4.2.61.0 en hoger gebruiken. Een groeiend aantal bedrijven erkent de noodzaak om internettoegang te bieden aan zijn klanten, partners en consultants wanneer ze hun faciliteiten bezoeken. IT-managers kunnen draadloze, beveiligde en beheerste toegang tot het internet bieden aan gasten met dezelfde draadloze LAN-controller.

Guest gebruikers moeten toestemming krijgen om verbinding te maken met aangewezen Ethernet-poorten en toegang te krijgen tot het gastnetwerk zoals dat door de beheerder wordt ingesteld nadat ze de geconfigureerde authenticatiemethoden hebben voltooid. Draadloze gastgebruikers kunnen eenvoudig verbinding maken met de WLAN-controllers met de huidige gasttoegangsfuncties. Daarnaast biedt Wireless Control System (WCS), naast de basisconfiguratie en het beheer van WLAN-controllers, uitgebreide gastgebruikersservices. Voor klanten die reeds WLAN-controllers en WCS in hun netwerk hebben geïmplementeerd of van plan zijn te implementeren, kunnen zij dezelfde infrastructuur gebruiken voor bekabelde gasttoegang. Dit voorziet in een verenigde draadloze en bekabelde ervaring van de gasttoegang tot de eindgebruikers.

De bekabelde gasthavens worden voorzien in een aangewezen plaats en in een toegangsschakelaar aangesloten. De configuratie op de toegangsschakelaar zet deze poorten in één van de bekabelde gastlaag 2 VLAN's. De klanten beschikken over twee afzonderlijke oplossingen:

- Een enkele WLAN-controller (VLAN-vertaalmodus) - de toegangsswitch zet het bekabelde gastenverkeer in het gastVLAN op naar de WLAN-controller die de bekabelde gasttoegangsoplossing biedt. Deze controller voert de VLAN-vertaling uit van de ingesloten gast VLAN naar de uitgang VLAN.
- Twee WLAN-controllers (Auto Anchor Mode) - de toegangsswitch slaat het bekabelde gastenverkeer naar een lokale WLAN-controller (de controller die het dichtst bij de toegangsswitch ligt). Deze lokale WLAN-controller ankert de client op een gedemilitariseerde zone (DMZ) analoge WLAN-controller die is geconfigureerd voor bekabelde en draadloze gasttoegang. Na een geslaagde overdracht van de client naar de DMZ ankercontroller worden de DHCP IP-adrestoewijzing, verificatie van de client enzovoort verwerkt in de DMZ WLC. Nadat de verificatie is voltooid, mag de cliënt verkeer verzenden/ontvangen.



Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De ondersteuning van de bekabelde toegangsfunctie voor Cisco WLAN-controllers wordt ondersteund door Cisco Unified Wireless-softwarerelease 4.2.61.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Configuratie van toegangslaag

Om de bekabelde gasttoegang te verlenen, moeten de aangewezen havens in de Layer 2 toegangslaagschakelaar op de gast VLAN door de beheerder worden geconfigureerd. Het gastVLAN moet van elke andere VLANs worden gescheiden die op deze schakelaar worden gevormd. Het gastVLAN-verkeer wordt naar de dichtstbijzijnde WLAN-lokale controller geleid. De lokale controller tunnels het gastenverkeer over een Ethernet-over-IP (EoIP) tunnel naar een DMZ Anchor controller. Voor deze oplossing zijn ten minste twee controllers nodig.

In plaats hiervan vertaalt de toegangsschakelaar de gast VLAN naar de één controller de gast VLAN naar de noodopinterface van de WLAN-controller.

```
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
```

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Belangrijke punten voor bekabelde Guest-implementaties

- Op dit moment worden vijf gastLAN's voor bekabelde gasttoegang ondersteund. In totaal kunnen 16 WLAN's voor draadloze gebruikers en 5 WLAN's voor bekabelde gasttoegang worden geconfigureerd op de analoge WLC. Er bestaan geen afzonderlijke tunnels voor WLAN's. Alle gastWLAN's, die de WLAN's omvatten voor bekabelde gasttoegang, gebruiken dezelfde EoIP-tunnels naar de analoge WLC.
- Beheerders moeten dynamische interfaces maken in de WLAN-controller, ze markeren als "Guest LAN" en ze associëren met WLAN's die als Guest LAN's zijn gemaakt.
- Zorg ervoor dat de WLAN-configuraties, inclusief verificatie, identiek zijn aan zowel de analoge als de afstandsbediening om het clientverkeer door te geven.
- WLC's moeten beschikken over compatibele softwareversies. Zorg ervoor dat ze dezelfde belangrijke versie uitvoeren.
- Web-verificatie is het standaardbeveiligingsmechanisme dat beschikbaar is in een bekabeld gastnetwerk. De huidige opties zijn: Open, Web Auth en Web Passthrough.
- In geval van mislukking van de EoIP-tunnel tussen de verafgelegen en verankerende WLC, wordt de client-database schoongemaakt vanaf de Anchor WLC. De cliënt moet opnieuw associëren en reauthentiseren.
- Layer 2-beveiliging wordt niet ondersteund.
- Multicast/Broadcast-verkeer op de bekabelde gast LAN's wordt verbroken.
- DHCP-proxyinstellingen moeten identiek zijn aan zowel de analoge als de afstandsbediening.

Voor de bekabelde gast is er een ondoorzichtige tijd die in de controller loopt. Als er binnen de ingestelde periode geen pakketten van de client worden ontvangen, wordt de client van de controller verwijderd. Wanneer een client een adresoplossing Protocol (ARP) verstuurt, wordt er de volgende keer een nieuwe client gecreëerd en naar de webauth/run-status verplaatst, overeenkomstig de beveiligingsconfiguratie.

Platform-ondersteuning

De bekabelde toegang van gasten wordt op deze platforms ondersteund:

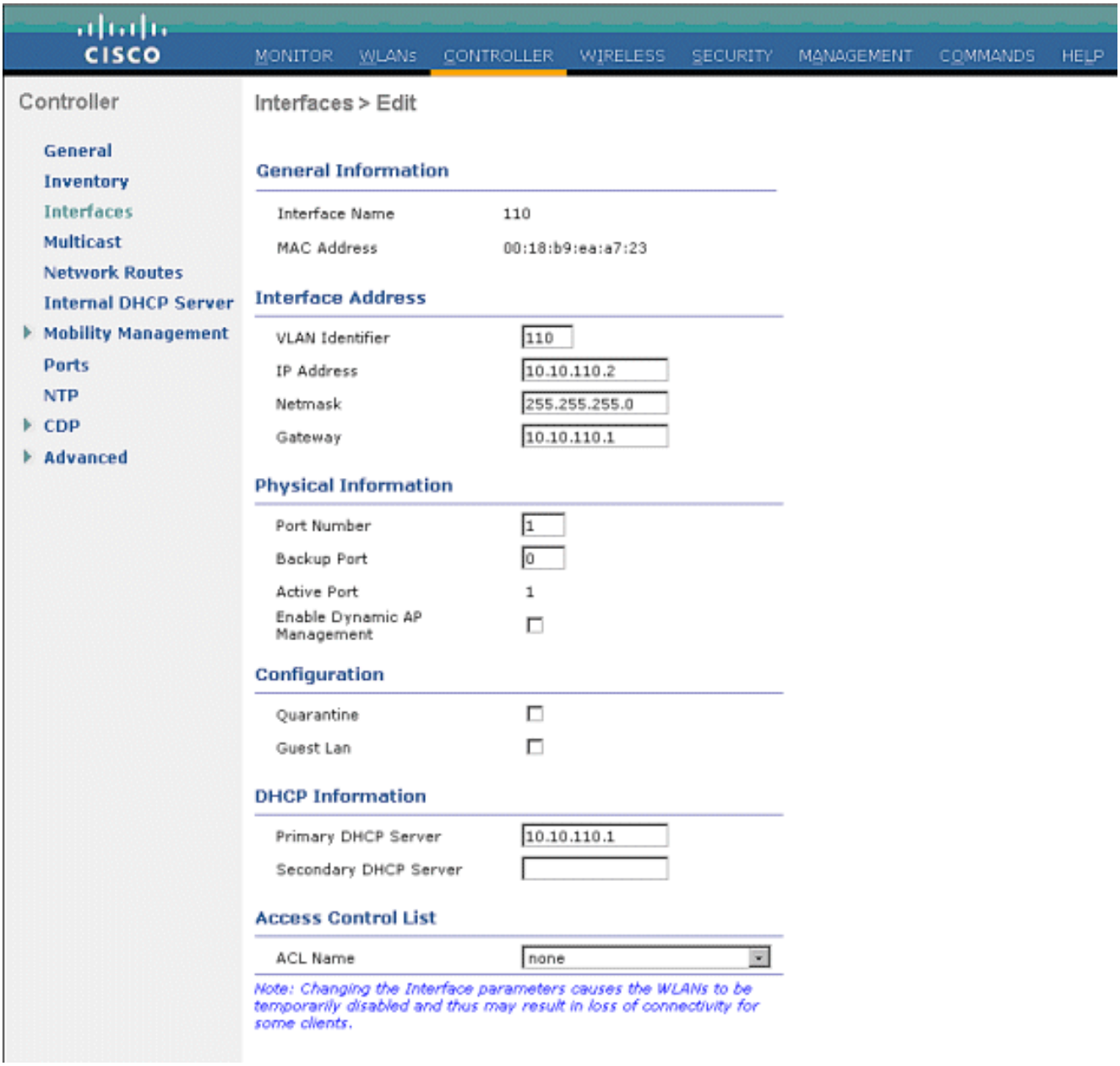
- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM-2, virtuele WLC

Draadloze LAN-configuratie

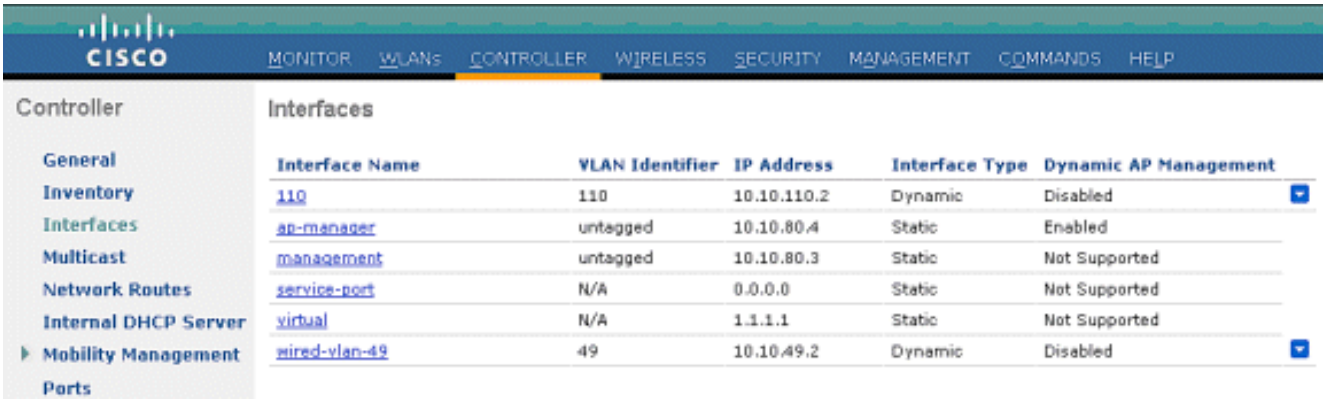
In dit voorbeeld wordt de basisconfiguratie van de draadloze LAN-controller verondersteld. De nadruk ligt op de extra configuratie die nodig is om de bekabelde implementatie van de gasttoegang te voltooien.

1. Maak een dynamische interface en merk dat het een "Gast LAN" is. Wanneer u deze dynamische interface in de huidige release maakt, moet u een IP-adres en standaardgateway verstrekken, ook al bestaat deze niet omdat Layer 2 VLAN is; u hoeft geen DHCP-adres in te vullen. Wiens gastklanten zijn fysiek verbonden met dit VLAN.

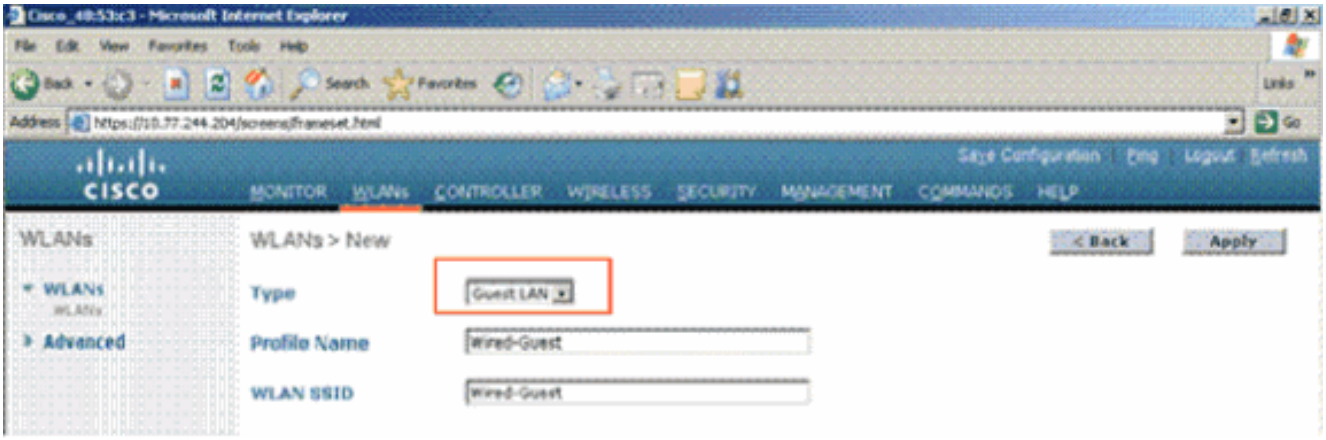
2. Maak een andere dynamische interface waar de bekabelde gastenklanten een IP-adres ontvangen.**Opmerking:** U moet een IP-adres/standaard gateway/DHCP-serveradres in deze interface
opgeven.



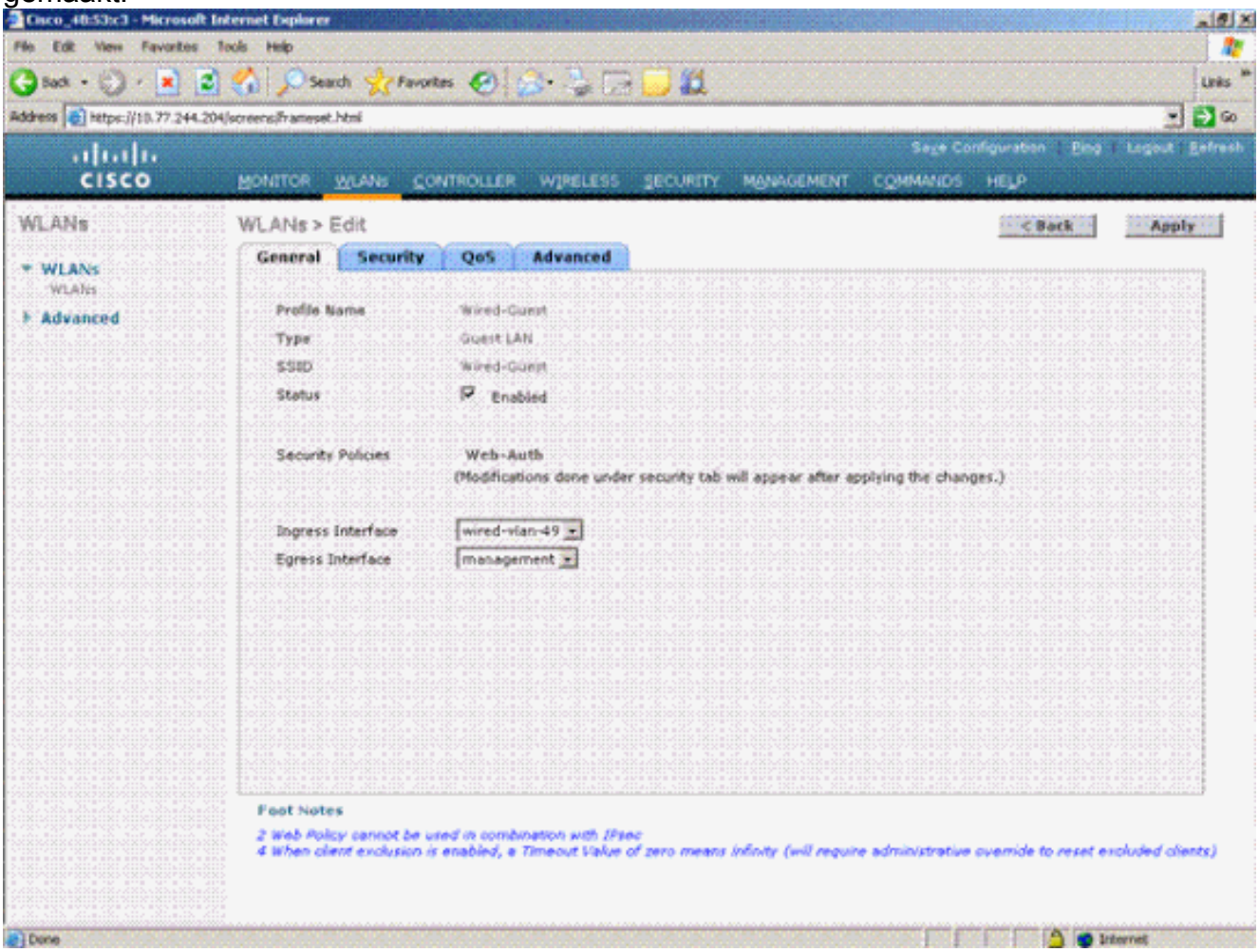
3. Dit zijn de dynamische interfaces:



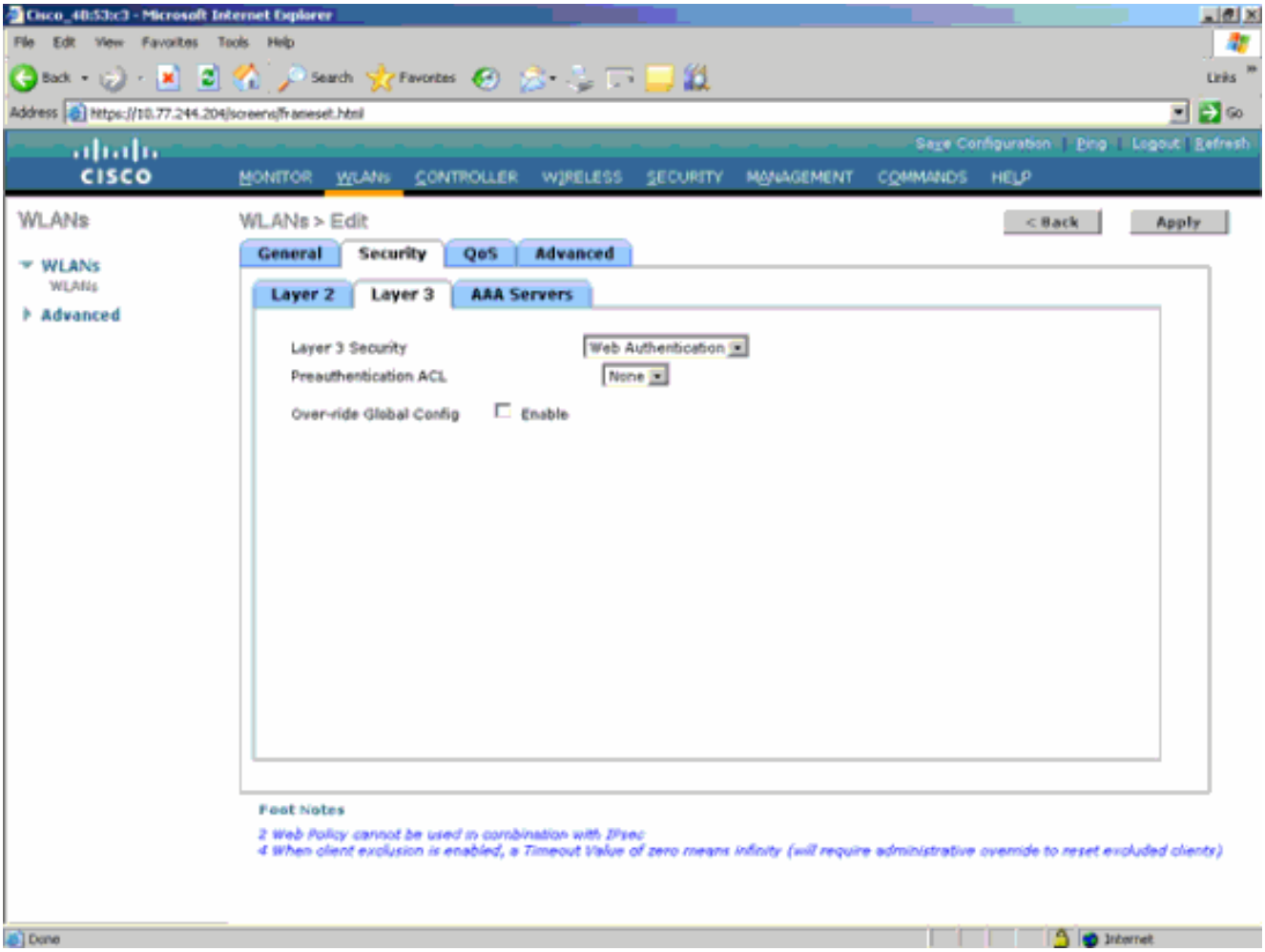
4. Voeg een nieuw WLAN toe: Type=Gast LAN.



5. WLAN inschakelen; Geef de ingangsinterface aan het "Gast LAN" dat in Stap 1 is gemaakt en de IP-interface kan een beheerinterface of een andere dynamische interface zijn, maar bij voorkeur een dynamische interface zoals die welke in Stap 2 is gemaakt.

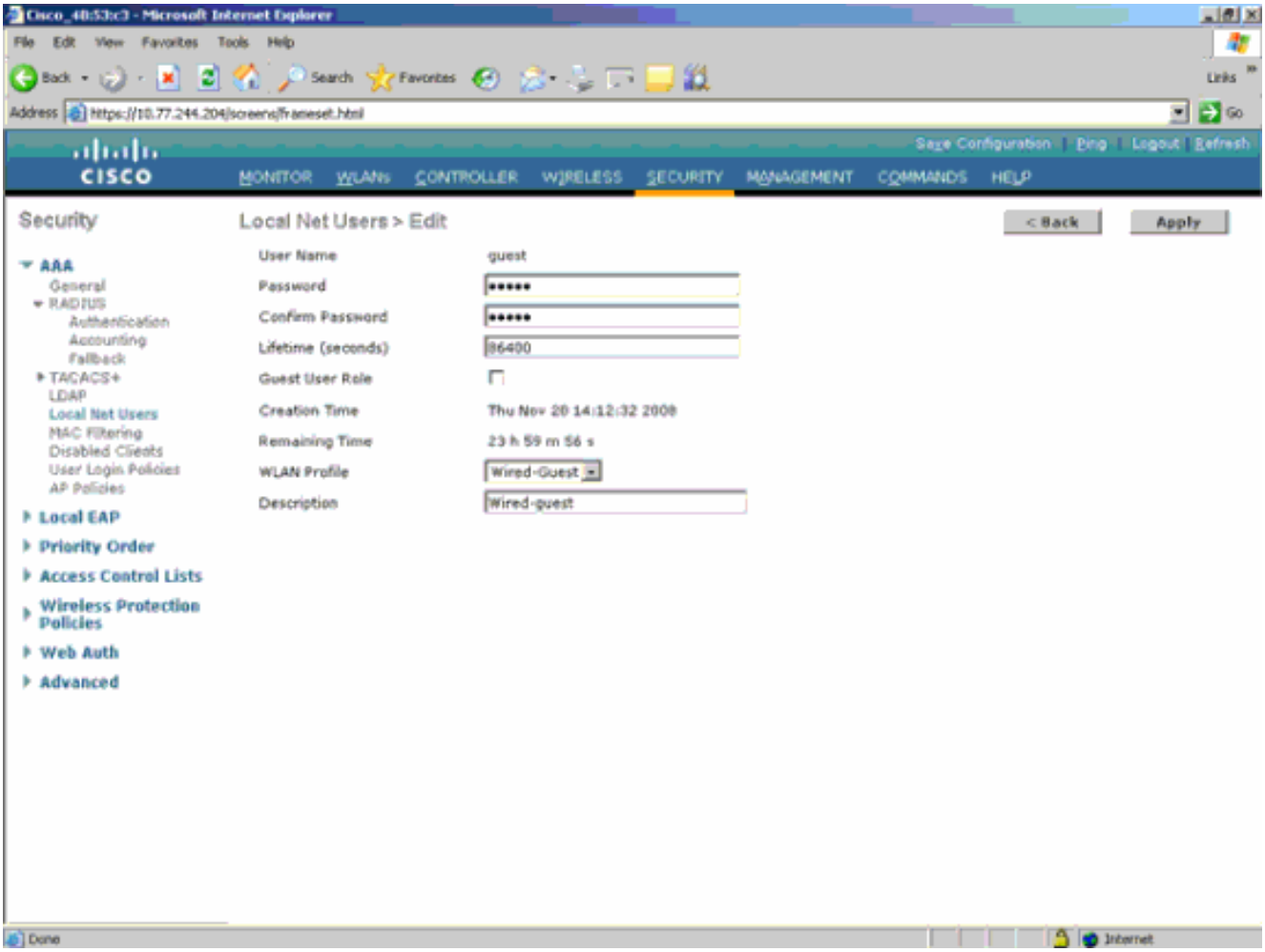


6. Webverificatie is standaard ingeschakeld als de beveiligingsoptie die in het Guest LAN is ingesteld. Kan worden gewijzigd in *Geen* of *doorgifte via het web*.



7. Dit is de laatste configuratie van het WLAN.

8. Voeg een gastgebruiker in de lokale databank van de WLC toe.

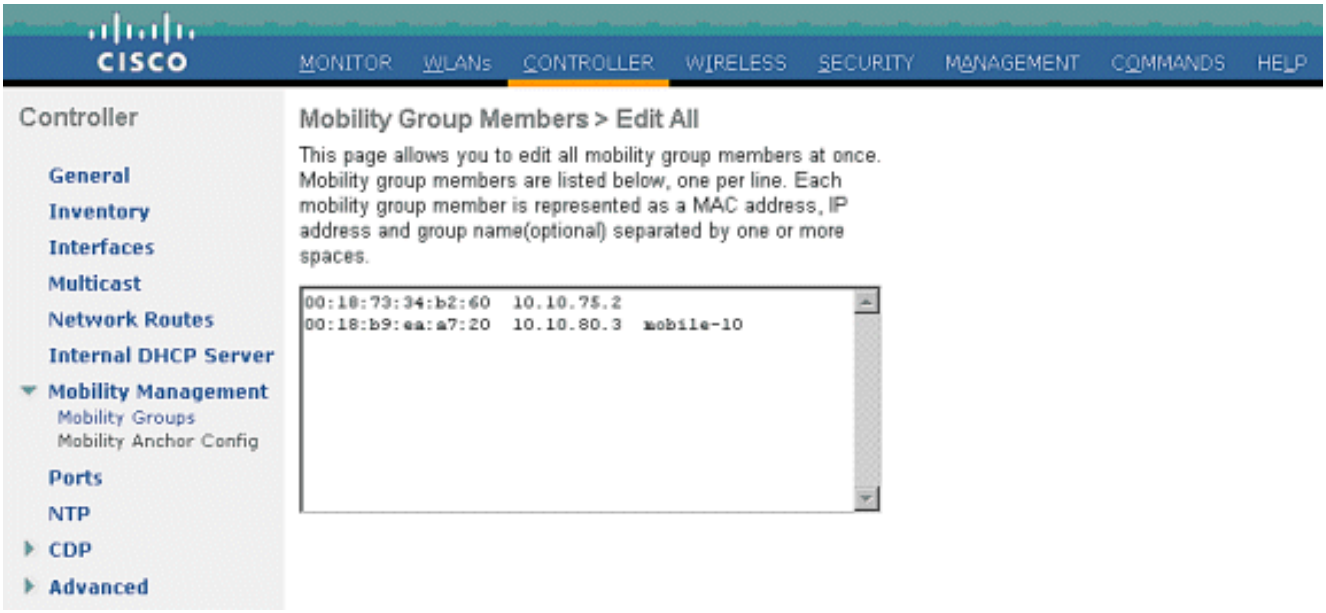


In het buitenland moet u de inloop instellen als het geconfigureerde "Gast LAN". Bij het begin moet je het op een interface instellen, mogelijk de beheersinterface. Zodra de EoIP-tunnel echter is gebouwd, wordt het verkeer automatisch door de tunnel verstuurd in plaats van het beheeradres.

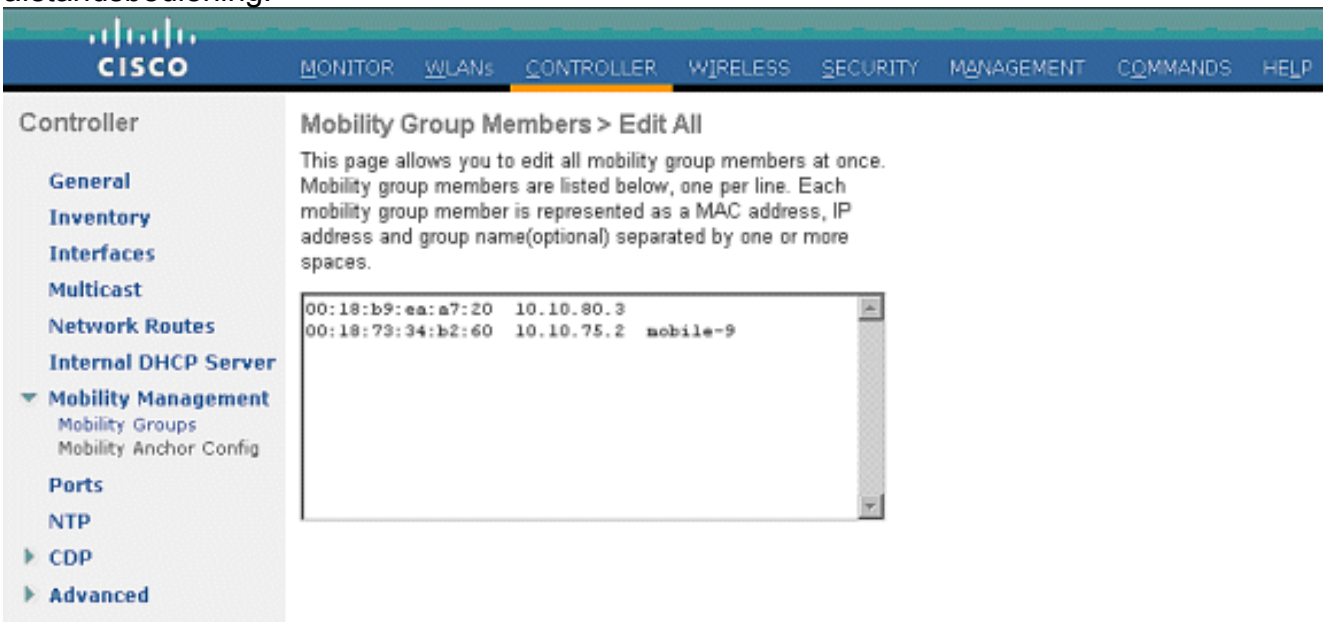
Connected Guest Access met analoge WLAN-controller

In dit voorbeeld is het IP-adres van de externe draadloze LAN-controller 10.10.80.3 en het IP-adres van de Anchor DMZ-controller 10.10.75.2. Beide maken deel uit van twee verschillende mobiliteitsgroepen.

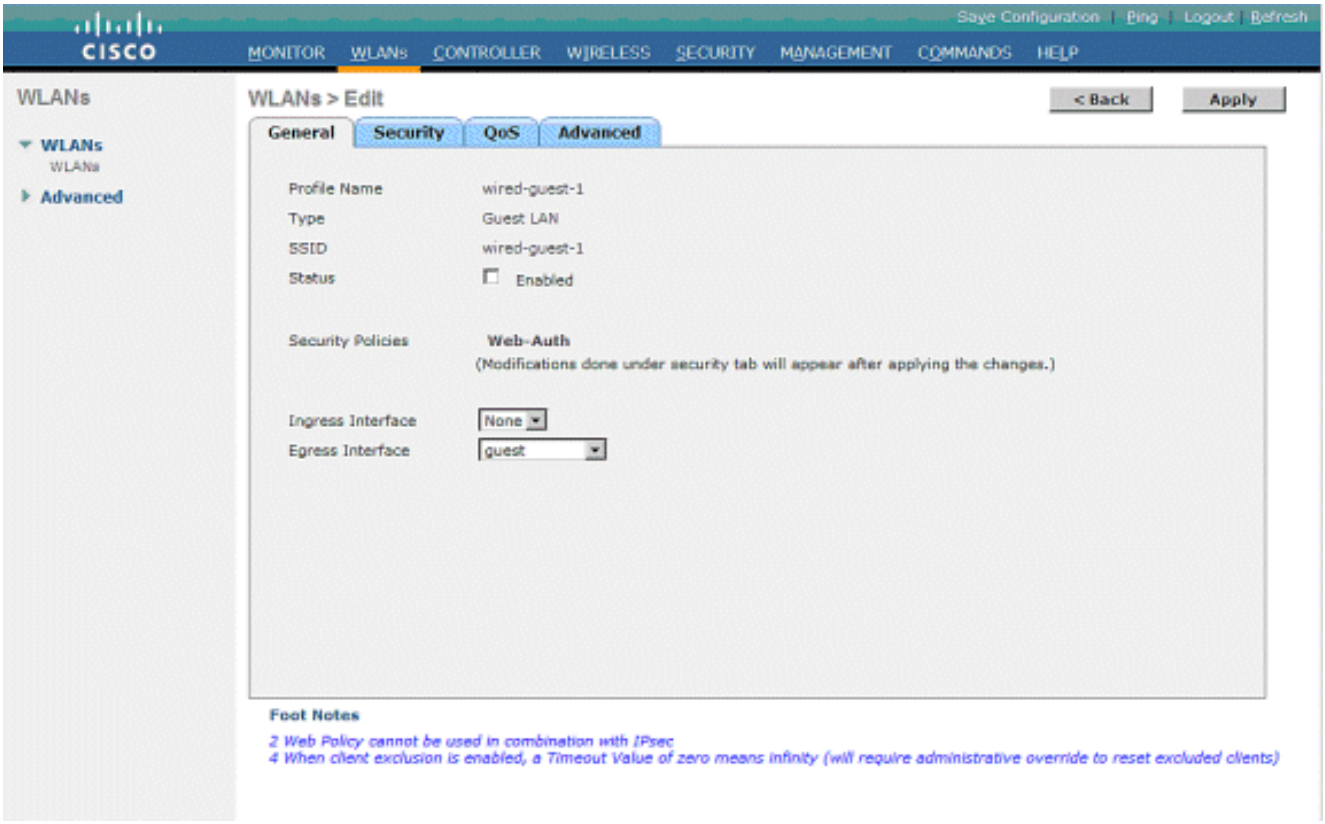
1. Configureer de mobiliteitsgroep van de Anchor DMZ-controller wanneer u het MAC-adres, IP-adres en de naam van de mobiliteitsgroep van de externe controller toevoegt.



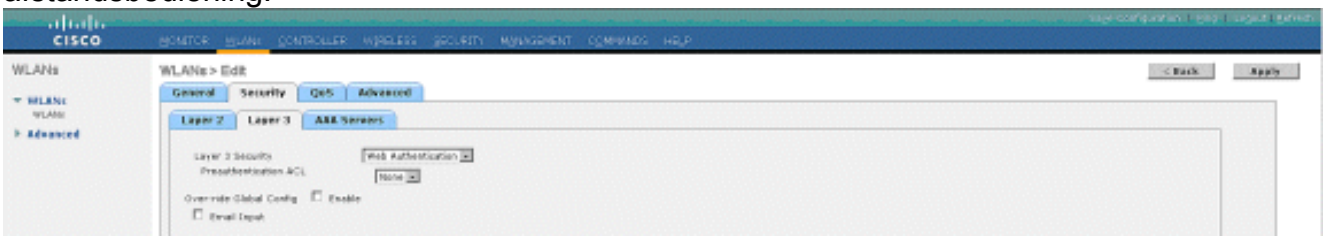
2. Configureer tevens de mobiliteitsgroep in de afstandsbediening.



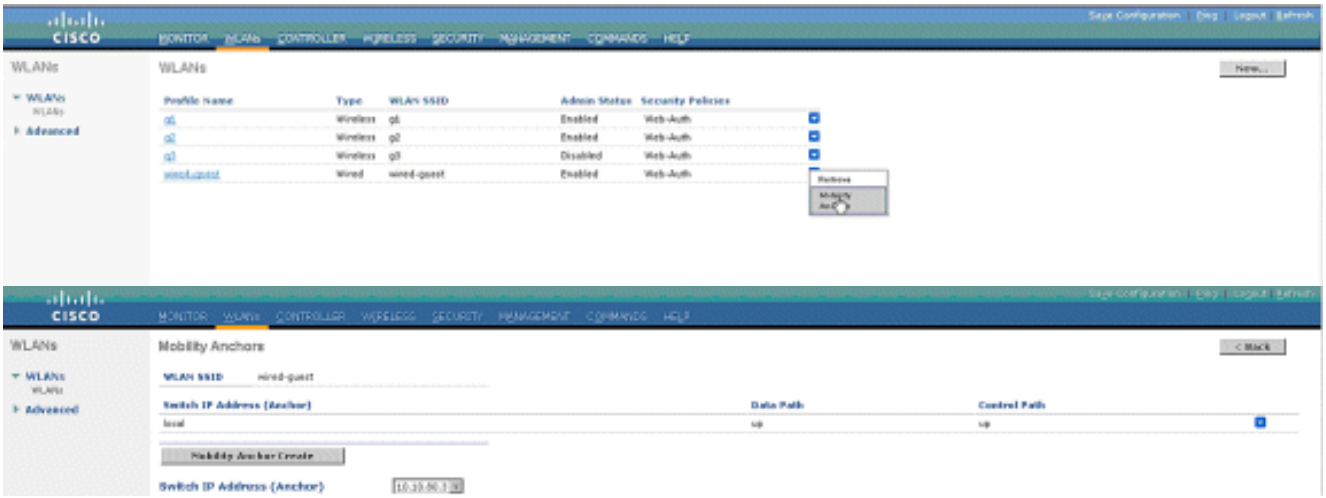
3. Maak de bekabelde WLAN met de exacte naam in de ankerkamer. De ingangsinterface in dit geval is "geen" omdat de ingangsinterface logisch gezien de EoIP-tunnel is van de afstandscontroller. De ress interface is een andere interface, waar de bekabelde klanten het IP-adres willen ontvangen. In dit voorbeeld wordt een dynamische interface met de naam *gast* gecreëerd. In deze fase kunt u echter niet het WLAN inschakelen omdat er een foutmelding wordt weergegeven die aangeeft dat een ingangsinterface niet *nul* kan zijn.



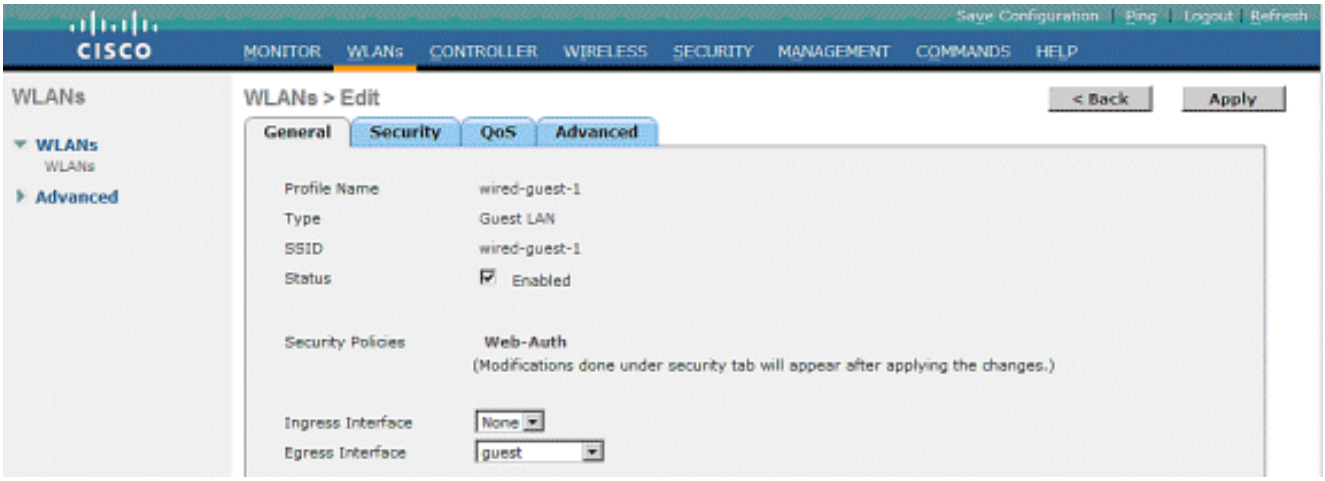
4. Layer 3 beveiliging configureren als *webverificatie*, vergelijkbaar met de afstandsbediening.



5. Maak het mobiliteitsanker op de ankercontroller en breng het in kaart.



6. Nadat het mobiliteitshandel is gemaakt, gaat u terug en stelt u het bekabelde WLAN in.



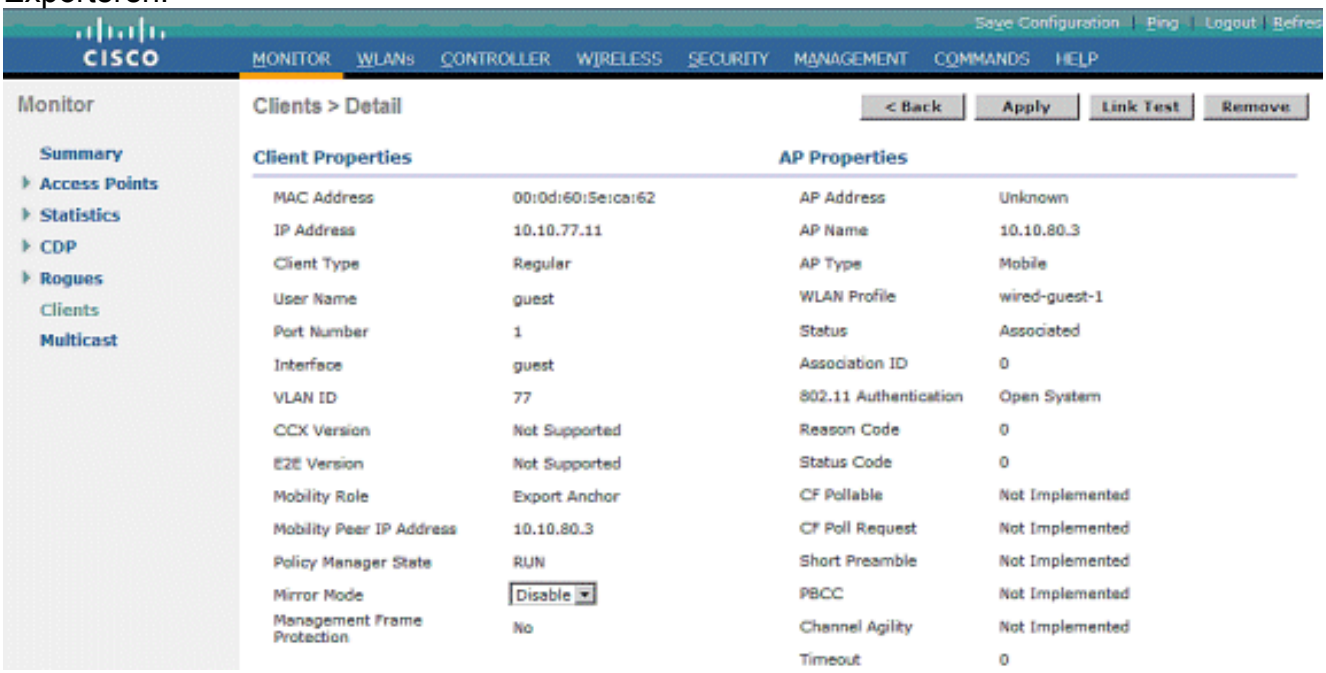
7. Creëer op dezelfde manier het mobiliteitsanker op de afstandsbediening van WLC voor de bekabelde gast
WLAN.

Kies het IP-adres van de analoge WLC en maak het mobiliteitshandel
aan.

Controleer of het gegevens- en bedieningspaneel omhoog zijn. Als dit niet het geval is, zorg er dan voor dat deze poorten open zijn tussen de vaste en externe draadloze LAN-controller: UDP 1666 of IP 97.

8. Zodra een bekabelde gastgebruiker op de schakelaar is aangesloten en de web authenticatie heeft voltooid, moet de Policy Manager State worden gerund en is de Mobility Rol Exporteren Buitenlandse
Zaken.

Controleer op dezelfde manier de status in de Anchor WLC. De Policy Manager-staat moet worden uitgevoerd en de Mobiliteitsrol is
Exporteren.

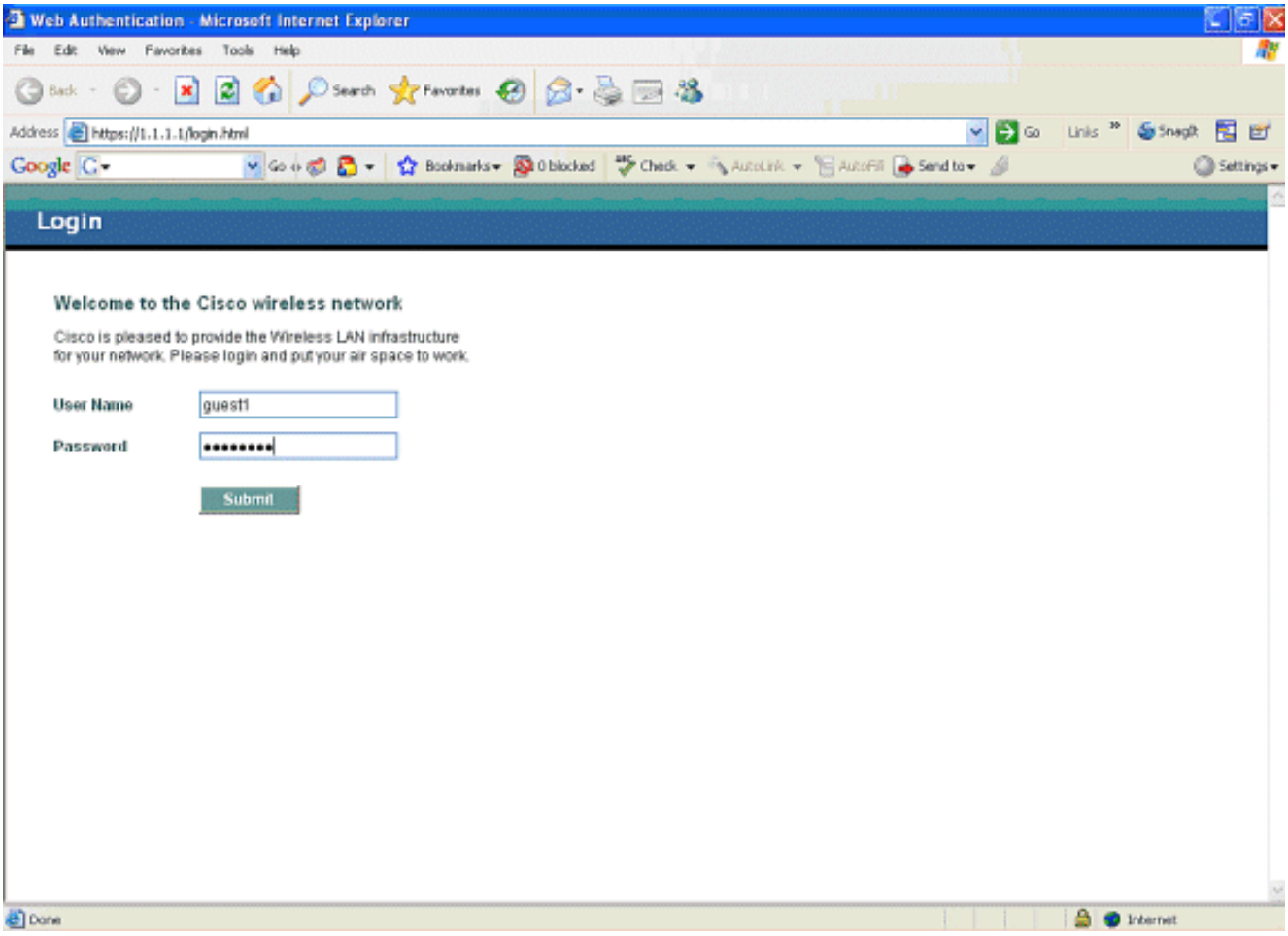


Clientconfiguratie voor bekabeld programma

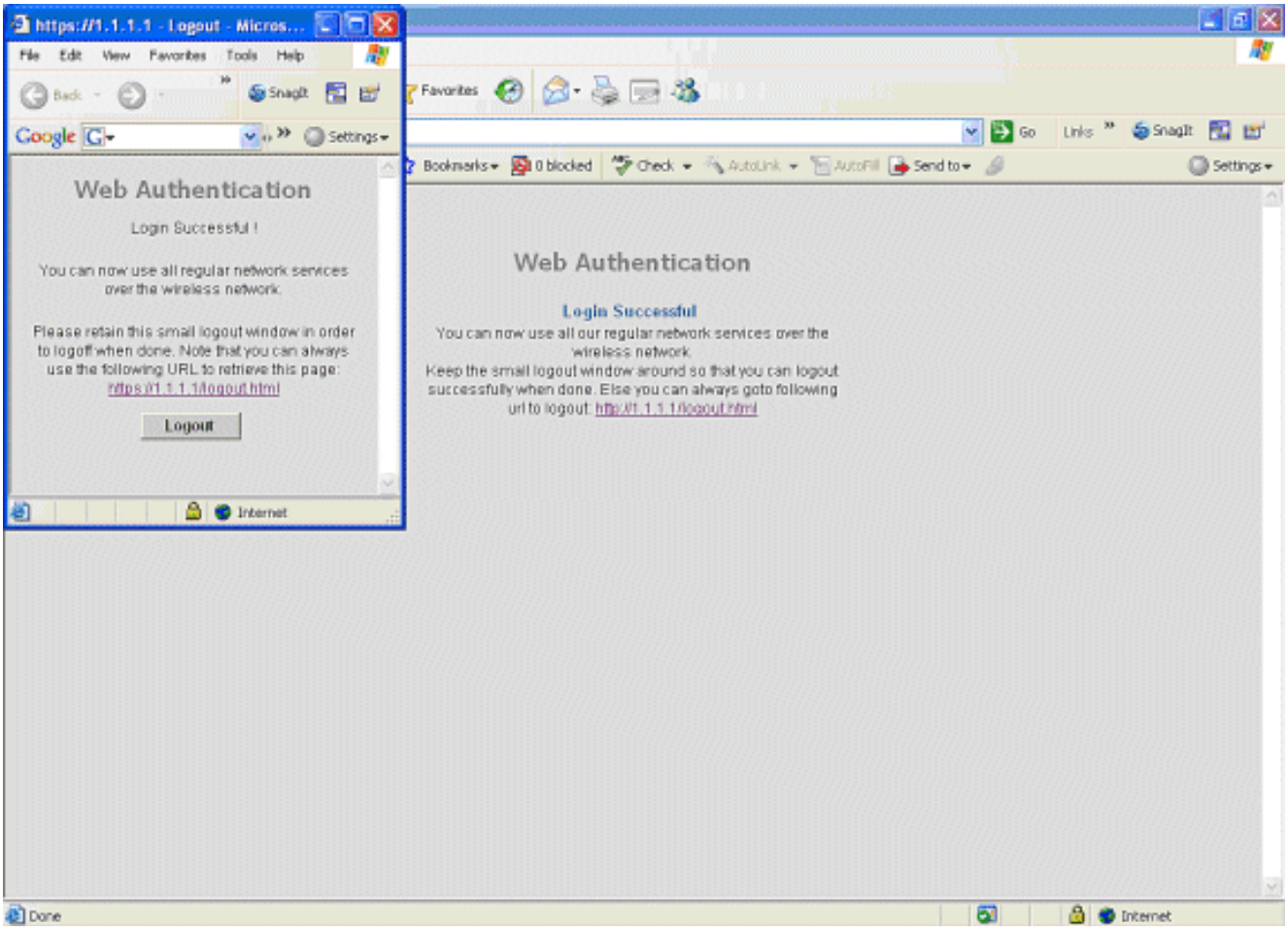
De bekabelde gastclient ontvangt een IP-adres van het egress VLAN maar kan geen verkeer doorgeven totdat deze de webverificatie voltooid heeft.

Als u wilt inloggen als gastgebruiker, volgt u de volgende stappen:

1. Open een browser venster en voer de gewenste URL naam in (bijvoorbeeld www.cisco.com). De gast wordt opnieuw gericht naar de standaardwebpagina van de draadloze LAN controller als web authenticatie is ingeschakeld en een DNS resolutie kan worden ingevuld voor de URL die wordt ingevoerd. Voer anders deze URL in: https://1.1.1.1/login.html, waar het IP-adres 1.1.1 het virtuele IP-adres van de draadloze LAN-controller
is.



2. Voer de opgegeven gebruikersnaam en wachtwoord in.
3. Als de inlognaam een succes is, merkt een browser op dat.



Debugs voor bekabelde Guest Connection op lokaal WLC

Dit debug verschaft alle informatie met betrekking tot de bekabelde gastenclient.

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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Automatische bevestiging van mobiliteit configureren
- Gast WLAN en interne WLAN-toepassing met WLC-configuratievoorbeeld
- Configuratievoorbeeld voor externe webverificatie met draadloze LAN-controllers
- Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.2
- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie – Cisco Systems