

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Parte 1 - Configuração 5508 na âncora WLC](#)

[Parte 2 - Configuração convergida da mobilidade do acesso entre o 5508/5760 Series WLC e o Catalyst 3850 Series Switch](#)

[Parte 3: Configuração no Catalyst 3850 Series Switch estrangeiro](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Isto documenta descreve como configurar os controladores do Wireless LAN do 5508/5760 Series (WLC) e o Catalyst 3850 Series Switch para a âncora do convidado do cliente Wireless no desenvolvimento novo da mobilidade setup onde o 5508 Series WLC atua como a âncora da mobilidade e o Catalyst 3850 Series Switch atua como um controlador estrangeiro da mobilidade para os clientes. Adicionalmente, o Catalyst 3850 Series Switch atua como um agente da mobilidade a um 5760 Series WLC que atue como um controlador da mobilidade de onde o Catalyst 3850 Series Switch adquira a licença do Access Point (AP).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente esta configuração:

- [®] GUI ou CLI do Cisco IOS com o 5760 e 3650 Series convergido WLC do acesso e o Catalyst 3850 Series Switch
- Acesso GUI e CLI com o 5508 Series WLC
- Configuração do Service Set Identifier (SSID)
- Autenticação da Web

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Liberação 3.3.3 de Cisco 5760 ([NGWC] do armário de fiação da próxima geração)
- Catalyst 3850 Series Switch
- Liberação 7.6.120 do Cisco 5508 Series WLC
- Cisco 3602 Series AP de pouco peso
- Cisco Catalyst 3560 Series Switches

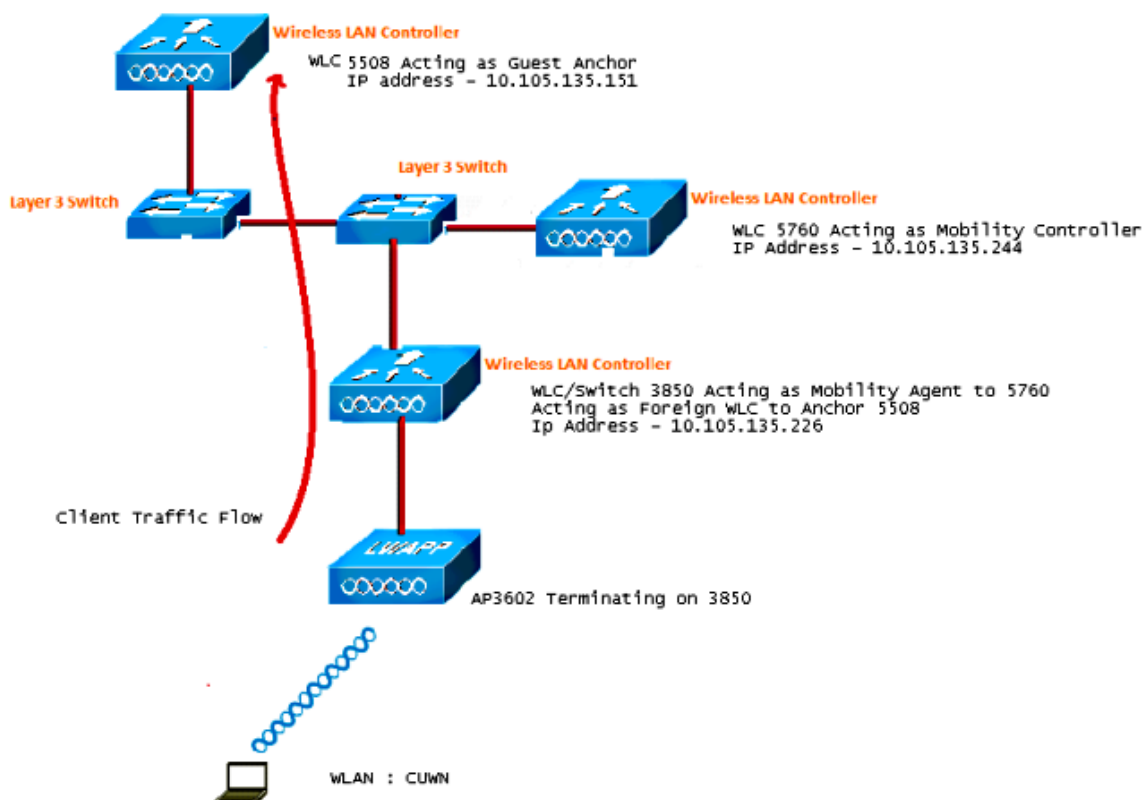
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

O 5508 Series WLC atua como um controlador da âncora, e o Catalyst 3850 Series Switch atua como um controlador estrangeiro e o agente da mobilidade que obtém a licença do controlador 5760 da mobilidade.



Nota: No diagrama da rede, o 5508 Series WLC atua como o controlador da âncora, o 5760

Series WLC atua como o controlador da mobilidade, e o Catalyst 3850 Series Switch atua como o agente da mobilidade e o WLC estrangeiro. Em qualquer momento a tempo, o controlador da âncora para o Catalyst 3850 Series Switch é o 5760 Series WLC ou o 5508 Series WLC. Ambas não podem ser âncoras ao mesmo tempo, porque a âncora dobro não funciona.

Configurações

A configuração inclui três porções:

[Parte 1 - Configuração 5508 na âncora WLC](#)

[Parte 2 - Configuração convergida da mobilidade do acesso entre o 5508/5760 Series WLC e o Catalyst 3850 Series Switch](#)

[Parte 3 - Configuração no Catalyst 3850 Series Switch estrangeiro](#)

Parte 1 - Configuração 5508 na âncora WLC

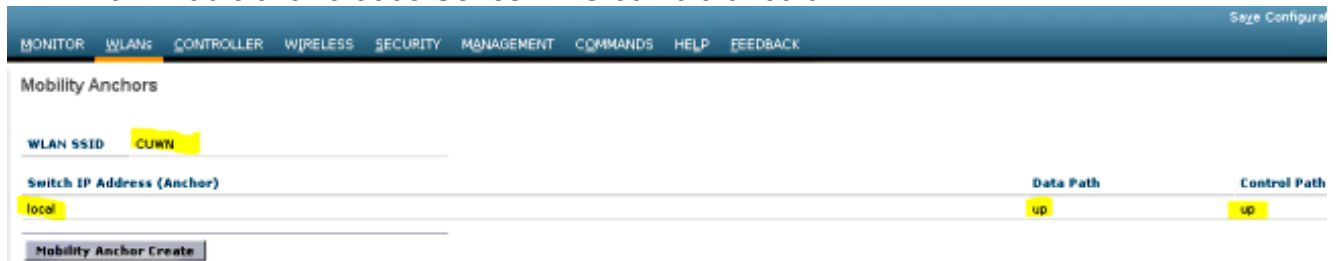
1. No 5508 Series WLC, paio sobre **WLAN > novo** a fim criar um Wireless LAN novo (WLAN).



2. O paio sobre **WLAN > WLAN edita o > segurança > a autenticação da Web permitida da camada 3** a fim configurar a Segurança da camada 3.



3. Faça o endereço da âncora **local** sob a janela de configuração da âncora da mobilidade WLAN a fim adicionar o 5508 Series WLC como a âncora.

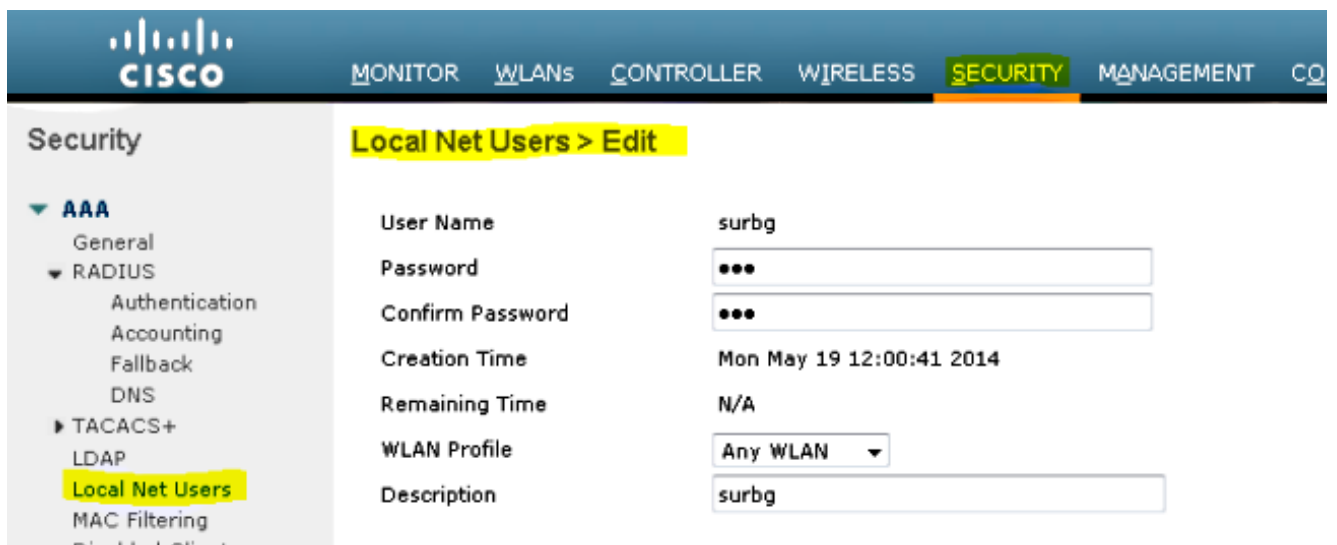


4. Paire sobre a **página da Segurança > do Webauth > do Webauth** a fim configurar a página de Webauth a ser usada para a autenticação do cliente.

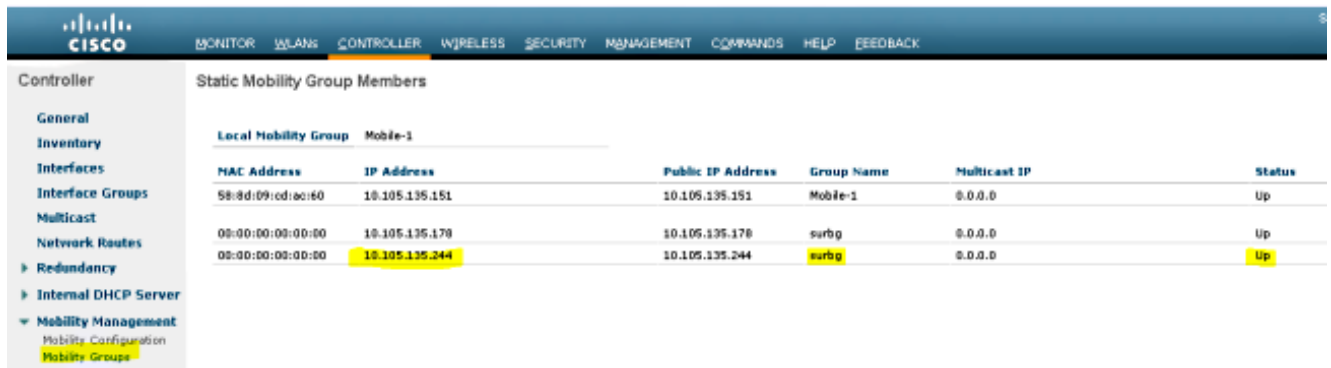
Neste exemplo, a página interna WLC Webauth é selecionada:



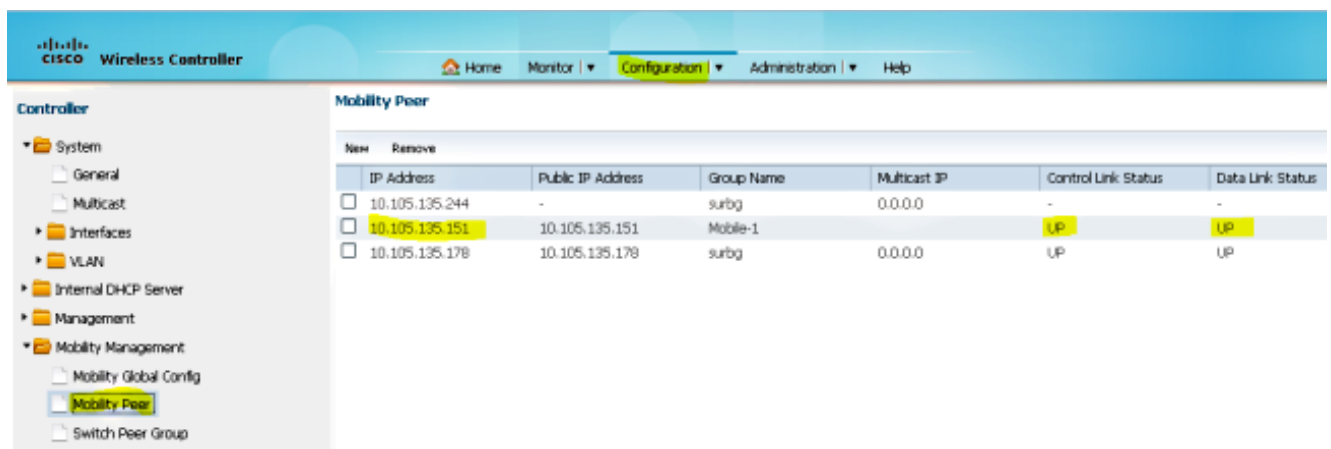
5. Crie um usuário líquido local. Este par de nome de usuário/senha é usado pelo usuário quando alertado na página de Webauth.



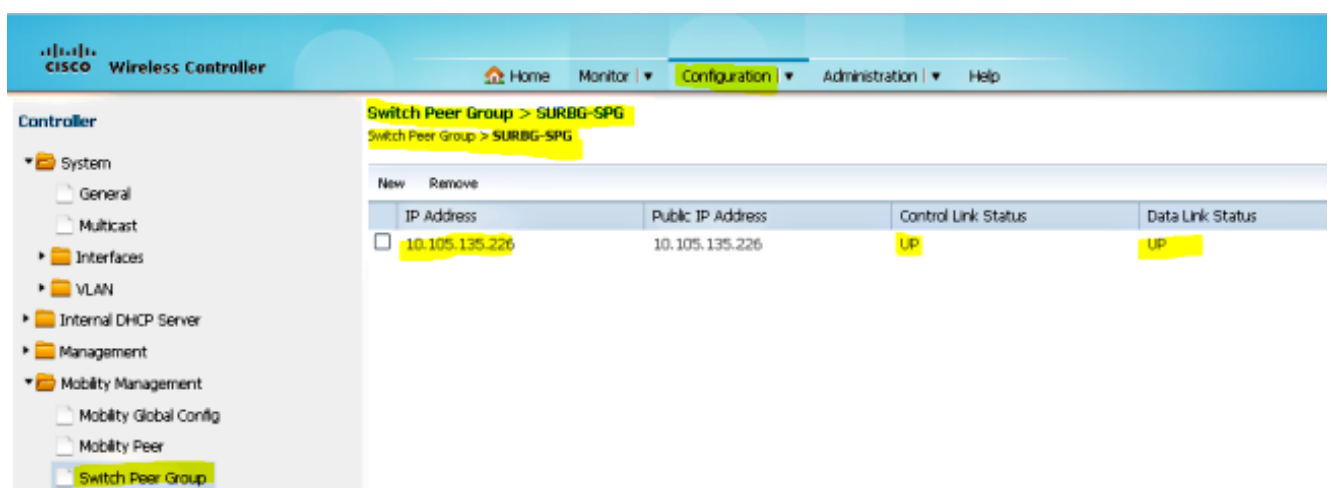
1. No 5508 Series WLC, adicionar o 5760 Series WLC como o par da mobilidade.



2. No 5760 Series WLC, atuando como um controlador da mobilidade, adicionar o 5508 Series WLC como o par da mobilidade.



3. Esta etapa é muito importante! Adicionar o Catalyst 3850 Series Switch como o agente da mobilidade no 5760 Series WLC sob a aba do peer-group do interruptor sob o Gerenciamento de mobilidade.



4. No Catalyst 3850 Series Switch, adicionar o 5760 Series WLC como o controlador da mobilidade. Uma vez que você faz este, o Catalyst 3850 Series Switch agarra a licença do coult AP do controlador 5760 da mobilidade.

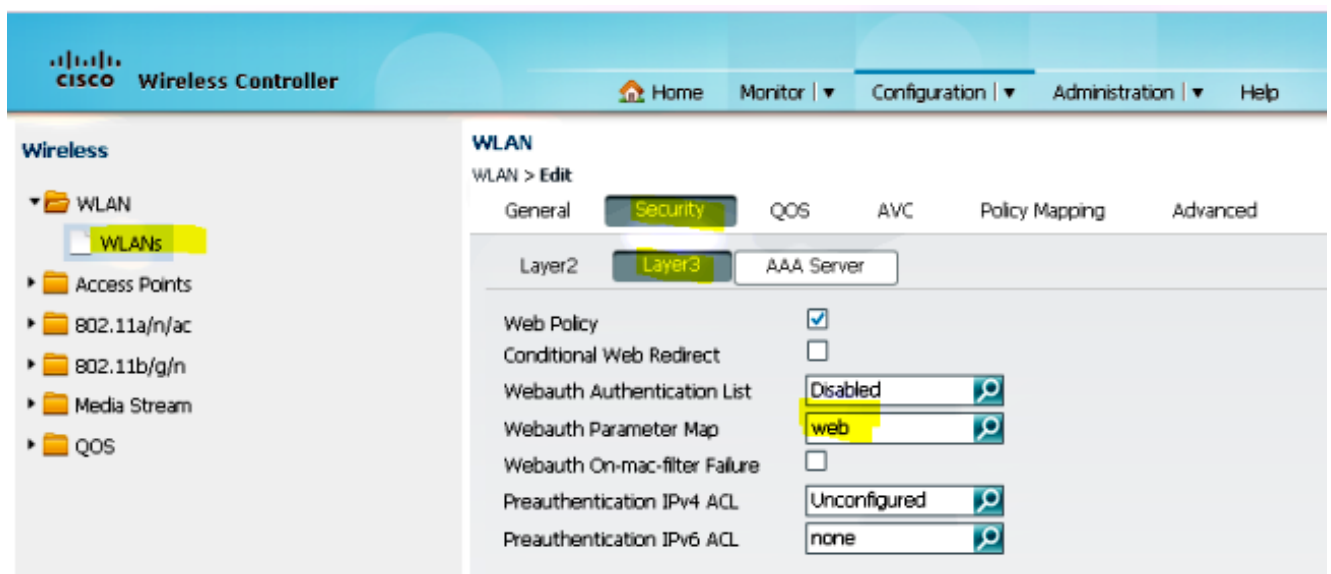


Parte 3: Configuração no Catalyst 3850 Series Switch estrangeiro

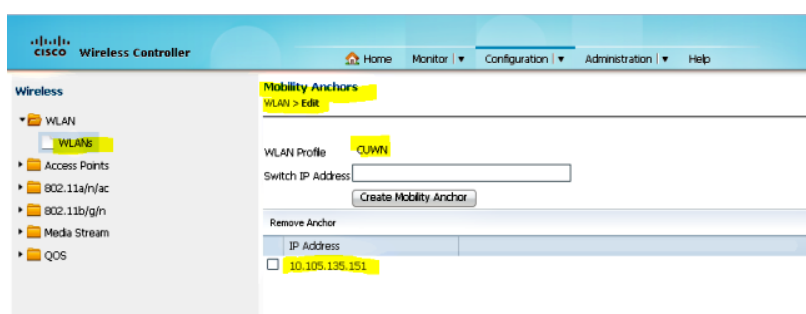
1. Paio sobre GUI > configuração > Sem fio > WLAN > novo a fim configurar o SSID/WLAN exato no Catalyst 3850 Series Switch.



2. O paio sobre WLAN > WLAN edita o > segurança > a autenticação da Web permitida da camada 3 a fim configurar a Segurança da camada 3.



3. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do 5508 Series WLC como a âncora sob a configuração da âncora da mobilidade WLAN

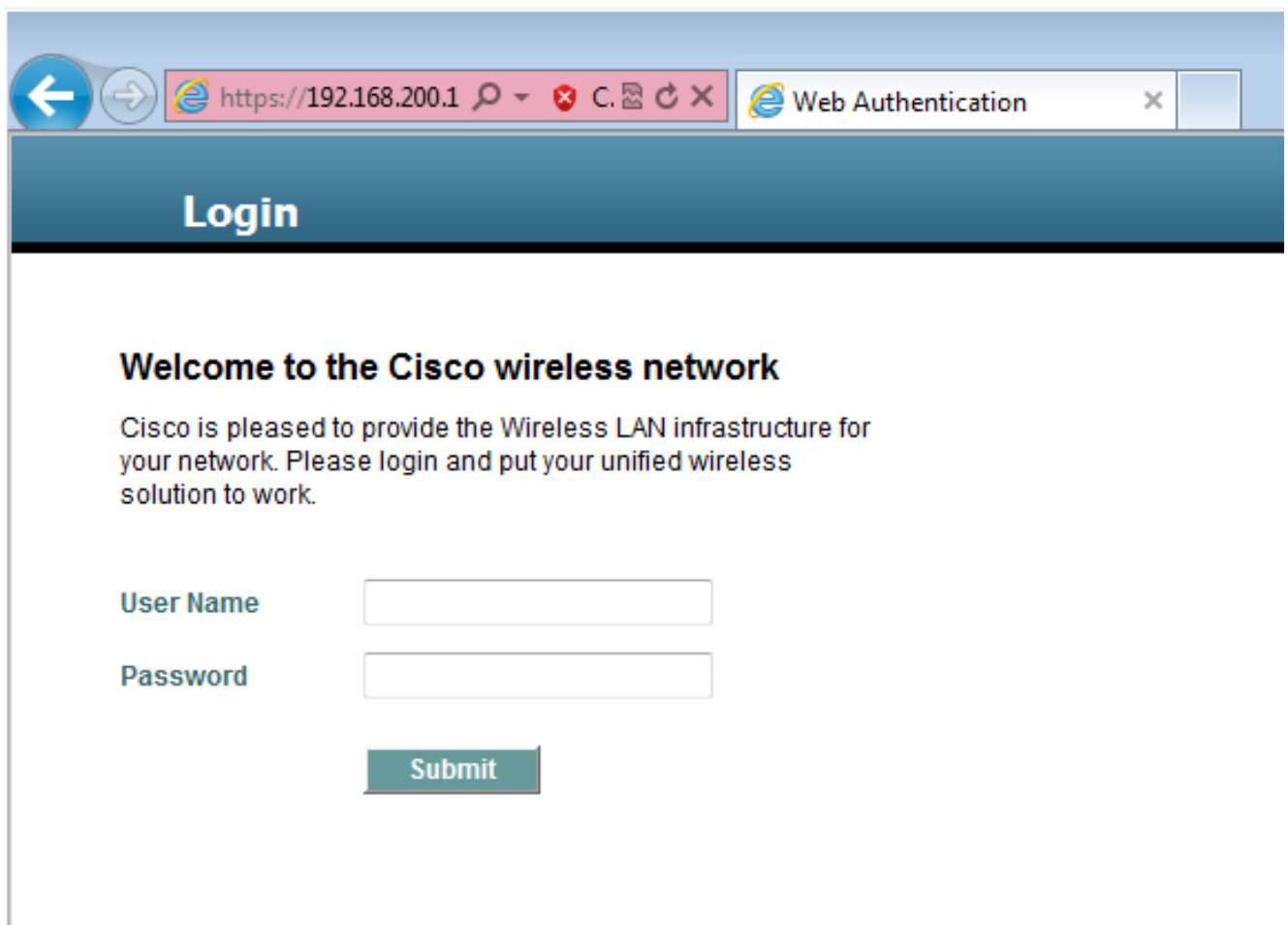


Verificar

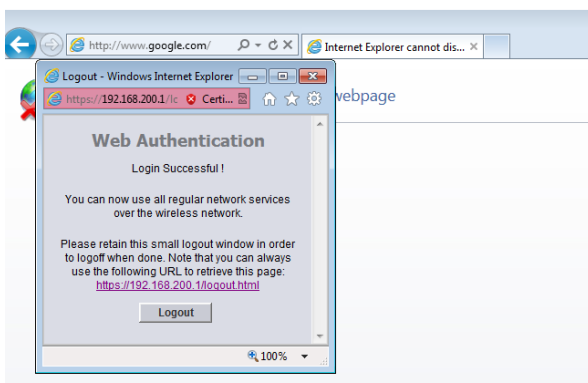
Use esta seção para confirmar se a sua configuração funciona corretamente.

Conecte o cliente à rede de Cisco Unified Wireless WLAN (CUWN). Está aqui o fluxo de trabalho:

1. O cliente recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT.
2. O cliente abre um navegador e alcança todo o Web site.
3. O primeiro pacote de TCP enviado pelo cliente é sequestrado pelo WLC, e o WLC intercepta e envia a página de Webauth.
4. Se o DNS é configurado corretamente, o cliente obtém a página de Webauth.
5. O cliente deve fornecer o username/senha a fim obter autenticado.
6. Após a autenticação bem sucedida, o cliente é reorientado à página original do acesso.



7. Depois que o cliente fornece as credenciais direitas, o cliente passa o AUTH.



Troubleshooting

A fim pesquisar defeitos sua configuração, entre nestes debuga no 5508 Series WLC, que atua como uma âncora do convidado:

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

Aqui está um exemplo:

```
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(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 default 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 default 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 PLUMBFASPATH: 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 =

```

Está aqui a captura de pacote de informação do lado do cliente.

O cliente obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT.

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

O cliente abre um navegador e datilografa 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
60.60.60.11	50.50.50.251	DNS	76 Standard query 0xab1b AAAA www.facebnk.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

```

O WLC intercepta o primeiro pacote de TCP do cliente e empurra seu endereço IP de Um ou Mais Servidores Cisco ICM NT virtual e a página interna de Webauth.

```

56.56.56.56 60.60.60.11 TCP 54 http > 49720 [ACK] Seq=1 Ack=207 win=6656 Len=0
56.56.56.56 60.60.60.11 HTTP 524 HTTP/1.1 200 OK (text/html)
56.56.56.56 60.60.60.11 TCP 54 http > 49720 [ACK] Seq=1 Ack=207 win=6656 Len=0
Frame 550: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0
Ethernet II, Src: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8), Dst: Smartlin_2f:b6:9a (00:17:7c:2f:b6:9a)
Internet Protocol version 4, Src: 56.56.56.56 (56.56.56.56), Dst: 60.60.60.11 (60.60.60.11)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49720 (49720), Seq: 1, Ack: 207, Len: 470
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico\r\n
  Content-Type: text/html\r\n
  Content-Length: 323\r\n
  \r\n
  [HTTP response 1/1]

```

Após a autenticação da Web bem sucedida, o resto do fluxo de trabalho termina.

60.60.60.11	50.50.50.251	DNS	86 Standard query 0x64dd A fe9cv11st.fe.microsoft.com
60.60.60.11	192.168.200.1	TCP	66 49724 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
192.168.200.1	60.60.60.11	TCP	66 https > 49724 [SYN, ACK] Seq=0 Ack=1 win=3560 Len=0 MSS=1390 SACK_PERM=1 WS=64
60.60.60.11	192.168.200.1	TCP	54 49724 > https [ACK] Seq=1 Ack=1 win=16680 Len=0
60.60.60.11	192.168.200.1	TLSv1	190 Client Hello
192.168.200.1	60.60.60.11	TCP	54 https > 49724 [ACK] Seq=1 Ack=137 win=6656 Len=0
192.168.200.1	60.60.60.11	TLSv1	192 Server Hello, Change Cipher Spec, Encrypted Handshake Message
60.60.60.11	192.168.200.1	TLSv1	113 change cipher spec, encrypted Handshake Message
60.60.60.11	50.50.50.251	DNS	83 Standard query 0xb814 A ct1d1.windowsupdate.com
192.168.200.1	60.60.60.11	TCP	54 https > 49724 [ACK] Seq=139 Ack=196 win=6656 Len=0
60.60.60.11	50.50.50.251	DNS	83 Standard query 0xb814 A ct1d1.windowsupdate.com