

Exemple de configuration d'ancrage invité des contrôleurs LAN sans fil Unified Access avec accès convergé

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Partie 1 - Configuration sur le WLC d'ancrage 5508](#)

[Partie 2 - Configuration de la mobilité d'accès convergé entre le WLC de la gamme 5508/5760 et le commutateur de la gamme Catalyst 3850](#)

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

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer les contrôleurs LAN sans fil (WLC) de la gamme 5508/5760 et le commutateur de la gamme Catalyst 3850 pour l'ancre d'invité du client sans fil dans la nouvelle configuration de déploiement de mobilité où le WLC de la gamme 5508 agit en tant qu'ancre de mobilité et le commutateur de la gamme Catalyst 3850 agit en tant que contrôleur étranger de mobilité pour les clients. En outre, le commutateur de la gamme Catalyst 3850 agit comme agent de mobilité pour un WLC de la gamme 5760 qui agit comme contrôleur de mobilité à partir duquel le commutateur de la gamme Catalyst 3850 acquiert la licence de point d'accès (AP).

Conditions préalables

Exigences

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

- Interface graphique utilisateur ou CLI de Cisco IOS[®] avec les WLC d'accès convergé des gammes 5760 et 3650 et le commutateur de la gamme Catalyst 3850
- Accès GUI et CLI avec le WLC 5508
- Configuration 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 :

- Cisco 5760 version 3.3.3 (armoire de répartition nouvelle génération [NGWC])
- Commutateur de la gamme Catalyst 3850
- WLC de la gamme Cisco 5508, version 7.6.120
- Points d'accès légers Cisco 3602
- Commutateurs Cisco Catalyst, série 3560

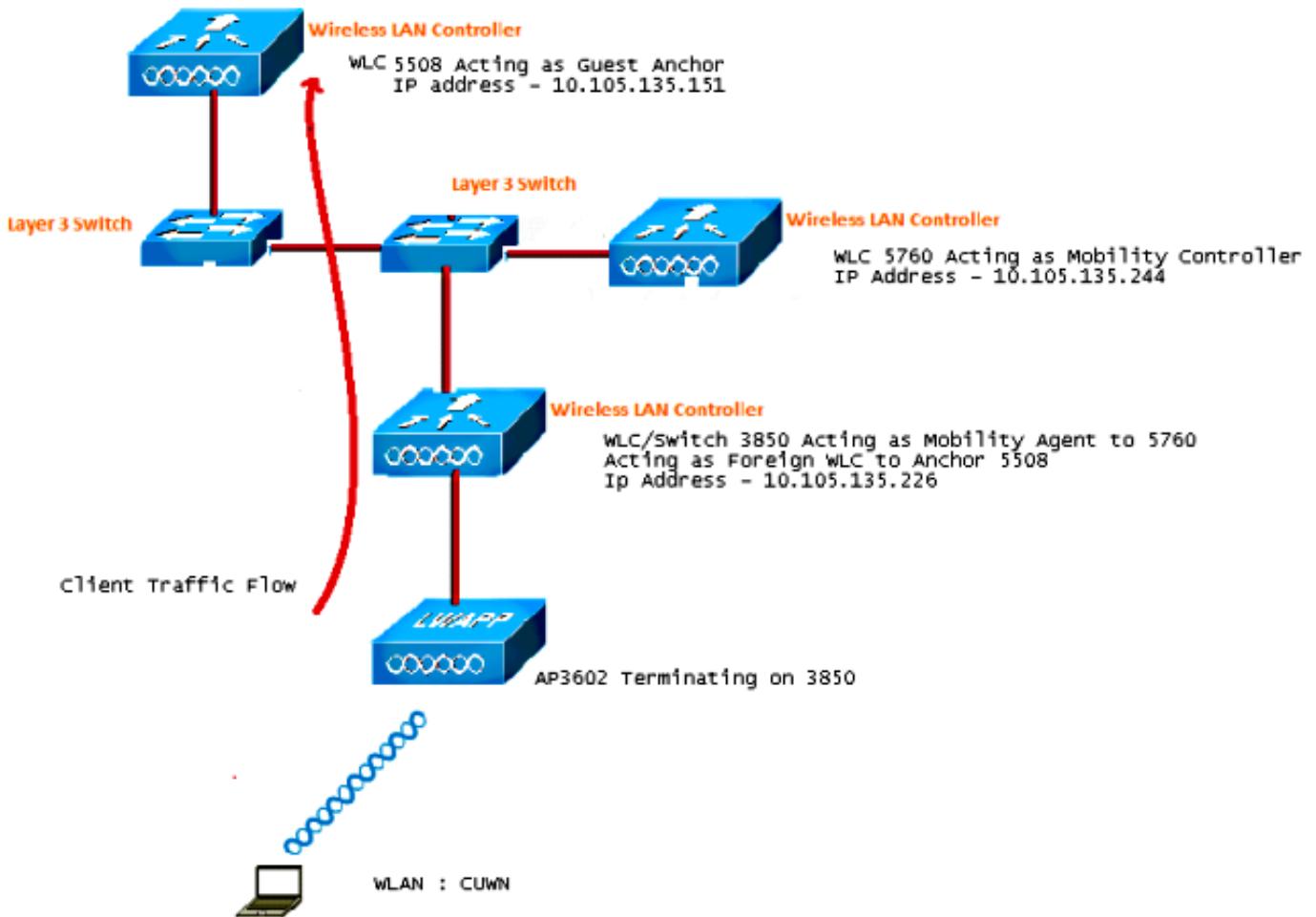
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Le WLC de la gamme 5508 agit en tant que contrôleur d'ancre, et le commutateur de la gamme Catalyst 3850 agit en tant que contrôleur étranger et agent de mobilité qui obtient la licence du contrôleur de mobilité 5760.



Remarque : dans le schéma de réseau, le WLC de la gamme 5508 agit en tant que contrôleur d'ancrage, le WLC de la gamme 5760 agit en tant que contrôleur de mobilité et le commutateur de la gamme Catalyst 3850 agit en tant qu'agent de mobilité et WLC étranger. À tout moment, le contrôleur d'ancrage pour le commutateur de la gamme Catalyst 3850 est le WLC de la gamme 5760 ou le WLC de la gamme 5508. Les deux ne peuvent pas être des ancrages en même temps, car la double ancre ne fonctionne pas.

Configurations

La configuration comprend trois parties :

Partie 1 - Configuration sur le WLC d'ancrage 5508

Partie 2 - Configuration de la mobilité d'accès convergé entre le WLC de la gamme 5508/5760 et le commutateur de la gamme Catalyst 3850

Partie 3 - Configuration sur le commutateur étranger de la gamme Catalyst 3850

Partie 1 - Configuration sur le WLC d'ancrage 5508

1. Sur le WLC de la gamme 5508, passez le curseur sur **WLAN > New** afin de créer un

nouveau WLAN (Wireless LAN).

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes MONITOR, WLANS (highlighted in yellow), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar has a tree view with WLANS expanded, showing WLANS and Advanced. Under Advanced, there is a 'WLANs' entry. The main content area is titled 'WLANS > Edit 'CUWN''. A tab bar at the top of this section includes General, Security (highlighted in blue), QoS, Policy-Mapping, and Advanced. The General tab displays the following configuration:

Profile Name	CUWN
Type	WLAN
SSID	CUWN
Status	<input checked="" type="checkbox"/> Enabled

Below this, under 'Security Policies', it says 'WEB POLICY, Web-Auth'. A note states '(Modifications done under security tab will appear after applying the changes.)'. The following parameters are listed:

Radio Policy	All
Interface/Interface Group(G)	vlan60
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	5508

2. Passez le curseur sur WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication afin de configurer la sécurité de la couche 3.

The screenshot shows the same Cisco WLC interface, but the focus is on the 'Layer 3' tab of the 'Security' section for the 'CUWN' WLAN. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled 'WLANS > Edit 'CUWN''. The tab bar now includes General, Security (highlighted in blue), QoS, Policy-Mapping, Advanced, Layer 2, Layer 3 (highlighted in yellow), and AAA Servers. The Layer 3 tab displays the following configuration:

Layer 3 Security: Web Policy

Authentication (radio button selected):

- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter failure

Preattentation ACL: IPv4 None, IPv6 None, WebAuth FlexAc None

Sleeping Client: Enable

Over-ride Global Config: Enable

3. Définissez l'adresse d'ancre local dans la fenêtre de configuration de l'ancre de mobilité WLAN afin d'ajouter le WLC de la gamme 5508 en tant qu'ancre.

WLAN SSID: CUWN

Switch IP Address (Anchor): local

Data Path: up Control Path: up

Mobility Anchor Create

4. Passez le curseur sur **Security > Webauth > Webauth** page afin de configurer la page Webauth à utiliser pour l'authentification du client.

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

Web Login Page

Web Authentication Type: Internal (Default)

Redirect URL after login:

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo: Show Hide

Headline

Message

5. Créez un utilisateur réseau local. Cette paire nom d'utilisateur/mot de passe est utilisée par l'utilisateur lorsque vous y êtes invité sur la page Webauth.

Local Net Users > Edit

User Name:	surbg
Password:	***
Confirm Password:	***
Creation Time:	Mon May 19 12:00:41 2014
Remaining Time:	N/A
WLAN Profile:	Any WLAN
Description:	surbg

Partie 2 - Configuration de la mobilité d'accès convergé entre le WLC de la gamme 5508/5760 et le commutateur de la gamme Catalyst 3850

1. Sur le WLC de la gamme 5508, ajoutez le WLC de la gamme 5760 comme homologue de mobilité.

The screenshot shows the Cisco Wireless Controller (WLC) interface. The navigation bar at the top includes links for MONITOR, WLANS, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a tree view under 'Controller' shows 'Static Mobility Group Members'. Under 'Mobility Management', 'Mobility Groups' is selected. The main pane displays a table titled 'Local Mobility Group Mobile-1' with three rows:

MAC Address	IP Address	Public IP Address	Group Name	Multicast IP	Status
58:8d:09:cd:e0:60	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

- Sur le WLC de la gamme 5760, agissant en tant que contrôleur de mobilité, ajoutez le WLC de la gamme 5508 en tant qu'homologue de mobilité.

The screenshot shows the 'Configuration' tab of the Cisco WLC interface. The left sidebar shows 'Controller' settings, including 'Mobility Management' with 'Mobility Peer' selected. The main pane is titled 'Mobility Peer' and displays a table with three entries:

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

- Cette étape est très importante ! Ajoutez le commutateur de la gamme Catalyst 3850 en tant qu'agent de mobilité sur le WLC de la gamme 5760 sous l'onglet Switch Peer Group sous Mobility Management.

The screenshot shows the 'Configuration' tab of the Cisco WLC interface. The left sidebar shows 'Controller' settings, including 'Mobility Management' with 'Switch Peer Group' selected. The main pane is titled 'Switch Peer Group > SURBG-SPG' and displays a table with one entry:

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

- Sur le commutateur de la gamme Catalyst 3850, ajoutez le WLC de la gamme 5760 en tant que contrôleur de mobilité. Une fois que vous avez fait cela, le commutateur de la gamme Catalyst 3850 saisit la licence AP coult du contrôleur de mobilité 5760.

Mobility Agent Configuration

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 la gamme Catalyst 3850

- Passez le curseur sur GUI > Configuration > Wireless > WLAN > New afin de configurer le SSID/WLAN exact sur le commutateur de la gamme Catalyst 3850.

WLAN
WLAN > Edit

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

- Passez le curseur sur WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication afin de configurer la sécurité de la couche 3.

The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'WLAN' is expanded, and 'WLANS' is selected. The main panel title is 'WLAN' with 'WLAN > Edit'. Below it, tabs for 'General', 'Security' (highlighted in yellow), 'QoS', 'AVC', 'Policy Mapping', and 'Advanced' are present. Under 'Layer2' and 'Layer3' (also highlighted in yellow), several configuration options are listed with checkboxes and dropdown menus. The 'Web Policy' checkbox is checked. The 'Conditional Web Redirect' checkbox is unchecked. The 'Webauth Authentication List' dropdown is set to 'Disabled'. The 'Webauth Parameter Map' dropdown is set to 'web'. The 'Webauth On-mac-filter Failure' checkbox is unchecked. The 'Preauthentication IPv4 ACL' dropdown is set to 'Unconfigured'. The 'Preauthentication IPv6 ACL' dropdown is set to 'none'.

- Ajoutez l'adresse IP WLC de la gamme 5508 comme point d'ancre dans la configuration d'ancre de mobilité WLAN

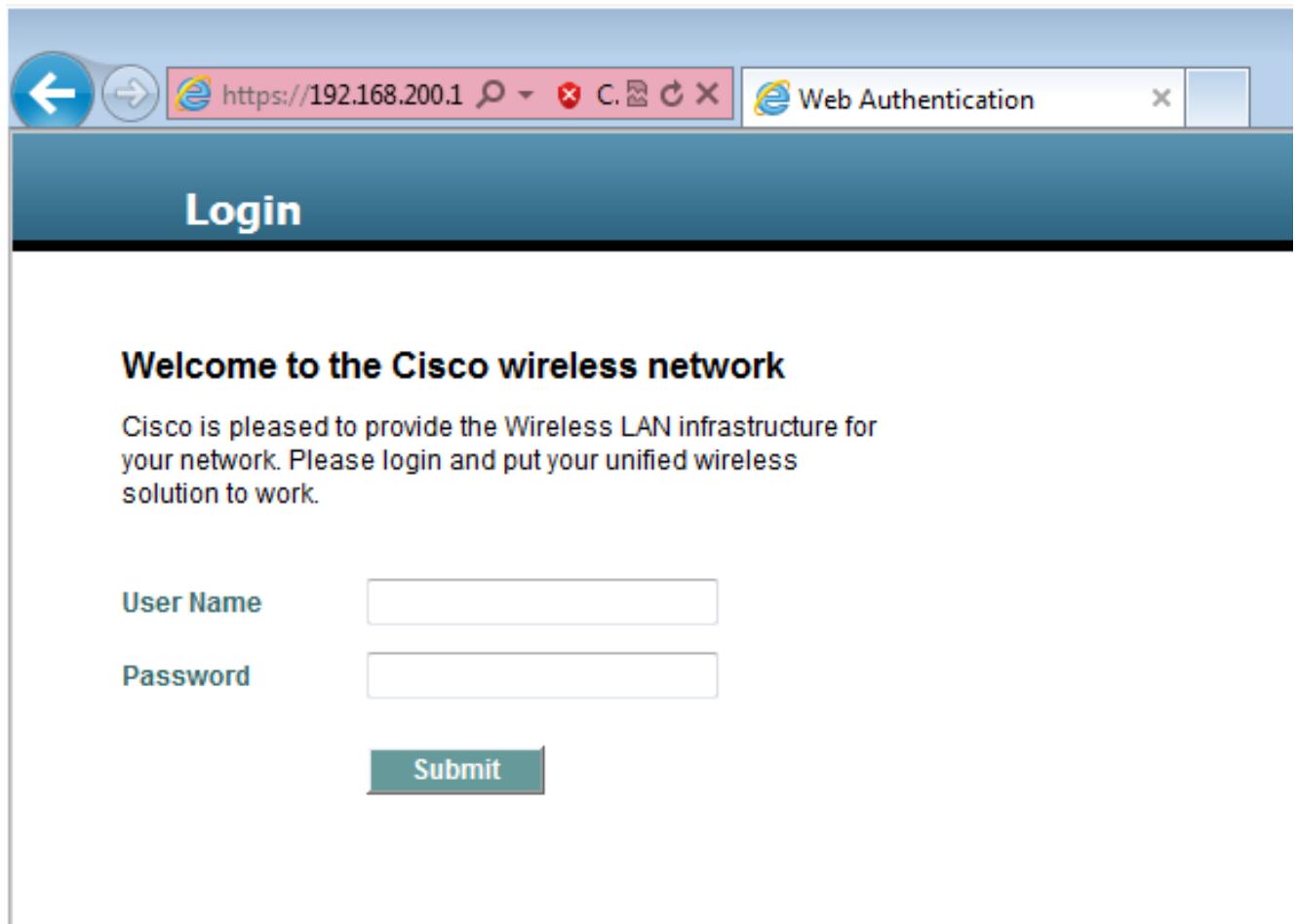
The screenshot shows the Cisco Wireless Controller interface. In the left sidebar under 'Wireless', 'WLAN' is expanded, and 'WLANS' is selected. The main panel title is 'Mobility Anchors' with 'WLAN > Edit'. Below it, 'WLAN Profile' is set to 'CUWN'. A 'Switch IP Address' input field is empty. A 'Create Mobility Anchor' button is visible. Under 'Remove Anchor', there is a table with one row. The first column is 'IP Address' and the second column contains '10.105.135.151' with an associated checkbox.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

- Le client reçoit une adresse IP.
- Le client ouvre un navigateur et accède à n'importe quel site Web.
- Le premier paquet TCP envoyé par le client est détourné par le WLC, qui intercepte et envoie la page Webauth.
- Si le DNS est correctement configuré, le client obtient la page Webauth.
- Le client doit fournir le nom d'utilisateur/mot de passe pour être authentifié.
- Une fois l'authentification réussie, le client est redirigé vers la page d'accès d'origine.



The screenshot shows a web browser window with the URL <https://192.168.200.1>. The title bar says "Web Authentication". The main content is a "Login" page with the heading "Welcome to the Cisco wireless network". It instructs the user to log in and provides fields for "User Name" and "Password", along with a "Submit" button.

Welcome to the Cisco wireless network

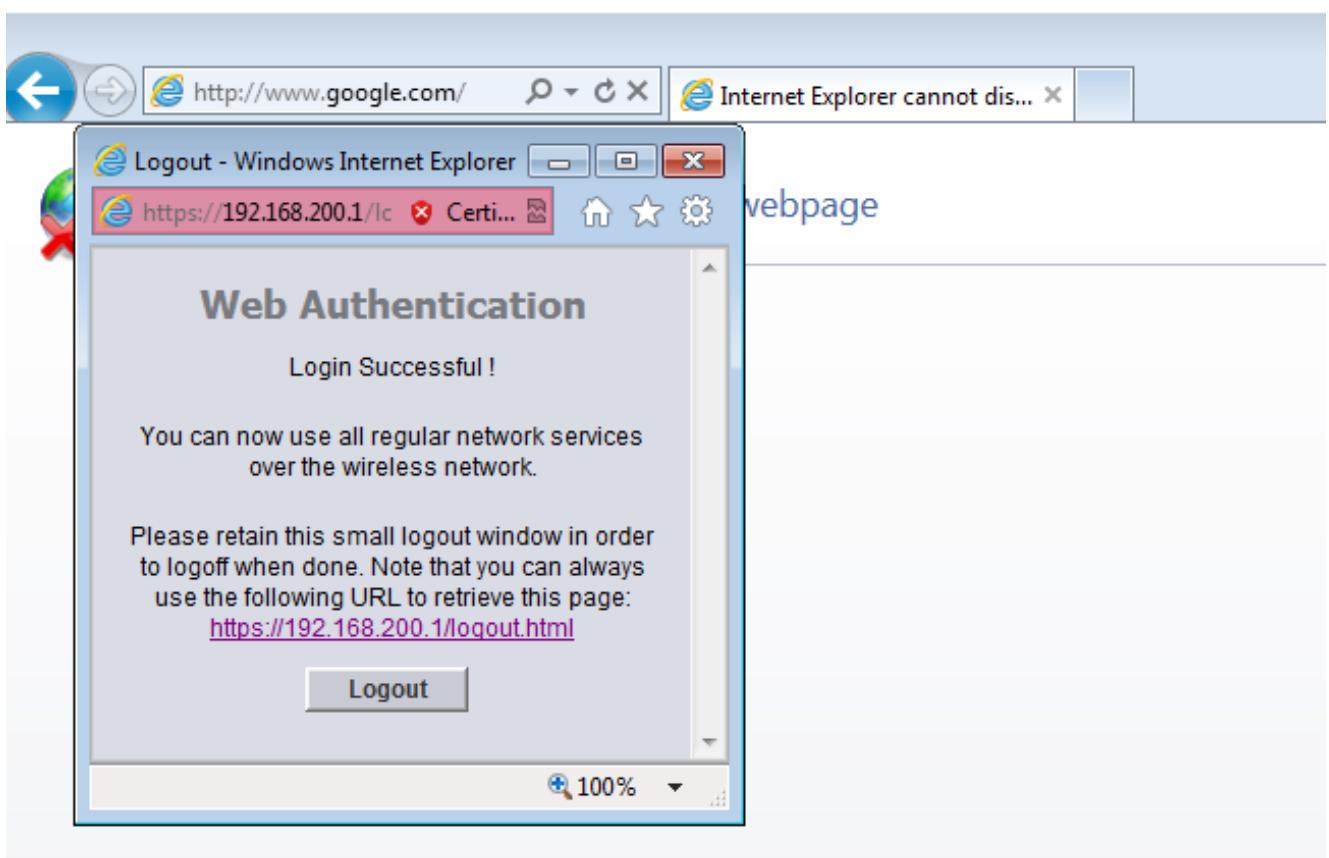
Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

Submit

7. Une fois que le client a fourni les informations d'identification appropriées, il passe l'authentification.



Dépannage

Afin de dépanner votre configuration, entrez ces débogages sur le WLC de la gamme 5508, qui agit comme un ancrage invité :

```
Debug Client
```

```
Debug web-auth redirect enable mac
```

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 msrb

*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: fe80:0000:0000:6cla: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: fe80:0000:0000:0000:6cla: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 fe80:0000:0000:0000:6cla: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::6cla:b253:d711:c7f updated to msrb. Not Advancing pem state.Current state: msrb 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:
fe80:0000:0000:6cla: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)
*DHP 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
*DHP 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
*DHP 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)
*DHP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
REQUEST (3)
*DHP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP op: BOOTREQUEST,
htype: Ethernet, hlen: 6, hops: 1
*DHP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP xid: Oxad00ada3
(2902502819), secs: 3072, flags: 0
*DHP Socket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a

```

```

*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 0.0.0.0
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 60.60.60.2
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP requested ip:
60.60.60.11
*DHCPSocket 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)
*DHCPSocket 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
*DHCPSocket 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)
*DHCPSocket 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 0x0c00)
*DHCPSocket 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)
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCPSocket 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 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
*DHCPSocket 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)
*DHCPSocket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCPSocket 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 PLUMBAUTHPATH: 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 paquets 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.

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 0xah1b 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 transmet son adresse IP virtuelle et la page Webauth interne.

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

Une fois l'authentification Web réussie, le reste du processus est terminé.

60.60.60.11	50.50.50.251	DNS	86 Standard query 0x64dd A fe9cvlist.ie.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 ctld1.windowsupdate.com
192.168.200.1	60.60.60.11	TCP	54 https > 49724 [ACK] Seq=139 Ack=196 win=6656 Len=0

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.