

# Comprendre le flux CWA sur un client

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Flux CWA - Suivi radioactif \(RA\)](#)

[Première connexion : client vers serveur ISE](#)

[Deuxième connexion : du client au réseau](#)

[Flux CWA - Capture de paquets intégrée \(EPC\)](#)

[Première connexion : client vers serveur ISE](#)

[Deuxième connexion : du client au réseau](#)

---

## Introduction

Ce document décrit le flux du client final lors de la connexion à un WLAN CWA.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir des connaissances de base sur :

- Contrôleur LAN sans fil Cisco (WLC) série 9800
- Compréhension générale de l'authentification Web centrale (CWA) et de sa configuration sur Identity Services Engine (ISE)

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

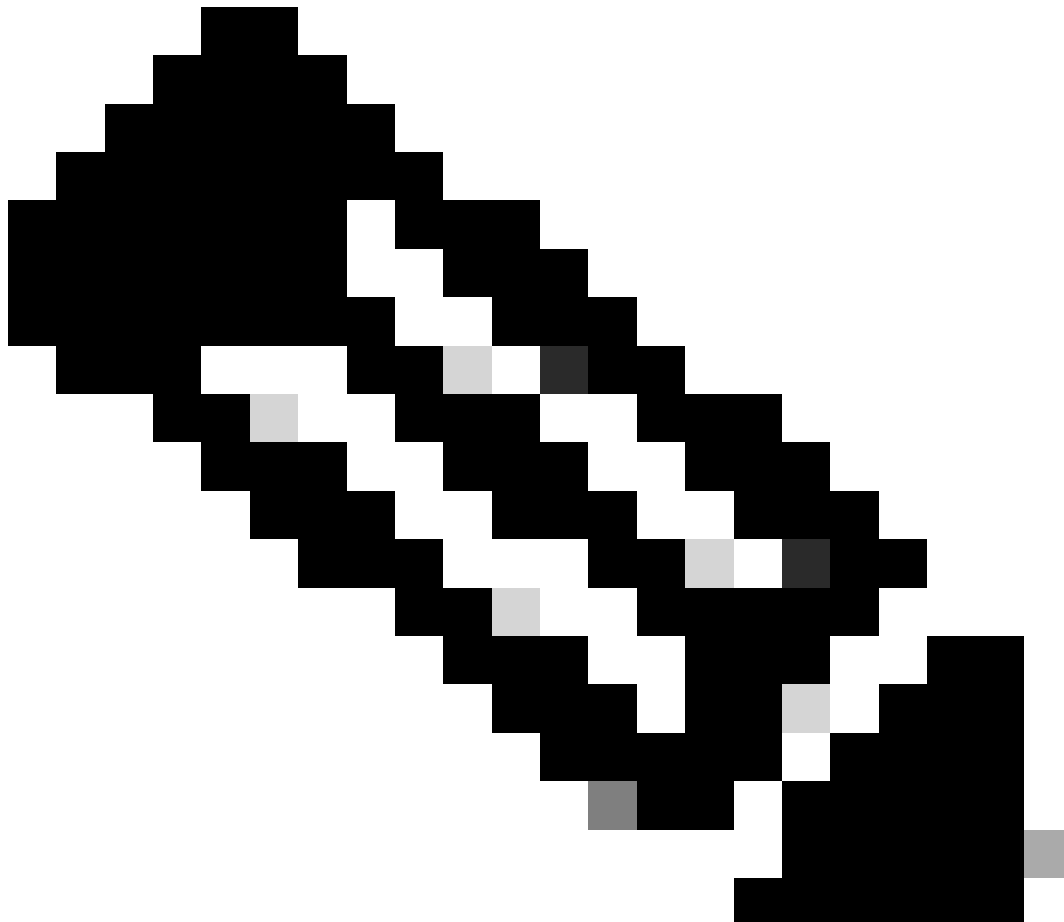
- WLC 9800-CL
- Cisco AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- Identity Service Engine (ISE) v3.1

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

CWA est un type d'authentification SSID qui peut être configuré sur le WLC où le client final essayant de se connecter est invité à entrer son nom d'utilisateur et son mot de passe sur un portail Web qui lui est présenté. En bref, le flux du client final lors de la connexion au WLAN est le suivant :

1. Le client final se connecte au SSID affiché sur son périphérique
2. Le client final est redirigé vers le portail Web pour entrer ses informations d'identification
3. Le client final est authentifié par ISE avec les informations d'identification entrées
4. ISE répond au WLC en disant que le client final a été authentifié. ISE peut transmettre certains attributs supplémentaires que le client doit respecter lors de l'accès au réseau (tels que des listes de contrôle d'accès spécifiques)
5. Le client final est ré-associé et ré-authentifié, puis accède au réseau



Remarque : il est important de noter que le client final authentifié deux fois est transparent pour le client final

Le processus sous-jacent par lequel le client doit passer est divisé en deux : une connexion du client au serveur ISE et, une fois authentifié, une autre connexion du client au réseau lui-même. Le contrôleur et ISE communiquent toujours entre eux via le protocole RADIUS. Ci-dessous, une analyse approfondie d'une trace radioactive (RA) et d'une capture de paquets intégrée (EPC).

## Flux CWA - Suivi radioactif (RA)

Une trace RA est un ensemble de journaux capturés pour un client spécifique. Elle montre l'ensemble du processus que le client est en train de suivre lors de la connexion à un WLAN. Pour plus d'informations sur ce qu'ils sont et comment récupérer des traces RA, veuillez visiter [Comprendre les débogages sans fil et la collection de journaux sur les contrôleurs LAN sans fil Catalyst 9800.](#)

### Première connexion : client vers serveur ISE

Le WLC n'autorise pas une connexion au réseau si le client n'a pas été autorisé par ISE auparavant.

#### Association au WLAN

Le WLC détecte que le client veut s'associer au WLAN « cwa », qui est lié au profil de politique « cwa-policy-profile » et se connecte au point d'accès « BC-3802 »

```
<#root>
```

```
[client-orch-sm] [17558]: (note): MAC: 4203.9522.e682
```

```
Association received.
```

```
  BSSID dc8c.37d0.83af,
```

```
WLAN cwa
```

```
, Slot 1 AP dc8c.37d0.83a0, BC-3802
```

```
[client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Received Dot11 association request. Processing s
```

```
SSID: cwa
```

```
,
```

```
Policy profile: cwa-policy-profile
```

```
,
```

```
AP Name: BC-3802
```

```
, Ap Mac Address: dc8c.37d0.83a0 BSSID MAC0000.0000.0000 wlan ID: 1RSSI: -46, SNR: 40
```

```
[client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition:
```

```
  s_CO_INIT -> s_CO_ASSOCIATING
```

```
[dot11-validate] [17558]: (info): MAC: 4203.9522.e682 WiFi direct: Dot11 validate P2P IE. P2P IE not pr
```

## Filtrage MAC

### Tester la connectivité du serveur ISE

Une fois que le WLC a reçu la demande d'association du client, la première étape consiste à effectuer le filtrage MAC (également connu sous le nom de MAB). Le filtrage MAC est une méthode de sécurité dans laquelle l'adresse MAC du client est comparée à une base de données pour vérifier si ces derniers sont autorisés à se connecter au réseau ou non.

```
<#root>
```

```
[dot11] [17558]: (info): MAC: 4203.9522.e682 DOT11 state transition:
```

```
S_DOT11_INIT -> S_DOT11_MAB_PENDING <-- The WLC is waiting for ISE to authenticate the user. It does not
```

```
[client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_CO_ASSOCIATING -> S_CO_ASSOCIATED
```

```
[client-auth] [17558]: (note): MAC: 4203.9522.e682 MAB Authentication initiated.
```

```
Policy VLAN 0, AAA override = 1, NAC = 1 <-- no VLAN is assigned as ISE can do that
```

```
[sanet-shim-translate] [17558]: (ERR): 4203.9522.e682 wlan_profile Not Found : Device information attri
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Session Start event called from SANET-SHIM
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wireless session sequence, create context
```

```
[auth-mgr-feat_wireless] [17558]: (info): [4203.9522.e682:capwap_90000005] -
```

```
authc_list: cwa_authz <-- Authentication method list used
```

```
[auth-mgr-feat_wireless] [17558]: (info): [4203.9522.e682:capwap_90000005] - authz_list: Not present un
```

```
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_INITIATED
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:unknown] auth mgr attr change notification is received for .
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Retrieved Client IIF ID 0x530002f1
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Allocated audit session id 0E1E140A0000000
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Applying policy for WlanId: 1, bssid : dc8
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wlan vlan-id from bssid hd1 0
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] SM Reauth Plugin: Received valid timeout=
```

```
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

```
MAB authentication started for 4203.9522.e682
```

```
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_AWAITING
```

```
[ewlc-infra-evq] [17558]: (note): Authentication Success. Resolved Policy bitmap:11 for client 4203.9522.e682
```

```
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_MAB_PENDING
```

```
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '
```

```
MAB_CONTINUE
```

```
' on handle 0x8A000002
```

```
<-- ISE server connectivity has been tested, the WLC is about to send the MAC address to ISE
```

```
[caaa-author] [17558]: (info): [CAAA:AUTHOR:92000002] DEBUG: mlist=cwa_authz for type=1
```

## WLC envoie une requête à ISE

Le WLC envoie un paquet de demande d'accès RADIUS à ISE contenant l'adresse MAC du client qui veut s'authentifier auprès du WLAN.

```
<#root>
```

```
[radius] [17558]: (info): RADIUS: Send
```

```
Access-Request
```

```
to
```

```
<ise-ip-addr>:1812
```

```
id 0/
```

```
28
```

```
, len 415
```

```
<-- The packet is traveling via RADIUS port 1812. The "28" is the session ID and it is unique for every
```

```
[radius] [17558]: (info): RADIUS: authenticator e7 85 1b 08 31 58 ee 91 - 17 46 82 79 7d 3b c4 30
```

```
[radius] [17558]: (info): RADIUS: User-Name [1] 14 "
```

```
42039522e682
```

```
"
```

```
<-- MAC address that is attempting to authenticate
```

```
[radius] [17558]: (info): RADIUS: User-Password [2] 18 *
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 25 "
```

```
service-type=Call Check
```

```
"
```

```
<-- This indicates a MAC filtering process
```

```
[radius] [17558]: (info): RADIUS: Framed-MTU [12] 6 1485
```

```
[radius] [17558]: (info): RADIUS: Message-Authenticator[80] 18 ...
```

```
[radius] [17558]: (info): RADIUS: EAP-Key-Name [102] 2 *
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 43 "audit-session-id=0E1E140A0000000C8E2
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 12 "
```

```
method=mab
```

```
"
```

```
<-- Controller sends an AVpair with MAB method
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 26 "client-iif-id=1392509681"
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 14 "vlan-id=1000"
```

```
[radius] [17558]: (info): RADIUS: NAS-IP-Address [4] 6
```

```
<wmi-ip-addr> <-- WLC WMI IP address
```

```
[radius] [17558]: (info): RADIUS: NAS-Port-Id [87] 17 "capwap_90000005"
```

```
[radius] [17558]: (info): RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19]
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 30 "
```

```
cisco-wlan-ssid=cwa
```

```
"
```

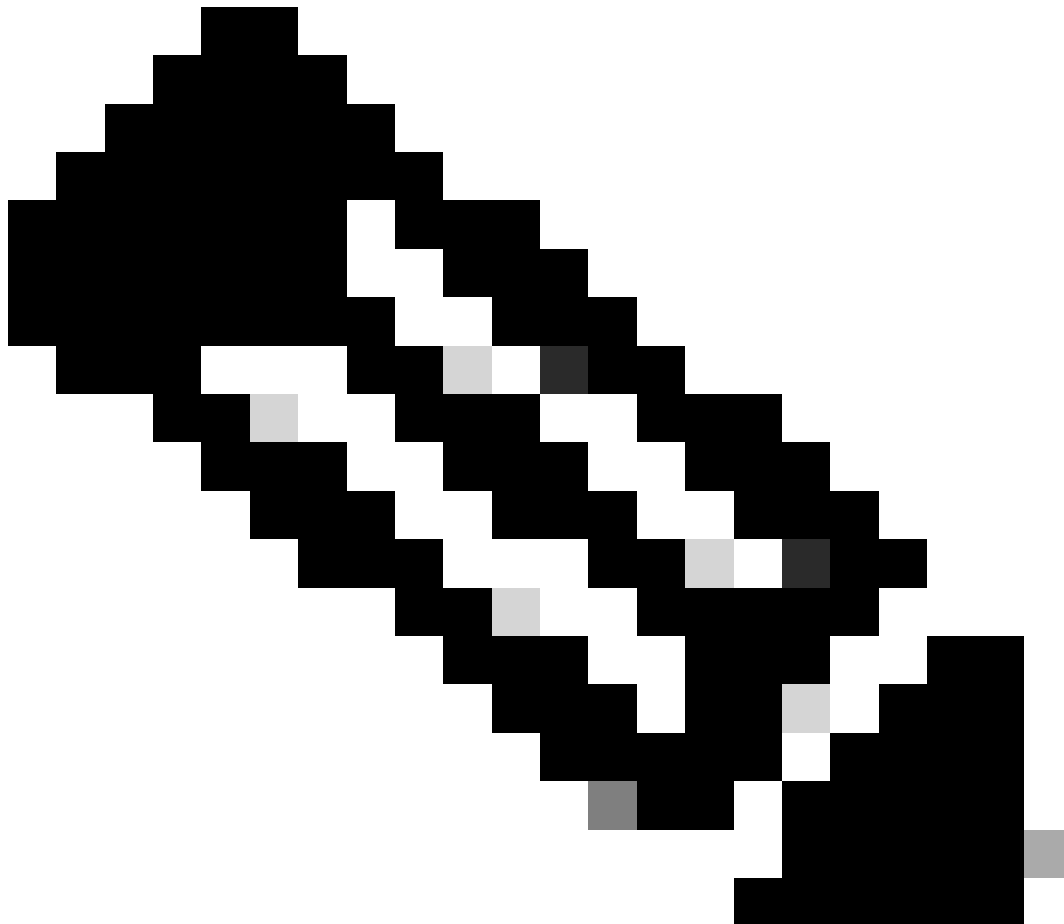
```
<-- SSID and WLAN the client is attempting to connect
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 32 "
```

```
wlan-profile-name=cwa
```

```
"
```

```
[radius] [17558]: (info): RADIUS: Called-Station-Id [30] 32 "dc-8c-37-d0-83-a0:cwa"
[radius] [17558]: (info): RADIUS: Calling-Station-Id [31] 19 "42-03-95-22-e6-82"
[radius] [17558]: (info): RADIUS: Airespace-WLAN-ID [1] 6 1
[radius] [17558]: (info): RADIUS: Nas-Identifier [32] 9 "BC-9800"
[radius] [17558]: (info): RADIUS: Started 5 sec timeout
```



Remarque : une paire AV est « Attribute-Value » utilisée par ISE. Il s'agit d'une structure

---

Key-Value d'informations prédéfinies qui peuvent être envoyées au WLC. Ces valeurs sont appliquées à ce client spécifique pour cette session spécifique.

Exemples de paires AV :

- Nom ACL
- URL de redirection
- Attribution de VLAN
- Temporisation de session
- Minuteurs de réauthentification

---

## ISE répond à la requête WLC

Si l'adresse MAC envoyée par le WLC est acceptée par ISE, alors ISE envoie un paquet Access-Accept RADIUS. En fonction de la configuration ISE, s'il s'agit d'une adresse MAC inconnue, ISE doit l'accepter et poursuivre le flux. Si vous voyez un Access-Reject, alors il y a quelque chose de mal configuré sur ISE qui doit être vérifié.

```
<#root>
```

```
[radius] [17558]: (info): RADIUS: Received from id
```

```
1812
```

```
/
```

```
28
```

```
<ise-ip-addr>
```

```
:0,
```

```
Access-Accept
```

```
, len 334
```

```
<-- The packet is traveling via RADIUS port 1812 and is has a session ID of 28 (as a response to the abo
```

```
[radius] [17558]: (info): RADIUS: authenticator 14 0a 6c f7 01 b2 77 6a - 3d ba f0 ed 92 54 9b d6
```

```
[radius] [17558]: (info): RADIUS: User-Name [1] 19 "
```

```
42-03-95-22-E6-82
```

```
"
```

```
<-- MAC address of the client that was authorized by ISE
```

```
[radius] [17558]: (info): RADIUS: Class [25] 51 ...
```

```
[radius] [17558]: (info): RADIUS: Message-Authenticator[80] 18 ...
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 31 "
```

```
url-redirect-acl=cwa-acl
```

```
"
```

```
<-- ACL to be applied to the client
```

```
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 183 "
```

```
url-redirect=https://<ise-ip-addr>:8443/portal/[...]
```

```
"
```

```
<-- Redirection URL for the client
```

```
[radius] [17558]: (info): Valid Response Packet, Free the identifier
```

```
[eap-auth] [17558]: (info): SUCCESS for EAP method name: Identity on handle 0xB0000039
```

```
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

```
MAB received an Access-Accept
```

```
for 0x8A000002
```

```
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '
```

```
MAB_RESULT
```

```
' on handle 0x8A000002
```

```
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Authc success from MAB,
```

```
Auth event success
```

## Processus WLC des informations reçues d'ISE

Le WLC traite toutes les informations reçues d'ISE. Avec elle, il applique le profil utilisateur qu'il avait créé à l'origine avec celui des données envoyées par ISE. Le WLC attribue une nouvelle liste de contrôle d'accès à l'utilisateur, par exemple. Si AAA Override n'est pas activé sur le WLAN, ce traitement par le WLC ne se produit pas.

```
<#root>
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
```

```
<< username 0 "42-03-95-22-E6-82">> <-- Processing username received from ISE
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
```

```
<< class 0 43 41 43 53 3a 30 45 31 45 31 34 30 41 30 30 30 30 30 30 43 38 45 32 44 41 36 34 32 3a 62
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
```

```
<<Message-Authenticator 0 <hidden>>>
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
```

```
<<
```

```
url-redirect-acl 0 "cwa-acl"
```

```
>>
```

```
<-- Processing ACL redirection received from ISE
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
```

```
<<
```

```
url-redirect 0 "https://<ise-ip-addr>:8443/portal/[...]"
```



>>

<-- Processing URL redirection received from ISE

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< dnis 0 "DC-8C-37-D0-83-A0">>

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< formatted-clid 0 "42-03-95-22-E6-82">>

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< audit-session-id 0 "0E1E140A0000000C8E2DA642">>

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< method 0 2 [mab]>>

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< clid-mac-addr 0 42 03 95 22 e6 82 >>

{wncd\_x\_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< intf-id 0 2415919109 (0x90000005)>>

{wncd\_x\_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap\_90000005] auth mgr attr change not

{wncd\_x\_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap\_90000005]

Received User-Name 42-03-95-22-E6-82

for client 4203.9522.e682

{wncd\_x\_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap\_90000005]

User profile is to be applied

. Authz mlist is not present,

Authc mlist cwa\_authz

,session push flag is unset

{wncd\_x\_R0-0}{1}: [webauth-dev] [17558]: (info): Central Webauth URL Redirect,

Received a request to create a CWA session

for a mac [42:03:95:22:e6:82]

{wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [17558]: (info): [0000.0000.0000:unknown] Retrieved zone id

{wncd\_x\_R0-0}{1}: [webauth-dev] [17558]: (info): No parameter map is associated with mac 4203.9522.e682

{wncd\_x\_R0-0}{1}: [epm-redirect] [17558]: (info): [0000.0000.0000:unknown]

URL-Redirect-ACL = cwa-acl

{wncd\_x\_R0-0}{1}: [epm-redirect] [17558]: (info): [0000.0000.0000:unknown]

URL-Redirect = https://<ise-ip-addr>:8443/portal/[...]

{wncd\_x\_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap\_90000005]

User Profile applied

successfully

for 0x92000002 -

REPLACE

<-- WLC replaces the user profile it had originally created

## Authentification MAB terminée

Une fois que le profil utilisateur du client a été modifié avec succès, le WLC termine l'authentification de l'adresse MAC du client. Si la liste de contrôle d'accès reçue d'ISE n'existe pas sur le WLC, le WLC ne sait pas quoi faire avec ces informations, et par conséquent l'action REPLACE échoue complètement provoquant l'échec de l'authentification MAB aussi bien. Le client ne peut pas s'authentifier.

<#root>

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (debug): MAC: 0000.0000.0000 Sending pmk_update of XID (0) to (M
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682
```

```
MAB Authentication success
```

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
```

```
S_AUTHIF_MAB_AUTH_DONE
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Processing MAB authentication
```

```
CO_AUTH_STATUS_SUCCESS
```

## WLC envoie une réponse d'association au client

Maintenant que le client a été authentifié par ISE et que la liste de contrôle d'accès correcte a été appliquée, le WLC envoie finalement une réponse d'association au client. L'utilisateur peut à présent continuer à se connecter au réseau.

<#root>

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
{wncd_x_R0-0}{1}: [dot11] [17558]: (debug): MAC: 4203.9522.e682 dot11 send association response.
```

```
Sending association response
```

```
with resp_status_code: 0
```

```
{wncd_x_R0-0}{1}: [dot11] [17558]: (debug): MAC: 4203.9522.e682 Dot11 Capability info byte1 1, byte2: 1
```

```
{wncd_x_R0-0}{1}: [dot11-frame] [17558]: (info): MAC: 4203.9522.e682 WiFi direct: skip build Assoc Resp
```

```
{wncd_x_R0-0}{1}: [dot11] [17558]: (info): MAC: 4203.9522.e682 dot11 send association response. Sending
```

```
{wncd_x_R0-0}{1}: [dot11] [17558]: (note): MAC: 4203.9522.e682 Association success. AID 1, Roaming = Fa
```

```
{wncd_x_R0-0}{1}: [dot11] [17558]: (info): MAC: 4203.9522.e682 DOT11 state transition: S_DOT11_MAB_PEND
```

```
S_DOT11_ASSOCIATED
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682
```

```
Station Dot11 association is successful.
```

## Authentication L2

Selon le processus qu'un client doit suivre lorsqu'il s'associe à un WLAN, l'authentification L2 « démarre ». Cependant, en réalité, l'authentification L2 a déjà été effectuée en raison de l'authentification MAB effectuée auparavant. Le client termine immédiatement l'authentification L2.

```
<#root>
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682
```

```
Starting L2 authentication
```

```
. Bssid in state machine:dc8c.37d0.83af Bssid in request is:dc8c.37d0.83af
```

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682 L2 WEBAUTH Authentication Successf
```

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
```

```
S_AUTHIF_L2_WEBAUTH_DONE
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682
```

```
L2 Authentication of station is successful
```

```
., L3 Authentication : 1
```

## Plomb de données

Le WLC attribue des ressources au client qui se connecte afin que le trafic puisse circuler à travers le réseau.

```
<#root>
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (note): MAC: 4203.9522.e682 Mobility discovery triggered. C
```

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

```
{wncd_x_R0-0}{1}: [mm-transition] [17558]: (info): MAC: 4203.9522.e682 MMIF FSM transition: S_MA_INIT -
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (info): MAC: 4203.9522.e682 Invalid transmitter ip in build clie
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (debug): MAC: 4203.9522.e682 Sending mobile_announce of XID (0)
```

```
{mobilityd_R0-0}{1}: [mm-client] [18482]: (debug): MAC: 4203.9522.e682 Received mobile_announce, sub ty
```

```
{mobilityd_R0-0}{1}: [mm-transition] [18482]: (info): MAC: 4203.9522.e682 MMFSM transition: S_MC_INIT -
```

```
{mobilityd_R0-0}{1}: [mm-client] [18482]: (debug): MAC: 4203.9522.e682 Add MCC by tdl mac: client_ifid (
```

```
{mobilityd_R0-0}{1}: [mm-client] [18482]: (debug): MAC: 4203.9522.e682 Sending capwap_msg_unknown (100)
```

```
{mobilityd_R0-0}{1}: [mm-client] [18482]: (debug): MAC: 0000.0000.0000 Sending mobile_announce_nak of X
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (debug): MAC: 4203.9522.e682 Received mobile_announce_nak, sub t
```

```
{wncd_x_R0-0}{1}: [mm-transition] [17558]: (info): MAC: 4203.9522.e682 MMIF FSM transition: S_MA_INIT_W
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (info): MAC: 4203.9522.e682 Roam type changed - None -> None
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (info): MAC: 4203.9522.e682 Mobility role changed - Unassoc -> L
```

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (note): MAC: 4203.9522.e682 Mobility Successful. Roam Type None,
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Processing mobility response f
```

```
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS add mobile cb
```

```
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
```

```
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
```

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682 ADD MOBILE sent. Client state flag
```

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

S\_CO\_DPATH\_PLUMB\_IN\_PROGRESS

```
{wncd_x_R0-0}{1}: [dot11] [17558]: (note): MAC: 4203.9522.e682
```

Client datapath entry params

```
- ssid:training_cwa,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90000003, wlan_ifid: 0xf0400001
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS dpath create params
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
{wncd_x_R0-0}{1}: [avc-afc] [17558]: (debug): AVC enabled for client 4203.9522.e682
{wncd_x_R0-0}{1}: [dpath_svc] [17558]: (note): MAC: 4203.9522.e682
```

Client datapath entry created

for ifid 0xa0000001

## Une adresse IP est attribuée à l'utilisateur

L'utilisateur final a besoin d'une adresse IP pour naviguer sur le réseau. Il est soumis au processus DHCP. Si l'utilisateur était déjà connecté et qu'il se souvient de son adresse IP, le processus DHCP est ignoré. Si l'utilisateur ne peut pas recevoir d'adresse IP, l'utilisateur final ne peut pas afficher le portail Web. Sinon, il passe par les étapes suivantes :

1. Un paquet DISCOVER est envoyé par le client qui se connecte en tant que diffusion pour rechercher les serveurs DHCP disponibles
2. Si un serveur DHCP est disponible, le serveur DHCP répond par une OFFRE. L'offre contient des informations telles que l'adresse IP à attribuer au client qui se connecte, la durée du bail, etc. De nombreuses OFFRES peuvent être reçues de divers serveurs DHCP
3. Le client accepte une OFFRE de l'un des serveurs et répond par une REQUÊTE pour l'adresse IP qu'il a sélectionnée
4. Enfin, le serveur DHCP envoie un paquet ACKNOWLEDGMENT au client avec sa nouvelle adresse IP attribuée

Le WLC enregistre la méthode utilisée par le client pour recevoir son adresse IP.

<#root>

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

S\_CO\_IP\_LEARN\_IN\_PROGRESS

```
{wncd_x_R0-0}{1}: [client-iplearn] [17558]: (info): MAC: 4203.9522.e682 IP-learn state transition: S_IP
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
{wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [17558]: (info): [4203.9522.e682:capwap_90000005] Skipping DH
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface capwap_90000005 on vlan 1000
```

SISF\_DHCPDISCOVER

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface capwap_90000005 on vlan 1000
```

SISF\_DHCPDISCOVER

```
, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [17558]: (info): [4203.9522.e682:capwap_90000005] Skipping DHCP
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface capwap_90000005 on vlan 1000

SISF_DHCPDISCOVER

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface capwap_90000005 on vlan 1000

SISF_DHCPDISCOVER

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPOFFER

, giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPOFFER,

    giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPOFFER

, giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPOFFER

, giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [17558]: (info): [4203.9522.e682:capwap_90000005] Skipping DHCP
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface capwap_90000005 on vlan 1000

SISF_DHCPREQUEST

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface capwap_90000005 on vlan 1000

SISF_DHCPREQUEST

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): RX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPACK

, giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (info): TX: DHCPv4 from interface Tw0/0/0 on vlan 1000 Src MAC

SISF_DHCPACK

, giaddr: 0.0.0.0, yiaddr: <end-user-ip-addr>, CMAC: 4203.9522.e682
{wncd_x_R0-0}{1}: [client-iplearn] [17558]: (note): MAC: 4203.9522.e682

Client IP learn successful. Method: DHCP

    IP: <end-user-ip-addr>
{wncd_x_R0-0}{1}: [epm] [17558]: (info): [0000.0000.0000:unknown] HDL = 0x0 vlan 1000 fail count 0 dirt
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not
{wncd_x_R0-0}{1}: [client-iplearn] [17558]: (info): MAC: 4203.9522.e682 IP-learn state transition: S_IP
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Received ip learn response. me

IPLEARN_METHOD_DHCP
```

L'authentification C3 démarre

Maintenant que l'utilisateur final a reçu une adresse IP, l'authentification de couche 3 commence par CWA détecté comme méthode d'authentification souhaitée.

<#root>

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Triggered L3 authentication. s
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682
```

**L3 Authentication initiated. CWA**

Tests d'adresses IP saines

Pour poursuivre la connexion, le client doit exécuter deux requêtes ARP :

1. Vérifiez que personne d'autre n'a son adresse IP. S'il existe une réponse ARP pour l'adresse IP de l'utilisateur final, elle est une adresse IP dupliquée
2. Validez l'accessibilité à la passerelle. Cela permet de s'assurer que le client peut quitter le réseau. La réponse ARP doit provenir de la passerelle

<#root>

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST**

, ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: 0.0.0.0

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST**

, ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: 0.0.0.0

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST**

, ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: 0.0.0.0

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST**

, ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: 0.0.0.0

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: 0.0.0.0

```
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 S
```

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: 0.0.0.0, ARP target IP: <{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 4203.9522.e682 ARP sender IP: <dhcp-server-ip-addr>, AR  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**REPLY,**

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 4203.9522.e682 ARP sender IP: <dhcp-server-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REQUEST,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 000c.290e.1c37 ARP target MAC: 4203.9522.e682 ARP sender IP: 10.20.30.17, ARP target I  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REPLY,**

ARP sender MAC: 000c.290e.1c37 ARP target MAC: 4203.9522.e682 ARP sender IP: 10.20.30.17, ARP target I  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REQUEST,**

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 0000.0000.0000 ARP sender IP: <dhcp-server-ip-addr>, AR  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

**ARP REQUEST,**

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 0000.0000.0000 ARP sender IP: <dhcp-server-ip-addr>, AR  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REPLY,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t  
{wncd\_x\_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap\_90000005 on vlan 1000 S

**ARP REPLY,**

ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t

## Deuxième connexion : du client au réseau

À ce stade, l'utilisateur final a été authentifié auprès d'ISE via son adresse MAC, mais il n'a pas

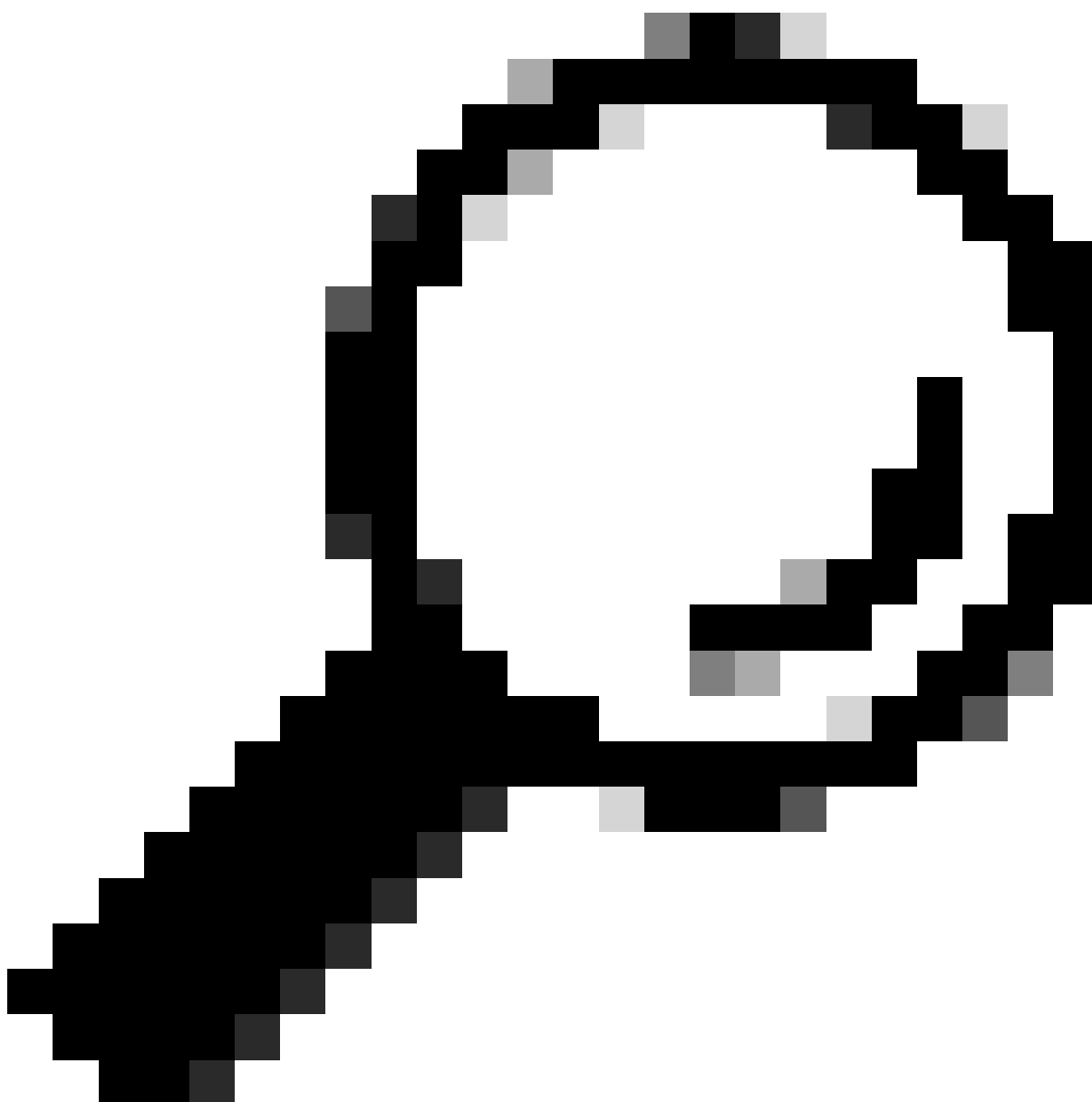


encore été entièrement autorisé. Le WLC doit à nouveau se référer à ISE pour autoriser le client à se connecter au réseau. À ce stade, le portail est présenté à l'utilisateur dans lequel le nom d'utilisateur doit entrer son nom d'utilisateur et son mot de passe. Sur le WLC, l'utilisateur final est vu dans l'état « Authentification Web en attente ».

### Changement d'autorisation (CoA)

C'est ici que la prise en charge de CoA dans la configuration du WLC prend effet. Jusqu'à présent, la liste de contrôle d'accès était utilisée. Une fois que le client final a vu le portail, la liste de contrôle d'accès n'est plus utilisée, car tout ce qu'il a fait était de rediriger le client vers le portail. À ce stade, le client entre ses informations d'identification pour se connecter afin de démarrer le processus CoA et de réauthentifier le client. Le WLC prépare le paquet à envoyer et le transmet à ISE

---



---

Conseil : CoA utilise le port 1700. Assurez-vous qu'il n'est pas bloqué par le pare-feu.

---

<#root>

```
{wncd_x_R0-0}{1}: [caaa-ch] [17558]: (info): [CAAA:COMMAND HANDLER:92000002]
```

Processing CoA request

under CH-ctx.

<-- ISE requests the client to reauthenticate

```
{wncd_x_R0-0}{1}: [caaa-ch] [17558]: (info): [CAAA:COMMAND HANDLER:92000002] Reauthenticate request (0x
```

```
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

MAB re-authentication started

for 2315255810 (4203.9522.e682)

<-- ISE requests the WLC to reauthenciate the CoA

```
{wncd_x_R0-0}{1}: [aaa-coa] [17558]: (info): radius coa proxy relay coa resp(wncd)
```

```
{wncd_x_R0-0}{1}: [aaa-coa] [17558]: (info):
```

CoA Response Details

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << ssg-command-code 0 32 >>
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << formatted-clid 0 "4203.9522.e682">>
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << error-cause 0 1 [
```

Success

]>>

<-- The WLC responds with a success after processing the packet to be sent to ISE

```
[aaa-coa] [17558]: (info): server:10.20.30.14 cfg_saddr:10.20.30.14 udpport:64016 sport:0, tableid:0ide
```

```
[caaa-ch] [17558]: (info): [CAAA:COMMAND HANDLER]
```

CoA response sent <-- The WLC sends the CoA response to ISE

## Deuxième authentification à ISE

La deuxième authentification ne commence pas à zéro. C'est la puissance de CoA. De nouvelles règles et/ou paris AV peuvent être appliqués à l'utilisateur. La liste de contrôle d'accès et l'URL de redirection reçues sur le premier Access-Accept ne sont plus transmises à l'utilisateur final.

## WLC envoie une requête à ISE

Le WLC envoie un nouveau paquet RADIUSAccess-Requestpacket à ISE avec la combinaison nom d'utilisateur/mot de passe entrée. Cela déclenche une nouvelle authentification MAB, et comme ISE connaît déjà le client, un nouvel ensemble de stratégies doit être appliqué (par exemple, Accès accordé).

<#root>

{wncd\_x\_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap\_90000005] Received event '

MAB\_REAUTHENTICATE

' on handle 0x8A000002

{wncd\_x\_R0-0}{1}: [caaa-author] [17558]: (info): [CAAA:AUTHOR:92000002] DEBUG: mlist=cwa\_authz for type

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Send

Access-Request

to

<ise-ip-addr>:1812

id 0/

29

, len 421

<-- The packet is traveling via RADIUS port 1812. The "29" is the session ID and it is unique for every

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: authenticator c6 ae ab d5 55 c9 65 e2 - 4d 28 01 75

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS:

User-Name

[1] 14 "

42039522e682

"

<-- MAC address that is attempting to authenticate

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: User-Password [2] 18 \*

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS:

Cisco AVpair

[1] 25

"service-type=Call Check" <-- This indicates a MAC filtering process

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Framed-MTU [12] 6 1485

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Message-Authenticator [80] 18 ...

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: EAP-Key-Name [102] 2 \*

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Cisco AVpair [1] 43 "audit-session-id=0

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS:

Cisco AVpai

r [1] 12

"method=mab" <-- Controller sends an AVpair with MAB method

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Cisco AVpair [1] 26 "client-iif-id=1392

{wncd\_x\_R0-0}{1}: [radius] [17558]: (info): RADIUS: Cisco AVpair [1] 14

"

vlan-id=200"

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS:
```

```
NAS-IP-Address
```

```
[4] 6
```

```
<wmi-ip-addr> <-- WLC WMI IP address
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: NAS-Port-Id [87] 17 "capwap_90000005"  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19]  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS:
```

```
Cisco AVpair
```

```
[1] 30
```

```
"cisco-wlan-ssid=cwa" <-- SSID and WLAN the client is attempting to connect
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS:
```

```
Cisco AVpair
```

```
[1] 32
```

```
"wlan-profile-name=cwa"
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Called-Station-Id [30] 32 "dc-8c-37-d0-83-a0:  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Calling-Station-Id [31] 19 "42-03-95-22-e6-82"  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Airespace-WLAN-ID [1] 6 1  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Nas-Identifier [32] 9 "BC-9800"  
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Started 5 sec timeout
```

## ISE répond à la requête WLC

ISE effectue une recherche de sa stratégie, et si le nom d'utilisateur reçu correspond au profil de stratégie, alors ISE répond au WLC une fois de plus, acceptant la connexion du client au WLAN. Elle renvoie le nom d'utilisateur de l'utilisateur final. Si elles sont configurées sur ISE, des règles supplémentaires et/ou des paires AV peuvent être appliquées à l'utilisateur et elles sont visibles sur Access-Accept.

```
<#root>
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Received from id
```

```
1812/29
```

```
<ise-ip-addr>
```

```
:0,
```

```
Access-Accept
```

```
, len 131
```

```
<-- The packet is traveling via RADIUS port 1812 and is has a session ID of 29 (as a response to the abo
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: authenticator a3 b0 45 d6 e5 1e 38 4a - be 15 fa 6b
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS:
```

User-Name

```
[1] 14 "
```

cwa-username

"

```
<-- Username entered by the end client on the portal that was shown
```

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Class [25] 51 ...
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Cisco AVpair [1] 22 "profile-name=Unknown"
{wncd_x_R0-0}{1}: [radius] [17558]: (info): Valid Response Packet, Free the identifier
{wncd_x_R0-0}{1}: [eap-auth] [17558]: (info): SUCCESS for EAP method name: Identity on handle 0xEE00003
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

MAB received an Access-Accept

```
for 0x8A000002
```

```
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '
```

MAB\_RESULT

```
' on handle 0x8A000002
```

```
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Authc success from
```

MAB, Auth event success

## Processus WLC des informations reçues d'ISE

Une fois de plus, le WLC traite les informations reçues par ISE. Il exécute une autre action REPLACE sur l'utilisateur avec les nouvelles valeurs reçues d'ISE.

<#root>

```
[aaa-attr-inf] [17558]: (info):
```

```
<< username 0 "cwa-username">> <-- Processing username received from ISE
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< class 0 43 41 43 53 3a 30 45 31 45 31 34 30 41 30 30 30 30 30 30 43 38 45 32 44 41 36 34 32 3a 62
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<<Message-Authenticator 0 <hidden>>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< dnis 0 "DC-8C-37-D0-83-A0">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< formatted-clid 0 "42-03-95-22-E6-82">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< audit-session-id 0 "0E1E140A0000000C8E2DA642">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< method 0 2 [mab]>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< clid-mac-addr 0 42 03 95 22 e6 82 >>
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):  
<< intf-id 0 2415919109 (0x90000005)>>  
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not  
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not  
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

Received User-Name cwa-username

```
for client 4203.9522.e682  
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

User profile is to be applied.

Authz mlist is not present,

Authc mlist cwa\_authz

```
,session push flag is unset  
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

User Profile applied

successfully

for 0x92000002 -

REPLACE <-- WLC replaces the user profile it had originally created

L'authentification L3 se termine

L'utilisateur final a été authentifié avec les données fournies. L'authentification L3 (authentification Web) est terminée.

<#root>

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682
```

L3 Authentication Successful

. ACL:[]

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
```

S\_AUTHIF\_WEBAUTH\_DONE

```
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS add mobile cb  
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re  
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re  
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682 ADD MOBILE sent. Client state flag  
{wncd_x_R0-0}{1}: [errmsg] [17558]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entr
```

cwa-username

) joined with ssid (

cwa

```
) for device with MAC: 4203.9522.e682 <-- End user "cwa-username" has joined the WLAN "cwa"  
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute : username 0 "
```

cwa-username

```
" ]  
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute : class 0 43 41 .  
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute :bsn-vlan-interface-name 0 "MGMT"  
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute : timeout 0 1800 (0x708) ]  
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS run state handler
```

L'utilisateur final atteint l'état d'exécution sur le WLC

Enfin, l'utilisateur est authentifié et associé au WLAN.

<#root>

```
{wncd_x_R0-0}{1}: [rog-proxy-capwap] [17558]: (debug):
```

**Managed client RUN state**

notification: 4203.9522.e682

```
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

s\_CO\_RUN

## Flux CWA - Capture de paquets intégrée (EPC)

Un EPC est une capture de paquets qui peut être récupérée directement à partir du WLC en affichant tous les paquets qui traversent le WLC ou qui en proviennent. Pour plus d'informations sur ce qu'ils sont et comment les récupérer, s'il vous plaît visitez [Comprendre les débogages sans fil et la collecte de journaux sur les contrôleurs LAN sans fil Catalyst 9800.](#)

Première connexion : client vers serveur ISE



Avertissement : les adresses IP sur les images de la capture de paquets ont été supprimées. Ils sont affichés comme et

## Association au WLAN et requête envoyée au serveur ISE

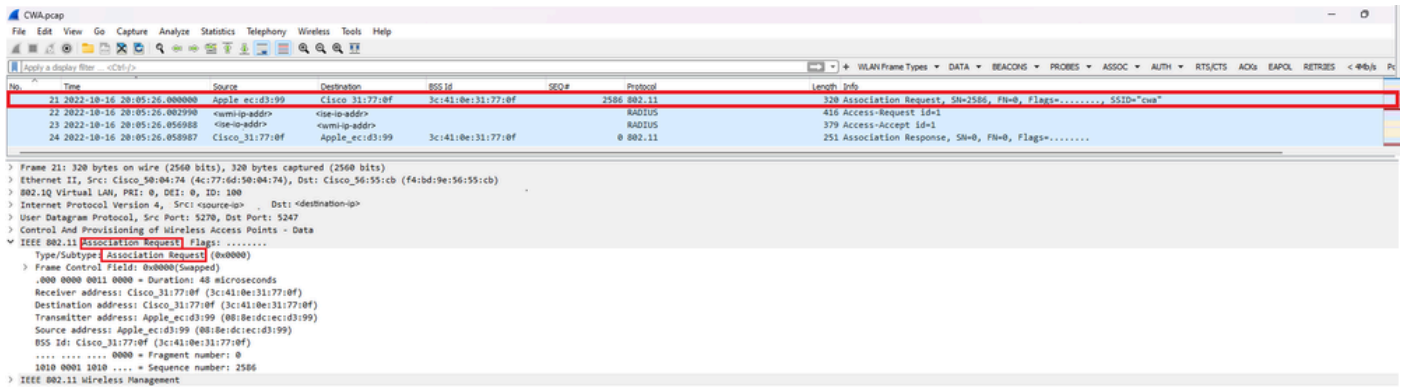
No.	Time	Source	Destination	BSS Id	Seq#	Protocol	Length	Info
21	2022-10-16 20:05:26.000000	Apple_ec:d3:99	Cisco_31:77:0f	3c:41:0e:31:77:0f		2586 802.11	320	Association Request, SH=2586, FN=0, Flags=....., SSID="cwa"
22	2022-10-16 20:05:26.002998	<source-ip-address>	<destination-ip-address>			RADIUS	416	Access-Request Id=1
23	2022-10-16 20:05:26.056808	<source-ip-address>	<destination-ip-address>			RADIUS	379	Access-Accept Id=1
24	2022-10-16 20:05:26.058987	Cisco_31:77:0f	Apple_ec:d3:99	3c:41:0e:31:77:0f		0 802.11	251	Association Response, SH=0, FN=0, Flags=.....

Premiers paquets

## Requête d'association du WLC au client

En regardant le premier paquet « Association Request », vous pouvez voir les adresses MAC des périphériques qui sont impliqués dans ce processus.

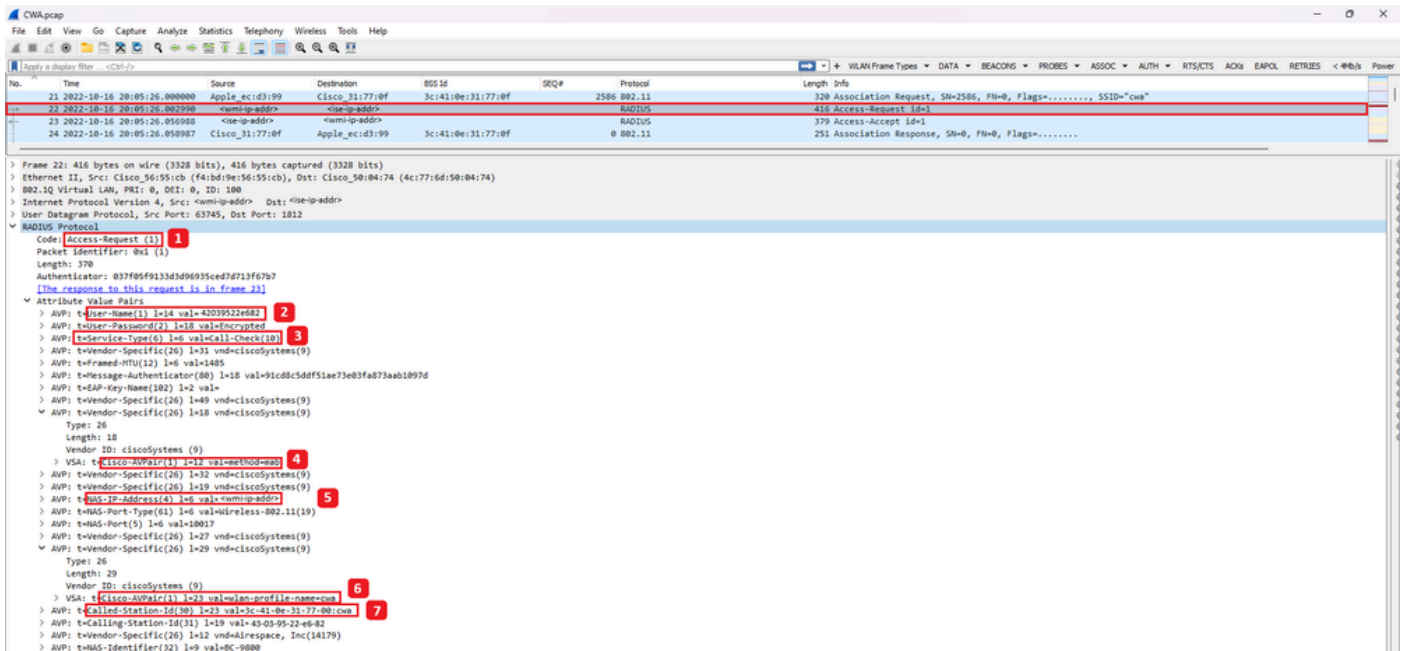




Demande D'Association

## Paquet de demande d'accès envoyé du WLC à ISE

Une fois que la demande d'association a été traitée par le WLC, le WLC envoie un paquet de demande d'accès au serveur ISE.



Analyse du paquet de demande d'accès

1. Nom du paquet.
2. Adresse MAC qui tente de s'authentifier.
3. Cela indique un filtrage MAC.
4. Paire AV envoyée par le contrôleur à ISE pour indiquer un processus de filtrage MAC.
5. Adresse IP WMI du WLC.
6. SSID auquel le client tente de se connecter.
7. Nom du réseau local sans fil auquel le client tente de se connecter.

## Paquet d'acceptation d'accès envoyé du WLC à ISE

Une fois qu'ISE a traité le paquet d'acceptation d'accès, il répond par un paquet d'acceptation d'accès s'il réussit ou par un paquet de refus d'accès s'il échoue.

Code: Access-Accept (2) 1  
 Packet Identifier: 0x1 (1)  
 Length: 333  
 Authenticator: d26cf085fabd72bc517b0d6ea94be0cc  
 [This is a response to a request in frame 22]  
 [Time from request: 0.053990000 seconds]  
 Attribute Value Pairs  
 > AVP: t=Cisco-Name(1) l=19 val=43-03-05-22-16-82 2  
 > AVP: t=Cisco(25) l=50 val=43143553a38333041418433030303030304353741463131303043626320697365.  
 > AVP: t=Message-Authenticator(80) l=18 val=sc2db7bb9243fa629580374790e9aade  
 > AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)  
 Type: 26  
 Length: 37  
 Vendor ID: ciscoSystems (9)  
 > VSA: t=Cisco-AVPair(1) l=31 val=url-redirect-acl=cwa-ad  
 Type: 1  
 Length: 31  
 Cisco-AVPair: url-redirect-acl=cwa-ad 3  
 > AVP: t=Vendor-Specific(26) l=189 vnd=ciscoSystems(9)  
 Type: 26  
 Length: 189  
 Vendor ID: ciscoSystems (9)  
 > VSA: t=Cisco-AVPair(1) l=183 val=url-redirect=https://<ip>:8443/portal/gateway/sessionId=030A8C0000000C57AF11044portal?cfsacId=5dbf4b36-aeec-b959fd24c82&action=cwa&token=231c2569050bc725ea8048feff99707e  
 Type: 1  
 Length: 183  
 Cisco-AVPair: url-redirect=https://<ip>:8443/portal/gateway/sessionId=030A8C0000000C57AF11044portal?cfsacId=5dbf4b36-aeec-b959fd24c82&action=cwa&token=231c2569050bc725ea8048feff99707e 4

Analyse du paquet d'acceptation d'accès

1. Nom du paquet.
2. Adresse MAC authentifiée.
3. La liste de contrôle d'accès à appliquer.
4. URL vers laquelle rediriger l'utilisateur.

Réponse d'association du WLC au client

IEEE 802.11 Association Response Flags: .....  
 Type/Subtype: Association Response (0x0001)  
 Frame Control Field: 0x0010 (Swapped)  
 .000 0000 0000 0000 = Duration: 0 microseconds  
 Receiver address: Apple\_ecid3:99 (08:0e:dc:ec:d3:99)  
 Destination address: Apple\_ecid3:99 (08:0e:dc:ec:d3:99)  
 Transmitter address: Cisco\_31:77:0f (3c:41:0e:31:77:0f)  
 Source address: Cisco\_31:77:0f (3c:41:0e:31:77:0f)  
 BSS Id: Cisco\_31:77:0f (3c:41:0e:31:77:0f)  
 .... = Fragment number: 0  
 0000 0000 0000 .... = Sequence number: 0  
 IEEE 802.11 Wireless Management

Réponse d'association

Processus DHCP

No.	Time	Source	Destination	BSS Id	Seq#	Protocol	Length	Info
47	2022-10-16 20:05:28.241976	0.0.0.0	255.255.255.255	3c:41:0e:31:77:00	2833	DHCP	424	DHCP Discover - Transaction ID 0x35a7cde
48	2022-10-16 20:05:28.241976	0.0.0.0	255.255.255.255	3c:41:0e:31:77:00		DHCP	346	DHCP Discover - Transaction ID 0x35a7cde
49	2022-10-16 20:05:28.290970	Cisco_31:77:00	Cisco_31:77:00	3c:41:0e:31:77:00	16	WLCCP	132	U, func=UI; SNAP, OUI 0x000496 (Cisco Systems, Inc.), PID 0x0000
50	2022-10-16 20:05:28.290970	Cisco_31:77:00	Cisco_31:77:00	3c:41:0e:31:77:00	16	WLCCP	517	U, func=UI; SNAP, OUI 0x000496 (Cisco Systems, Inc.), PID 0x0000
51	2022-10-16 20:05:28.307982	<dhcp-server-ip>	<assigned-ip>	3c:41:0e:31:77:0f		DHCP	355	DHCP Offer - Transaction ID 0x35a7cde
52	2022-10-16 20:05:28.308974	<dhcp-server-ip>	<assigned-ip>	3c:41:0e:31:77:0f		DHCP	425	DHCP Offer - Transaction ID 0x35a7cde
72	2022-10-16 20:05:29.409964	0.0.0.0	255.255.255.255	3c:41:0e:31:77:00	3089	DHCP	424	DHCP Request - Transaction ID 0x35a7cde
73	2022-10-16 20:05:29.409971	0.0.0.0	255.255.255.255	3c:41:0e:31:77:00		DHCP	346	DHCP Request - Transaction ID 0x35a7cde
74	2022-10-16 20:05:29.491963	<dhcp-server-ip>	<assigned-ip>	3c:41:0e:31:77:0f		DHCP	355	DHCP ACK - Transaction ID 0x35a7cde
75	2022-10-16 20:05:29.491963	<dhcp-server-ip>	<assigned-ip>	3c:41:0e:31:77:0f		DHCP	425	DHCP ACK - Transaction ID 0x35a7cde

Processus DHCP



Remarque : désormais, les paquets sont vus en double, mais c'est seulement parce que l'un est encapsulé CAPWAP et l'autre ne l'est pas

## ARP

78	2022-10-16 20:05:29.496968	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	3345 ARP	124 who has <assigned-ip-addr> (ARP Probe)
79	2022-10-16 20:05:29.496968	Apple_ecid3:99	Broadcast		ARP	60 who has <assigned-ip-addr> (ARP Probe)
80	2022-10-16 20:05:29.847948	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	3681 ARP	124 who has <assigned-ip-addr> (ARP Probe)
81	2022-10-16 20:05:29.847948	Apple_ecid3:99	Broadcast		ARP	60 who has <assigned-ip-addr> (ARP Probe)
82	2022-10-16 20:05:30.142982	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	3857 ARP	124 who has <assigned-ip-addr> (ARP Probe)
83	2022-10-16 20:05:30.142982	Apple_ecid3:99	Broadcast		ARP	60 who has <assigned-ip-addr> (ARP Probe)
84	2022-10-16 20:05:30.464972	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	17 ARP	124 ARP Announcement for <assigned-ip-addr>
85	2022-10-16 20:05:30.465064	Apple_ecid3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
88	2022-10-16 20:05:30.790844	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	785 ARP	124 ARP Announcement for <assigned-ip-addr>
89	2022-10-16 20:05:30.790944	Apple_ecid3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
90	2022-10-16 20:05:31.115991	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	1041 ARP	124 ARP Announcement for <assigned-ip-addr>
91	2022-10-16 20:05:31.116983	Apple_ecid3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
92	2022-10-16 20:05:31.117990	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	1297 ARP	124 who has 192.168.20.1 Tell <assigned-ip-addr>
93	2022-10-16 20:05:31.117990	Apple_ecid3:99	Broadcast		ARP	60 who has 192.168.20.1 Tell <assigned-ip-addr>
94	2022-10-16 20:05:31.118981	Cisco_50:04:74	Apple_ecid3:99		ARP	64 192.168.20.1 is at 4c:77:6d:50:04:74
95	2022-10-16 20:05:31.118981	Cisco_50:04:74	Apple_ecid3:99	3c:41:0e:31:77:0f	0 ARP	134 192.168.20.1 is at 4c:77:6d:50:04:74
97	2022-10-16 20:05:31.192083	Apple_ecid3:99	Broadcast	3c:41:0e:31:77:00	1809 ARP	124 who has 192.168.20.1 Tell <assigned-ip-addr>
98	2022-10-16 20:05:31.193074	Apple_ecid3:99	Broadcast		ARP	60 who has 192.168.20.1 Tell <assigned-ip-addr>
99	2022-10-16 20:05:31.193974	Cisco_50:04:74	Apple_ecid3:99		ARP	64 192.168.20.1 is at 4c:77:6d:50:04:74
100	2022-10-16 20:05:31.194981	Cisco_50:04:74	Apple_ecid3:99	3c:41:0e:31:77:0f	0 ARP	134 192.168.20.1 is at 4c:77:6d:50:04:74

Client ARPing pour sa propre adresse IP et pour le modem routeur

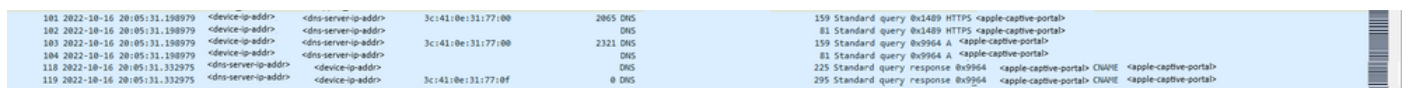
## Test de connectivité

Une fois le processus ARP terminé, le périphérique qui tente de se connecter effectue une

vérification pour vérifier si un portail est déclenché, également appelée « sondage ». Si le périphérique indique qu'il n'y a pas de connexion Internet, cela signifie que le processus ARP a échoué (par exemple, la passerelle n'a jamais répondu) ou que le périphérique n'a pas pu effectuer l'analyse.

Cette analyse n'est pas visible sur les traces RA, seule l'EPC est en mesure de fournir ces informations. La requête de sondage dépend de l'appareil qui tente une connexion. Dans cet exemple, l'appareil de test était un appareil Apple. Le sondage a donc été effectué directement vers le portail captif d'Apple.

Comme la recherche est effectuée à l'aide d'une URL, DNS est requis pour résoudre cette URL. Par conséquent, si le serveur DNS ne peut pas répondre aux requêtes du client, celui-ci continue à demander l'URL et le portail n'est jamais vu. À ce stade, si l'adresse IP du serveur ISE est entrée dans le navigateur Web du périphérique final, le portail doit être visible. Si c'est le cas, il y a un problème avec le serveur DNS.

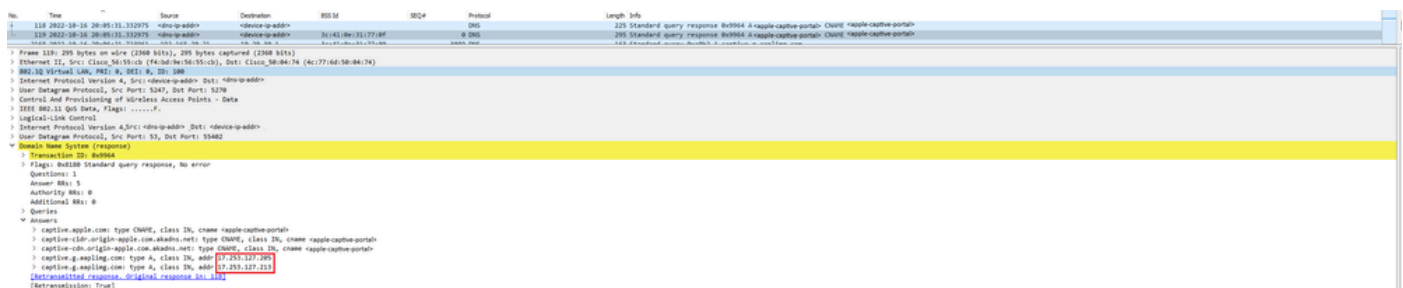


No.	Time	Source	Destination	OSI#	Seq#	Protocol	Length	Info
181	2022-10-16 20:05:31.180979	<device-ip-addr>	<dns-server-ip-addr>	3	41:0e:31:77:00	2065	DNS	159 Standard query 0x1409 HTTPS <apple-captive-portal>
182	2022-10-16 20:05:31.180979	<device-ip-addr>	<dns-server-ip-addr>	3	41:0e:31:77:00	0	DNS	81 Standard query 0x1409 HTTPS <apple-captive-portal>
183	2022-10-16 20:05:31.180979	<device-ip-addr>	<dns-server-ip-addr>	3	41:0e:31:77:00	2321	DNS	159 Standard query 0x9964 A <apple-captive-portal>
184	2022-10-16 20:05:31.180979	<device-ip-addr>	<dns-server-ip-addr>	3	41:0e:31:77:00	0	DNS	81 Standard query 0x9964 A <apple-captive-portal>
118	2022-10-16 20:05:31.332975	<dns-server-ip-addr>	<device-ip-addr>	3	41:0e:31:77:0f	0	DNS	225 Standard query response 0x9964 <apple-captive-portal> CNAME <apple-captive-portal>
119	2022-10-16 20:05:31.332975	<dns-server-ip-addr>	<device-ip-addr>	3	41:0e:31:77:0f	0	DNS	295 Standard query response 0x9964 <apple-captive-portal> CNAME <apple-captive-portal>

Test de connectivité du client - Requête DNS et réponse

### Adresse IP résolue par DNS

En examinant la réponse à la requête DNS, vous pouvez voir l'adresse IP qui a été résolue par le serveur DNS.



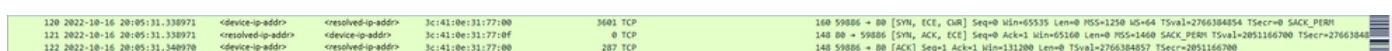
No.	Time	Source	Destination	OSI#	Seq#	Protocol	Length	Info
118	2022-10-16 20:05:31.332975	<dns-ip-addr>	<device-ip-addr>	3	41:0e:31:77:0f	0	DNS	225 Standard query response 0x9964 A <apple-captive-portal> CNAME <apple-captive-portal>
119	2022-10-16 20:05:31.332975	<dns-ip-addr>	<device-ip-addr>	3	41:0e:31:77:0f	0	DNS	295 Standard query response 0x9964 A <apple-captive-portal> CNAME <apple-captive-portal>

Flags: 0x200 Standard query response, No error  
Questions: 1  
Answer RRs: 5  
Authority RRs: 0  
Additional RRs: 0  
Queries  
Answers  
-> captive.apple.com: type CNAME, class IN, cname <apple-captive-portal>  
-> captive.cdn.origin=apple.com.akadns.net: type CNAME, class IN, cname <apple-captive-portal>  
-> captive-cdn.origin=apple.com.akadns.net: type CNAME, class IN, cname <apple-captive-portal>  
-> captive.g.mplinq.com: type A, class IN, addr [17.253.127.213]  
-> captive.g.mplinq.com: type A, class IN, addr [17.253.127.213]

Adresse IP résolue par le serveur DNS

### Établissement d'une connexion en trois étapes

Une fois l'adresse IP DNS résolue, une connexion TCP en trois étapes est établie entre le portail et le client. L'adresse IP utilisée est l'une des adresses IP résolues.



120	2022-10-16 20:05:31.338971	<device-ip-addr>	<resolved-ip-addr>	3	41:0e:31:77:00	3601	TCP	160 59886 -> 80 [SYN, ECE, CWR] Seq=0 Min=65535 Len=0 MSS=1250 WS=64 TSval=2766384854 TSecr=0 SACK_PERM
121	2022-10-16 20:05:31.338971	<resolved-ip-addr>	<device-ip-addr>	3	41:0e:31:77:0f	0	TCP	140 80 -> 59886 [SYN, ACK, ECE] Seq=0 Ack=1 Min=65160 Len=0 MSS=1460 SACK_PERM TSval=2851166700 TSecr=27663848
122	2022-10-16 20:05:31.340970	<device-ip-addr>	<resolved-ip-addr>	3	41:0e:31:77:00	287	TCP	140 59886 -> 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=2766384857 TSecr=2851166700

Établissement D'Une Connexion En Trois Étapes

### GET Hotspot

Une fois la session TCP établie, le client effectue une recherche et tente d'accéder au portail.

123	2022-10-16 20:05:31.341977	<device-ip-addr>	<device-ip-addr>	3c:41:0e:31:77:0f	272	HTTP	279	GET /hotspot-detect.html HTTP/1.0
124	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<dns-resolved-ip-addr>	3c:41:0e:31:77:0f	0	TCP	140	80 → 59886 [ACK] Seq=132 Win=65152 Len=0 TSval=2051166703 TSecr=2766384857

GET Hotspot

Paquet OK

Le paquet OK contient le portail ISE vers lequel le client doit être redirigé.

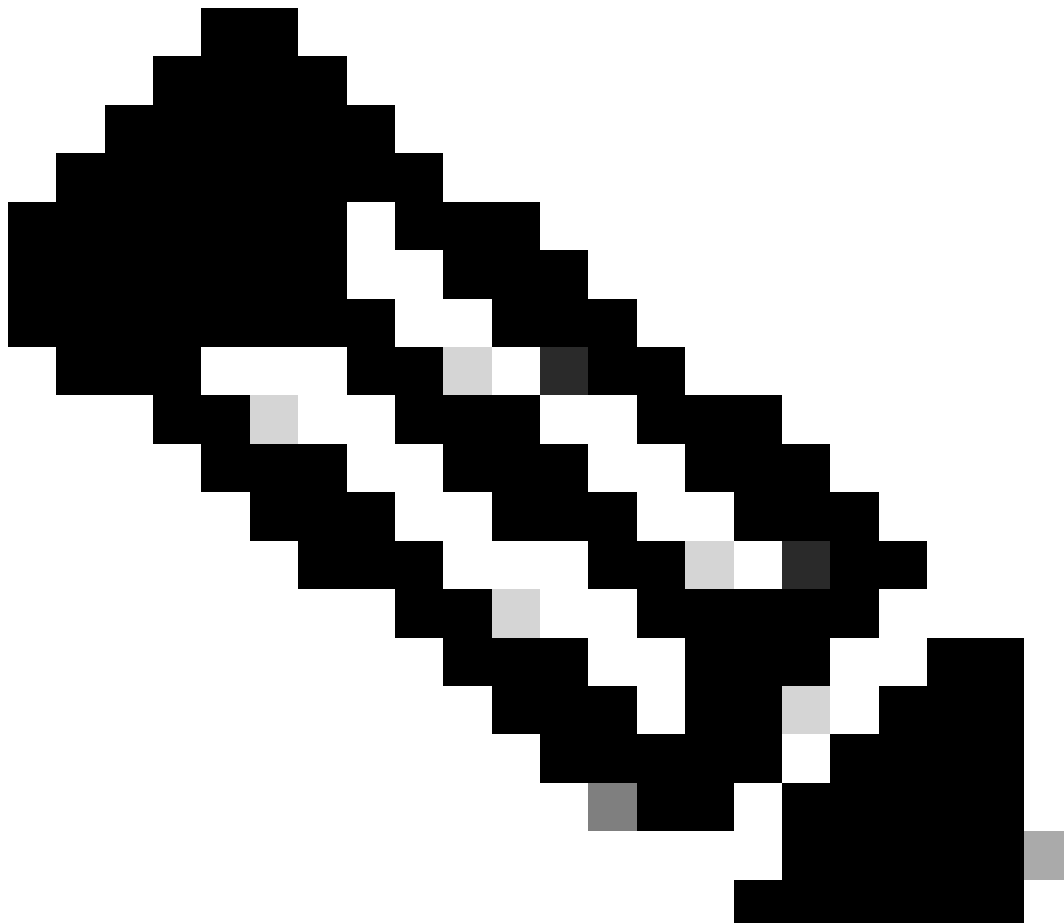
No.	Time	Source	Destination	OSID	SEQ#	Protocol	Length	Info
123	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<device-ip-addr>	3c:41:0e:31:77:0f	0	TCP	140	80 → 59886 [ACK] Seq=132 Win=65152 Len=0 TSval=2051166703 TSecr=2766384857
125	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<device-ip-addr>	3c:41:0e:31:77:0f	0	HTTP	988	HTTP/1.1 200 OK (text/html)
126	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<device-ip-addr>	3c:41:0e:31:77:0f	0	TCP	140	80 → 59886 [FIN, ACK] Seq=849 Ack=132 Win=0 Len=0 TSval=2051166703 TSecr=2766384857

```

> Frame 125: 988 bytes on wire (7904 bits), 988 bytes captured (7904 bits)
> Ethernet II, Src: Cisco_S6:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_S0:04:74 (4c:77:6d:50:04:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <source-ip-addr>, Dst: <destination-ip-addr>
> User Datagram Protocol, Src Port: 5247, Dst Port: 5278
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: <dns-resolved-addr>, Dst: <device-ip-addr>
> Transmission Control Protocol, Src Port: 80, Dst Port: 59886, Seq: 1, Ack: 132, Len: 848
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Location: https://<ise-ip-addr>:8441/portal/gateway?sessionId=030BAAC0000000C57AF1104&portal=7cf5ac1d-5dbf-4b36-aeec-b9590fd24c02&action=cwa&token=231e2569058bc725ea084feff99707e8&redirect=http://captive.apple.com/hotspot-detect.html\r\n
  > Content-Type: text/html\r\n
  > Content-Length: 949\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.000000000 seconds]
  [Request in frame: 125]
  [Request URL: http://captive.apple.com/hotspot-detect.html]
  File Data: 549 bytes
  > Line-based text data: text/html (9 lines)

```

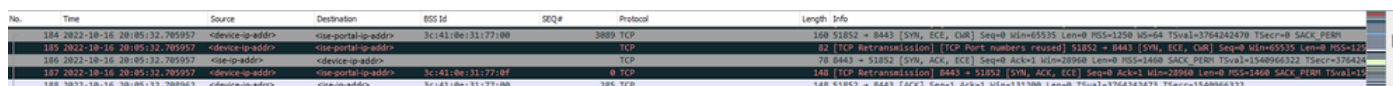
Paquet OK



Remarque : la plupart des personnes ont une autre URL retournée dans le paquet OK. Par conséquent, une autre requête DNS doit être effectuée pour obtenir l'adresse IP finale.

## Nouvelle session TCP établie

Maintenant que l'adresse IP du portail a été découverte, de nombreux paquets sont échangés, mais à la fin un paquet avec l'adresse IP de destination qui a été retourné dans le paquet OK (ou résolu par DNS) qui correspond à l'adresse IP d'ISE, montre une nouvelle session TCP en cours d'établissement sur le portail.



No.	Time	Source	Destination	ESS ID	SEQ#	Protocol	Length	Info
184	2022-10-16 20:05:32.705957	<device-ip-addr>	<ise-portal-ip-addr>	3c:41:0e:31:77:00		TCP	3889	TCP [RST] Seq=51852 Win=0 Len=0
185	2022-10-16 20:05:32.705957	<device-ip-addr>	<ise-portal-ip-addr>	3c:41:0e:31:77:00		TCP	62	TCP [RST] Seq=51852 Win=0 Len=0
186	2022-10-16 20:05:32.705957	<device-ip-addr>	<ise-portal-ip-addr>	3c:41:0e:31:77:00		TCP	78	TCP [RST] Seq=51852 Win=0 Len=0
187	2022-10-16 20:05:32.705957	<device-ip-addr>	<ise-portal-ip-addr>	3c:41:0e:31:77:00		TCP	148	TCP [RST] Seq=51852 Win=0 Len=0
188	2022-10-16 20:05:32.788962	<device-ip-addr>	<ise-ip-addr>	3c:41:0e:31:77:00		TCP	285	TCP [ACK] Seq=1 Ack=1 Win=131200 Len=0

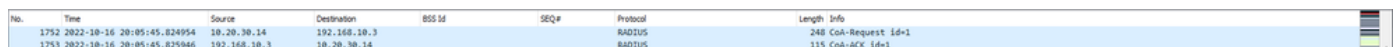
Deuxième connexion et nouvelle session TCP vers le portail ISE

## Le portail s'affiche pour l'utilisateur

À ce stade, le portail d'ISE s'affiche enfin sur le navigateur du navigateur client. Comme précédemment, de nombreux paquets sont échangés entre ISE et le périphérique ; par exemple, un Hello client et un Hello serveur, etc. C'est ici qu'ISE demande au client le nom d'utilisateur et le mot de passe, accepte les conditions générales ou tout autre élément configuré sur le serveur ISE.

## Demande CoA / Accusé de réception CoA

Une fois que l'utilisateur a entré toutes les données demandées, ISE envoie une requête CoA au contrôleur pour modifier l'autorisation de l'utilisateur. Si tout sur le WLC est configuré comme prévu, comme avoir l'état NAC, la prise en charge de CoA, et ainsi de suite, le WLC envoie un accusé de réception CoA (CoA ACK). Sinon, le WLC peut envoyer un CoA Non-Acknowledgement (CoA NACK) ou simplement il n'envoie même pas le CoA ACK.



No.	Time	Source	Destination	ESS ID	SEQ#	Protocol	Length	Info
1752	2022-10-16 20:05:45.824954	10.20.30.14	192.168.10.3			RADIUS	248	CoA-Request id=1
1753	2022-10-16 20:05:45.825946	192.168.10.3	10.20.30.14			RADIUS	115	CoA-ACK id=1

Demande et accusé de réception CoA

## Deuxième connexion : du client au réseau

### Nouvelle demande d'accès

Le WLC envoie un nouveau paquet de demande d'accès à ISE.

```
10.0.1.1:2000 -> 10.0.1.2:8080: 432 bytes captured (376 bytes) on interface 0
Ethernet II, Src: Cisco_S6155-cb (f4:bd:9e:56:15:cb), Dst: Cisco_S6155-cb (f4:bd:9e:56:15:cb)
802.3Q Virtual LAN, PVID: 4, Src: 0, Dst: 4, 201: 200
Internet Protocol Version 4, Src: 10.0.1.1, Dst: 10.0.1.2
User Datagram Protocol, Src Port: 63745, Dst Port: 8080
HTTP Protocol
Code: Access-Request (3)
Packet Length: 376 (3)
Length: 376
Authentication: #00ff74c2b2845b4f6c8d02402f800000
[This is a response to a request in frame 1754]
Attribute Value Pairs
-> AP: #00000000000000000000000000000000
  Type: 1
  Length: 14
  User-Name: 0000000000
  -> AP: t=User-Password(2) 1-18 val=encrypted
  -> AP: t=Service-Type(3) 1-4 val=all-check(10)
    Type: 6
    Length: 4
    Service-Type: #01-Check (10)
    -> AP: t=Vendor-Specific(20) 1-11 vnd=ciscoSystem(9)
    -> AP: t=Vendor-Specific(20) 1-2 val=100
    -> AP: t=Message-Authenticator(80) 1-18 val=487b7040214c0e080025d0f2c3aa60
    -> AP: t=IDM-req-Name(1802) 1-2 val=
    -> AP: t=Vendor-Specific(20) 1-49 vnd=ciscoSystem(9)
    -> AP: t=Vendor-Specific(20) 1-18 vnd=ciscoSystem(9)
      Type: 26
      Length: 18
      Vendor ID: ciscoSystem (9)
      -> VSA: t=Cisco-MPAC(1) 1-1 vnd=ciscoM(1)
      -> AP: t=Vendor-Specific(20) 1-4 val=100
      -> AP: t=Vendor-Specific(20) 1-12 vnd=ciscoSystem(9)
      -> AP: t=Vendor-Specific(20) 1-19 vnd=ciscoSystem(9)
      Type: 26
      Length: 28
      Vendor ID: ciscoSystem (9)
      -> VSA: t=Cisco-MPAC(1) 1-3 val=1an-Ld-200
      -> AP: t=Vendor-Specific(20) 1-4 val=100
      Type: 4
      Length: 4
      -> AP: t=MQ-Port-Type(65) 1-4 val=wireless-802.11(19)
      -> AP: t=MQ-Port(15) 1-4 val=80211
      -> AP: t=Vendor-Specific(20) 1-27 vnd=ciscoSystem(9)
      Type: 26
      Length: 27
      Vendor ID: ciscoSystem (9)
      -> VSA: t=Cisco-MPAC(1) 1-21 val=cisco-wlan-wiFiProc
      -> AP: t=Vendor-Specific(20) 1-29 vnd=ciscoSystem(9)
      Type: 26
      Length: 26
      Vendor ID: ciscoSystem (9)
      -> VSA: t=Cisco-MPAC(1) 1-1 val=wlan-profile-name=
      -> AP: t=Called-Station-ID(80) 1-27 val=3c-4d-3e-31-77-80com
      -> AP: t=Calling-Station-ID(15) 1-18 val=08-0e-4c-4c-42-99
      -> AP: t=Vendor-Specific(20) 1-13 vnd=airspan, Inc(14179)
      -> AP: t=MQ-Classifier(32) 1-4 val=MC-10000
```

Analyse du nouveau paquet de demande d'accès

1. Nom du paquet.
2. Adresse MAC qui tente de s'authentifier.
3. Cela indique un filtrage MAC.
4. Paire AV envoyée par le contrôleur à ISE pour indiquer un processus de filtrage MAC.
5. Adresse IP WMI du WLC.
6. SSID auquel le client tente de se connecter.
7. Nom du réseau local sans fil auquel le client tente de se connecter.

Nouvel accès - Acceptation

Le WLC envoie un nouveau paquet de demande d'accès à ISE.

```
10.0.1.1:2000 -> 10.0.1.2:8080: 376 bytes captured (376 bytes) on interface 0
Ethernet II, Src: Cisco_S6155-cb (f4:bd:9e:56:15:cb), Dst: Cisco_S6155-cb (f4:bd:9e:56:15:cb)
802.3Q Virtual LAN, PVID: 4, Src: 0, Dst: 4, 201: 200
Internet Protocol Version 4, Src: 10.0.1.1, Dst: 10.0.1.2
User Datagram Protocol, Src Port: 63745
HTTP Protocol
Code: Access-Request (3)
Packet Length: 376 (3)
Length: 376
Authentication: 7077f5af6a232615c638c0df93020f
[This is a response to a request in frame 1754]
[Time From request: 0.029997000 seconds]
Attribute Value Pairs
-> AP: #00000000000000000000000000000000
  Type: 1
  Length: 4
  User-Name: cba-customer
  -> AP: t=Class(25) 1-50 val=434147533a38033041413843380308080308043357440112108340426328097365
  -> AP: t=Message-Authenticator(80) 1-18 val=2300e18ff1506ab156ca07709cfd3e5
  -> AP: t=Vendor-Specific(20) 1-33 vnd=ciscoSystem(9)
```

Analyse du nouveau paquet d'acceptation d'accès

1. Nom du paquet.
2. Nom d'utilisateur entré par le client final sur le portail affiché.

Là encore, un nouveau test de connectivité de sondage est effectué à partir du client. Une fois que le client a confirmé qu'il dispose d'une connectivité Internet, le portail peut être fermé (il peut l'être automatiquement, en fonction du périphérique utilisé). Le client est maintenant connecté au réseau.

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.