Comprensión del flujo de CWA en un cliente

Contenido

Introducción

Este documento describe el flujo que experimenta el cliente final al conectarse a una WLAN CWA.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre:

- Cisco Wireless LAN Controller (WLC) serie 9800
- Información general sobre la autenticación web central (CWA) y su configuración en Identity Services Engine (ISE)

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de software y hardware:

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

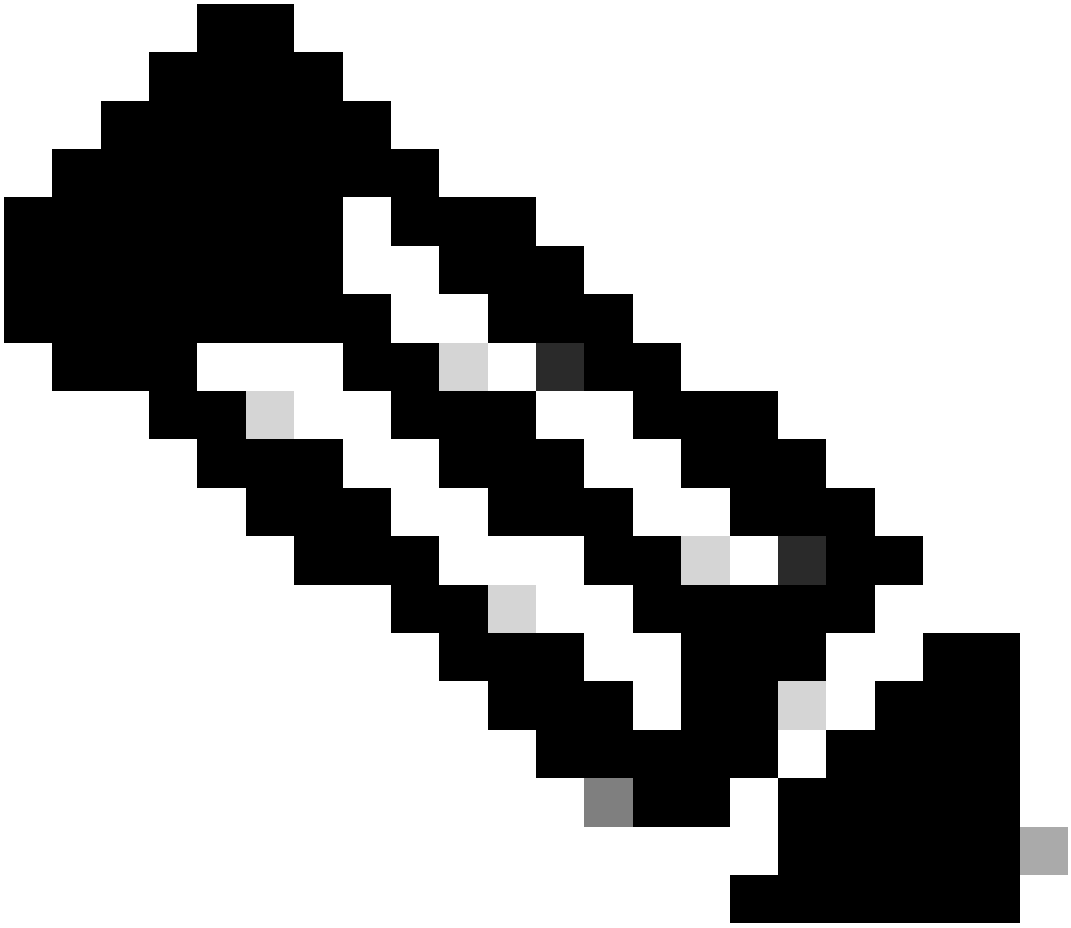
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

CWA es un tipo de autenticación SSID que se puede configurar en el WLC donde al cliente final que intenta conectarse se le pide que ingrese su nombre de usuario y contraseña a un portal web que se les presenta. En resumen, el flujo para el cliente final pasa cuando se conecta a la WLAN es:

1. El cliente final se conecta al SSID que se muestra en su dispositivo
2. El cliente final se redirige al portal web para introducir sus credenciales
3. ISE autentica el cliente final con las credenciales que se han introducido
4. ISE responde al WLC diciendo que el cliente final ha sido autenticado. ISE puede aportar algunos atributos adicionales que el cliente debe cumplir al acceder a la red (como ACL específicas)
5. El cliente final se vuelve a asociar y a autenticar, y finalmente obtiene acceso a la red

---



Nota: Es importante notar que el cliente final que se autentica dos veces es transparente para el cliente final

---

El proceso subyacente por el que debe pasar el cliente se divide básicamente en dos: una conexión del cliente al servidor ISE y, una vez autenticado, otra conexión del cliente a la propia red. El controlador e ISE siempre se comunican entre sí a través del protocolo RADIUS. A continuación, se incluye un análisis en profundidad de un seguimiento radiactivo (RA) y una captura de paquetes integrada (EPC).

CWA Flow - Seguimiento radiactivo (RA)

Un seguimiento de RA es un conjunto de registros capturados para un cliente específico. Muestra todo el proceso por el que pasa el cliente mientras se conecta a una WLAN. Para obtener más información sobre cuáles son y cómo recuperar los seguimientos de RA, visite Comprensión de las Depuraciones Inalámbricas y la Recopilación de Registros en los Controladores de LAN Inalámbrica Catalyst 9800.

Primera conexión: cliente a servidor ISE

El WLC no permite una conexión a la red si el cliente no ha sido autorizado antes por ISE.

Asociación a la WLAN

El WLC detecta que el cliente quiere asociarse a la WLAN "cwa", que se vincula al perfil de política "cwa-policy-profile" y se conecta al AP "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
```

Filtrado de MAC

Probar la conectividad del servidor ISE

Una vez que el WLC ha recibido la solicitud de asociación del cliente, el primer paso es realizar el filtrado de MAC (también conocido como MAB). El filtrado de MAC es un método de seguridad en el que la dirección MAC del cliente se compara con una base de datos para validar si se les permite unirse a la red o no.

<#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_
[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_INI
[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 hdl 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_AWA
[ewlc-infra-evq] [17558]: (note): Authentication Success. Resolved Policy bitmap:11 for client 4203.952
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_MAB
[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
```

El WLC envía la solicitud a ISE

El WLC envía un paquete RADIUS Access-Request a ISE que contiene la dirección MAC del cliente que desea autenticarse en la 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

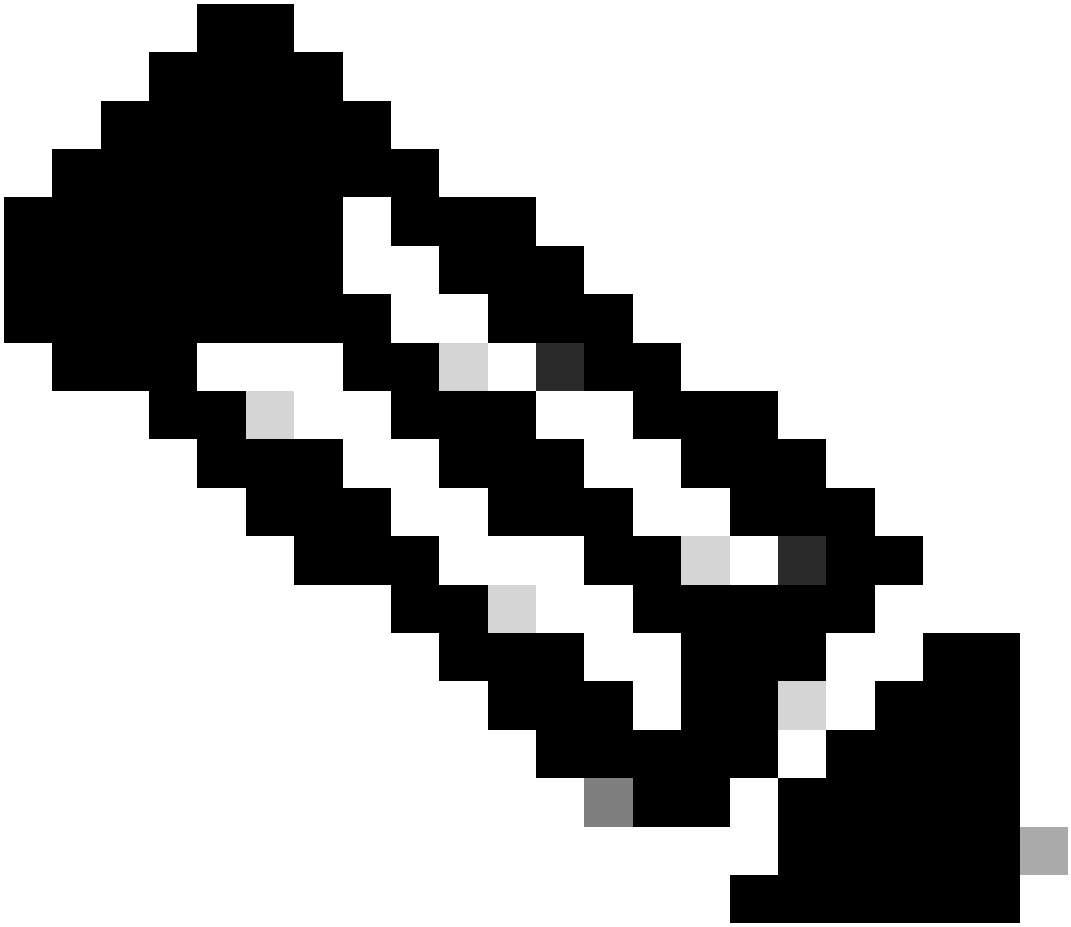
"

<-- 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
```



Nota: Un par AV es "Attribute-Value" que utiliza ISE. Es una estructura Key-Value de la

---

información predefinida que se puede enviar al WLC. Estos valores se aplican en ese cliente específico para esa sesión específica.

Ejemplos de pares AV:

- nombre de ACL
- URL de redireccionamiento
- asignación de VLAN
- Temporizadores de tiempo de espera de sesión
- Temporizadores de reautenticación

ISE responde a la solicitud del WLC

Si ISE acepta la dirección MAC enviada por el WLC, ISE envía un paquete RADIUS Access-Accept. En función de la configuración de ISE, si se trata de una dirección MAC desconocida, ISE debe aceptarla y continuar con el flujo. Si ve un mensaje de Access-Reject, significa que hay algo que no está configurado correctamente en ISE que debe verificarse.

<#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

Procesos WLC de información recibida de ISE

El WLC procesa toda la información recibida de ISE. Con ella, aplica el perfil de usuario que había creado originalmente con el de los datos enviados por ISE. El WLC asigna una nueva ACL al usuario, por ejemplo. Si AAA Override no se habilita en el WLAN, este procesamiento por el WLC no ocurre.

<#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 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

Finaliza la autenticación MAB

Después de que el perfil de usuario para el cliente se ha modificado con éxito, el WLC termina de autenticar la dirección MAC del cliente. Si la ACL recibida de ISE no existe en el WLC, el WLC no sabe qué hacer con esa información, y por lo tanto la acción REEMPLAZAR falla completamente causando que la autenticación MAB falle también. El cliente no puede autenticarse.

<#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

El WLC envía la respuesta de asociación al cliente

Ahora que el cliente ha sido autenticado por ISE y se ha aplicado la ACL correcta, el WLC finalmente envía una respuesta de asociación al cliente. Ahora, el usuario puede continuar conectándose a la red.

<#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.

Autenticación L2

Según el proceso que un cliente debe pasar cuando se asocia a una WLAN, la autenticación L2 "comienza". Sin embargo, en realidad, la autenticación L2 ya se ha realizado debido a la autenticación MAB realizada anteriormente. El cliente completa inmediatamente la autenticación 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
```

Data Plumb

El WLC asigna recursos al cliente de conexión para que el tráfico pueda fluir a través de la red.

<#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
```

Se asigna una dirección IP al usuario

El usuario final necesita una dirección IP para navegar por la red. Se somete al proceso DHCP. Si el usuario se conectó anteriormente y recuerda su dirección IP, se omite el proceso DHCP. Si el usuario no puede recibir una dirección IP, el usuario final no podrá ver el portal web. De lo contrario, sigue los siguientes pasos:

1. Se envía un paquete DISCOVER desde el cliente de conexión como una difusión para encontrar cualquier servidor DHCP disponible
2. Si hay un servidor DHCP disponible, el servidor DHCP responde con una OFERTA. La oferta contiene información como la dirección IP que se asignará al cliente de conexión, el tiempo de concesión, etc. Puede haber muchas OFERTAS recibidas de varios servidores DHCP
3. El cliente acepta una OFERTA de uno de los servidores y responde con una SOLICITUD para la dirección IP que ha seleccionado
4. Finalmente, el servidor DHCP envía un paquete de RECONOCIMIENTO al cliente con su nueva dirección IP asignada

El WLC registra el método que el cliente recibió su dirección 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 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}: [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 DH
{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

Comienza la autenticación L3

Ahora que el usuario final ha recibido una dirección IP, la autenticación L3 comienza con CWA detectado como el método deseado para la autenticación.

<#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

Pruebas de direcciones IP seguras

Para avanzar con la conexión, el cliente debe realizar dos solicitudes ARP:

1. Valide que nadie más tenga su dirección IP. Si hay una respuesta ARP para la dirección IP del usuario final, entonces es una dirección IP duplicada

2. Valide la disponibilidad para el gateway. Esto es para garantizar que el cliente pueda salir de la red. La respuesta ARP debe ser del gateway

<#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:
{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: 0.0.0.0, ARP target IP:
{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: 0.0.0.0, ARP target IP: <
{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>, AR
{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
```

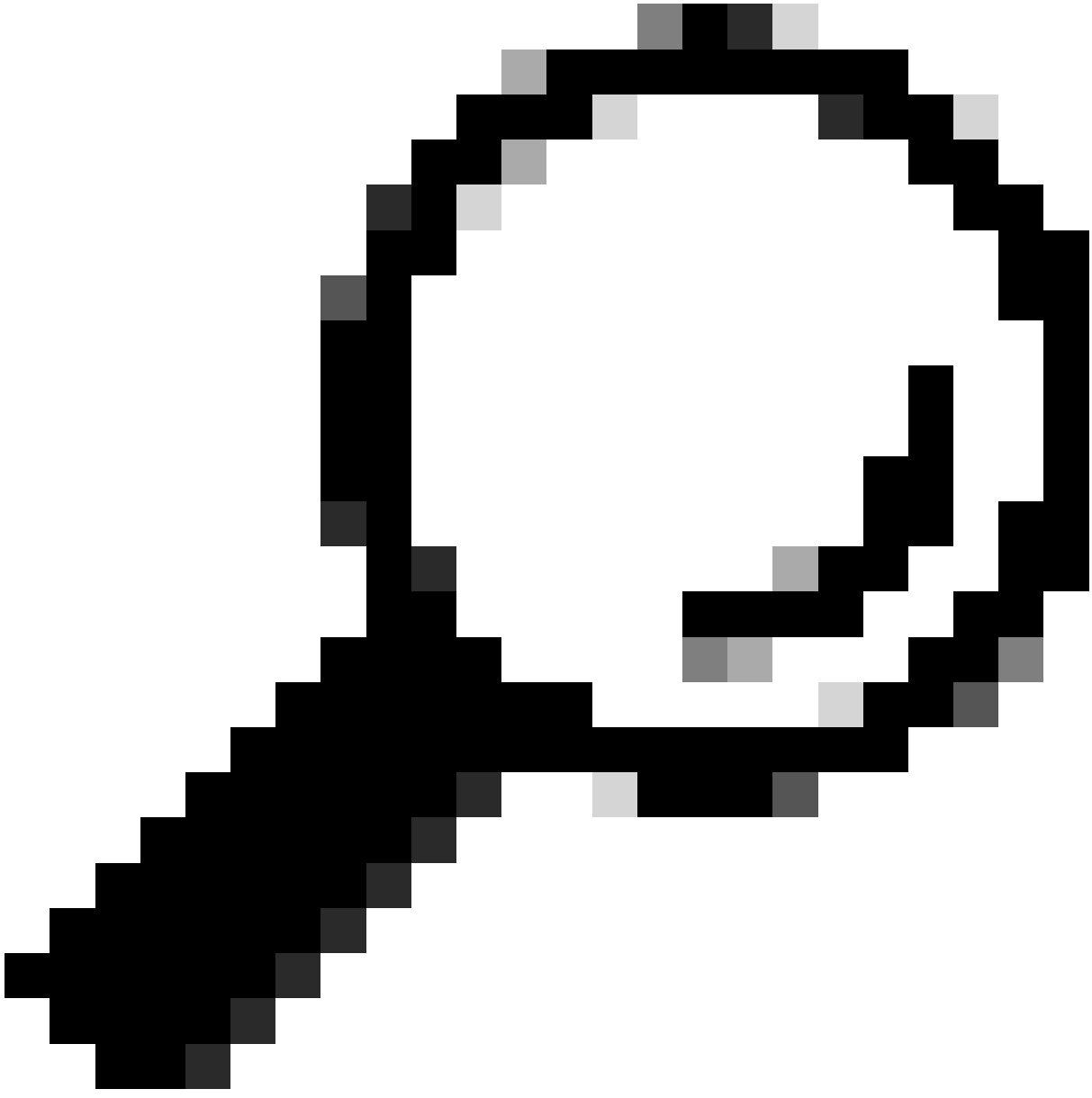
Segunda conexión: cliente a red

En este momento, el usuario final se ha autenticado con ISE a través de su dirección MAC, pero

aún no se ha autorizado completamente. El WLC debe hacer referencia a ISE una vez más para autorizar al cliente a conectarse a la red. En este punto, el portal se presenta al usuario en el cual el nombre de usuario debe ingresar su nombre de usuario y contraseña. En el WLC, el usuario final se ve en el estado "Pendiente de autenticación Web".

Cambio de autorización (CoA)

Aquí es donde el "soporte para CoA" en la configuración del WLC entra en efecto. Hasta este momento, se utilizaba la ACL. Una vez que el cliente final ve el portal, la ACL ya no se utiliza, ya que lo único que hizo fue redirigir al cliente al portal. En este punto, el cliente ingresa sus credenciales para iniciar el proceso CoA y reautenticar al cliente. El WLC prepara el paquete que se enviará y lo reenvía a ISE



Sugerencia: CoA utiliza el puerto 1700. Asegúrese de que el firewall no lo ha bloqueado.

<#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 sucess 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
```

Segunda autenticación para ISE

La segunda autenticación no comienza desde cero. Este es el poder del CoA. Se pueden aplicar nuevas reglas y/o pares AV al usuario. La ACL y la URL de redirección recibidas en la primera Access-Accept ya no se envían al usuario final.

El WLC envía la solicitud a ISE

El WLC envía un nuevo paquete RADIUSAccess-Request a ISE con la combinación de nombre de usuario/contraseña ingresada. Esto activa una nueva autenticación MAB y, dado que ISE ya conoce al cliente, se debe aplicar un nuevo conjunto de políticas (por ejemplo, Acceso concedido).

<#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 responde a la solicitud del WLC

ISE realiza una búsqueda de su política y, si el nombre de usuario recibido coincide con el perfil de política, ISE responde al WLC una vez más y acepta la conexión del cliente a la WLAN. Devuelve el nombre del usuario final. Si se configura en ISE, se pueden aplicar reglas adicionales o pares AV al usuario y se ven en 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

Procesos WLC de información recibida de ISE

Una vez más, el WLC procesa la información recibida por ISE. Realiza otra acción REEMPLAZAR en el usuario con los nuevos valores recibidos de 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 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

Finaliza la autenticación L3

El usuario final se ha autenticado con los datos proporcionados. La autenticación L3 (autenticación web) ha finalizado.

<#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
```

El usuario final alcanza el estado de ejecución en el WLC

Finalmente, el usuario se autentica y se asocia a la WLAN.

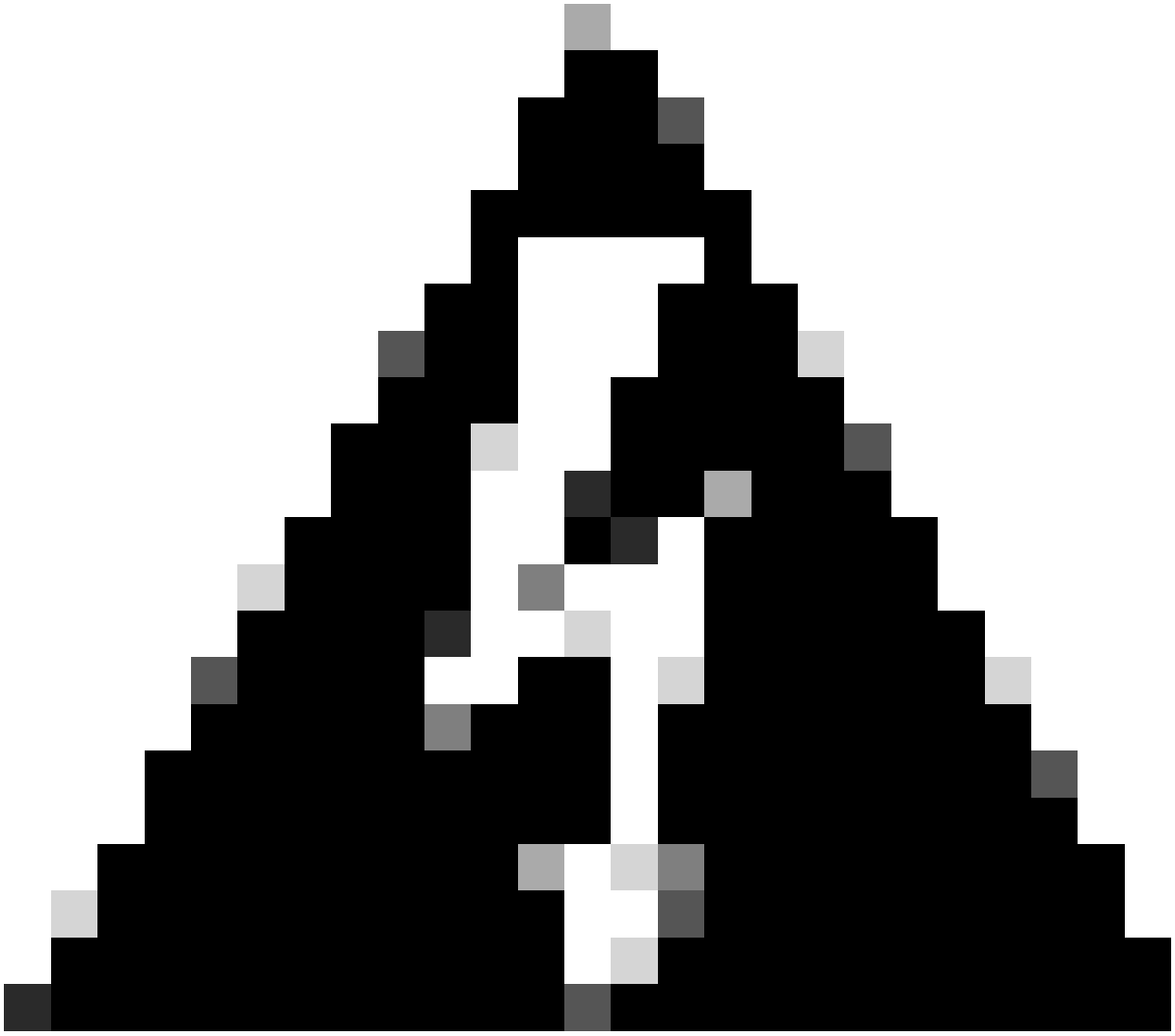
<#root>

```
{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
```

CWA Flow: captura de paquetes integrada (EPC)

Un EPC es una captura de paquetes que se puede recuperar directamente del WLC que muestra todos los paquetes que están pasando a través del WLC o que se están originando de él. Para obtener más información sobre cuáles son y cómo recuperarlos, visite Comprensión de las Depuraciones Inalámbricas y la Recopilación de Registros en los Controladores de LAN Inalámbrica Catalyst 9800.

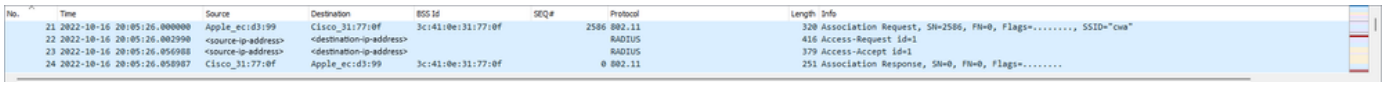
Primera conexión: cliente a servidor ISE



Advertencia: se han eliminado las direcciones IP de las imágenes de la captura de paquetes. Se muestran como y

---

Asociación a la WLAN y solicitud enviada al servidor ISE

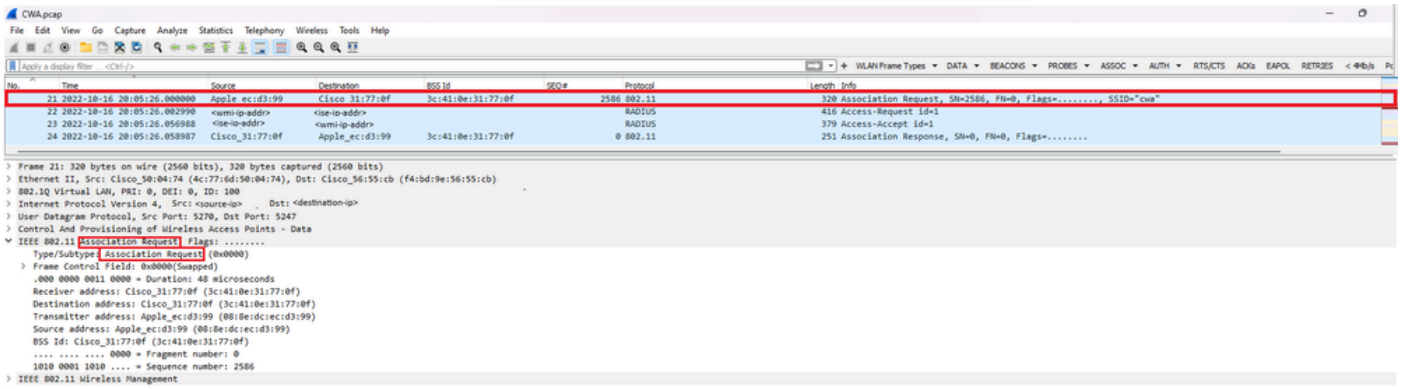


No.	Time	Source	Destination	BSS Id	SEQ#	Protocol	Length	Info
21	2022-10-16 20:05:26.000000	Apple_ec:d3:99	Cisco_31:77:0f	3c:41:0e:31:77:0f	2586	802.11	320	Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
22	2022-10-16 20:05:26.002990	<source-ip-address>	<destination-ip-address>			RADIUS	416	Access-Request id=1
23	2022-10-16 20:05:26.056988	<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, SN=0, FN=0, Flags=........

Primeros paquetes

Solicitud de asociación del WLC al cliente

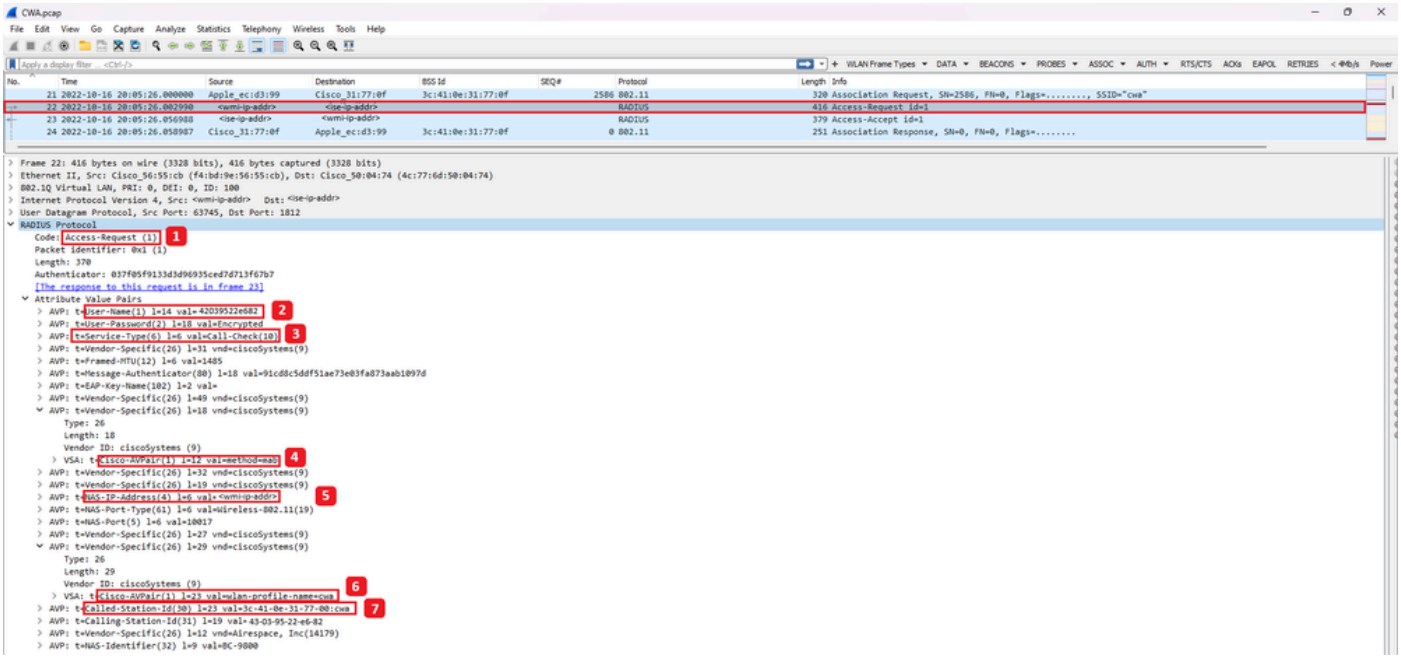
Si observa el primer paquete "Solicitud de asociación", puede ver las direcciones MAC de los dispositivos que participan en este proceso.



Solicitud de asociación

Paquete de solicitud de acceso enviado desde el WLC a ISE

Una vez que el WLC ha procesado la solicitud de asociación, el WLC envía un paquete Access-Request al servidor ISE.

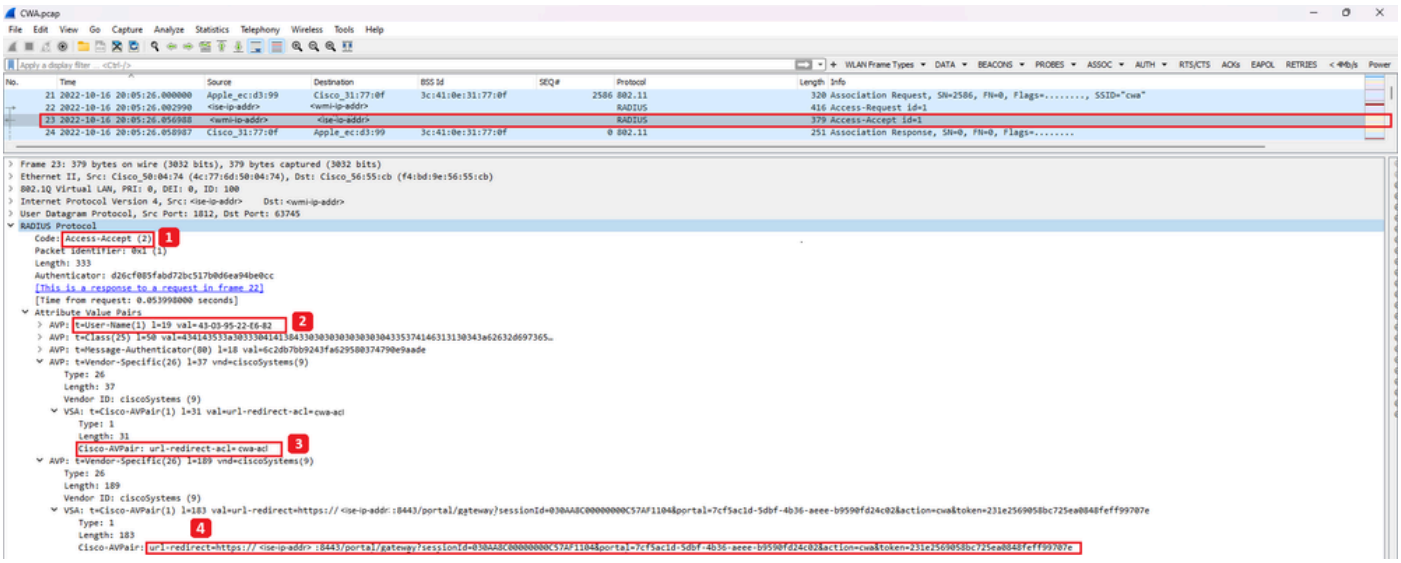


Análisis del paquete de solicitud de acceso

1. Nombre del paquete.
2. La dirección MAC que está intentando autenticarse.
3. Esto indica un filtrado de MAC.
4. El par AV enviado por el controlador a ISE para indicar un proceso de filtrado de MAC.
5. La dirección IP WMI del WLC.
6. El SSID que el cliente está intentando conectar.
7. El nombre de la WLAN que el cliente está intentando conectar.

Paquete de aceptación de acceso enviado desde el WLC a ISE

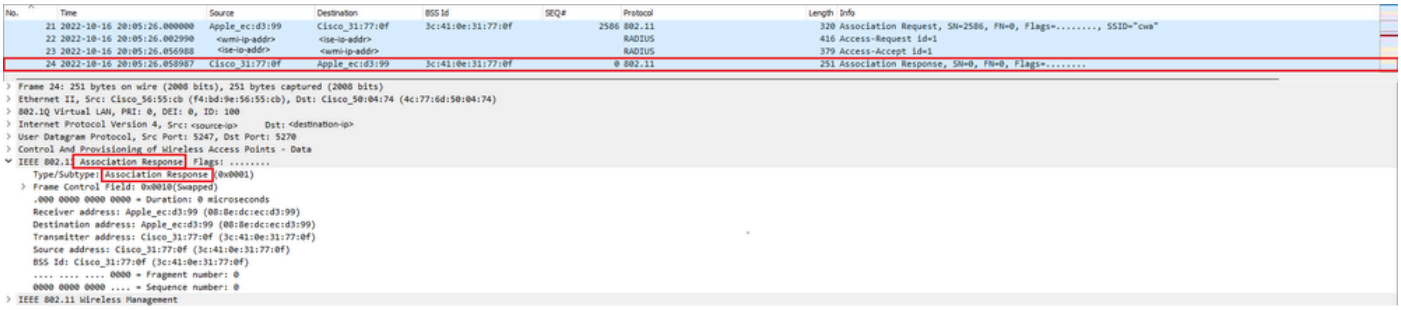
Una vez que ISE ha procesado el paquete Access-Accept, responde con un Access-Accept si es exitoso o con un Access-Reject si no lo es.



Análisis del paquete de aceptación de acceso

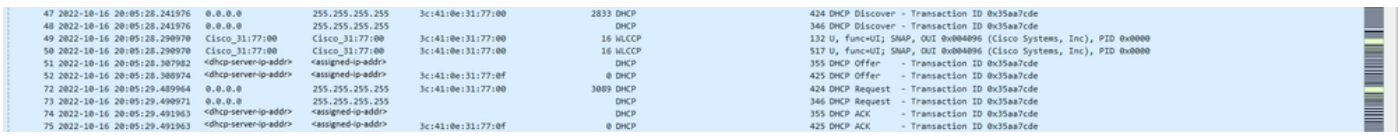
1. Nombre del paquete.
2. La dirección MAC autenticada.
3. ACL que se va a aplicar.
4. URL a la que se redirigirá al usuario.

Respuesta de Asociación del WLC al Cliente

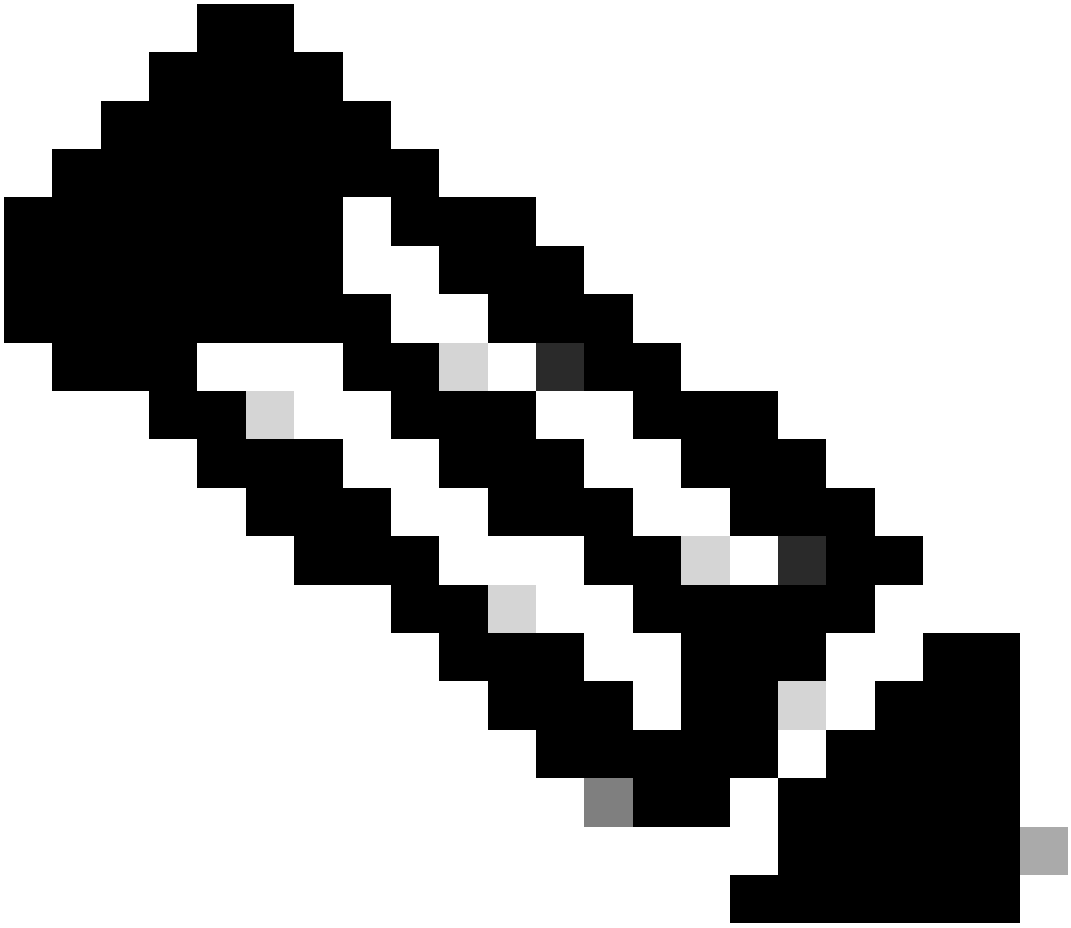


Respuesta de asociación

Proceso DHCP



Proceso DHCP



Nota: A partir de ahora, los paquetes se ven duplicados, pero eso es solo porque uno está encapsulado CAPWAP y el otro no

---

ARP

78	2022-10-16 20:05:29.496968	Apple_ec:d3:99	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_ec:d3:99	Broadcast			ARP	60 Who has <assigned-ip-addr> (ARP Probe)
80	2022-10-16 20:05:29.847948	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	3601	ARP	124 Who has <assigned-ip-addr> (ARP Probe)
81	2022-10-16 20:05:29.847948	Apple_ec:d3:99	Broadcast			ARP	60 Who has <assigned-ip-addr> (ARP Probe)
82	2022-10-16 20:05:30.142982	Apple_ec:d3:99	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_ec:d3:99	Broadcast			ARP	60 Who has <assigned-ip-addr> (ARP Probe)
84	2022-10-16 20:05:30.464972	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	17	ARP	124 ARP Announcement for <assigned-ip-addr>
85	2022-10-16 20:05:30.465964	Apple_ec:d3:99	Broadcast			ARP	60 ARP Announcement for <assigned-ip-addr>
88	2022-10-16 20:05:30.790944	Apple_ec:d3:99	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_ec:d3:99	Broadcast			ARP	60 ARP Announcement for <assigned-ip-addr>
90	2022-10-16 20:05:31.115991	Apple_ec:d3:99	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_ec:d3:99	Broadcast			ARP	60 ARP Announcement for <assigned-ip-addr>
92	2022-10-16 20:05:31.117990	Apple_ec:d3:99	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_ec:d3:99	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_ec:d3:99			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_ec:d3:99	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 20:05:31.192983	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	1809	ARP	124 Who has 192.168.20.1? Tell <assigned-ip-addr>
98	2022-10-16 20:05:31.193974	Apple_ec:d3:99	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_ec:d3:99			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_ec:d3:99	3c:41:0e:31:77:0f	0	ARP	134 192.168.20.1 is at 4c:77:6d:50:04:74

ARP del cliente para su propia dirección IP y para la puerta de enlace

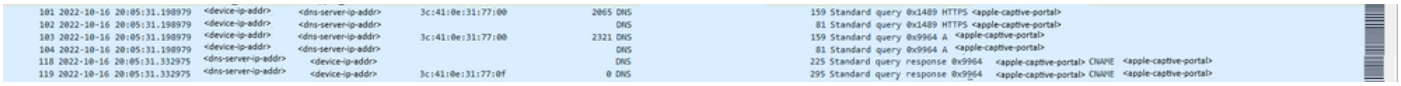
Prueba de conectividad

Una vez que el proceso ARP ha terminado, el dispositivo que está intentando conectar realiza una

comprobación para validar si se activa un portal, esto también se conoce como sondeo. Si el dispositivo indica que no hay conexión a Internet, significa que el proceso ARP ha fallado (por ejemplo, la puerta de enlace nunca contestó) o que el dispositivo no ha podido realizar el sondeo.

Este sondeo es algo que no se ve en los rastros de RA, solo el EPC puede proporcionar esta información. La consulta de sondeo depende del dispositivo que está intentando una conexión; en este ejemplo, el dispositivo de prueba era un dispositivo de Apple, por lo que la sonda se realizó directamente hacia el portal cautivo de Apple.

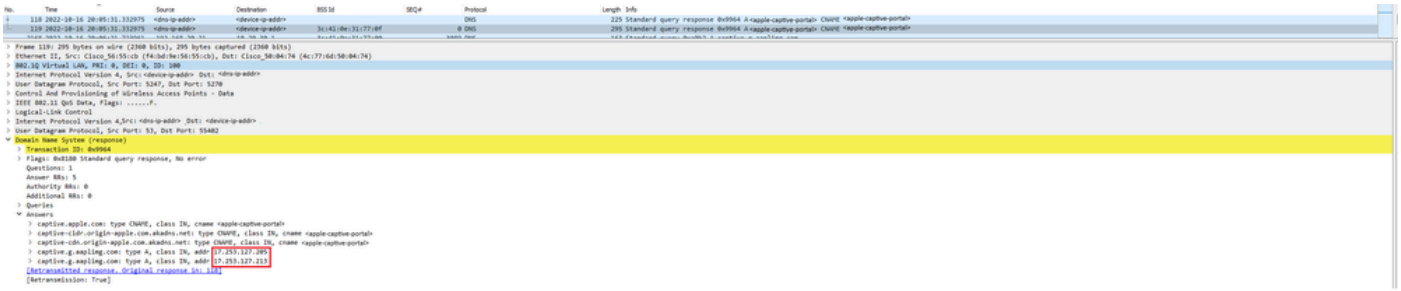
Dado que el sondeo se realiza mediante una URL, se requiere DNS para resolver esta URL. Por lo tanto, si el servidor DNS no puede responder a las consultas del cliente, el cliente continúa consultando la URL y el portal nunca se ve. En este momento, si la dirección IP del servidor ISE se introduce en el navegador web del dispositivo final, el portal debe estar visible. Si es así, hay un problema con el servidor DNS.



Prueba de conectividad del cliente: consulta y respuesta de DNS

Dirección IP resuelta de DNS

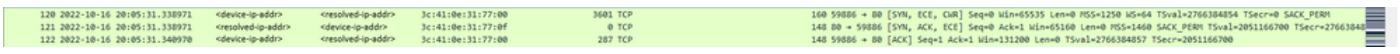
Después de inspeccionar la respuesta a la consulta DNS, puede ver la dirección IP que resolvió el servidor DNS.



Dirección IP resuelta por servidor DNS

Establecer protocolo de enlace de 3 vías

Ahora que se ha resuelto la dirección IP de DNS, se establece un protocolo de enlace TCP de 3 vías entre el portal y el cliente. La dirección IP utilizada es cualquiera de las direcciones IP resueltas.

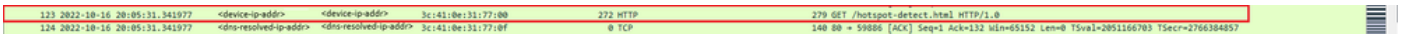


Establecimiento de contacto de 3 vías

GET Hotspot

Una vez que se ha establecido la sesión TCP, el cliente realiza un sondeo e intenta acceder al

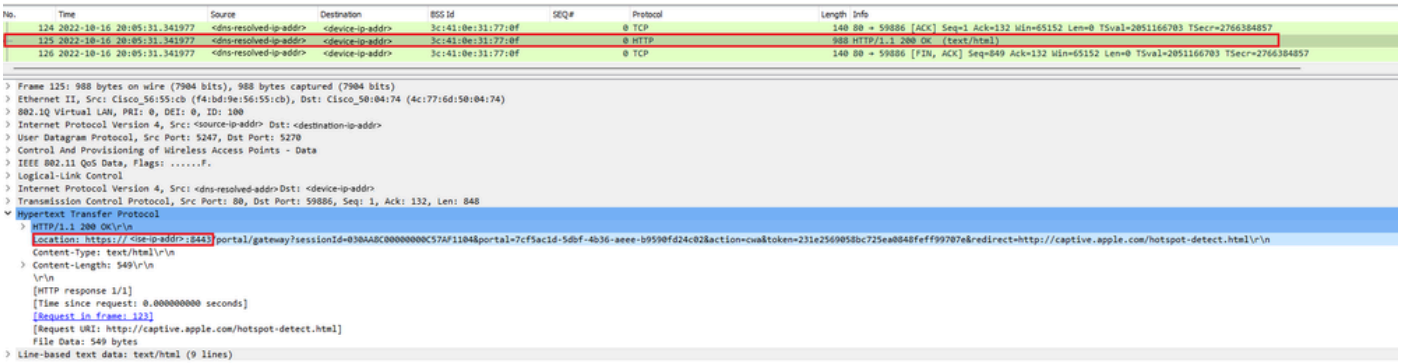
portal.



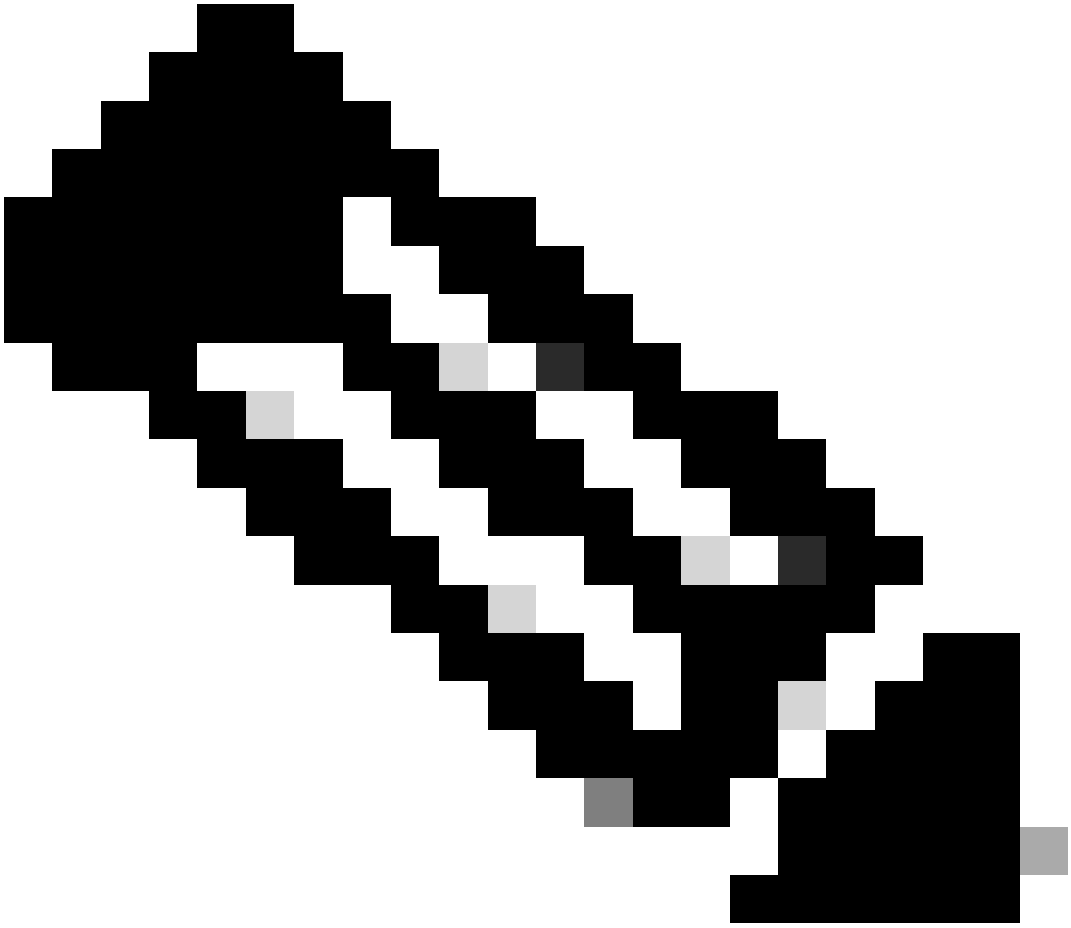
GET Hotspot

Aceptar paquete

El paquete OK contiene el portal de ISE al que se debe redirigir al cliente.



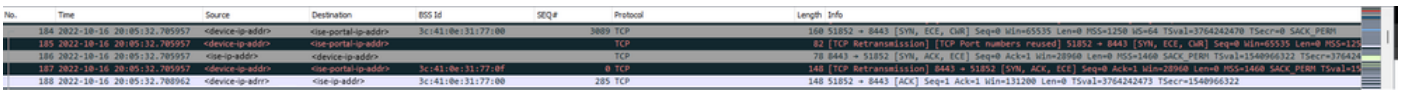
Aceptar paquete



Nota: La mayoría de las personas tienen otra URL devuelta en el paquete OK. Por lo tanto, es necesario realizar otra consulta DNS para obtener la dirección IP final.

Nueva sesión TCP establecida

Ahora que se ha descubierto la dirección IP del portal, se intercambian muchos paquetes, pero al final un paquete con la IP de destino que se devolvió en el paquete OK (o resuelto por DNS) que corresponde a la dirección IP de ISE, muestra una nueva sesión TCP que se establece en el portal.



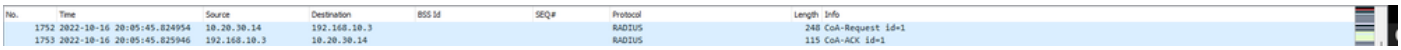
Segunda conexión y nueva sesión TCP al portal ISE

El portal se muestra al usuario

Llegados a este punto, el portal de ISE se muestra finalmente en el navegador del navegador del cliente. Como antes, muchos paquetes se intercambian entre ISE y el dispositivo; cosas como un saludo de cliente y un saludo de servidor, etc. Aquí es donde ISE solicita al cliente el nombre de usuario y la contraseña, acepta los términos y condiciones o lo que sea que se haya configurado en el servidor de ISE.

Solicitud de CoA/Reconocimiento de CoA

Una vez que el usuario ha introducido todos los datos solicitados, ISE envía una solicitud de CoA al controlador para cambiar la autorización del usuario. Si todo en el WLC se configura como se espera, como tener el estado NAC, el soporte para el CoA, y así sucesivamente, el WLC envía un reconocimiento CoA (CoA ACK). De lo contrario, el WLC puede enviar un CoA Non-Acknowledgement (CoA NACK) o simplemente no envía el CoA ACK.

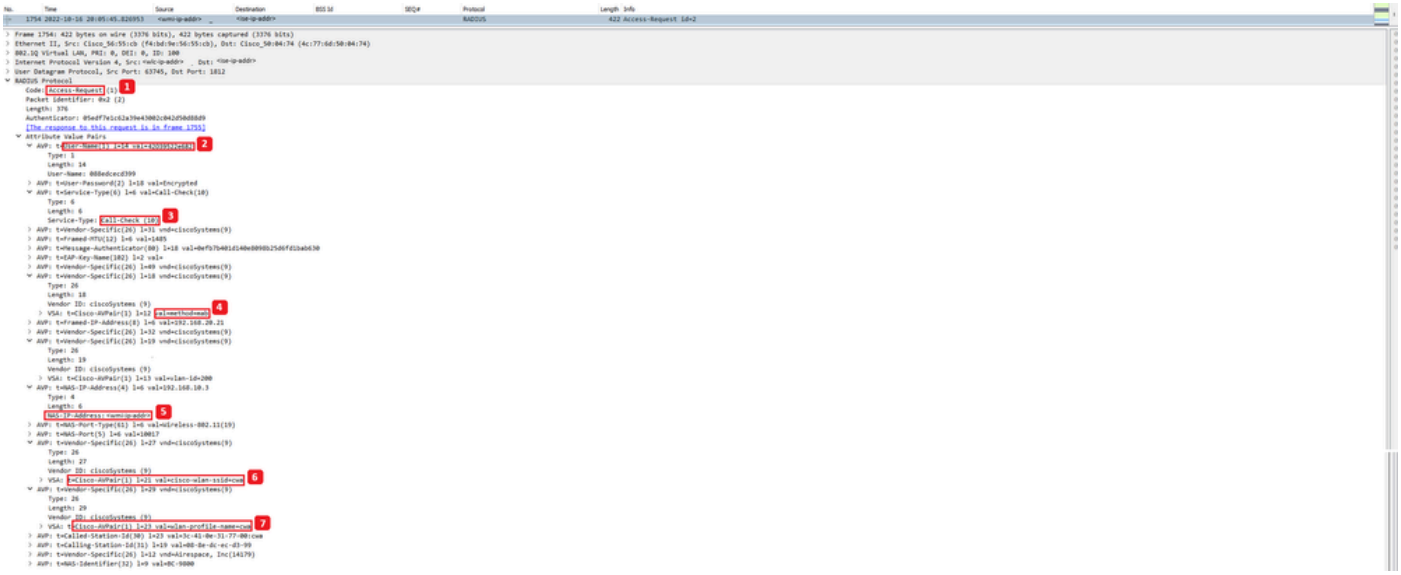


Solicitud y confirmación de CoA

Segunda conexión: cliente a red

Nueva solicitud de acceso

El WLC envía un nuevo paquete Access-Request a ISE.

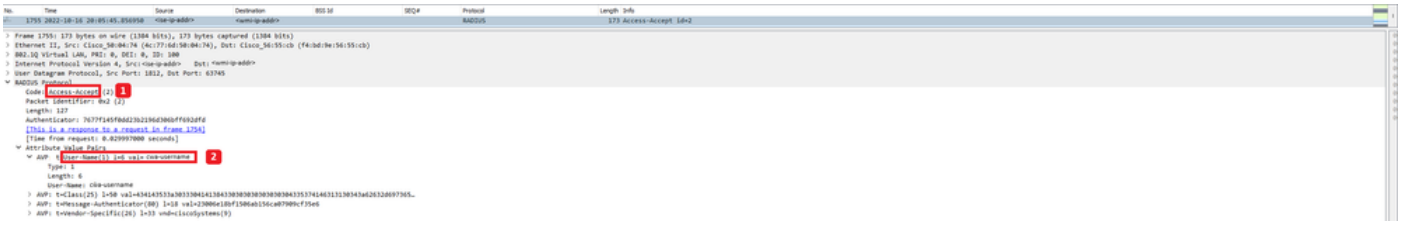


Análisis del nuevo paquete de solicitud de acceso

1. Nombre del paquete.
2. La dirección MAC que está intentando autenticarse.
3. Esto indica un filtrado de MAC.
4. El par AV enviado por el controlador a ISE para indicar un proceso de filtrado de MAC.
5. La dirección IP WMI del WLC.
6. El SSID que el cliente está intentando conectar.
7. El nombre de la WLAN que el cliente está intentando conectar.

Nuevo Access-Accept

El WLC envía un nuevo paquete Access-Request a ISE.



Análisis del nuevo paquete de aceptación de acceso

1. Nombre del paquete.
2. El nombre de usuario ingresado por el cliente final en el portal que se mostró.

Una vez más, se realiza una nueva prueba de conectividad de sondeo desde el cliente. Una vez que el cliente ha confirmado que dispone de conexión a Internet, el portal se puede cerrar (se puede cerrar automáticamente, en función del dispositivo utilizado). El cliente está ahora conectado a la red.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).