

# Ancre Sans fil unifiée d'invité de contrôleurs LAN d'Access avec l'exemple convergé de configuration d'Access

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Partie - Configuration sur 5508 l'ancre WLC](#)

[Partie - La configuration convergée de mobilité d'accès entre la gamme 5508/5760 WLC et la gamme Catalyst 3850 commutent](#)

[Partie 3 : Configuration sur le commutateur étranger de gamme Catalyst 3850](#)

[Vérifiez](#)

[Dépannez](#)

## Introduction

Ceci documente décrit comment configurer les contrôleurs LAN Sans fil de gamme 5508/5760 (WLCs) et la gamme Catalyst 3850 commute pour l'ancre Sans fil d'invité de client dans le nouveau déploiement de mobilité installé où la gamme 5508 WLC agit en tant qu'ancre de mobilité et la gamme Catalyst 3850 commute agit en tant que contrôleur étranger de mobilité pour les clients. Supplémentaire, la gamme Catalyst 3850 commute agit en tant qu'agent de mobilité à une gamme 5760 WLC qui agit en tant que Mobility Controller d'où le commutateur de gamme Catalyst 3850 saisit le permis du Point d'accès (AP).

## Conditions préalables

### Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- Le GUI ou le CLI de Cisco IOS® avec les gammes 5760 et 3650 convergées WLCs d'accès et la gamme Catalyst 3850 commutent
- Accès GUI et CLI avec la gamme 5508 WLC
- Configuration d'Identifiant SSID (Service Set Identifier)
- Authentification Web

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 3.3.3 de Cisco 5760 (armoire de câblage de nouvelle génération [NGWC])
- Commutateur de gamme Catalyst 3850
- Version 7.6.120 de la gamme Cisco 5508 WLC
- Gamme Cisco 3602 aps légers
- Commutateurs de la gamme Cisco Catalyst 3560

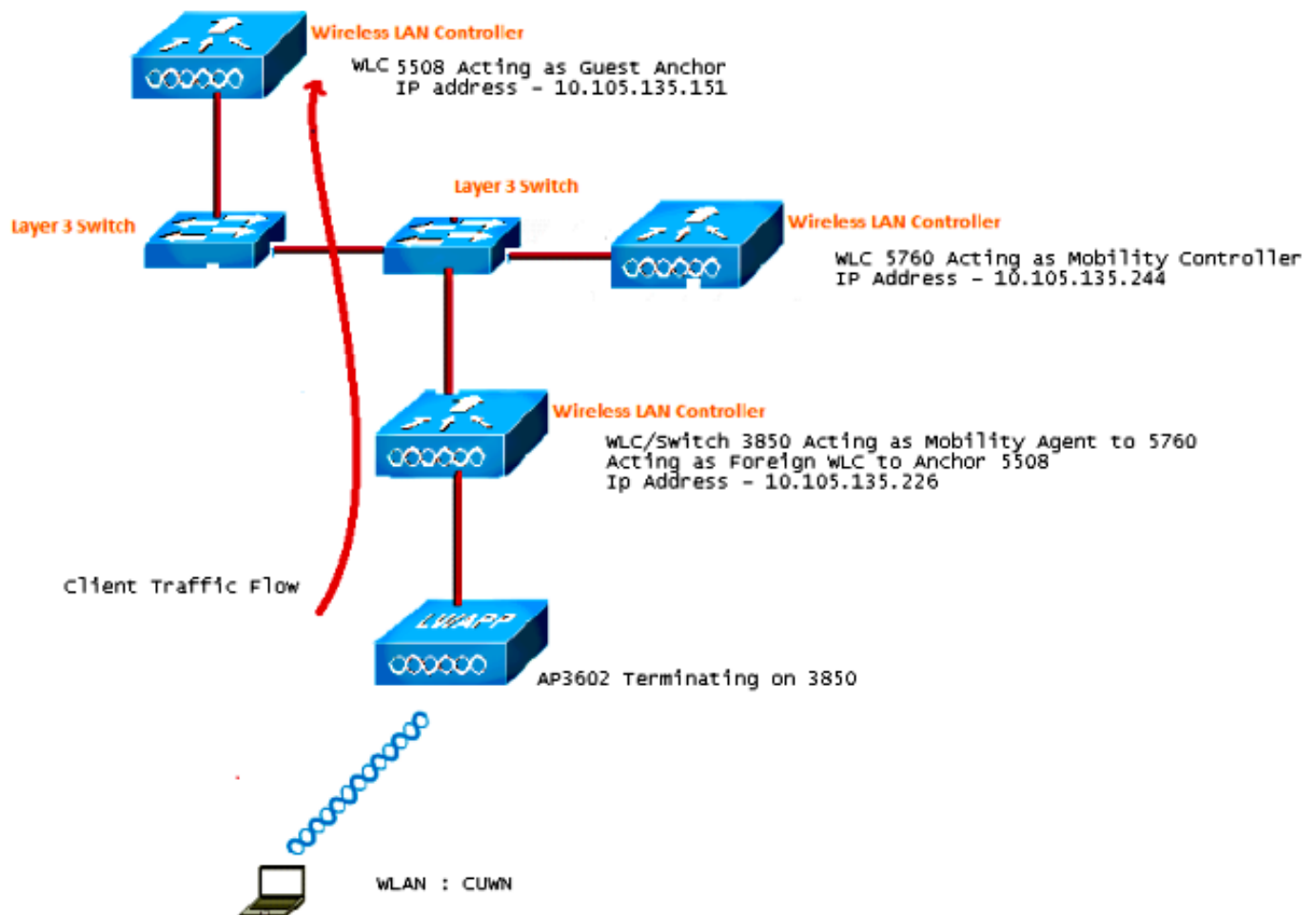
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Configurez

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

La gamme 5508 WLC agit en tant que contrôleur d'ancre, et la gamme Catalyst 3850 commute agit en tant que contrôleur étranger et agent de mobilité qui obtient le permis de Mobility Controller 5760.



Remarque: Dans le schéma de réseau, la gamme 5508 WLC agit en tant que contrôleur d'ancre, la gamme 5760 WLC agit en tant que Mobility Controller, et la gamme Catalyst 3850 commutateur agit en tant qu'agent de mobilité et WLC étranger. À un point quelconque à temps, le contrôleur d'ancre pour le commutateur de gamme Catalyst 3850 est la gamme 5760 WLC ou la gamme 5508 WLC. Chacun des deux ne peuvent pas être des ancres en même temps, parce que la double ancre ne fonctionne pas.

## Configurations

La configuration inclut trois parts :

[Partie - Configuration sur 5508 l'ancre WLC](#)

[Partie - La configuration convergée de mobilité d'accès entre la gamme 5508/5760 WLC et la gamme Catalyst 3850 commutent](#)

[Partie - Configuration sur le commutateur étranger de gamme Catalyst 3850](#)

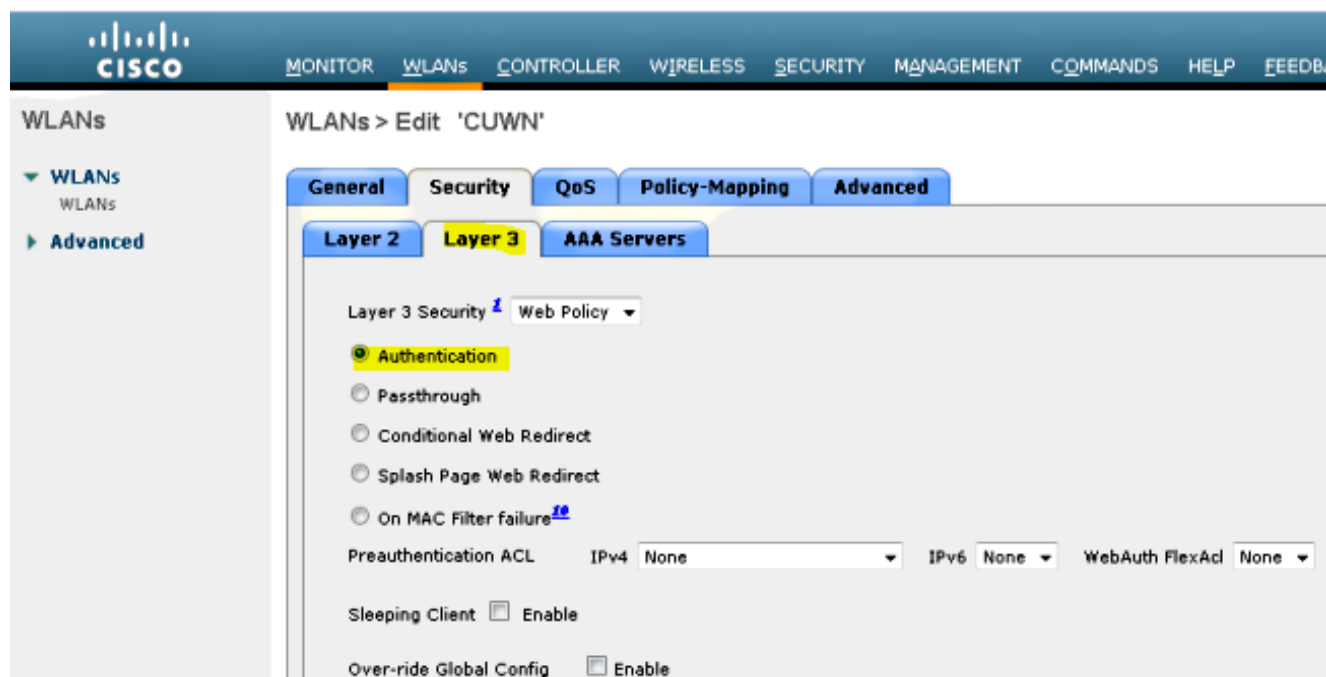
**Partie - Configuration sur 5508 l'ancre WLC**

1. Sur la gamme 5508 WLC, vol plané au-dessus de **WLAN > nouveau** afin de créer un

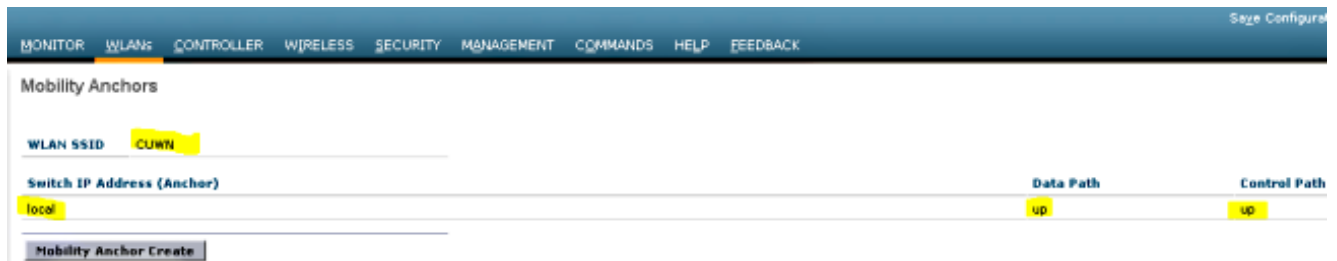
nouveau réseau local de radio (WLAN).



2. Le vol plané au-dessus de **WLAN > WLAN éditent > authentification Web activée par Security > Layer 3** afin de configurer le degré de sécurité de la couche 3.

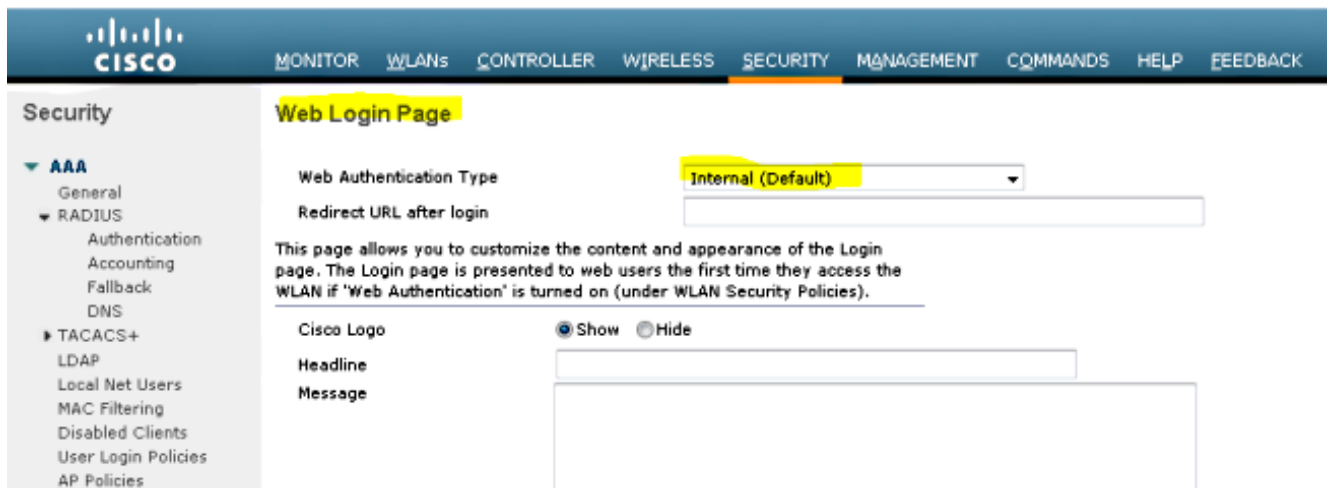


3. Faites les gens du pays d'adresse d'ancre sous la fenêtre de configuration d'ancre de mobilité WLAN afin d'ajouter la gamme 5508 WLC comme ancre.

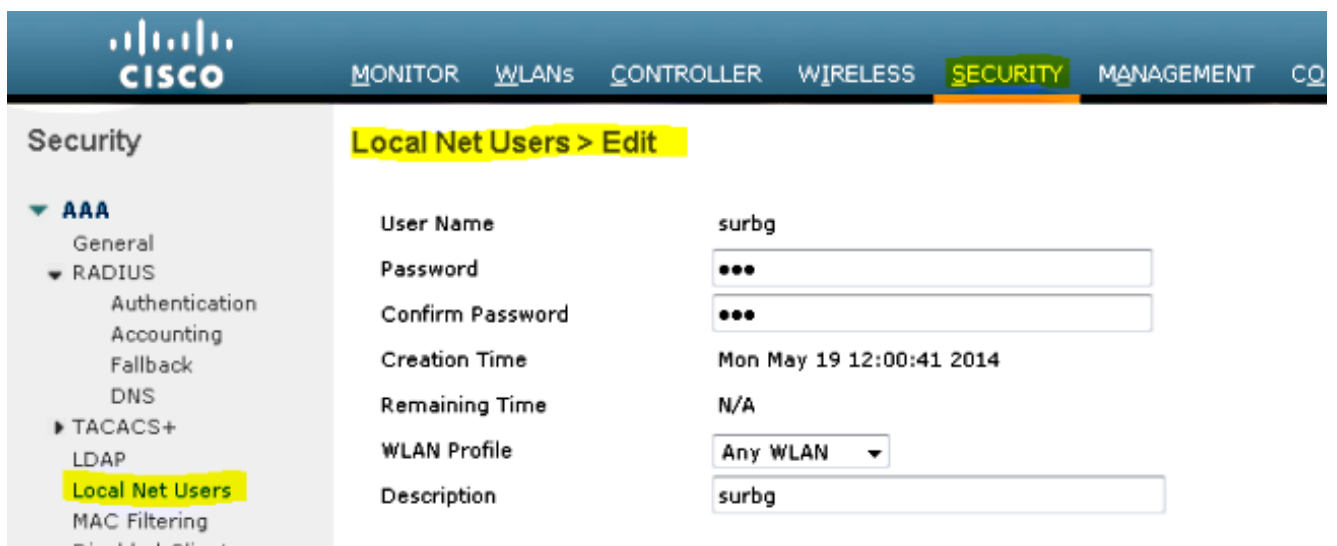


4. Cliquez au-dessus de la **page de Sécurité > de Webauth > de Webauth** afin de configurer la page de Webauth à utiliser pour l'authentification client.

Dans cet exemple, la page interne WLC Webauth est sélectionnée :



5. Créez un utilisateur du réseau local. Cette paire de nom d'utilisateur/mot de passe est utilisée par l'utilisateur une fois incitée à la page de Webauth.



## Partie - La configuration convergée de mobilité d'accès entre la gamme 5508/5760 WLC et la gamme Catalyst 3850 commutent

1. Sur la gamme 5508 WLC, ajoutez la gamme 5760 WLC en tant que pair de mobilité.

Static Mobility Group Members

Local Mobility Group	Mobile-1					
MAC Address	IP Address	Public IP Address	Group Name	Multicast IP		Status
58:8d:09:cd:ac:e60	10.105.135.151	10.105.135.151	Mobile-1	0.0.0.0		Up
00:00:00:00:00:00	10.105.135.178	10.105.135.178	surbg	0.0.0.0		Up
00:00:00:00:00:00	10.105.135.244	10.105.135.244	surbg	0.0.0.0		Up

2. Sur la gamme 5760 WLC, agissant en tant que Mobility Controller, ajoutez la gamme 5508 WLC en tant que pair de mobilité.

Mobility Peer

IP Address	Public IP Address	Group Name	Multicast IP	Control Link Status	Data Link Status
<input type="checkbox"/> 10.105.135.244	-	surbg	0.0.0.0	-	-
<input type="checkbox"/> 10.105.135.151	10.105.135.151	Mobile-1	0.0.0.0	UP	UP
<input type="checkbox"/> 10.105.135.178	10.105.135.178	surbg	0.0.0.0	UP	UP

3. Cette étape est très importante ! Ajoutez la gamme Catalyst 3850 commutant comme agent de mobilité sur la gamme 5760 WLC sous l'onglet de groupe de homologues de commutateur sous la gestion Peer de la mobilité.

Switch Peer Group > SURBG-SPG

IP Address	Public IP Address	Control Link Status	Data Link Status
<input type="checkbox"/> 10.105.135.226	10.105.135.226	UP	UP

4. Sur la gamme Catalyst 3850 commutez, ajoutez la gamme 5760 WLC comme Mobility Controller. Une fois que vous faites ceci, la gamme Catalyst 3850 commute des grippages le permis de coult AP de Mobility Controller 5760.

The screenshot shows the Cisco Wireless Controller GUI. The left sidebar is expanded to 'Mobility Management' > 'Mobility Global Config'. The main content area is titled 'Mobility Agent Configuration' and contains the following settings:

Mobility Role	Mobility Agent
Mobility Controller IP Address	10.105.135.244
Control Link Status	UP
Data Link Status	UP
Mobility Protocol Port	16666
Mobility Switch Peer Group Name	SURBG-SPG
DTLS Mode	Enabled
Mobility Domain ID for 802.11r	0xe699
Mobility Keepalive Interval (1-30)sec	10

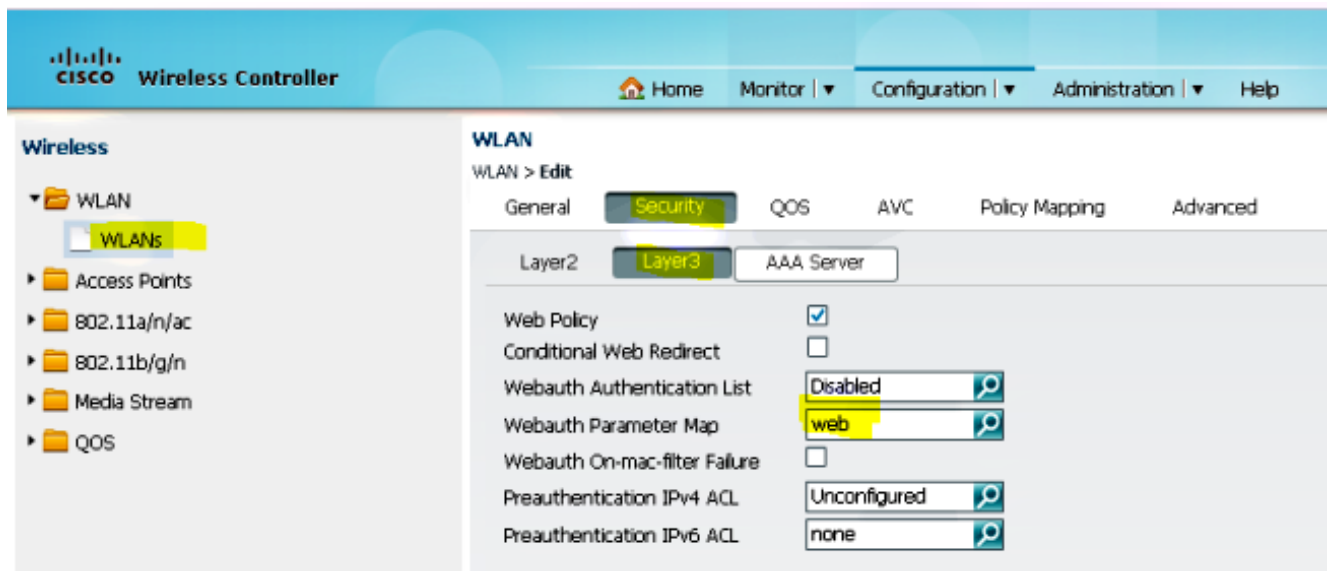
### Partie 3 : Configuration sur le commutateur étranger de gamme Catalyst 3850

1. Planent au-dessus de le **GUI > la configuration > la radio > le WLAN > nouveau** afin de configurer le SSID/WLAN précis sur la gamme Catalyst 3850 commutent.

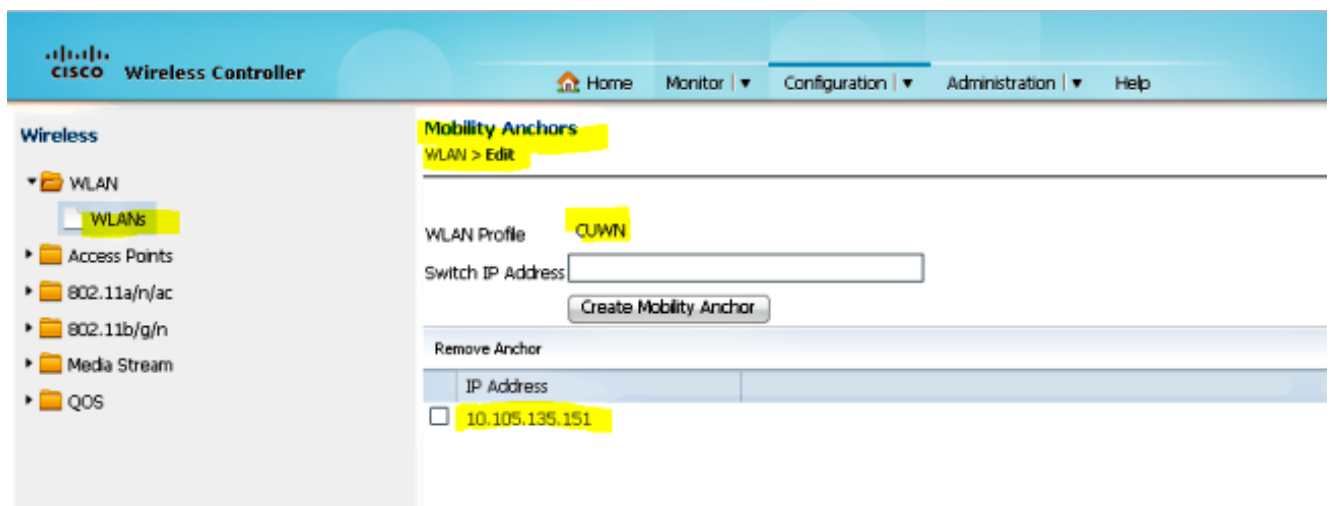
The screenshot shows the Cisco Wireless Controller GUI with the 'Configuration' tab selected. The left sidebar is expanded to 'WLAN' > 'WLANs'. The main content area is titled 'WLAN' and shows the configuration for a WLAN named 'CUWN'.

Profile Name	CUWN
Type	WLAN
SSID	CUWN
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth <small>(Modifications done under security tab will appear after applying the changes.)</small>
Radio Policy	All
Interface/Interface Group(G)	VLAN0060
Broadcast SSID	<input checked="" type="checkbox"/>
Multicast VLAN Feature	<input type="checkbox"/>

2. Le vol plané au-dessus de **WLAN > WLAN éditent > authentification Web activée par Security > Layer 3** afin de configurer le degré de sécurité de la couche 3.



3. Ajoutez l'IP address de la gamme 5508 WLC comme ancre sous la configuration d'ancre de mobilité WLAN



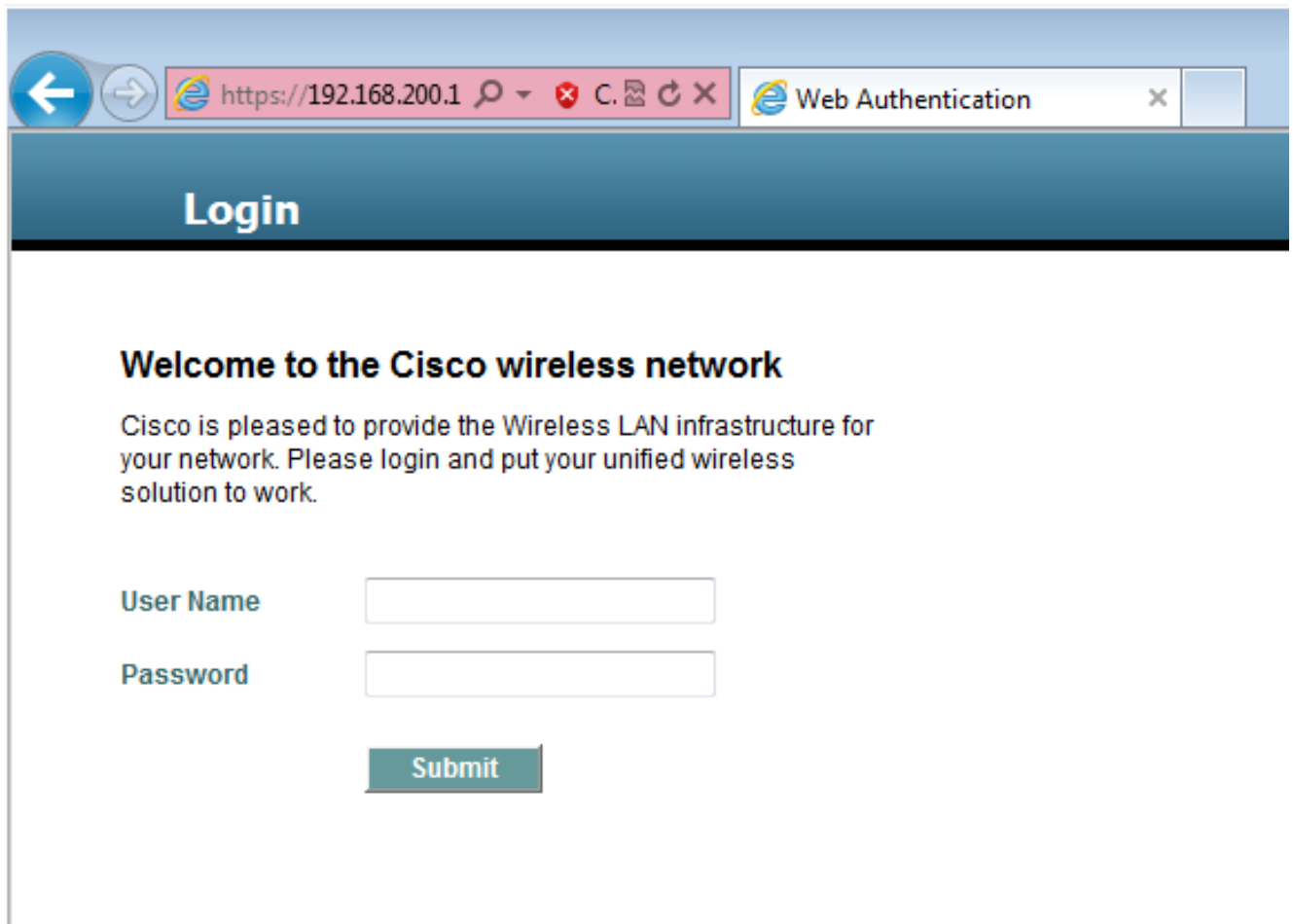
## Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

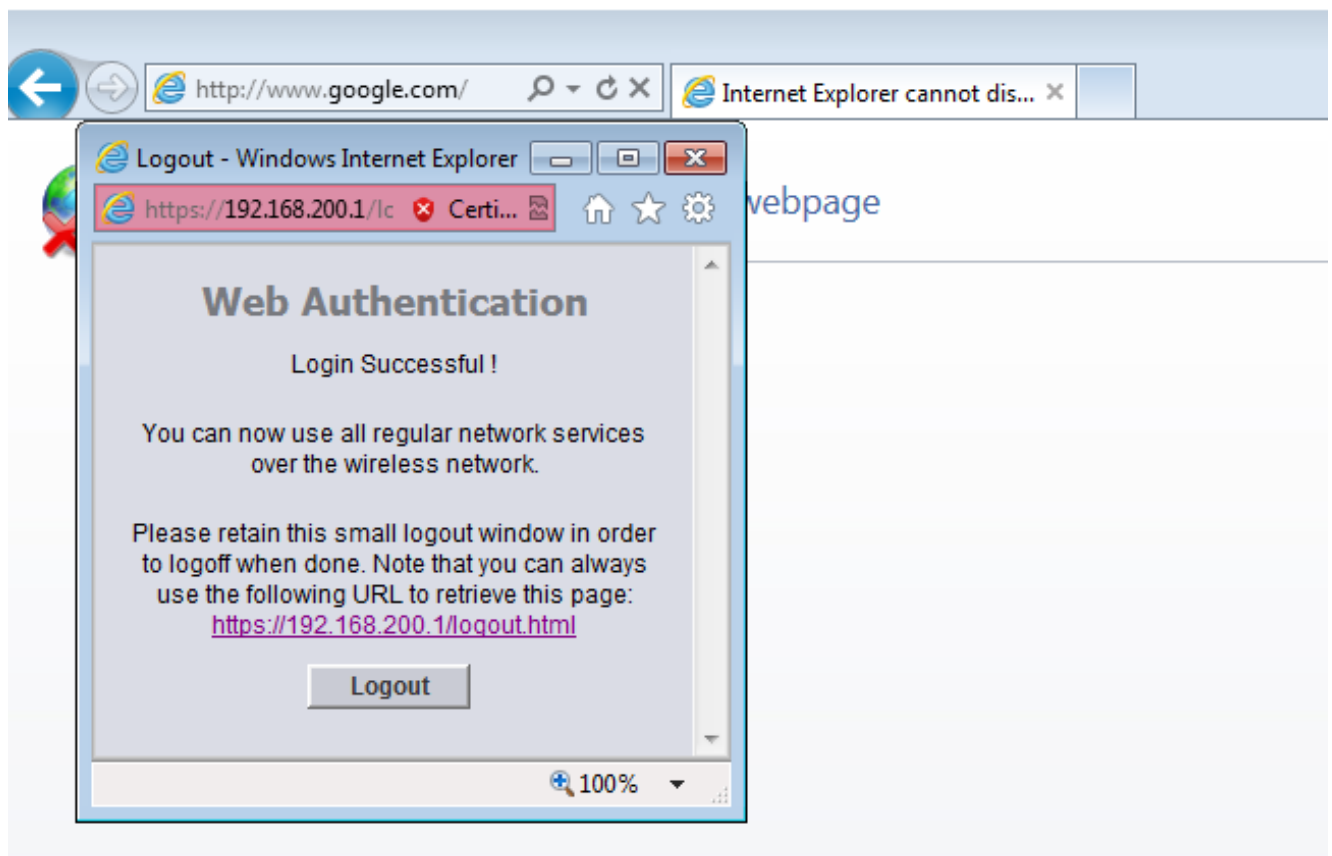
Connectez le client au réseau sans fil unifié Cisco WLAN (CUWN). Voici le flux des tâches :

1. Le client reçoit une adresse IP.
2. Le client ouvre un navigateur et accède à n'importe quel site Web.
3. Le premier paquet TCP envoyé par le client est détourné par le WLC, et le WLC intercepte et envoie la page de Webauth.
4. Si les DN est correctement configurés, le client obtient la page de Webauth.
5. Le client doit fournir le nom d'utilisateur/mot de passe afin d'obtenir authentifié.
6. Après l'authentification réussie, le client est réorienté à la page d'origine d'accès.





7. Après que le client fournisse les qualifications droites, le client passe l'authentique.



Dépannez

Afin de dépanner votre configuration, entrez dans ces derniers met au point sur la gamme 5508 WLC, qui agit en tant qu'ancre d'invité :

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

Voici un exemple :

```
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 msch  
  
*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 =

```

Voici la capture de paquet de côté client.

Le client obtient l'adresse 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

Le client ouvre un navigateur et tape [www.facebook.com](http://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.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

```

Le WLC intercepte le premier paquet TCP du client et pousse son adresse IP virtuelle et la page interne 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 [EIN ACK] Seq=471 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]

```

Après l'authentification Web réussie, le reste du flux des tâches se termine.

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=6192 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=1560 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 ctld1.windowsupdate.com
192.168.200.1	60.60.60.11	TCP	54 https > 49724 [ACK] Seq=139 Ack=196 win=6656 Len=0