Ancla unificada del invitado de los reguladores del Wireless LAN del acceso con el ejemplo de configuración convergido del acceso

Contenido

Introducción

Esto documenta describe cómo configurar los reguladores del Wireless LAN de las 5508/5760 Series (WLCs) y el Catalyst 3850 Series Switch para el ancla del invitado del cliente de red inalámbrica en el nuevo despliegue de la movilidad puso donde el WLC de las 5508 Series actúa como el ancla de la movilidad y el Catalyst 3850 Series Switch actúa como regulador no nativo de la movilidad para los clientes. Además, el Catalyst 3850 Series Switch actúa como agente de la movilidad a un WLC de las 5760 Series que actúe como regulador de la movilidad de donde el Catalyst 3850 Series Switch adquiere la licencia del punto de acceso.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente esta configuración:

- ® GUI o CLI del Cisco IOS con el WLCs convergido de las 5760 y 3650 Series del acceso y el Catalyst 3850 Series Switch
- Acceso GUI y CLI con el WLC de las 5508 Series
- Configuración del Service Set Identifier (SSID)
- Autenticación Web

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 3.3.3 ([NGWC] de Cisco 5760 del Wiring Closet de la última generación)
- Catalyst 3850 Series Switch
- Versión 7.6.120 del WLC de las Cisco 5508 Series
- Cisco 3602 Series AP ligeros
- Cisco Catalyst 3560 Series Switches

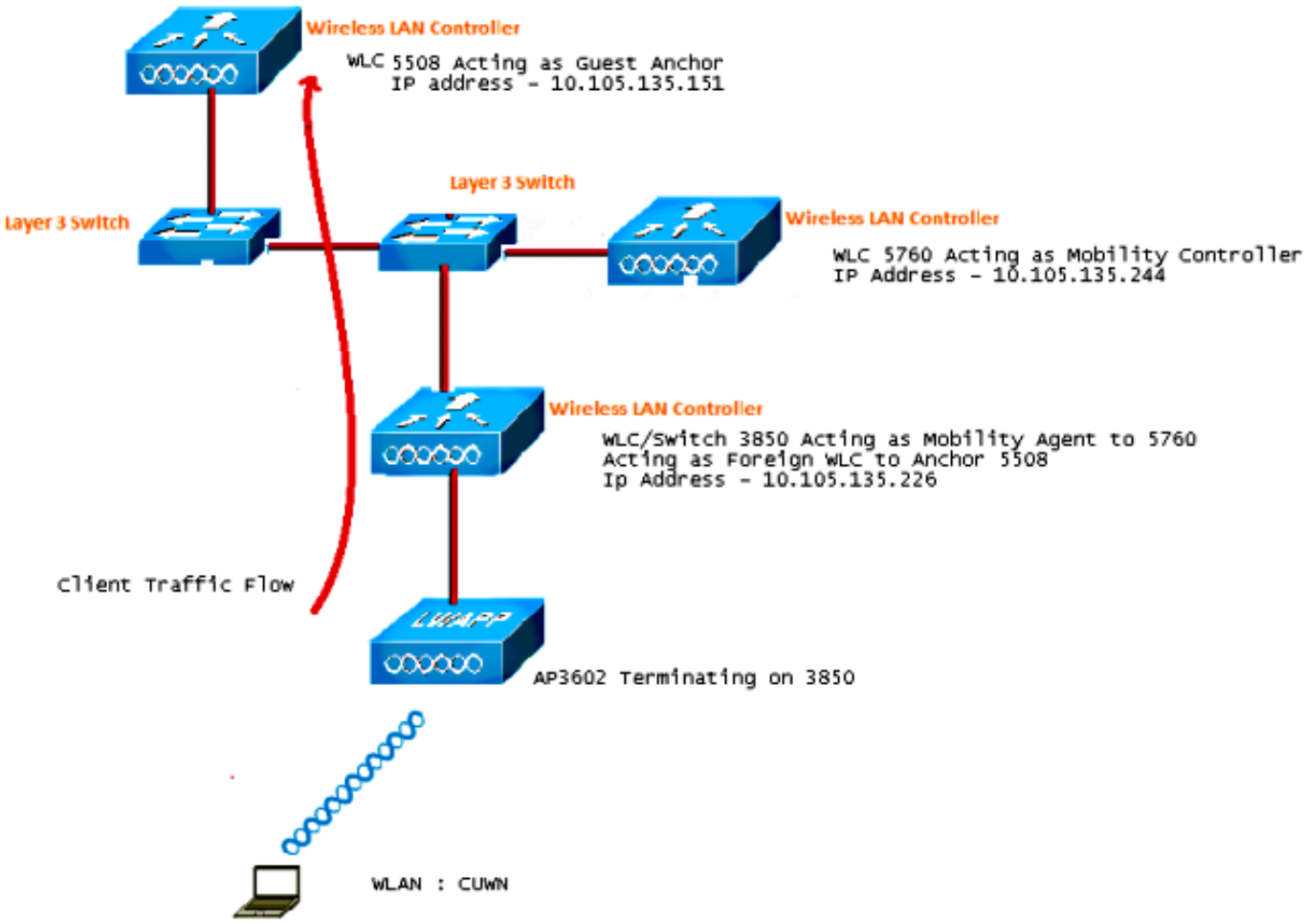
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

El WLC de las 5508 Series actúa como regulador del ancla, y el Catalyst 3850 Series Switch actúa como un regulador no nativo y el agente de la movilidad que obtiene la licencia del regulador 5760 de la movilidad.



Note: En el diagrama de la red, el WLC de las 5508 Series actúa como el regulador del ancla, el WLC de las 5760 Series actúa como el regulador de la movilidad, y el Catalyst 3850 Series Switch actúa como el agente de la movilidad y el WLC no nativo. En cualquier momento, el regulador del ancla para el Catalyst 3850 Series Switch es el WLC de las 5760 Series o el WLC de las 5508 Series. Ambas no pueden ser anclas al mismo tiempo, porque el ancla doble no funciona.

Configuraciones

La configuración incluye tres porciones:

Parte 1 - Configuración en los 5508 WLC del ancla

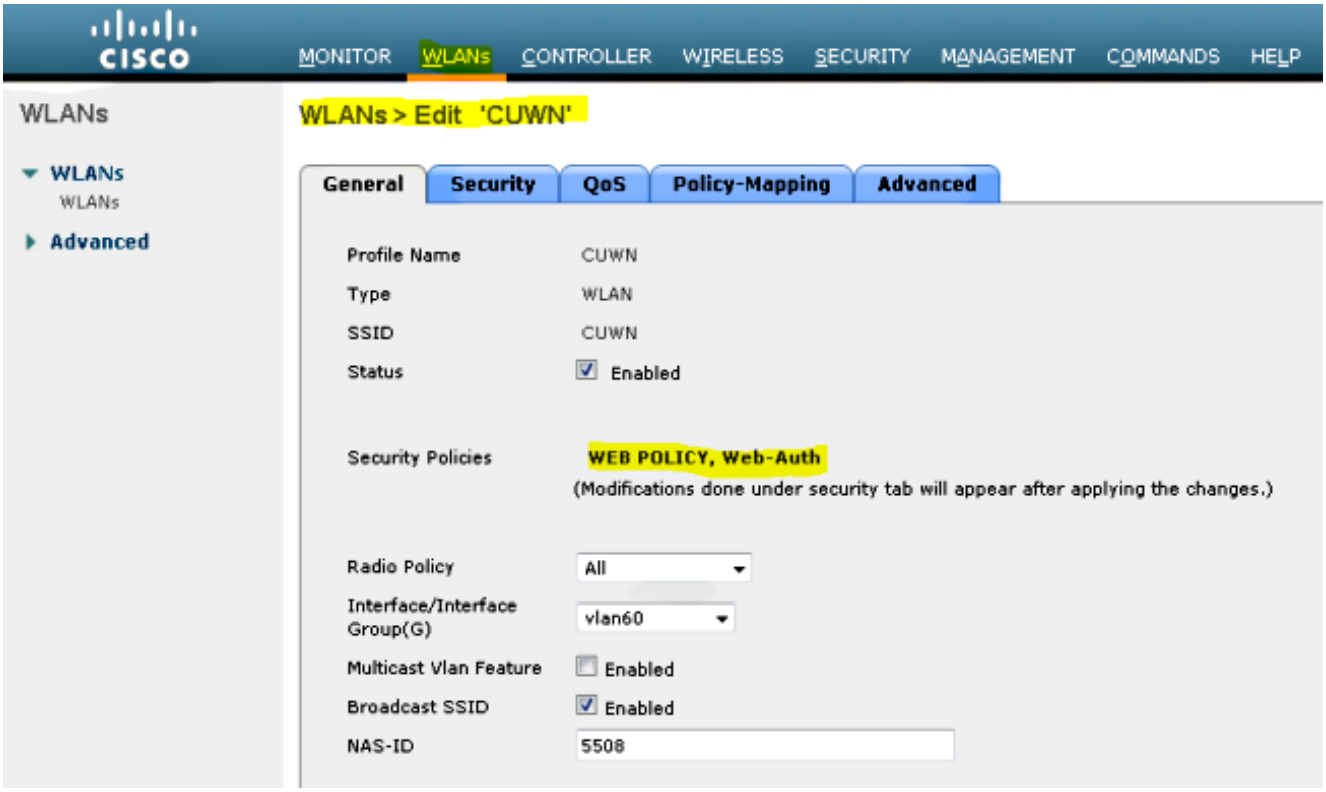
Parte 2 - Configuración convergida de la movilidad del acceso entre el WLC de las 5508/5760 Series y el Catalyst 3850 Series Switch

Parte 3 - Configuración en el Catalyst 3850 Series Switch no nativo

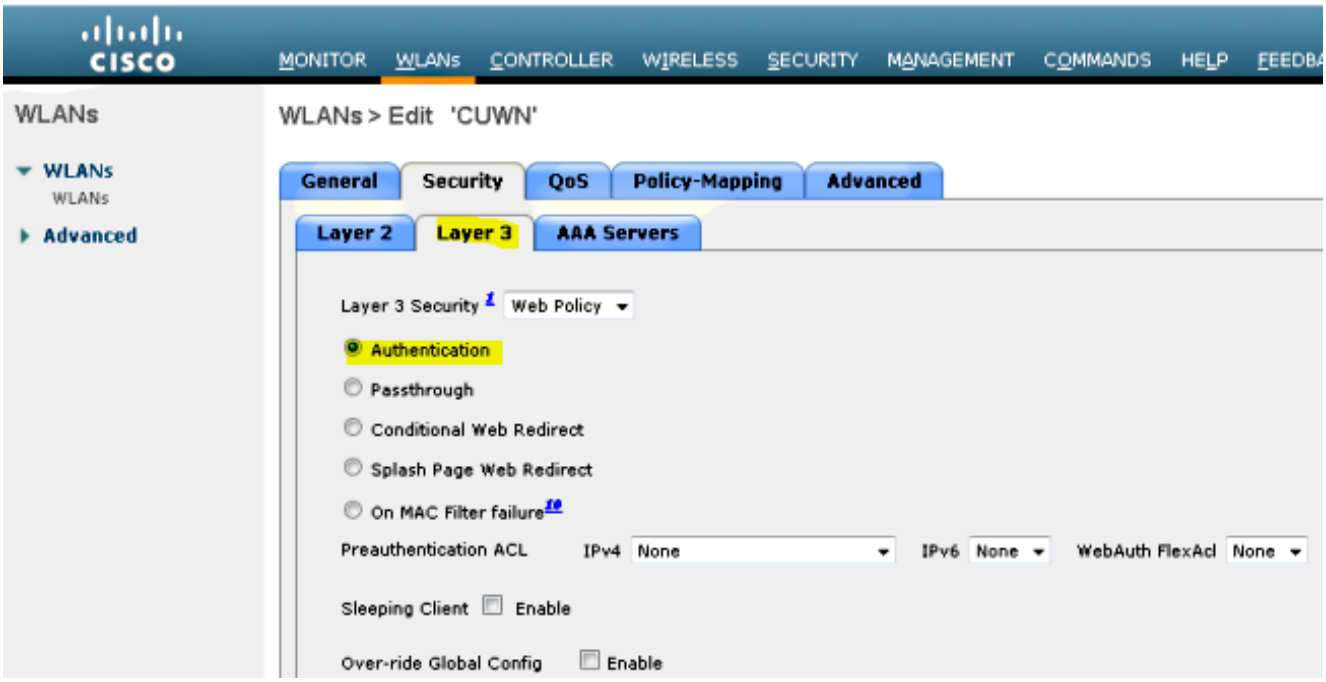
Parte 1 - Configuración en los 5508 WLC del ancla

1. En el WLC de las 5508 Series, libración sobre la **red inalámbrica (WLAN) > nuevo** para crear

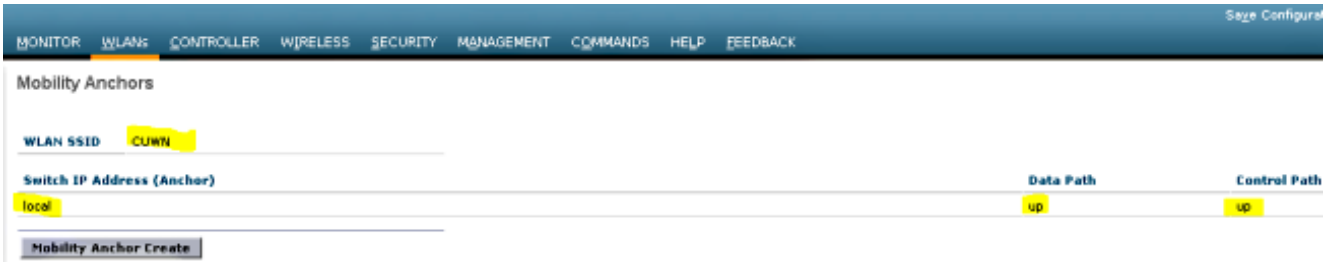
un nuevo Wireless LAN (red inalámbrica (WLAN)).



2. La libración sobre la **red inalámbrica (WLAN) > la red inalámbrica (WLAN) edita el > Security (Seguridad) > la autenticación Web habilitada de la capa 3** para configurar la Seguridad de la capa 3.



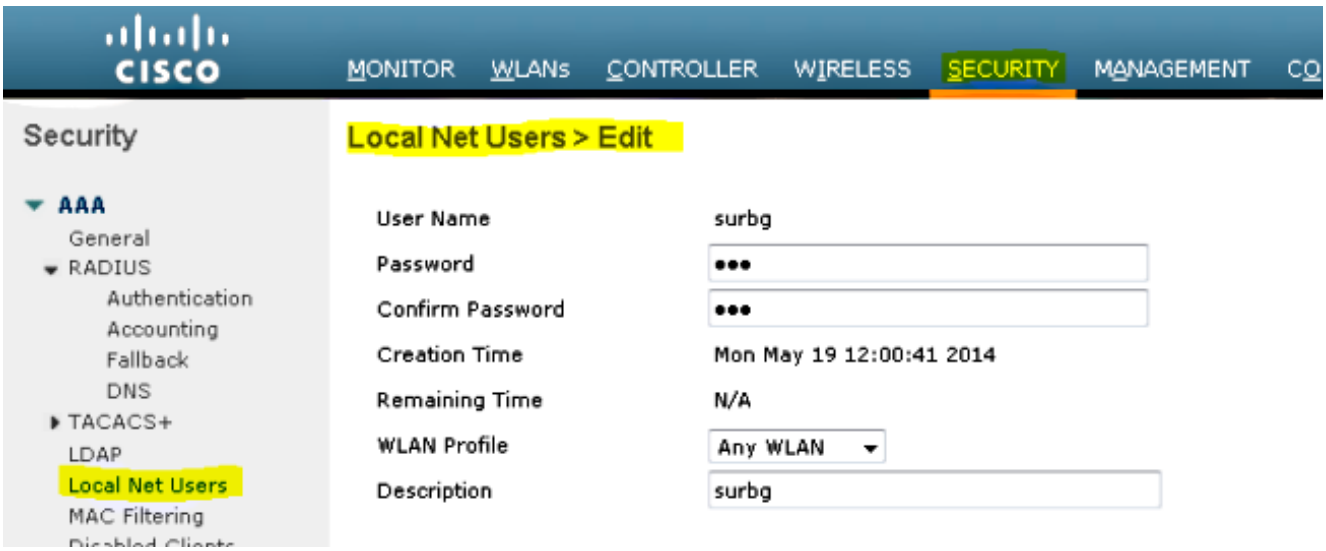
3. Haga el direccionamiento del ancla **local** bajo la ventana de configuración del ancla de la movilidad de la red inalámbrica (WLAN) para agregar el WLC de las 5508 Series como el ancla.



4. Asome sobre la **página de la Seguridad > de Webauth > de Webauth** para configurar la página de Webauth que se utilizará para la autenticación de cliente.

   En este ejemplo, se selecciona la página interna de Webauth del WLC:

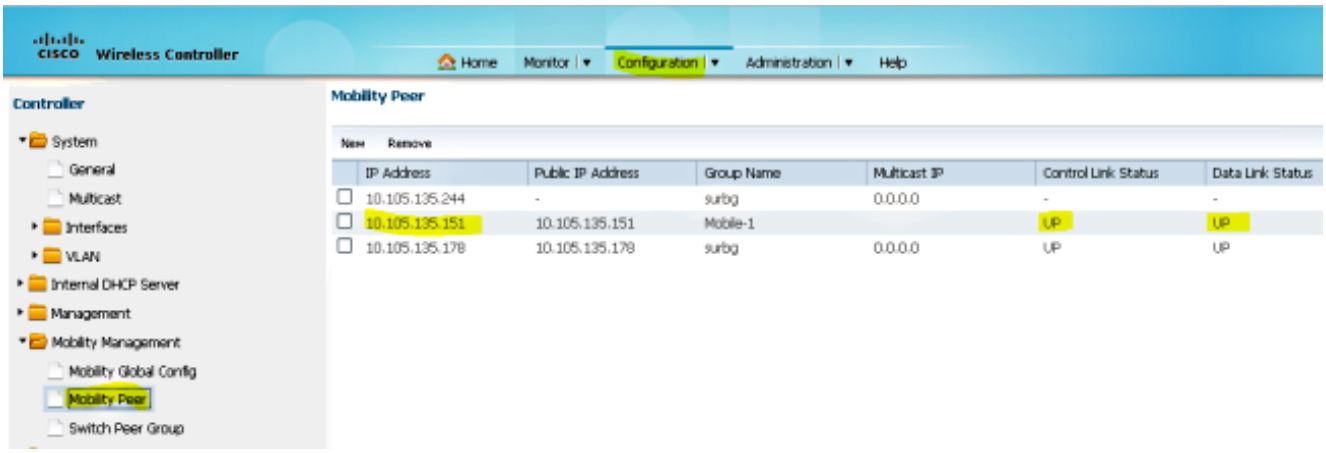
5. Cree a un usuario de red local. Este par de nombre de usuario/contraseña es utilizado por el usuario cuando está indicado en la página de Webauth.



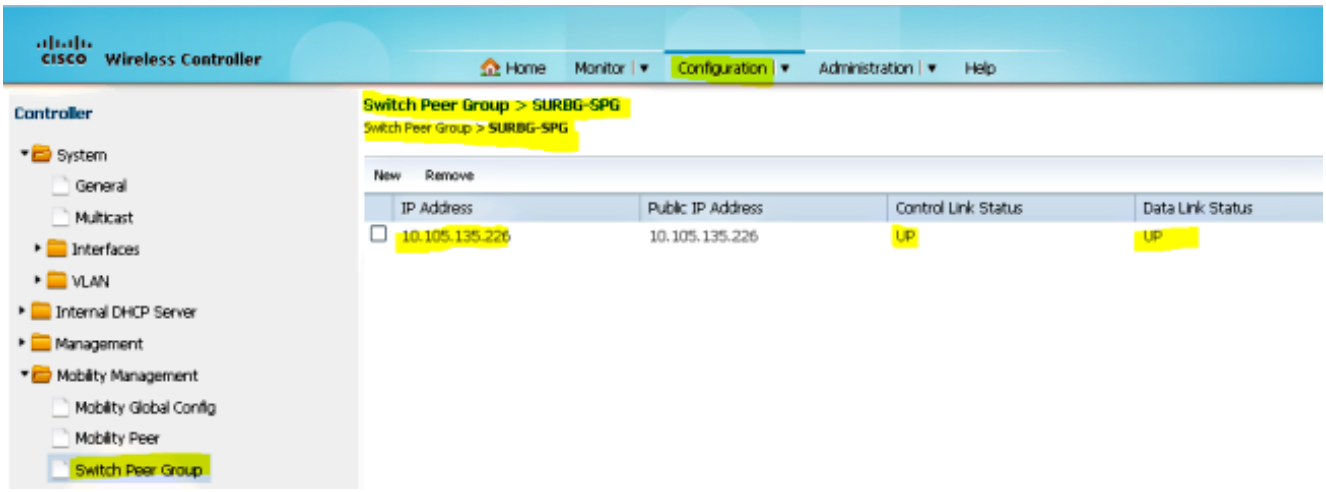
Parte 2 - Configuración convergida de la movilidad del acceso entre el WLC de las 5508/5760 Series y el Catalyst 3850 Series Switch

1. En el WLC de las 5508 Series, agregue el WLC de las 5760 Series como el par de la movilidad.

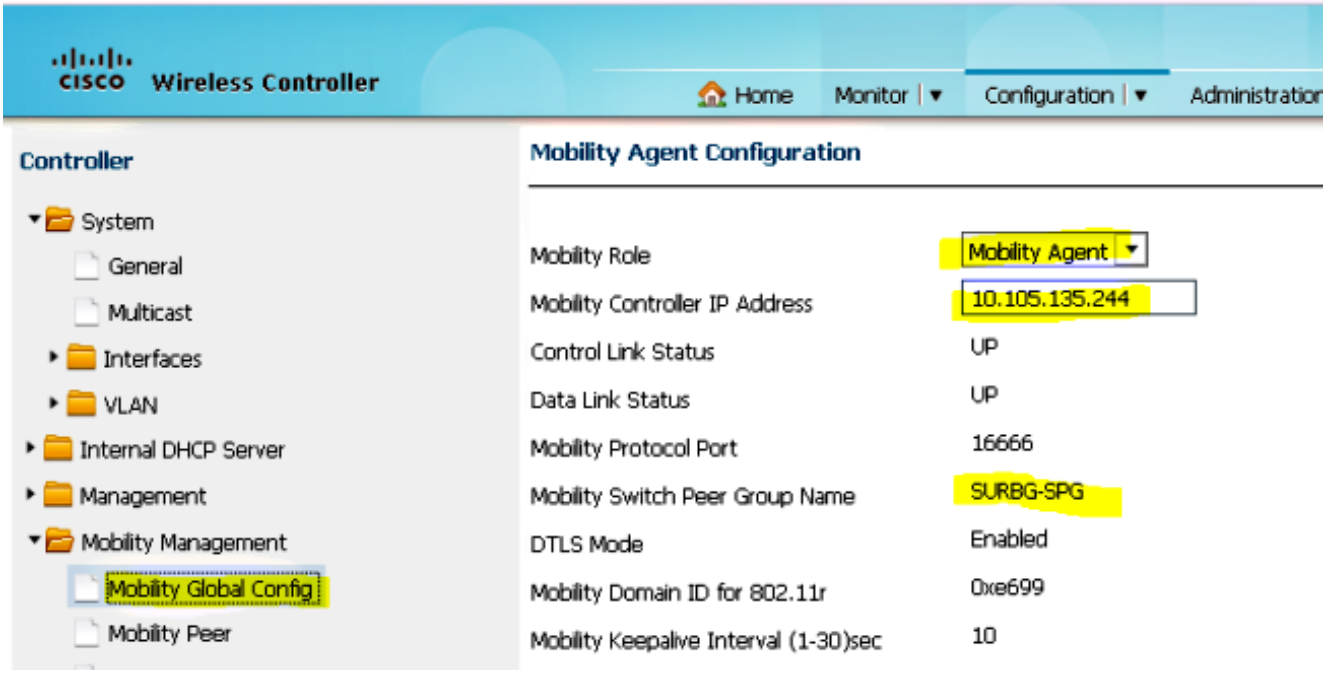
2. En el WLC de las 5760 Series, actuando como regulador de la movilidad, agregue el WLC de las 5508 Series como el par de la movilidad.



3. ¡Este paso es muy importante! Agregue el Catalyst 3850 Series Switch como el agente de la movilidad en el WLC de las 5760 Series bajo lengueta del grupo de peer del Switch bajo Administración de movilidad.



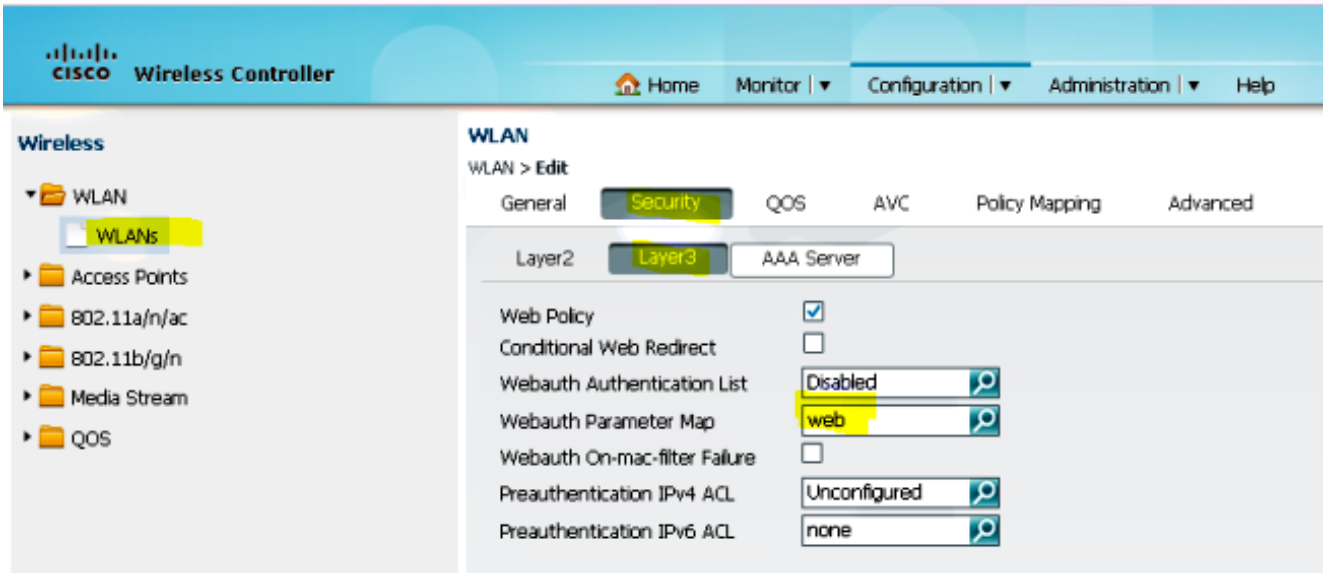
4. En el Catalyst 3850 Series Switch, agregue el WLC de las 5760 Series como el regulador de la movilidad. Una vez que usted hace esto, el Catalyst 3850 Series Switch ase la licencia del coult AP del regulador 5760 de la movilidad.



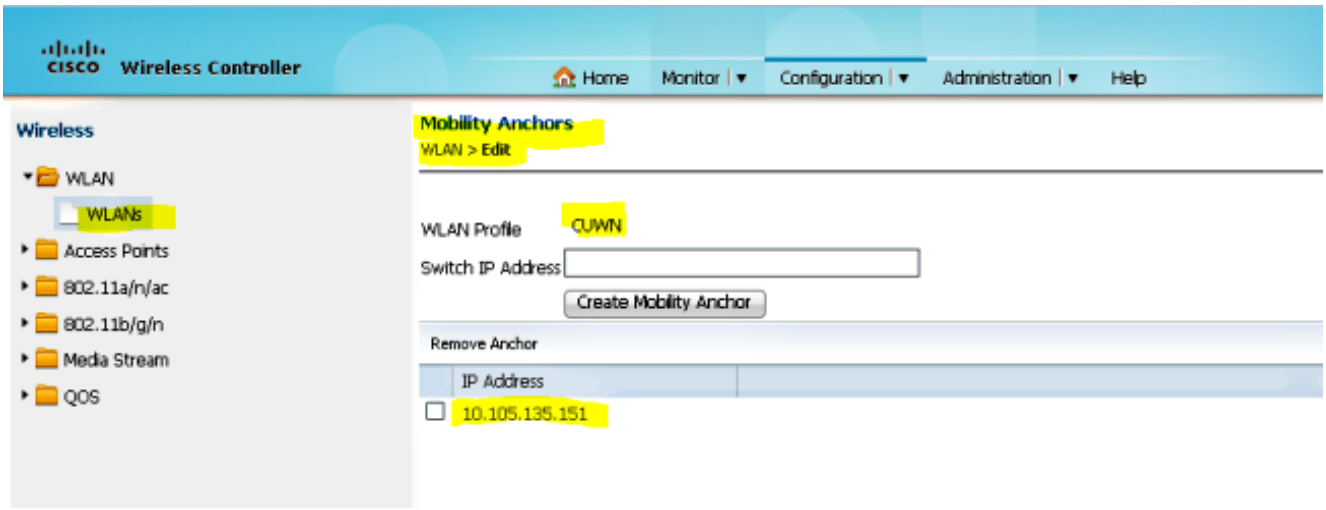
Parte 3: Configuración en el Catalyst 3850 Series Switch no nativo

1. Libración sobre **GUI > configuración > Tecnología inalámbrica > red inalámbrica (WLAN) > nuevo** para configurar el SSID/WLAN exacto en el Catalyst 3850 Series Switch.

2. La libración sobre la **red inalámbrica (WLAN) > la red inalámbrica (WLAN) edita el > Security (Seguridad) > la autenticación Web habilitada de la capa 3** para configurar la Seguridad de la capa 3.



3. Agregue la dirección IP del WLC de las 5508 Series como el ancla bajo configuración del ancla de la movilidad de la red inalámbrica (WLAN)

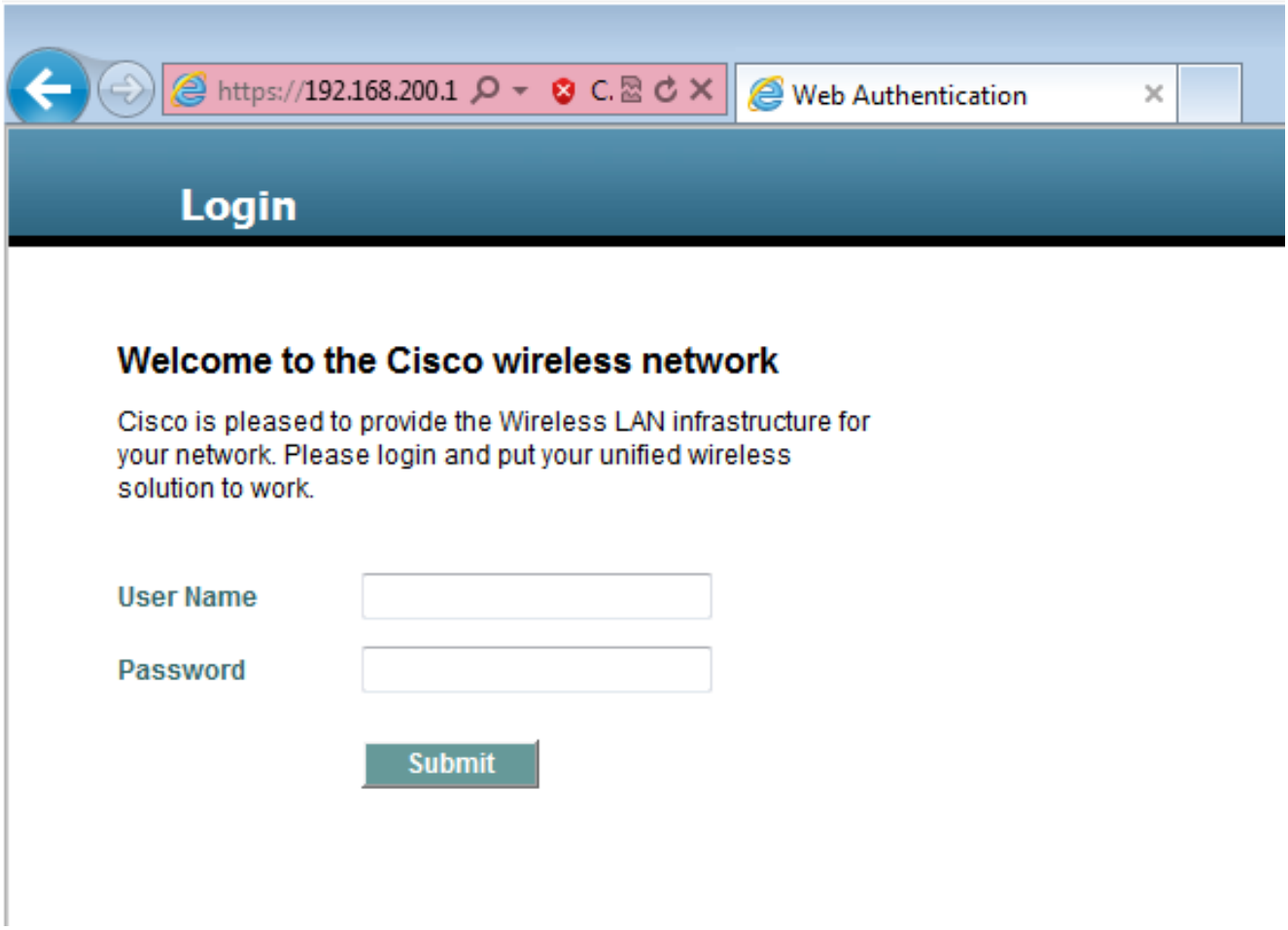


Verificación

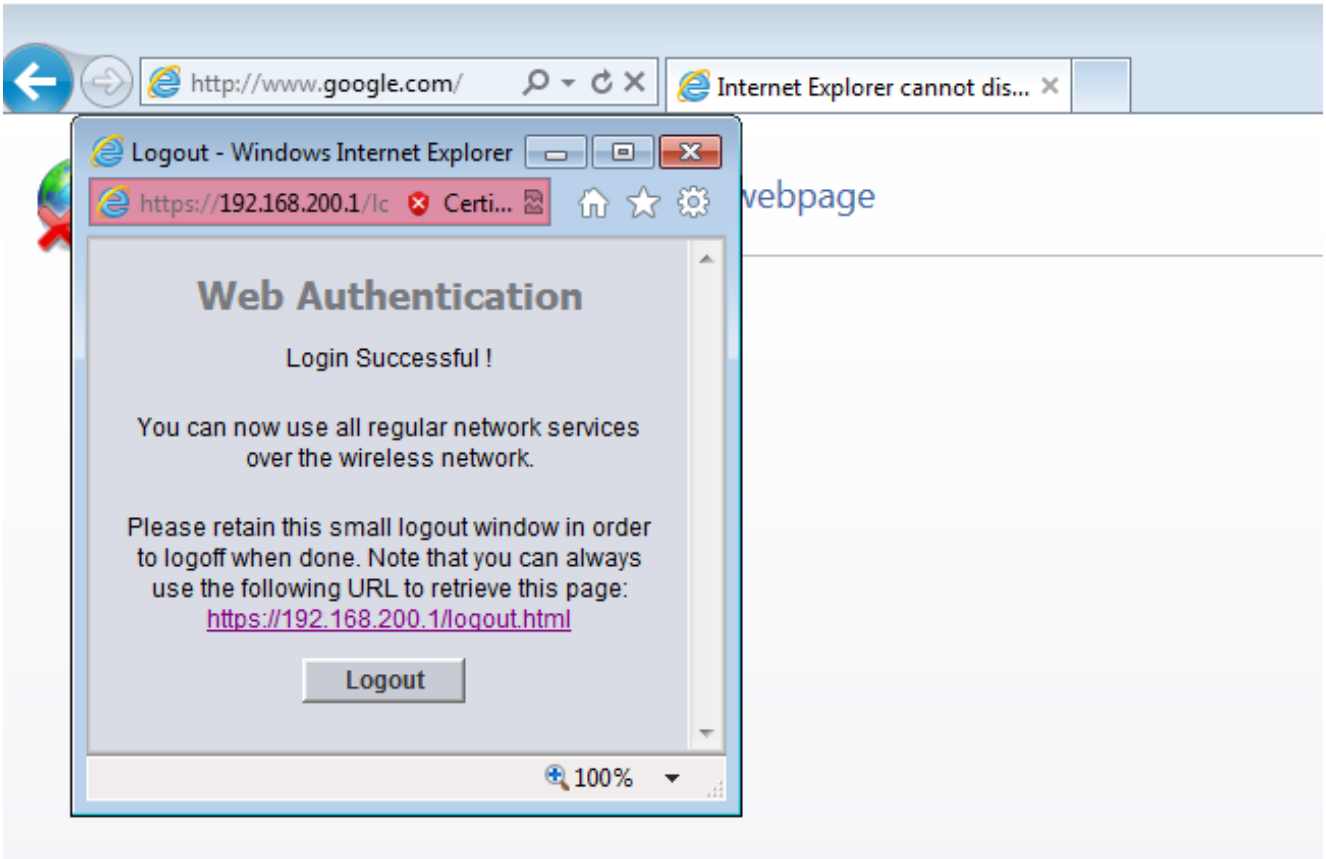
Utilize esta sección para confirmar que su configuración funcione correctamente.

Conecte al cliente con la red del Cisco Unified Wireless de la red inalámbrica (WLAN) (CUWN). Aquí está el flujo de trabajo:

1. El cliente recibe una dirección IP.
2. El cliente abre a un navegador y accede cualquier sitio web.
3. El primer paquete TCP enviado por el cliente es secuestrado por el WLC, y el WLC intercepta y envía la página de Webauth.
4. Si el DNS se configura correctamente, el cliente consigue la página de Webauth.
5. El cliente debe proporcionar el nombre de usuario/la contraseña para conseguir autenticado.
6. Después de la autenticación satisfactoria, reorientan al cliente a la página original del acceso.



7. Después de que el cliente proporcione las credenciales derechas, el cliente pasa el auth.



Troubleshooting

Para resolver problemas su configuración, ingrese estos debugs en el WLC de las 5508 Series, que actúa como ancla del invitado:

Debug Client <client mac addr>
Debug web-auth redirect enable mac <client mac addr>

Aquí tiene un ejemplo:

Debug Client 00:17:7C:2F:B6:9A
Debug web-auth redirect enable mac 00:17:7C:2F:B6:9A

```
show debug

MAC Addr 1..................................... 00:17:7C:2F:B6:9A

Debug Flags Enabled:
 dhcp packet enabled.
 dot11 mobile enabled.
 dot11 state enabled
 dot1x events enabled.
 dot1x states enabled.
 FlexConnect ft enabled.
 pem events enabled.
 pem state enabled.
 CCKM client debug enabled.
 webauth redirect enabled.
```

***mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP 00:00:00:00:00:00(0)**
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group, marking intgrp NULL
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy for client

***mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2219)**
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2240)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an intf for roamed client - removing intf group from mscb

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

***mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)**

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from 255 to 255

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl from 65535 to 65535

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile Station: (callerId: 53)

***mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 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
 IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor, client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Change state to DHCP_REQD (7) last state DHCP_REQD (7)

*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x4
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf ID 13: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling mmSendIpv6AddrUpdate for addition of IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , for MAC: 00:17:7C:2F:B6:9A
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800 Assigning an IPv6 Addr fe80:0000:0000:0000:6c1a:b253:d711:0c7f to the client in Anchor state update the foreign switch 10.105.135.226
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::6c1a:b253:d711:c7f updated to mscb. Not Advancing pem state.Current state: mscb in apfMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x4
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to interface vlan60 which can support client subnet.

***dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)**

*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) pemAdvanceState2 6717, Adding TMP rule
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 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
 IPv4 ACL
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) Fast Path rule (contd...) 802.1P = 0, **DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60, Local Bridging intf id = 13**
***dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)**
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect rule due to user logout
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148 Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign switch 10.105.135.226
*dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11 to mobile
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU entry of type 2, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to Data Plane. SUCCESS !!
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame

(5508-MC) >
(5508-MC) >
(5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received op BOOTREQUEST (1) (len 314,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07) mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a 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
*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 - 60.60.60.251 (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3 (2902502819), secs: 3072, flags: 0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   chaddr: 00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0, giaddr: 60.60.60.2
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP   requested ip: 60.60.60.11
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to 60.60.60.251 (len 358, port 1, vlan 60)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 - control block settings:
           dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
           dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2 VLAN: 60
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -

```
NONE (server address 0.0.0.0,local address 0.0.0.0, gateway 60.60.60.251, VLAN 60,
port 1)
*DHCP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op BOOTREPLY
(2) (len 308,vlan 60, port 1, encap 0xec00)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server from ACK
(server 60.60.60.251, yiaddr 60.60.60.11)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   chaddr:
00:17:7c:2f:b6:9a
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCP Socket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP   server id:
192.168.200.1  rcvd server id: 60.60.60.251
*webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a-  parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=,
URL is now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 312


*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is
 HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/
Content-Type: text/html
Content-Length: 312

<HTML><HEAD
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection

*emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a
```

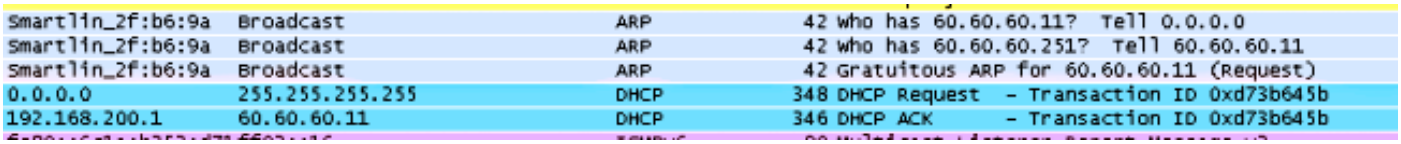
```
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL
according to configured Web-Auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting defualt login page to user
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a-  parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is
/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is
now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is
 HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
Content-Type: text/html
Content-Length: 323


*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op
BOOTREQUEST (1) (len 308,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
           dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0,
           dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2  VLAN: 60


*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1
```

***emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for Web-Auth page /login.html**
***emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for Web-Auth page /login.html**
***emWeb: May 19 13:38:47.215:**

```
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_NOL3SEC
(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASTPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
  type = Airespace AP Client
 on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID =
```

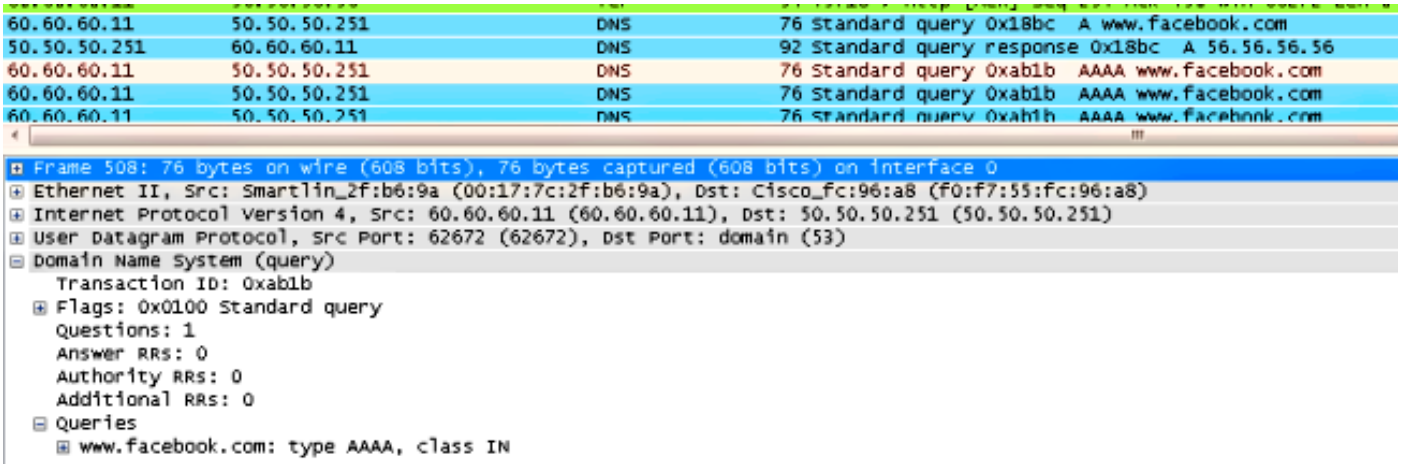
Aquí está la captura de paquetes del client cara.

El cliente consigue la dirección IP.



Smartlin_2f:b6:9a	Broadcast	ARP	42 Who has 60.60.60.11? Tell 0.0.0.0
Smartlin_2f:b6:9a	Broadcast	ARP	42 Who has 60.60.60.251? Tell 60.60.60.11
Smartlin_2f:b6:9a	Broadcast	ARP	42 Gratuitous ARP for 60.60.60.11 (Request)
0.0.0.0	255.255.255.255	DHCP	348 DHCP Request - Transaction ID 0xd73b645b
192.168.200.1	60.60.60.11	DHCP	346 DHCP ACK - Transaction ID 0xd73b645b

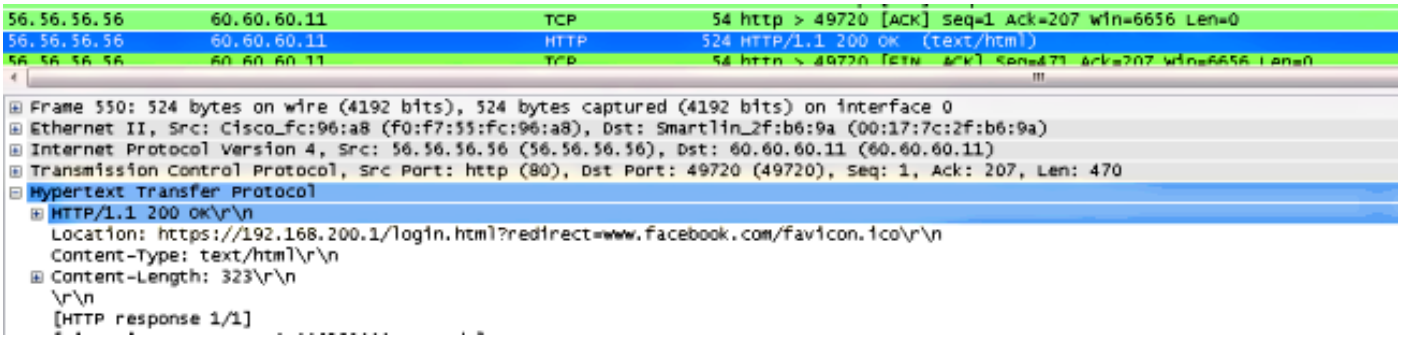
El cliente abre a un navegador y teclea **www.facebook.com**.



60.60.60.11	50.50.50.251	DNS	76 Standard query 0x18bc A www.facebook.com
50.50.50.251	60.60.60.11	DNS	92 Standard query response 0x18bc A 56.56.56.56
60.60.60.11	50.50.50.251	DNS	76 Standard query 0xab1b AAAA www.facebook.com
60.60.60.11	50.50.50.251	DNS	76 Standard query 0xab1b AAAA www.facebook.com

```
Frame 508: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a), Dst: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8)
Internet Protocol Version 4, Src: 60.60.60.11 (60.60.60.11), Dst: 50.50.50.251 (50.50.50.251)
User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53)
Domain Name System (query)
    Transaction ID: 0xab1b
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.facebook.com: type AAAA, class IN
```

El WLC intercepta el primer paquete TCP del cliente y avanza su dirección IP virtual y la página interna de Webauth.



Después de la autenticación Web acertada, el resto del flujo de trabajo completa.