Acceso a Invitado Conectado con Ejemplo de configuración de Cisco WLAN Controllers

Contenido

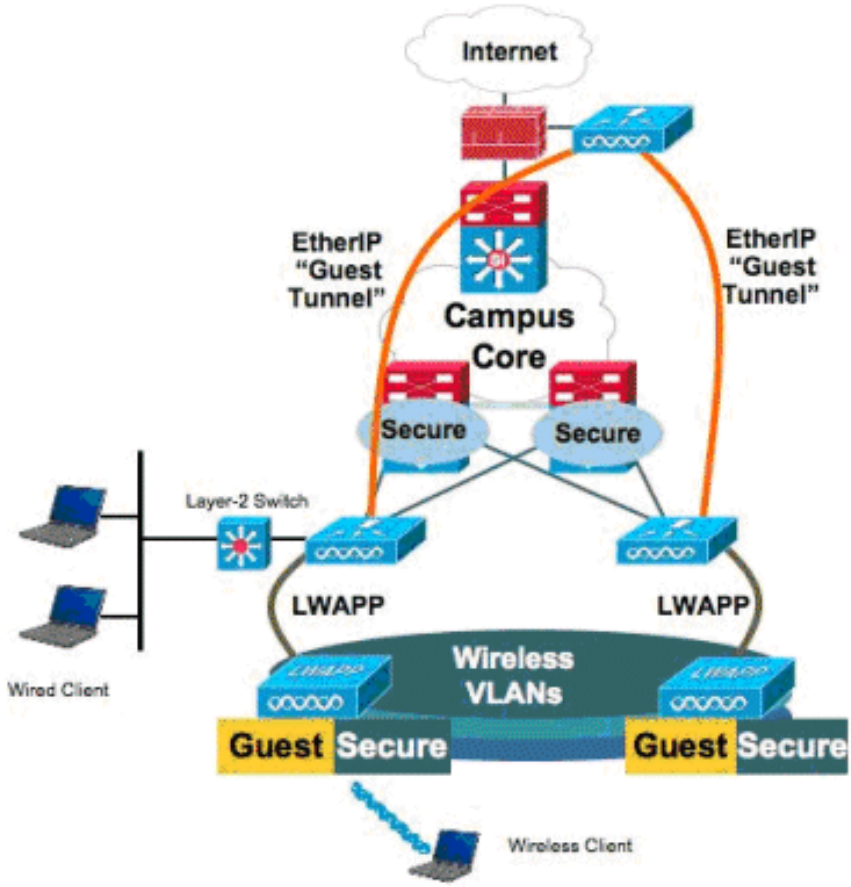
Introducción

En este documento, se describe cómo configurar el acceso de invitado con la nueva característica de acceso de invitado por cable admitida en los controladores WLAN (WLC) de Cisco que utilizan la versión 4.2.61.0 o versiones posteriores del software de red inalámbrica unificada de Cisco. Cada vez más empresas reconocen la necesidad de brindar acceso a Internet a sus clientes, partners y consultores cuando visitan sus instalaciones. Los administradores de TI pueden brindar acceso a Internet por cable o inalámbrico, seguro y controlado a los invitados en el mismo controlador LAN inalámbrico.

Los usuarios invitados deben tener permiso para conectarse a los puertos Ethernet designados y acceder a la red de invitado de acuerdo con la configuración establecida por el administrador una vez que realizan los métodos de autenticación configurados. Los usuarios invitados que se conectan de forma inalámbrica pueden conectarse fácilmente a los controladores WLAN con las características de acceso de invitado actuales. Además, el sistema Wireless Control System (WCS), en combinación con la configuración básica y la administración de controladores WLAN, proporciona servicios mejorados para los usuarios invitados. Los clientes que ya implementaron o que planean implementar controladores WLAN y WCS en su red pueden utilizar la misma infraestructura para el acceso de invitado por cable. De esta manera, los usuarios finales pueden disfrutar de una experiencia de acceso de invitado inalámbrico y por cable unificada.

Los puertos de invitado por cable se proporcionan en una ubicación designada y se conectan a un switch de acceso. La configuración del switch de acceso coloca estos puertos en una de las VLAN de capa 2 de invitado por cable. Los clientes tienen dos soluciones diferentes a su disposición:

- Un solo controlador WLAN (modo de traducción de VLAN): el switch de acceso establece un enlace troncal entre el tráfico de invitado por cable en la VLAN de invitado y el controlador WLAN que brinda la solución de acceso de invitado por cable. Este controlador realiza la traducción de VLAN: de la VLAN de invitado por cable de ingreso a la VLAN de egreso.
- Dos controladores WLAN (modo de anclaje automático): el switch de acceso establece un enlace troncal entre el tráfico de invitado por cable y un controlador WLAN local (el controlador más próximo al switch de acceso). Este controlador WLAN local realiza el anclaje del cliente en un controlador WLAN de anclaje en zona perimetral (DMZ) que está configurado para el acceso de invitado por cable o inalámbrico. Después de una transferencia correcta del cliente al controlador de anclaje en DMZ, la asignación de direcciones IP de DHCP, la autenticación del cliente, etc. se administran en el WLC en DMZ. Una vez que realiza la autenticación, el cliente tiene permiso para enviar y recibir tráfico.



Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La versión 4.2.61.0 y las versiones posteriores del software de red inalámbrica unificada de Cisco admiten la característica de acceso de invitado por cable habilitada en los controladores WLAN de

Cisco.

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.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Configuración de switch de capa de acceso

Para brindar acceso de invitado por cable, los puertos designados en el switch de capa de acceso 2 deben ser configurados por el administrador en la VLAN de invitado. La VLAN de invitado debe ser independiente de otras VLAN configuradas en este switch. Se establece un enlace troncal entre el tráfico de VLAN de invitado y el controlador WLAN local más próximo. El controlador local transporta el tráfico de invitado a través de un túnel Ethernet por IP (EoIP) hacia un controlador de anclaje en DMZ. Esta solución requiere al menos dos controladores.

Como alternativa, el switch de acceso establece un enlace troncal entre la VLAN de invitado el controlador único y traduce la VLAN de invitado a la interfaz de egreso del controlador 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
```

Nota: Utilice la Command Lookup Tool **(sólo para clientes** registrados**) para obtener más información sobre los comandos utilizados en este documento.**

Puntos importantes para la implementación de invitado por cable

- En este momento, se admiten cinco redes LAN de invitado para el acceso de invitado por cable. En total, se pueden configurar 16 WLAN para usuarios inalámbricos y 5 WLAN para el acceso de invitado por cable en el WLC de anclaje. No existen túneles separados para las WLAN. Todas las WLAN de invitado, incluida la WLAN para el acceso de invitado por cable, utilizan los mismos túneles de EoIP hacia el WLC de anclaje.
- Los administradores deben crear interfaces dinámicas en el controlador WLAN, marcarlas como "LAN de invitado" y asociarlas a las WLAN creadas como LAN de invitado.
- Asegúrese de que las configuraciones de WLAN, incluida la autenticación, sean idénticas tanto en el controlador de anclaje como en el controlador remoto para transmitir el tráfico de clientes.
- Los WLC deben tener versiones de software compatibles. Asegúrese de que ejecuten la misma versión principal.
- La autenticación web es el mecanismo de seguridad predeterminado disponible en una LAN de invitado por cable. Las opciones disponibles en este momento son las siguientes: Open (Abierta), Web Auth (Autenticación web) y Web Passthrough (Redireccionamiento web).
- En caso de que el túnel EoIP entre el WLC remoto y el WLC de anclaje falle, la base de datos de clientes se limpia del WLC de anclaje. El cliente debe repetir la asociación y la autenticación.
- No se admite ninguna característica de seguridad de capa 2.
- Se descarta el tráfico de multidifusión/transmisión en las LAN de invitado por cable.
- La configuración proxy DHCP debe ser la misma tanto en el controlador de anclaje como en el controlador remoto.

En el caso de los invitados por cable, se ejecuta un tiempo de espera de inactividad en el controlador. Si no se reciben paquetes del cliente durante el período configurado, el cliente se elimina del controlador. Cuando un cliente envía una solicitud de protocolo de resolución de direcciones (ARP) la próxima vez, una nueva entrada de cliente se crea y se pasa al estado ejecución/autenticación web según corresponda de acuerdo con la configuración de seguridad.

Soporte de la plataforma

El acceso de invitado por cable se admite en las siguientes plataformas:

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

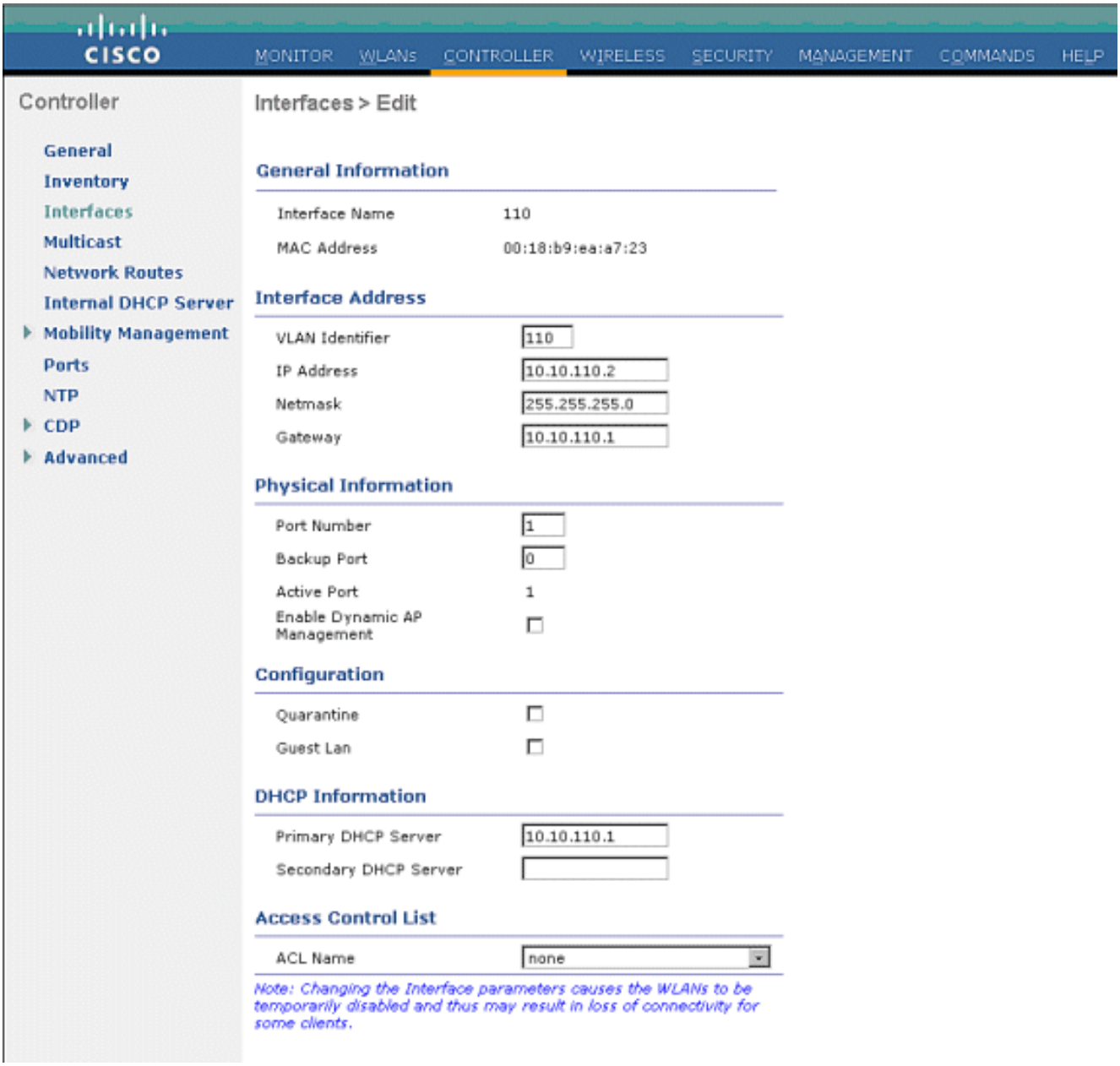
Configuración de LAN inalámbrica

En este ejemplo, se supone la configuración básica del controlador LAN inalámbrico. El centro de atención es la configuración adicional necesaria para completar la implementación de acceso de invitado por cable.

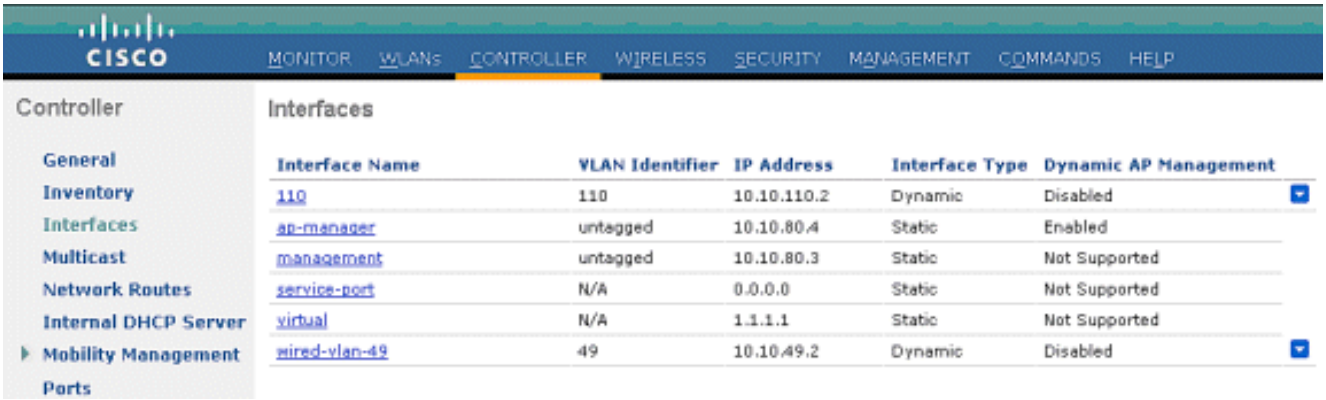
1. Cree una interfaz dinámica y marque como "LAN de invitado". Cuando crea esta interfaz dinámica en la versión actual, debe proporcionar una dirección IP y un gateway

predeterminado, a pesar de que no existen porque es una VLAN de capa 2. No debe proporcionar ninguna dirección DHCP. Los clientes invitados por cable están conectados físicamente a esta
VLAN.

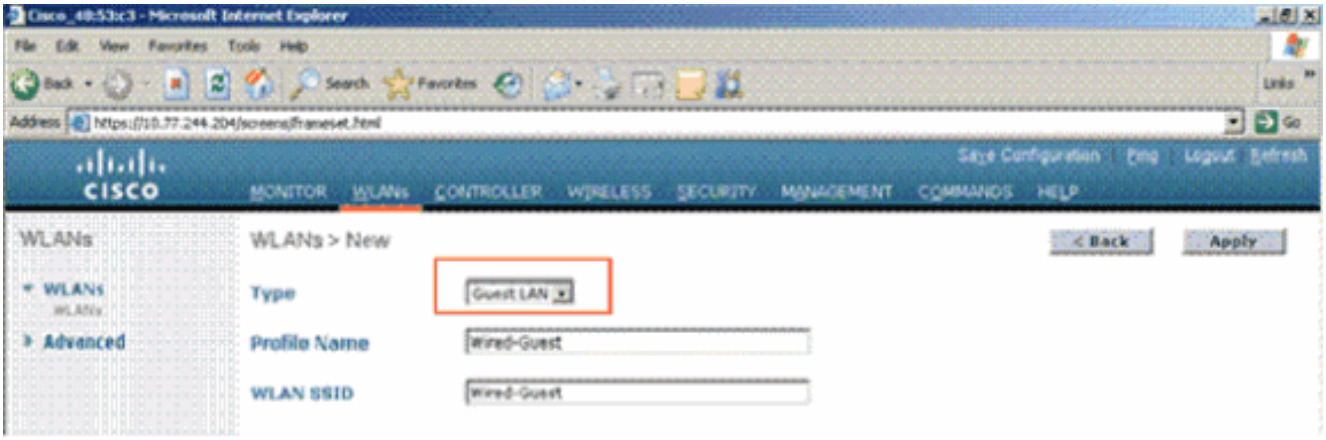
2. Cree otra interfaz dinámica en la cual los clientes invitados por cable reciban una dirección IP.**Nota:** Debe proporcionar una dirección IP/gateway predeterminado/dirección de servidor DHCP en esta
interfaz.



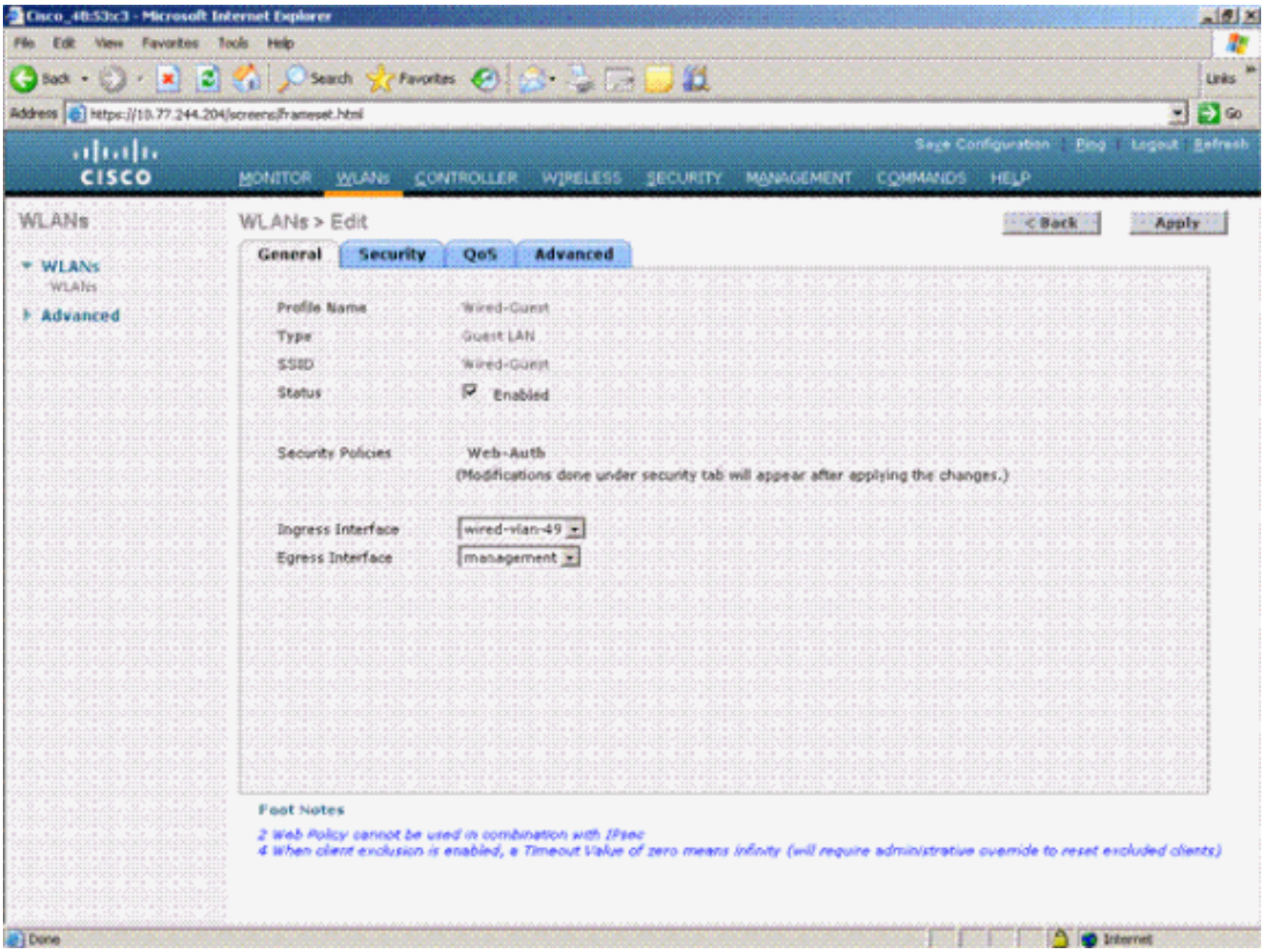
3. Estas son las interfaces dinámicas:



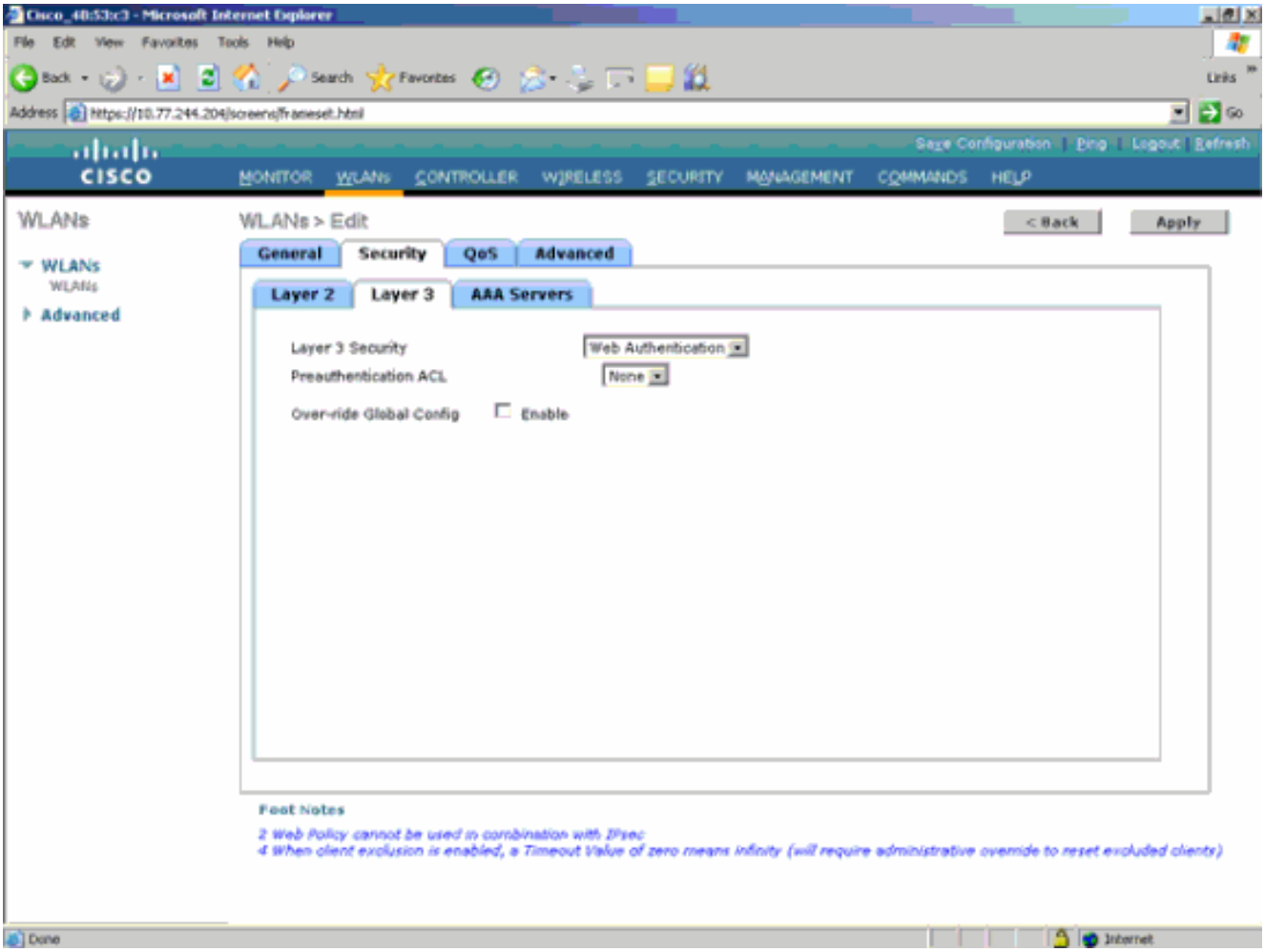
4. Agregue una WLAN nueva: Escriba “LAN de invitado”.



5. Habilite la WLAN. mapee la interfaz de ingreso a la "LAN de invitado" creada en el Paso 1, y la interfaz de egreso puede ser una interfaz de administración o cualquier otra interfaz dinámica, aunque preferiblemente una interfaz dinámica como la creada en el Paso 2.

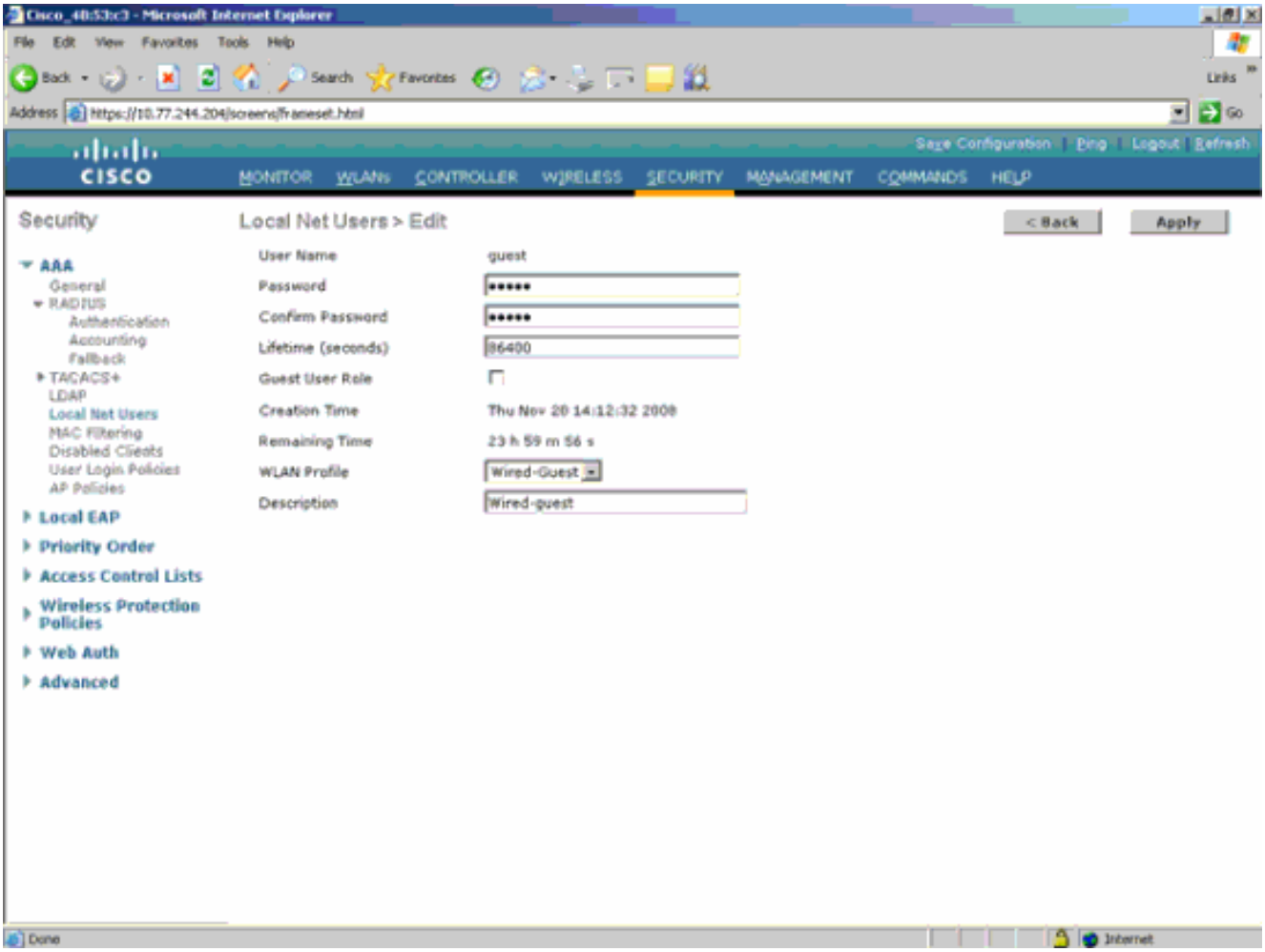


6. La autenticación web está habilitada de manera predeterminada como la opción de seguridad configurada en la LAN de invitado. Esta opción puede cambiarse por *None (Ninguna) o Web Passthrough* (Redireccionamiento web).



7. Esta es la última configuración de la WLAN.

8. Agregue un usuario invitado en la base de datos local del WLC.

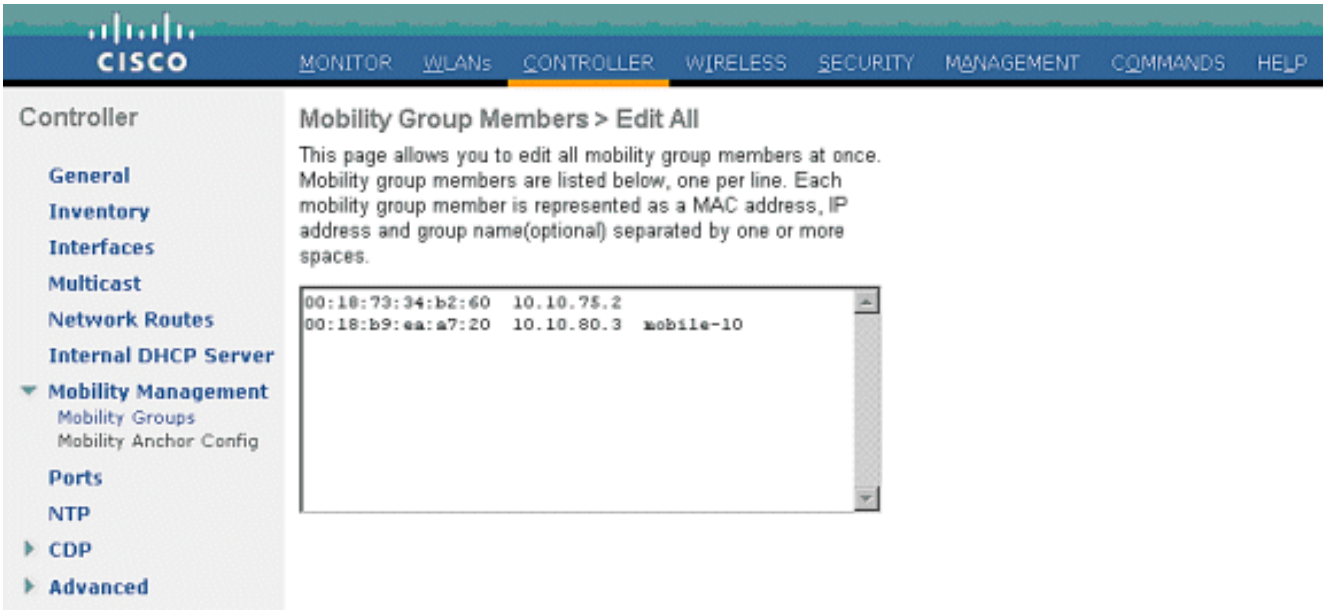


En el Foreign, debe configurar el ingreso como la "LAN de invitado" configurada. Debe establecer el egreso en alguna interfaz, en lo posible, la interfaz de administración. Sin embargo, una vez que se crea el túnel EoIP, este envía el tráfico automáticamente a través del túnel en lugar de la dirección de administración.

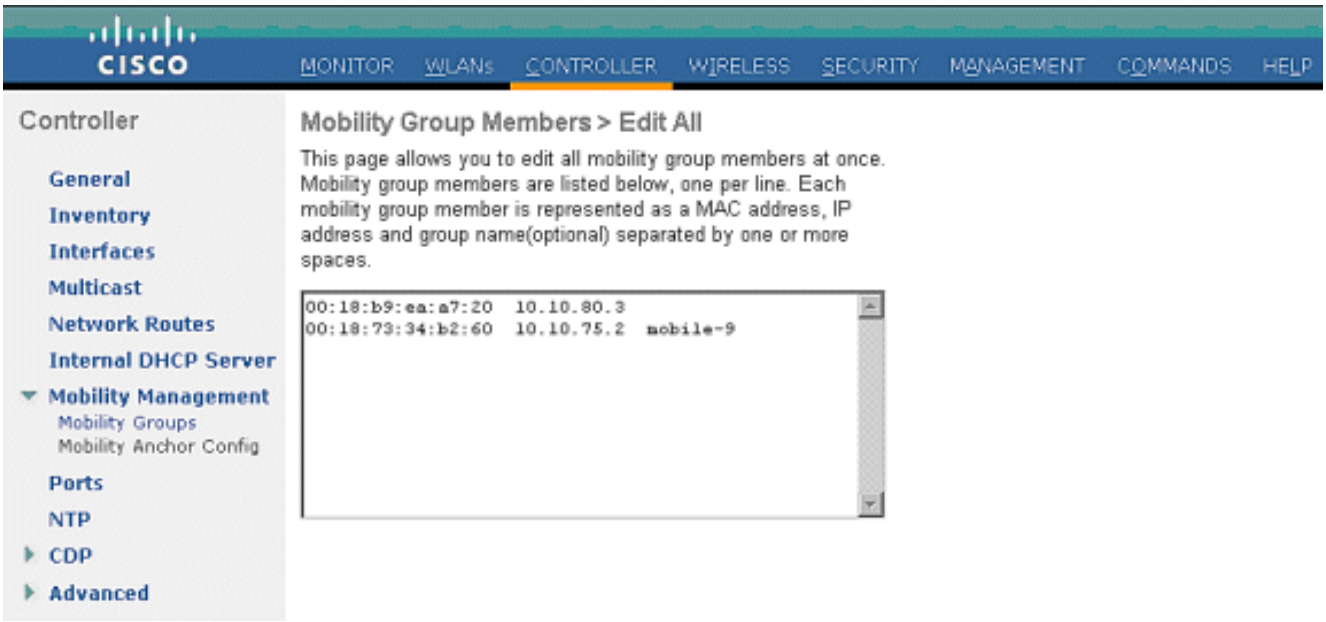
Acceso de invitado por cable con controlador WLAN de anclaje

En este ejemplo, la dirección IP del controlador de LAN inalámbrica remoto es 10.10.80.3, y la dirección IP del controlador de anclaje en DMZ es 10.10.75.2. Ambos son parte de dos grupos de movilidad diferentes.

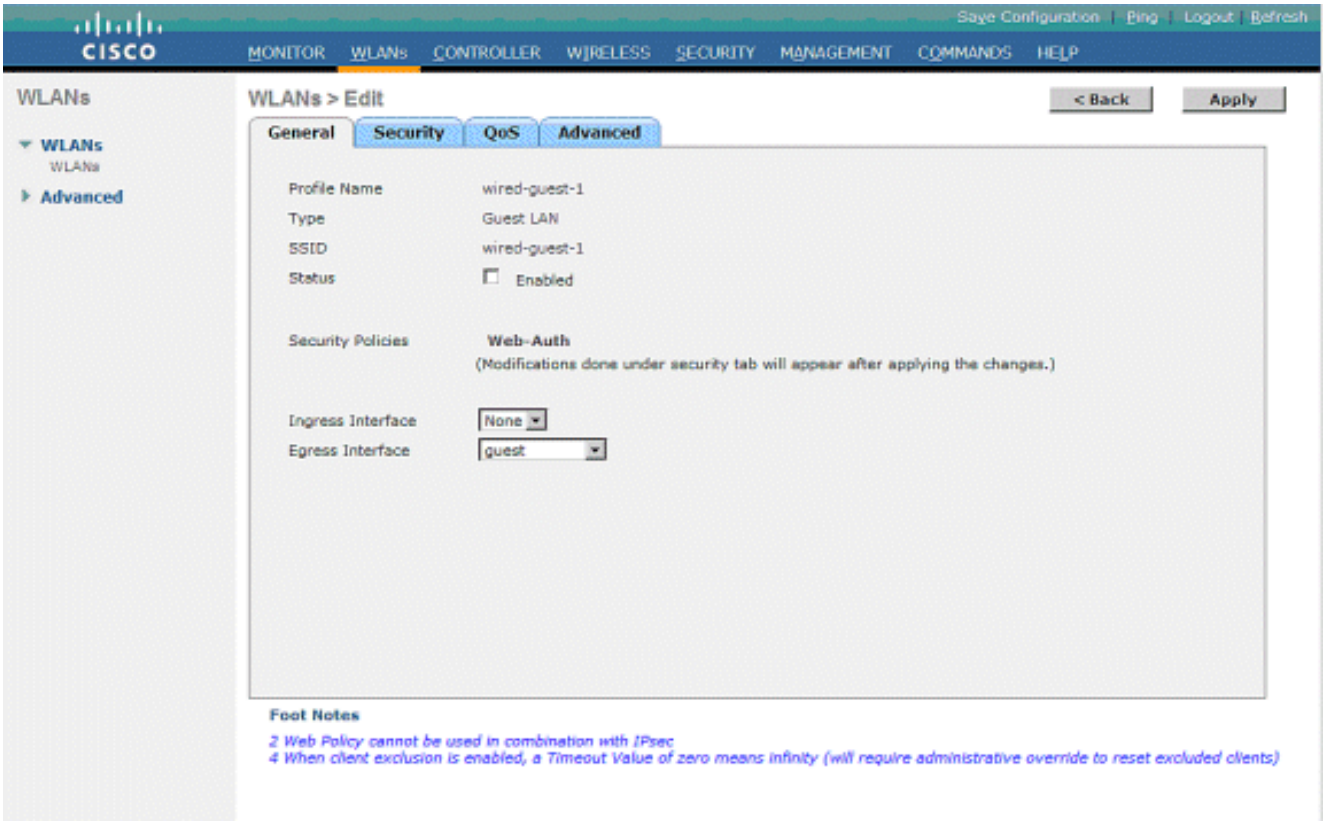
1. Configure el grupo de movilidad del controlador de anclaje en DMZ cuando agrega la dirección MAC, la dirección IP y el nombre del grupo de movilidad del controlador remoto.



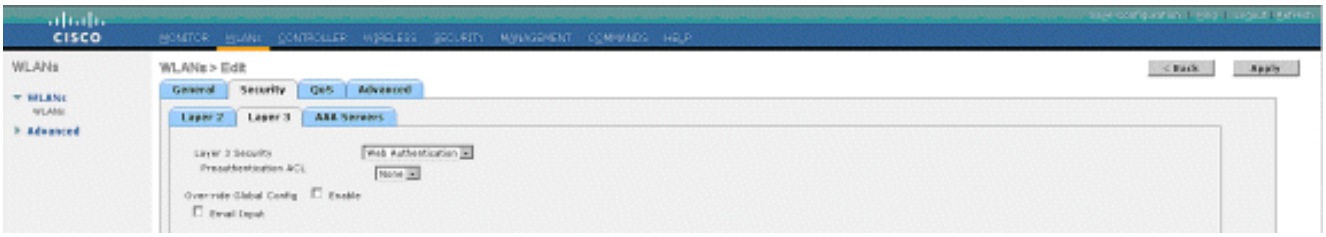
2. De manera similar, configure el grupo de movilidad en el controlador remoto.



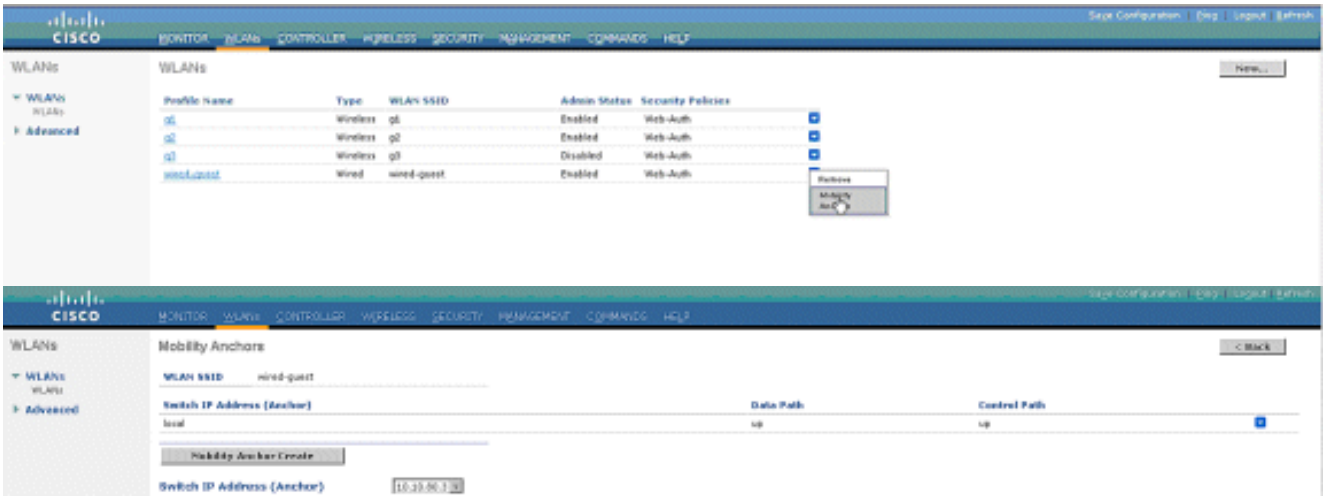
3. Cree la WLAN por cable con el nombre exacto en el WLC de anclaje. La interfaz de ingreso en este caso es "none" porque, lógicamente, la interfaz de ingreso es el túnel EoIP del controlador remoto. La interfaz de egreso es una interfaz diferente, a la que se dirigen los clientes por cable para recibir la dirección IP. En este ejemplo, se crea una interfaz dinámica denominada *guest (invitado).* Sin embargo, en este punto, no puede habilitar la WLAN porque arroja un mensaje de error que indica que una interfaz de ingreso no puede establecerse en *none*
(ninguna).



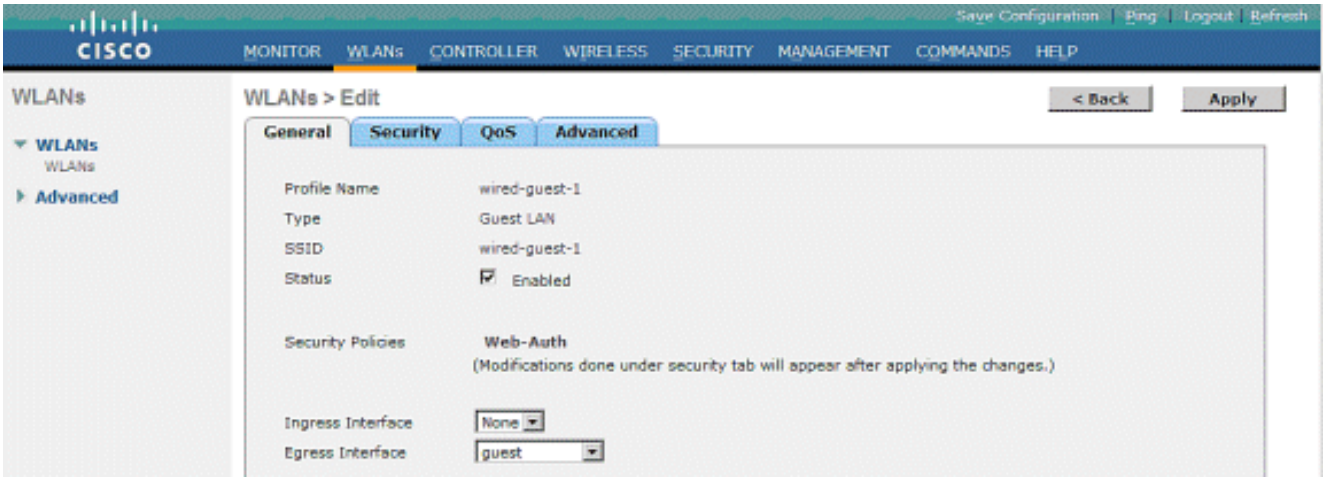
4. Configure la seguridad de capa 3 en *web authentication* (autenticación web), de un modo similar al controlador
remoto.



5. Cree el controlador de anclaje o anclaje de movilidad, y asígnelo a sí mismo.



6. Una vez creado el anclaje de movilidad, regrese y habilite la WLAN por cable.



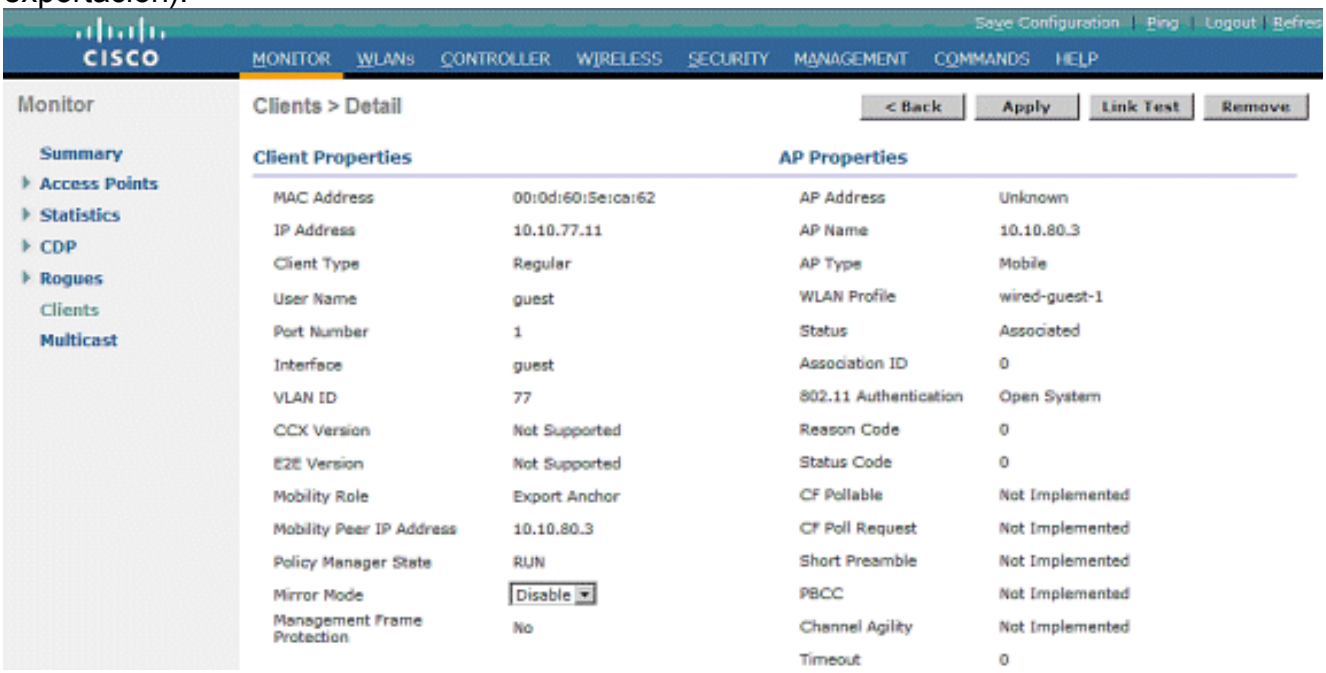
7. De manera similar, cree el anclaje de movilidad en el WLC remoto para la WLAN de invitado por
cable.

Elija la dirección IP del WLC de anclaje y cree el anclaje de movilidad.

Verifique que la ruta de datos y control esté activa. De lo contrario, asegúrese de que estos puertos estén abiertos entre el anclaje y el controlador de LAN inalámbrica remoto: UDP 16666 o IP 97.

8. Una vez que un usuario invitado por cable se conecta al switch y realiza la autenticación web, el estado del administrador de políticas debe ser RUN (Ejecutar) y el rol de movilidad es Export Foreign (Externo de
exportación).

De manera similar, verifique el estado en el WLC de anclaje. El estado del administrador de políticas debe ser RUN (Ejecutar) y el rol de movilidad es Export Anchor (Anclaje de exportación).



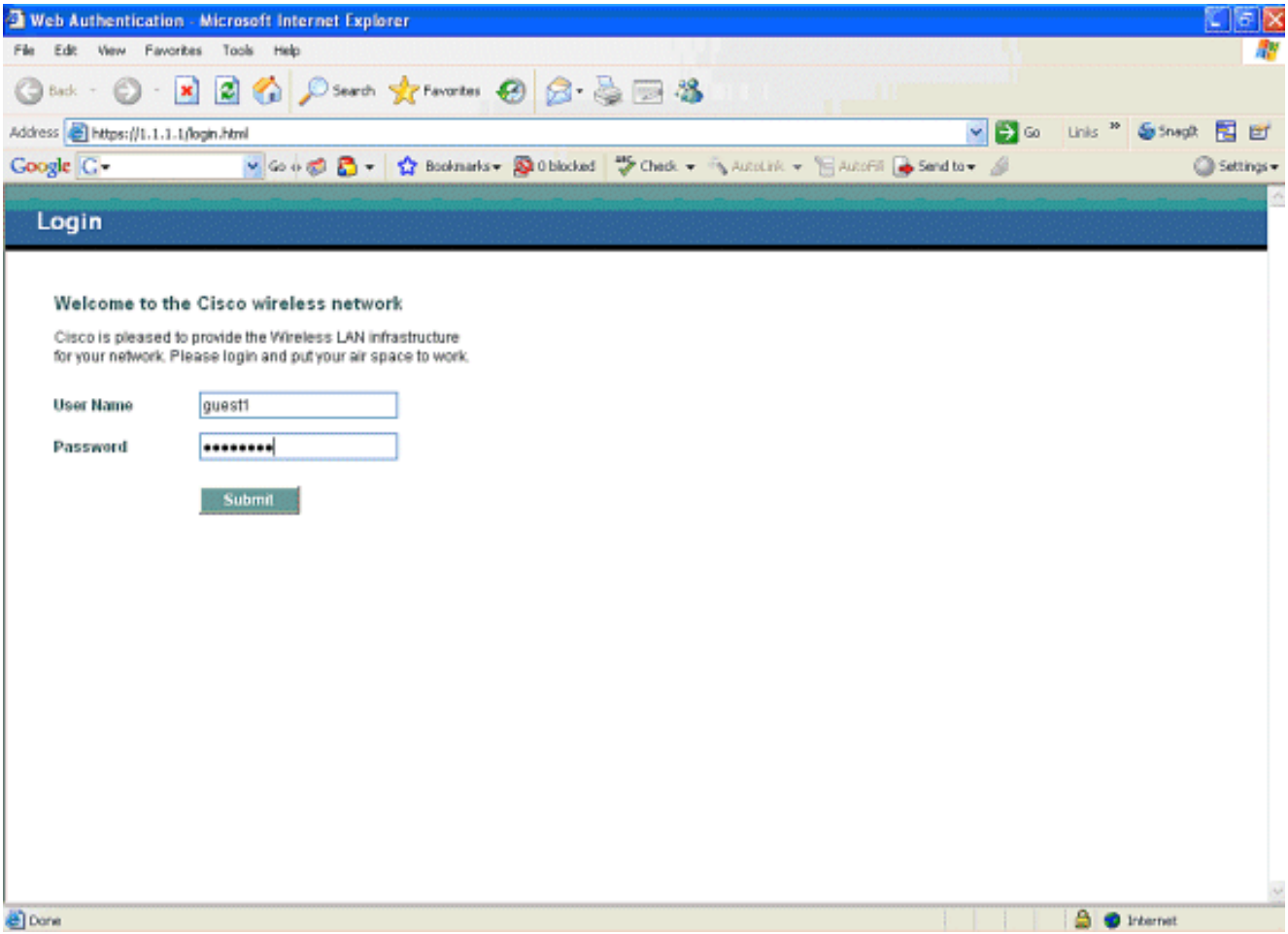
Configuración de cliente invitado por cable

El cliente invitado por cable recibe una dirección IP de la VLAN de egreso, pero no puede transmitir el tráfico hasta que realiza el proceso de autenticación web.

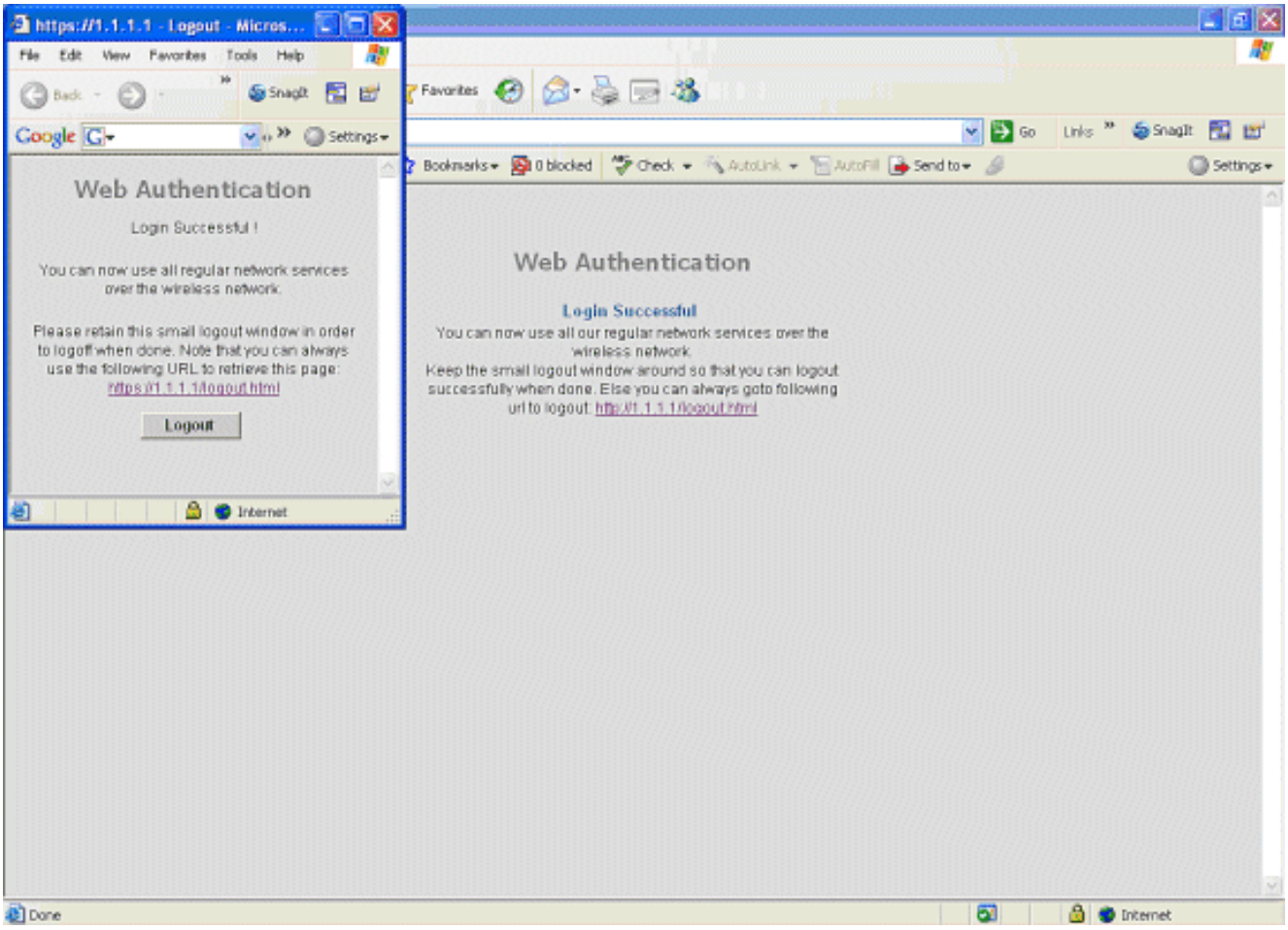
Para iniciar sesión como usuario invitado, siga estos pasos:

1. Abra una ventana del navegador e introduzca el nombre de la URL deseada (por ejemplo, www.cisco.com). El invitado se redirige a la página web predeterminada del controlador de LAN inalámbrica si se habilita la autenticación web, y se puede completar una resolución DNS para la URL que se introduce. De lo contrario, introduzca esta URL: https://1.1.1.1/login.html, donde la dirección IP 1.1.1.1 es la dirección IP virtual del controlador de LAN

inalámbrica.



2. Introduzca el nombre de usuario y la contraseña que se proporcionan.
3. Si el inicio de sesión se realiza correctamente, una ventana del navegador se lo notificará.



Depuraciones para la conexión de invitado por cable en el WLC local

Esta depuración brinda toda la información relacionada con el cliente invitado por cable.

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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Configuración de movilidad de anclaje automático
- Ejemplo de Configuración de WLAN Guest y WLAN Interna mediante WLCs
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Guía de configuración de controlador de LAN inalámbrica de Cisco, versión 4.2
- Soporte de Productos de Red Inalámbrica

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).