

Informazioni sul flusso CWA in un client

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Flusso CWA - traccia radioattiva \(RA\)](#)

[Prima connessione: dal client al server ISE](#)

[Seconda connessione: da client a rete](#)

[CWA Flow - EPC \(Embedded Packet Capture\)](#)

[Prima connessione: dal client al server ISE](#)

[Seconda connessione: da client a rete](#)

Introduzione

Questo documento descrive il flusso del client finale quando si connette a una WLAN CWA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza base di:

- Cisco Wireless LAN Controller (WLC) serie 9800
- Informazioni generali su CWA (Central Web Authentication) e la relativa configurazione su ISE (Identity Services Engine)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software e hardware:

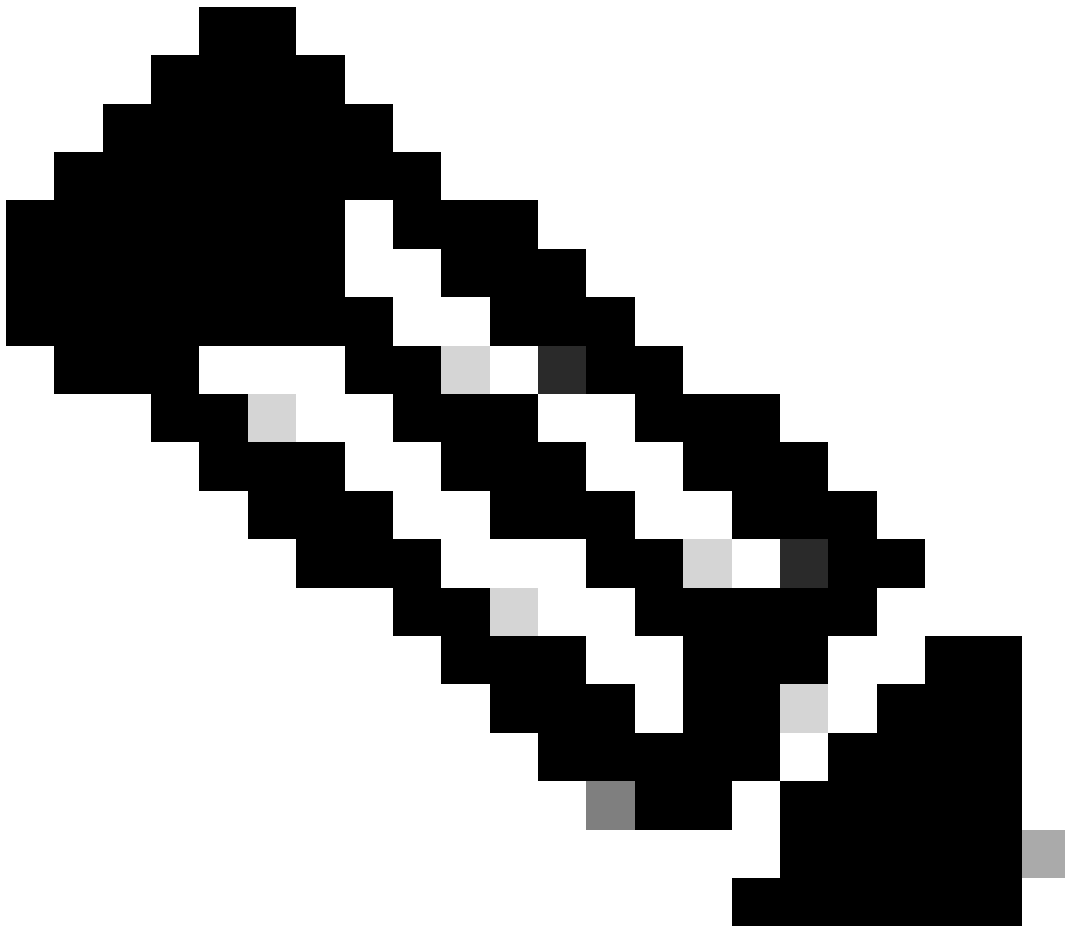
- 9800-CL WLC
- Cisco AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- Identity Service Engine (ISE) v3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

CWA è un tipo di autenticazione SSID che può essere configurato sul WLC in cui al client finale che tenta di connettersi viene richiesto di immettere il nome utente e la password per il portale Web che gli viene presentato. In breve, il flusso per il client finale quando ci si connette alla WLAN è:

1. Il client finale si connette all'SSID visualizzato sul dispositivo
2. Il client finale viene reindirizzato al portale Web per immettere le credenziali
3. Il client finale viene autenticato da ISE con le credenziali immesse
4. ISE risponde al WLC dicendo che il client finale è stato autenticato. ISE può eseguire il push di alcuni attributi aggiuntivi che il client deve rispettare quando accede alla rete (ad esempio, ACL specifici)
5. Il client terminale viene riassociato e riautenticato e infine ottiene l'accesso alla rete



Nota: è importante notare che il client finale autenticato due volte è trasparente per il client finale

Il processo sottostante che il client deve eseguire è fondamentalmente diviso in due: una connessione dal client al server ISE e, una volta autenticato, un'altra connessione dal client alla rete stessa. Il controller e l'ISE comunicano sempre tra loro tramite il protocollo RADIUS. Di seguito viene riportata un'analisi approfondita di una traccia Radioattiva (RA) e di un'acquisizione EPC (Embedded Packet Capture).

Flusso CWA - traccia radioattiva (RA)

Una traccia RA è un insieme di registri acquisiti per un client specifico. Mostra l'intero processo che il client sta attraversando durante la connessione a una WLAN. Per ulteriori informazioni su questi parametri e su come recuperare le tracce di registrazione, consultare il documento sulla [descrizione dei debug wireless e la raccolta dei log sui controller Catalyst 9800 Wireless LAN](#).

Prima connessione: dal client al server ISE

Il WLC non consente la connessione alla rete se il client non è stato autorizzato da ISE in precedenza.

Associazione alla WLAN

Il WLC rileva che il client desidera associare la WLAN "cwa", che utilizza il profilo della policy "cwa-policy-profile" e si connette all'access point "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
```

Filtro MAC

Test connettività server ISE

Dopo che il WLC ha ricevuto la richiesta di associazione dal client, il primo passaggio è eseguire il filtro MAC (noto anche come MAB). Il filtro MAC è un metodo di sicurezza in cui l'indirizzo MAC del client viene confrontato con un database per verificare se è consentito o meno il collegamento alla rete.

<#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 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_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
```

WLC invia una richiesta ad ISE

Il WLC invia un pacchetto Access-Request RADIUS ad ISE contenente l'indirizzo MAC del client che desidera autenticarsi sulla 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
```

```
"
```

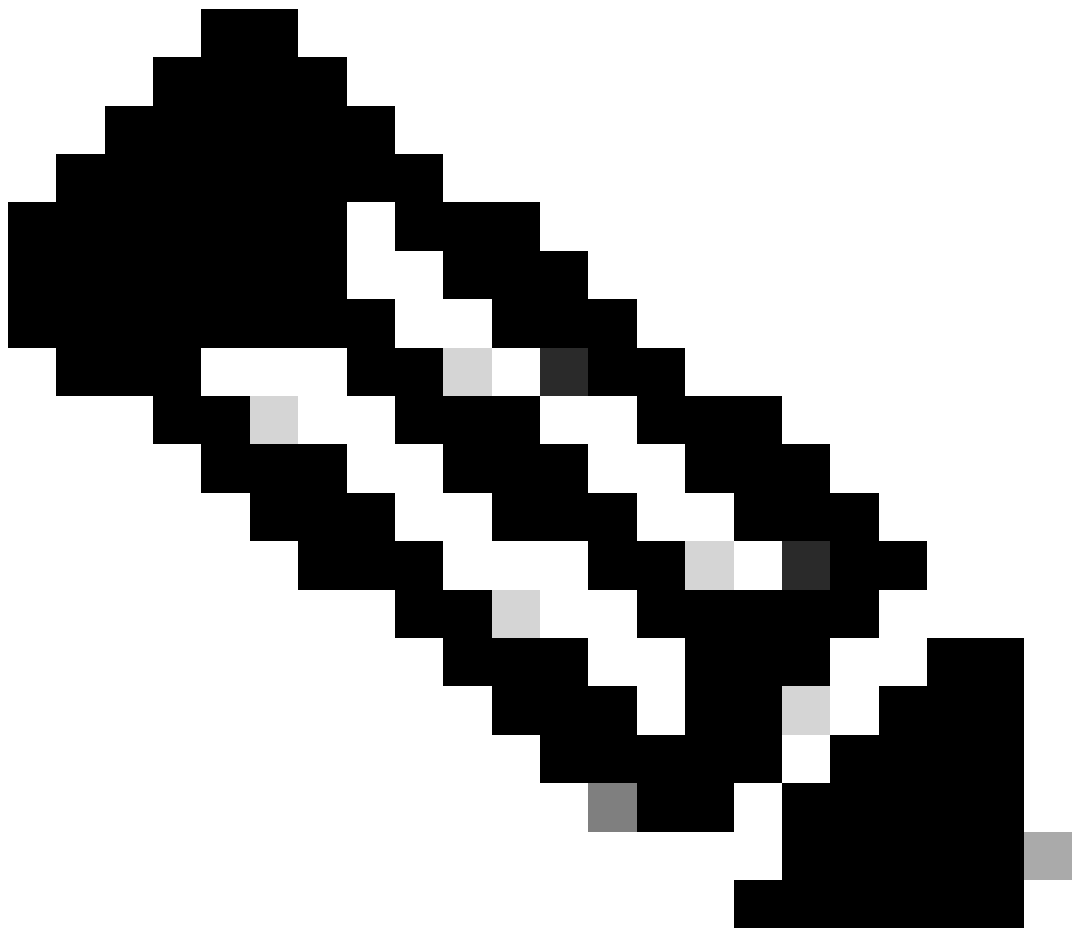
```
<-- SSID and WLAN the client is attempting to connect
```

```
[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: una coppia AV è "Attribute-Value" utilizzata da ISE. Si tratta di una struttura Key-

Value di informazioni predefinite che possono essere inviate al WLC. Questi valori vengono applicati al client specifico per la sessione specifica.

Esempi di coppie AV:

- Nome ACL
- Reindirizza URL
- Assegnazione VLAN
- Timer di timeout della sessione
- Timer di riautenticazione

ISE risponde alla richiesta WLC

Se l'indirizzo MAC inviato dal WLC viene accettato da ISE, ISE invia un pacchetto RADIUS Access-Accept. A seconda della configurazione ISE, se si tratta di un indirizzo MAC sconosciuto, ISE deve accettarlo e continuare con il flusso. Se viene visualizzato un messaggio di rifiuto dell'accesso, significa che è presente un elemento non configurato correttamente in ISE che deve essere verificato.

<#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 ab
```

```
[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

```

Processi WLC delle informazioni ricevute da ISE

Il WLC elabora tutte le informazioni ricevute da ISE. e applica il profilo utente creato inizialmente con i dati inviati da ISE. Ad esempio, il WLC assegna un nuovo ACL all'utente. Se l'opzione AAA Override non è abilitata sulla WLAN, l'elaborazione da parte del WLC non viene eseguita.

```
<#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

Fine autenticazione MAB

Una volta modificato correttamente il profilo utente per il client, il WLC completa l'autenticazione dell'indirizzo MAC del client. Se l'ACL ricevuto da ISE non esiste sul WLC, il WLC non sa cosa fare con queste informazioni e quindi l'azione REPLACE non riesce completamente causando il fallimento dell'autenticazione MAB. Il client non è in grado di eseguire l'autenticazione.

<#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 invia una risposta di associazione al client

Ora che il client è stato autenticato da ISE e che è stato applicato l'ACL corretto, il WLC invia una risposta di associazione al client. A questo punto, l'utente può continuare a connettersi alla rete.

<#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.
```

Autenticazione L2

In base al processo che un client deve eseguire quando si associa a una WLAN, l'autenticazione L2 "viene avviata". Tuttavia, in realtà, l'autenticazione L2 è già stata eseguita a causa dell'autenticazione MAB eseguita in precedenza. Il client completa immediatamente l'autenticazione 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 Successful
```

```
{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

Il WLC assegna le risorse al client che si connette in modo che il traffico possa passare attraverso la rete.

<#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 clien
```

```
{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
```

All'utente viene assegnato un indirizzo IP

L'utente finale ha bisogno di un indirizzo IP per navigare attraverso la rete. Viene sottoposta al processo DHCP. Se l'utente era connesso in precedenza e ricorda il proprio indirizzo IP, il processo DHCP viene ignorato. Se l'utente non è in grado di ricevere un indirizzo IP, non potrà visualizzare il portale Web. In caso contrario, verranno eseguite le operazioni seguenti:

1. Un pacchetto DISCOVER viene inviato dal client che si connette come trasmissione per trovare tutti i server DHCP disponibili
2. Se è disponibile un server DHCP, il server DHCP risponde con un'OFFERTA. L'offerta contiene informazioni quali l'indirizzo IP da assegnare al client che esegue la connessione, la durata del lease e così via. È possibile ricevere molte OFFERTE da diversi server DHCP
3. Il client accetta un'OFFERTA da uno dei server e risponde con una RICHIESTA per l'indirizzo IP selezionato
4. Infine, il server DHCP invia un pacchetto di CONFERMA al client con il nuovo indirizzo IP assegnato

Il WLC registra il metodo con cui il client ha ricevuto l'indirizzo IP.

<#root>

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

Avvio autenticazione L3

Ora che l'utente finale ha ricevuto un indirizzo IP, l'autenticazione L3 inizia con CWA rilevato come metodo di autenticazione desiderato.

```
<#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

Test degli indirizzi IP casuali

Per procedere con la connessione, il client deve eseguire due richieste ARP:

1. Verificare che nessun altro utente disponga del proprio indirizzo IP. Se è presente una risposta ARP per l'indirizzo IP dell'utente finale, l'indirizzo IP è duplicato
2. Verificare la raggiungibilità del gateway. In questo modo, il client può uscire dalla rete. La risposta ARP deve provenire dal 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

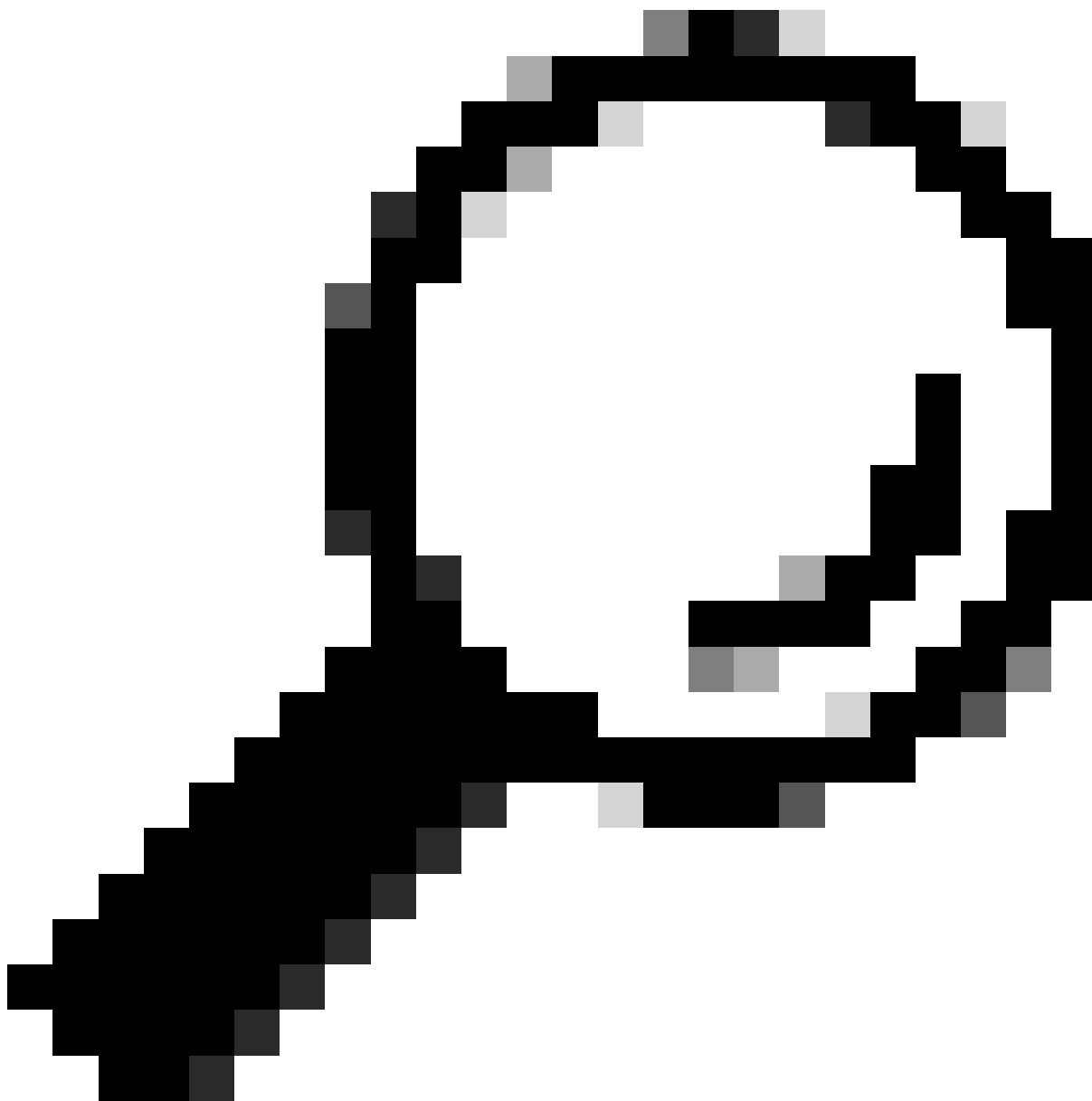
Seconda connessione: da client a rete

A questo punto, l'utente finale è stato autenticato attraverso il suo indirizzo MAC, ma non ha ancora ricevuto l'autorizzazione completa. Per autorizzare il client a connettersi alla rete, il WLC deve fare nuovamente riferimento all'ISE. A questo punto, il portale viene presentato all'utente in

cui il nome utente deve immettere il nome utente e la password. Sul WLC, l'utente finale è visualizzato nello stato "Web Auth Pending".

Cambiamento di autorizzazione (CoA)

In questo caso, il "supporto per CoA" nella configurazione WLC diventa effettivo. Fino a questo punto, è stato usato l'ACL. Dopo che il client finale ha rilevato il portale, l'ACL non viene più utilizzato, in quanto tutto ciò che ha fatto è reindirizzare il client al portale. A questo punto, il client immette le proprie credenziali per l'accesso per avviare il processo CoA e riautenticare il client. Il WLC prepara il pacchetto da inviare e lo inoltra all'ISE



Suggerimento: la CoA utilizza la porta 1700. Assicurarsi che non sia bloccato dal firewall.

```
{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
```

Seconda autenticazione ad ISE

La seconda autenticazione non inizia da zero. Questo è il potere della CoA. È possibile applicare all'utente nuove regole e/o parametri AV. L'ACL e l'URL di reindirizzamento ricevuti al primo accesso-accettazione non vengono più inviati all'utente finale.

WLC invia una richiesta ad ISE

Il WLC invia un nuovo pacchetto RADIUSccess-Requested ad ISE con la combinazione di nome utente e password immessa. Ciò attiva una nuova autenticazione MAB e, poiché ISE conosce già il client, deve essere applicata una nuova serie di criteri (ad esempio, Accesso concesso).

```
<#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 risponde alla richiesta WLC

ISE esegue una ricerca della policy e se il nome utente ricevuto corrisponde al profilo della policy, ISE risponde al WLC un'altra volta, accettando la connessione del client alla WLAN. Restituisce il nome utente dell'utente finale. Se configurato sull'ISE, è possibile applicare all'utente regole aggiuntive e/o coppie AV, che vengono visualizzate sulla scheda 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
```

Processi WLC delle informazioni ricevute da ISE

Ancora una volta, il WLC elabora le informazioni ricevute da ISE. Esegue un'altra azione REPLACE sull'utente con i nuovi valori ricevuti da 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

Fine autenticazione L3

L'utente finale è stato autenticato con i dati specificati. Autenticazione L3 (autenticazione Web) completata.

<#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'utente finale raggiunge lo stato RUN sul WLC

Infine, l'utente viene autenticato e associato alla 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 - EPC (Embedded Packet Capture)

Un EPC è un'acquisizione di pacchetti che può essere recuperata direttamente dal WLC e mostra tutti i pacchetti che passano attraverso il WLC o che vengono originati da esso. Per ulteriori informazioni su cosa sono e come recuperarli, consultare il documento sulla [descrizione dei debug wireless e la raccolta dei log sui controller Catalyst 9800 Wireless LAN](#).

Prima connessione: dal client al server ISE



Avviso: gli indirizzi IP nelle immagini acquisite sono stati eliminati. Vengono visualizzati come e

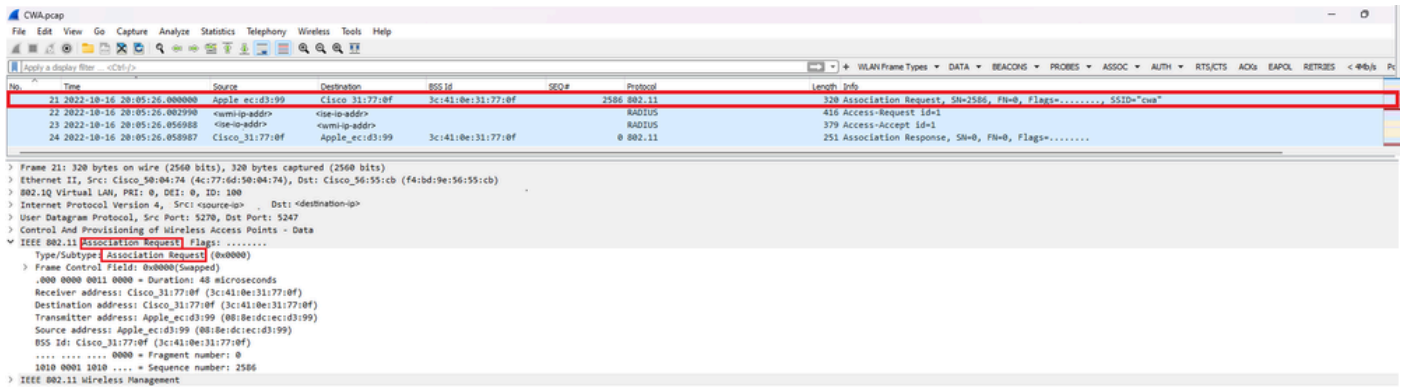
Associazione alla WLAN e richiesta inviata al server ISE

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, SM=2586, FN=0, Flags=....., SSID="cwa"
22	2022-10-16 20:05:26.002900	<source-ip-address>	<destination-ip-address>			RADIUS	416	Access-Request Id=1
23	2022-10-16 20:05:26.056000	<source-ip-address>	<destination-ip-address>			RADIUS	379	Access-Accept Id=1
24	2022-10-16 20:05:26.058907	Cisco_31:77:0f	Apple_ec:d3:99	3c:41:0e:31:77:0f		0 802.11	251	Association Response, SM=0, FN=0, Flags=.....

Primi pacchetti

Richiesta di associazione dal WLC al client

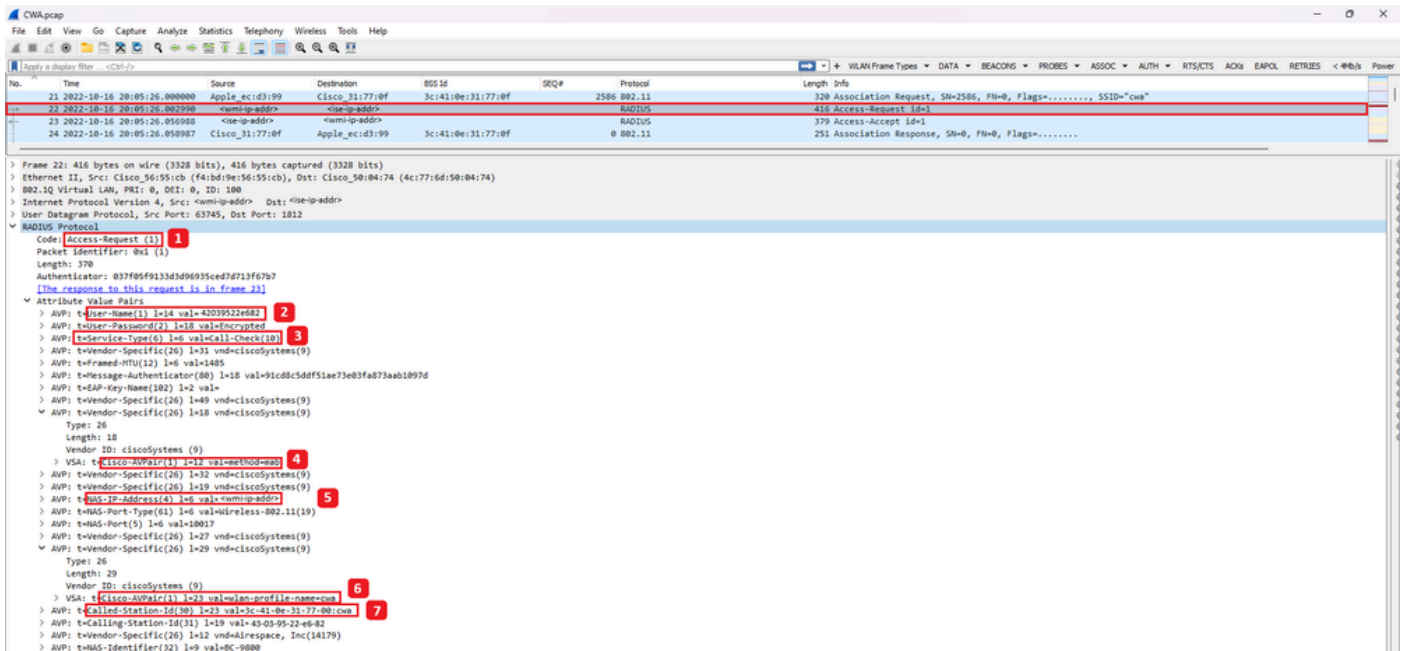
Guardando il primo pacchetto "Association Request" si possono vedere gli indirizzi MAC dei dispositivi coinvolti in questo processo.



Richiesta associazione

Pacchetto Access-Request inviato dal WLC ad ISE

Una volta che la richiesta di associazione è stata elaborata dal WLC, il WLC invia un pacchetto Access-Request al server ISE.



Analisi del pacchetto di richiesta di accesso

1. Nome del pacchetto.
2. L'indirizzo MAC che sta tentando di autenticare.
3. Indica un filtro MAC.
4. La coppia AV inviata dal controller all'ISE per indicare un processo di filtraggio MAC.
5. Indirizzo IP WMI del WLC.
6. SSID che il client sta tentando di connettere.
7. Il nome della WLAN che il client sta tentando di connettere.

Pacchetto Access-Accept inviato dal WLC ad ISE

Una volta elaborato il pacchetto Access-Accept, ISE risponde con Access-Accept in caso di esito positivo o con Access-Reject in caso contrario.

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=43-03-95-22-f6-82 2
 > AVP: t=Cisco(25) l=50 val=43143553a38333041418433030303030304353741663131303043626320697365.
 > AVP: t=Message-Authenticator(80) l=18 val=sc2db7bb9243f629580374790e9aade
 > AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
 Type: 26
 Length: 37
 Vendor ID: ciscoSystems (9)
 > VSA: t=Cisco-APPair(1) l=31 val=url-redirect-acl=cwa-ad
 Type: 1
 Length: 31
 Cisco-APPair: 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-APPair(1) l=183 val=url-redirect=https://<ip>:8443/portal/gateway/sessionId=030A8C0000000C57AF11044portal?cfsacId=5dbf-4b36-aeec-b959fd24c82&action=cwa&token=231e256905b0c725ea8048feff99707e
 Type: 1
 Length: 183
 Cisco-APPair: url-redirect=https://<ip>:8443/portal/gateway/sessionId=030A8C0000000C57AF11044portal?cfsacId=5dbf-4b36-aeec-b959fd24c82&action=cwa&token=231e256905b0c725ea8048feff99707e 4

Analisi del pacchetto di accettazione dell'accesso

1. Nome del pacchetto.
2. Indirizzo MAC autenticato.
3. ACL da applicare.
4. URL a cui reindirizzare l'utente.

Risposta di associazione dal WLC al client

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)
 0000 = Fragment number: 0
 0000 0000 0000 = Sequence number: 0
 > IEEE 802.11 Wireless Management

Risposta associazione

Processo 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 0x004896 (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 0x004896 (Cisco Systems, Inc), PID 0x0000
51	2022-10-16 20:05:28.307982	<dhcp-server-ip>	<assigned-ip>			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	3080	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 20:05:29.491363	<dhcp-server-ip>	<assigned-ip>			DHCP	355	DHCP ACK - Transaction ID 0x35a7cde
75	2022-10-16 20:05:29.491363	<dhcp-server-ip>	<assigned-ip>	3c:41:0e:31:77:0f		DHCP	425	DHCP ACK - Transaction ID 0x35a7cde

Processo DHCP

Nota: da ora in poi, i pacchetti vengono visti duplicati, ma questo solo perché uno è incapsulato in CAPWAP e l'altro no

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 20:05:30.790944	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 192.168.20.17 Tell <assigned-ip-addr>
93	2022-10-16 20:05:31.117990	Apple_ecid3:99	Broadcast			ARP	60 who has 192.168.20.17 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 192.168.20.17 Tell <assigned-ip-addr>
98	2022-10-16 20:05:31.193974	Apple_ecid3:99	Broadcast			ARP	60 who has 192.168.20.17 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

ARP client per il proprio indirizzo IP e per il gateway

Test di connettività

Al termine del processo ARP, il dispositivo che tenta di connettersi esegue un controllo per

verificare se un portale è stato attivato. Questa operazione è nota anche come probe. Se il dispositivo indica che non è disponibile una connessione a Internet, significa che il processo ARP non è riuscito (ad esempio, il gateway non ha mai risposto) oppure che il dispositivo non è stato in grado di eseguire il probe.

Questo tipo di indagine non è presente nelle tracce dell'RA, solo l'EPC è in grado di fornire queste informazioni. La query di probe dipende dal dispositivo che sta tentando una connessione, in questo esempio il dispositivo di prova era un dispositivo Apple, quindi la probe è stata effettuata direttamente verso il portale captive di Apple.

Poiché il probe viene eseguito utilizzando un URL, per risolvere l'URL è necessario il DNS. Pertanto, se il server DNS non è in grado di rispondere alle query del client, il client continua a eseguire query per l'URL e il portale non viene mai visualizzato. A questo punto, se l'indirizzo IP del server ISE viene immesso nel browser Web del dispositivo terminale, il portale deve essere visibile. In tal caso, si è verificato un problema con il server DNS.

181	2022-10-16 20:05:31.130979	<device-ip-addr>	<dns-server-ip-addr>	3c:41:0e:31:77:00	2065	DNS	159 Standard query 0x1409 HTTPS <apple-captive-portal>
182	2022-10-16 20:05:31.130979	<device-ip-addr>	<dns-server-ip-addr>			DNS	81 Standard query 0x1409 HTTPS <apple-captive-portal>
183	2022-10-16 20:05:31.130979	<device-ip-addr>	<dns-server-ip-addr>	3c:41:0e:31:77:00	2321	DNS	159 Standard query 0x9964 A <apple-captive-portal>
184	2022-10-16 20:05:31.130979	<device-ip-addr>	<dns-server-ip-addr>			DNS	81 Standard query 0x9964 A <apple-captive-portal>
118	2022-10-16 20:05:31.332975	<dns-server-ip-addr>	<device-ip-addr>			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>	3c:41:0e:31:77:0f	0	DNS	295 Standard query response 0x9964 <apple-captive-portal> CNAME <apple-captive-portal>

Test di connettività dal client - Query e risposta DNS

Indirizzo IP risolto DNS

Dopo aver esaminato la risposta alla query DNS, è possibile visualizzare l'indirizzo IP risolto dal server DNS.

No.	Time	Source	Destination	ESIid	SEQ#	Protocol	Length	Info
118	2022-10-16 20:05:31.332975	<dns-ip-addr>	<device-ip-addr>			DNS	225	Standard query response 0x9964 A <apple-captive-portal> CNAME <apple-captive-portal>
119	2022-10-16 20:05:31.332975	<device-ip-addr>	<dns-server-ip-addr>	3c:41:0e:31:77:0f		DNS	295	Standard query response 0x9964 A <apple-captive-portal> CNAME <apple-captive-portal>
<pre> > Frame 119: 295 bytes on wire (2308 bits), 295 bytes captured (2308 bits) on Ethernet II, Src: Cisco_S6155Gb (F4:6d:8c:95:0c), Dst: Cisco_S6-8b1x (Ac:77:6d:5b:84:74) > Internet Protocol Version 4, Src: <device-ip-addr>, Dst: <dns-server-ip-addr> > User Datagram Protocol, Src Port: 5487, Dst Port: 5378 > Control and Provisioning of Wireless Access Points - Data > IEEE 802.11 QoS Data, Flags:F. > Logical-Link Control > Internet Protocol Version 4, Src: <device-ip-addr>, Dst: <device-ip-addr> > User Datagram Protocol, Src Port: 53, Dst Port: 55482 </pre>								
<pre> Name: Name System (responses) > Transaction ID: 0x9964 > Flags: 0x00 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.mailing.com: type A, class IN, addr 17.253.127.213 > captive.g.mailing.com: type A, class IN, addr 17.253.127.213 </pre>								

Indirizzo IP risolto dal server DNS

Stabilisci handshake a 3 vie

Dopo la risoluzione dell'indirizzo IP DNS, viene stabilito un handshake TCP a 3 vie tra il portale e il client. L'indirizzo IP utilizzato è uno qualsiasi degli indirizzi IP risolti.

120	2022-10-16 20:05:31.338971	<device-ip-addr>	<resolved-ip-addr>	3c: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>	3c:41:0e:31:77:0f	0	TCP	140	80 → 59886 [SYN, ACK, ECE] Seq=0 Ack=1 Win=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>	3c:41:0e:31:77:00	287	TCP	140	59886 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=2766384857 TSecr=2851166700

Creazione handshake a 3 vie

OTTIENI hotspot

Una volta stabilita la sessione TCP, il client esegue un probe e tenta di accedere al portale.

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=1 Ack=132 Win=65152 Len=0 TSval=2051166703 TSecr=2766384857	

OTTIENI hotspot

Pacchetto OK

Il pacchetto OK contiene il portale dell'ISE a cui il client deve essere reindirizzato.

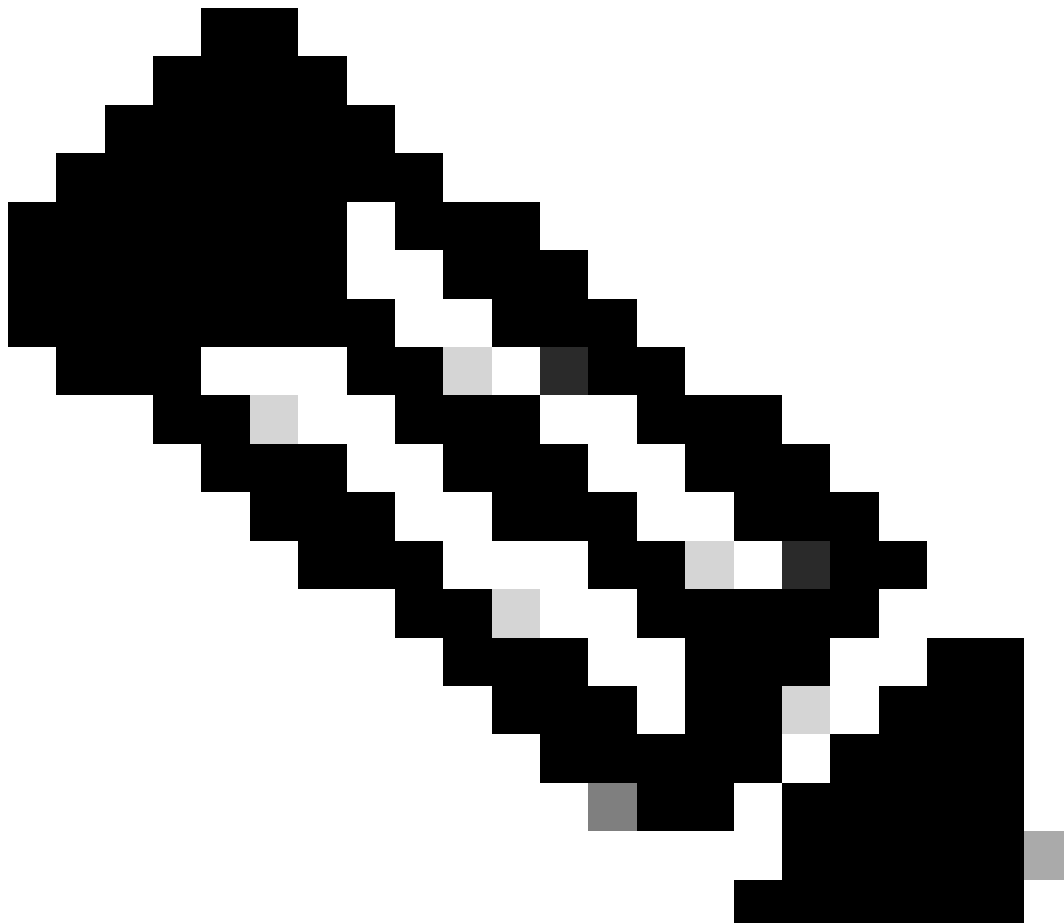
No.	Time	Source	Destination	OSID	SEQ#	Protocol	Length	Info
123	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<device-ip-addr>	3c:41:0e:31:77:0f	0	TCP	140	80 → 59886 [ACK] Seq=1 Ack=132 Win=65152 Len=0 TSval=2051166703 TSecr=2766384857
125	2022-10-16 20:05:31.341977	<dns-resolved-ip-addr>	<device-ip-addr>	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: 5270
> 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=030BA8C0000000C57AF11048portal=7cf5ac1d-5dbf-4b36-aeec-b9590fd24c02&action=cwa&token=231e2569058bc725ea084feff99707e8redirect=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)

```

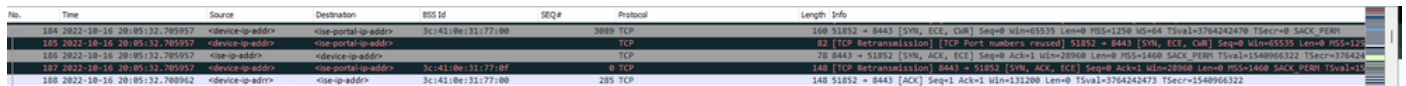
Pacchetto OK



Nota: la maggior parte delle persone ha restituito un altro URL nel pacchetto OK. È pertanto necessario eseguire un'altra query DNS per ottenere l'indirizzo IP finale.

Nuova sessione TCP stabilita

Dopo aver individuato l'indirizzo IP del portale, vengono scambiati molti pacchetti, ma alla fine un pacchetto con l'indirizzo IP di destinazione restituito nel pacchetto OK (o risolto dal DNS) che corrisponde all'indirizzo IP di ISE, indica che è stata stabilita una nuova sessione TCP per il portale.



No.	Time	Source	Destination	ESS Id	SEQ#	Protocol	Length	Info
184	2022-10-16 20:05:13.705957	<device-ip-addr>	<ise-portal-ip-addr>	3c:41:0e:13:177:00	3089	TCP	160	51852 → 8443 [SYN, ECE, CWR] Seq=0 Win=0 Len=0 TSval=3764242470 TSecr=0 SACK_PERM=0
185	2022-10-16 20:05:13.705957	<device-ip-addr>	<ise-portal-ip-addr>			TCP	62	[TCP Retransmission] [TCP Port numbers reused] 51852 → 8443 [SYN, ECE, CWR] Seq=0 Win=0 Len=0
186	2022-10-16 20:05:13.705957	<ise-ip-addr>	<device-ip-addr>		78	TCP	8443	→ 51852 [SYN, ACK, ECE] Seq=0 Ack=1 Win=2048 Len=0 SACK_PERM=0 TSval=154096322 TSecr=3764242470
187	2022-10-16 20:05:13.705957	<device-ip-addr>	<ise-portal-ip-addr>			TCP	140	[TCP Retransmission] 8443 → 51852 [SYN, ECE, CWR] Seq=0 Win=0 Len=0 TSval=3764242470 TSecr=154096322
188	2022-10-16 20:05:13.706062	<device-ip-addr>	<ise-ip-addr>	3c:41:0e:13:177:00	285	TCP	148	51852 → 8443 [ACK] Seq=1 Ack=1 Win=33280 Len=0 TSval=3764242473 TSecr=154096322

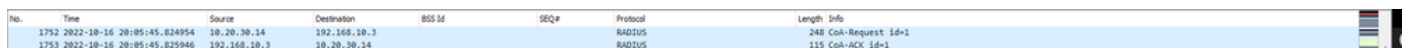
Seconda connessione e nuova sessione TCP sul portale ISE

Portale visualizzato all'utente

A questo punto, il portale dell'ISE viene finalmente visualizzato sul browser del client. Come in precedenza, vengono scambiati molti pacchetti tra ISE e il dispositivo, ad esempio il saluto di un cliente e di un server, e così via. A questo punto ISE chiede al client di fornire il nome utente e la password, di accettare i termini e le condizioni o qualsiasi altra configurazione effettuata sul server ISE.

Richiesta CoA / Conferma CoA

Una volta che l'utente ha immesso tutti i dati richiesti, ISE invia una richiesta CoA al controller per modificare l'autorizzazione dell'utente. Se tutto il contenuto del WLC è configurato nel modo previsto, ad esempio lo stato del NAC, il supporto per il CoA e così via, il WLC invia un messaggio di conferma CoA (CoA Acknowledgement). In caso contrario, il WLC può inviare un CoA non-Acknowledgement (CoA NACK) o semplicemente non invia neanche il CoA ACK.



No.	Time	Source	Destination	ESS Id	SEQ#	Protocol	Length	Info
1752	2022-10-16 20:05:45.824954	192.168.10.14	192.168.10.3			RADIUS	248	CoA-Request Id=1
1753	2022-10-16 20:05:45.825946	192.168.10.3	192.168.10.14			RADIUS	115	CoA-ACK Id=1

Richiesta e conferma CoA

Seconda connessione: da client a rete

Nuova richiesta di accesso

Il WLC invia un nuovo pacchetto di richiesta di accesso ad ISE.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).