瞭解客戶端上的CWA流程

目錄

簡介

本文檔介紹連線至CWA WLAN時終端客戶端所經歷的流程。

必要條件

需求

思科建議您具備以下基本知識：

- 思科無線LAN控制器(WLC) 9800系列
- 對中央Web驗證(CWA)及其在身份服務引擎(ISE)上的配置的一般瞭解

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- 9800-CL WLC
- Cisco AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- 身分辨識服務引擎(ISE) v3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

CWA是一種SSID驗證型別，可在WLC上設定，其中嘗試連線的終端使用者端會提示輸入其使用者名稱和密碼到向他們顯示的Web輸入網站。簡而言之，連線到WLAN時，終端客戶端的流量為：

1. 終端客戶端連線到其裝置上顯示的SSID
2. 終端客戶端被重定向到Web門戶以輸入其憑證
3. 終端客戶端使用輸入的憑證由ISE進行身份驗證
4. ISE回覆WLC表明終端客戶端已透過身份驗證。 ISE可以推送一些客戶端在訪問網路時必須遵守的其他屬性（例如特定ACL）
5. 終端客戶端重新關聯並重新進行身份驗證，最終獲得網路訪問許可權

注意：必須注意，兩次進行身份驗證的終端客戶端對終端客戶端是透明的

客戶端必須經過的基本過程基本上分為兩部分：從客戶端到ISE伺服器的連線，以及經過身份驗證後從客戶端到網路本身的另一個連線。控制器和ISE始終透過RADIUS協定相互通訊。以下是放射性(RA)追蹤和嵌入式封包擷取(EPC)的深入分析。

CWA流程-放射性(RA)追蹤

RA跟蹤是為特定客戶端捕獲的一組日誌。它顯示客戶端在連線到WLAN時經歷的整個過程。有關它們是什麼以及如何檢索RA跟蹤的詳細資訊，請訪問瞭解Catalyst 9800無線LAN控制器上的無線調試和日誌收集。

第一個連線：客戶端到ISE伺服器

如果客戶端以前未經ISE授權，則WLC不允許連線到網路。

與WLAN的關聯

WLC檢測到客戶端要關聯到WLAN「cwa」，CWA連結到策略配置檔案「cwa-policy-profile，並且正在連線到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
```

MAC過濾

測試ISE伺服器連線

WLC收到來自客戶端的關聯請求後，第一步是執行MAC過濾（也稱為MAB）。MAC過濾是一種安全方法，根據資料庫檢查客戶端的MAC地址，以驗證是否允許它們加入網路。

<#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_INIT
[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 0E1E140A000000
[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
```

WLC向ISE傳送請求

WLC向ISE傳送RADIUS Access-Request資料包，其中包含要向WLAN進行身份驗證的客戶端的MAC地址。

<#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
```

注意：AV對是ISE使用的「屬性值」。它是可傳送到WLC的預定義資訊的鍵-值結構。這些值會套用至該特定階段作業的特定使用者端。

AV-Pairs示例：

- ACL名稱
- 重定向URL
- VLAN分配
- 會話超時時間
- 重新驗證計時器

ISE響應WLC請求

如果ISE接受WLC傳送的MAC地址，則ISE傳送Access-Accept RADIUS資料包。根據ISE配置，如果它是未知MAC地址，ISE必須接受它並繼續流程。如果顯示Access-Reject，則表示在ISE上存在需要驗證的未正確配置。

<#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
```

從ISE接收資訊的WLC進程

WLC處理從ISE收到的所有資訊。藉助它，它將應用最初使用ISE傳送的資料建立的使用者配置檔案。例如，WLC會為使用者指派新的ACL。如果未在WLAN上啟用AAA Override，則不會發生WLC的此處理。

<#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 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
```

MAB身份驗證完成

成功修改客戶端的使用者配置檔案後，WLC將完成驗證客戶端的MAC地址。如果從ISE接收的ACL不存在於WLC上，則WLC不知道該如何處理該資訊，因此REPLACE操作完全失敗，導致MAB身份驗證也失敗。使用者端無法進行驗證。

<#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向客戶端傳送關聯響應

現在，客戶端已經過ISE身份驗證並且應用了正確的ACL，WLC最終會向客戶端傳送關聯響應。現在，使用者可以繼續連線到網路。

<#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.
```

L2驗證

根據客戶端在與WLAN關聯時必須經歷的過程，L2身份驗證「啟動」。但是，實際上已執行L2身份驗證，因為以前執行過MAB身份驗證。客戶端將立即完成L2身份驗證。

<#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
```

資料插塞

WLC將資源指派給連線的使用者端，以便流量可以透過網路傳輸。

<#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
```

已為使用者分配IP地址

終端使用者需要IP地址才能在網路間導航。它會經過DHCP程式。如果使用者以前曾連線過，並且記住其IP地址，則會跳過DHCP進程。如果使用者無法收到IP地址，則終端使用者無法檢視Web門戶。否則，它將執行後續步驟：

1. DISCOVER資料包作為廣播從連線的客戶端傳送，以查詢任何可用的DHCP伺服器
2. 如果有可用的DHCP伺服器，DHCP伺服器將以OFFER做出響應。該服務內容包含將分配給連線客戶端的IP地址、租用時間等資訊。從各種DHCP伺服器收到許多OFFER
3. 客戶端接受來自其中一台伺服器的OFFER，並以REQUEST響應所選的IP地址
4. 最後，DHCP伺服器向客戶端傳送確認資料包，並分配其新IP地址

WLC會記錄使用者端收到其IP位址的方法。

<#root>

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

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 dirty
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change noti
{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

L3身份驗證開始

現在，終端使用者已收到IP地址，L3身份驗證從檢測到作為所需身份驗證方法的CWA開始。

<#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

正常IP地址測試

為了繼續連線，客戶端必須執行兩個ARP請求：

1. 驗證其他人沒有其IP地址。如果終端使用者的IP地址有ARP應答，則它是重複的IP地址

2. 驗證網關的可達性。這是為了確保客戶端可以離開網路。ARP回覆必須來自網關

<#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
```

第二個連線：客戶端到網路

此時，終端使用者已經透過ISE的MAC地址對其進行身份驗證，但尚未獲得完全授權。WLC必須再次參考ISE以授權客戶端連線到網路。此時，入口將呈現給使用者，使用者必須在其中輸入其使用者名稱和密碼。在WLC上，可以看到終端使用者處於「Web Auth Pending」狀態。

授權變更(CoA)

以下是WLC組態中「支援CoA」的生效位置。在此之前，一直使用ACL。在終端使用者端看到入口網站後，不再使用ACL，因為它只會將使用者端重新導向入口網站。此時，客戶端輸入其憑證以登入，以啟動CoA進程並重新驗證客戶端。WLC準備要傳送的資料包並將其轉發到ISE

提示：CoA使用埠1700。請確保防火牆未阻止它。

<#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:0ider
[caaa-ch] [17558]: (info): [CAAA:COMMAND HANDLER]

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

ISE的第二次身份驗證

第二個身份驗證不是從零開始。這是美國二氧化碳的威力。新的規則和/或AV paris可以應用於使用者。在第一個Access-Accept上收到的ACL和重定向URL不再推送到終端使用者。

WLC向ISE傳送請求

WLC使用輸入的使用者名稱/密碼組合向ISE傳送新的RADIUSAccess-Requestpacket。這將觸發新的MAB身份驗證，並且由於ISE已經知道客戶端，將應用新的策略集（例如，授予訪問許可權）。

<#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響應WLC請求

ISE執行策略查詢，如果收到的使用者名稱與策略配置檔案匹配，則ISE再次響應WLC，接受與WLAN的客戶端連線。它返回終端使用者的使用者名稱。如果在ISE上配置，額外的規則和/或AV對可應用於使用者，且可以在Access-Accept上看到它們。

<#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
```

從ISE接收資訊的WLC進程

WLC將再次處理ISE接收的資訊。它使用從ISE接收的新值對使用者執行另一REPLACE操作。

<#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
```

L3身份驗證完成

終端使用者現在已使用給定資料進行了身份驗證。L3身份驗證（Web身份驗證）已完成。

<#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
```

終端使用者在WLC上達到RUN狀態

最後，使用者透過身份驗證並與WLAN關聯。

<#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
```

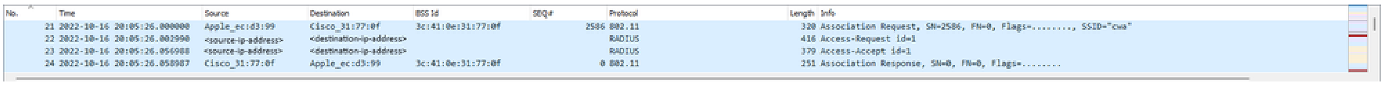
CWA流程-嵌入式封包擷取(EPC)

EPC是可直接從WLC檢索的資料包捕獲，其中顯示透過WLC或源自該WLC的所有資料包。有關它們是什麼以及如何檢索它們的詳細資訊，請訪問瞭解Catalyst 9800無線LAN控制器上的無線調試和日誌收集。

第一個連線：客戶端到ISE伺服器

警告：資料包捕獲映像上的IP地址已刪除。它們顯示為和

與WLAN的關聯和傳送到ISE伺服器的請求

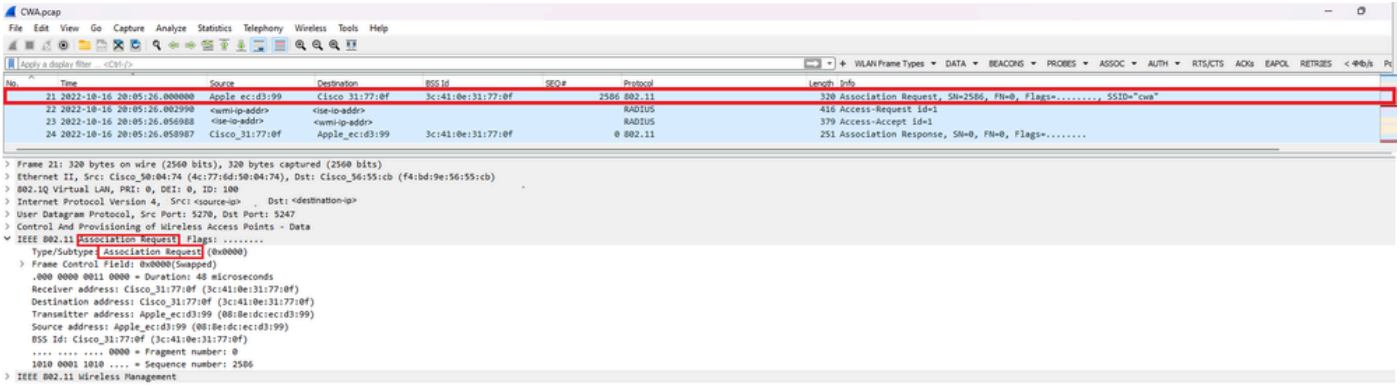


```
No.   Time                        Source                 Destination                 BSS Id              SEQ#   Protocol   Length  Info
   21 2022-10-16 20:05:26.000000  Apple_ec:d3:99         Cisco_31:77:0f              3c:41:0e:31:77:0f   2586   802.11     320 Association Request, SN=2586, FN=0, 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=........
```

第一個資料包

從WLC到客戶端的關聯請求

檢視第一個資料包「關聯請求」，您可以看到此過程中涉及的裝置的MAC地址。


CWA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
WLAN Frame Types DATA BEACONS PROBES ASSOC AUTH RTS/CTS ACKs EAPOL RETRIES <4Mb/s

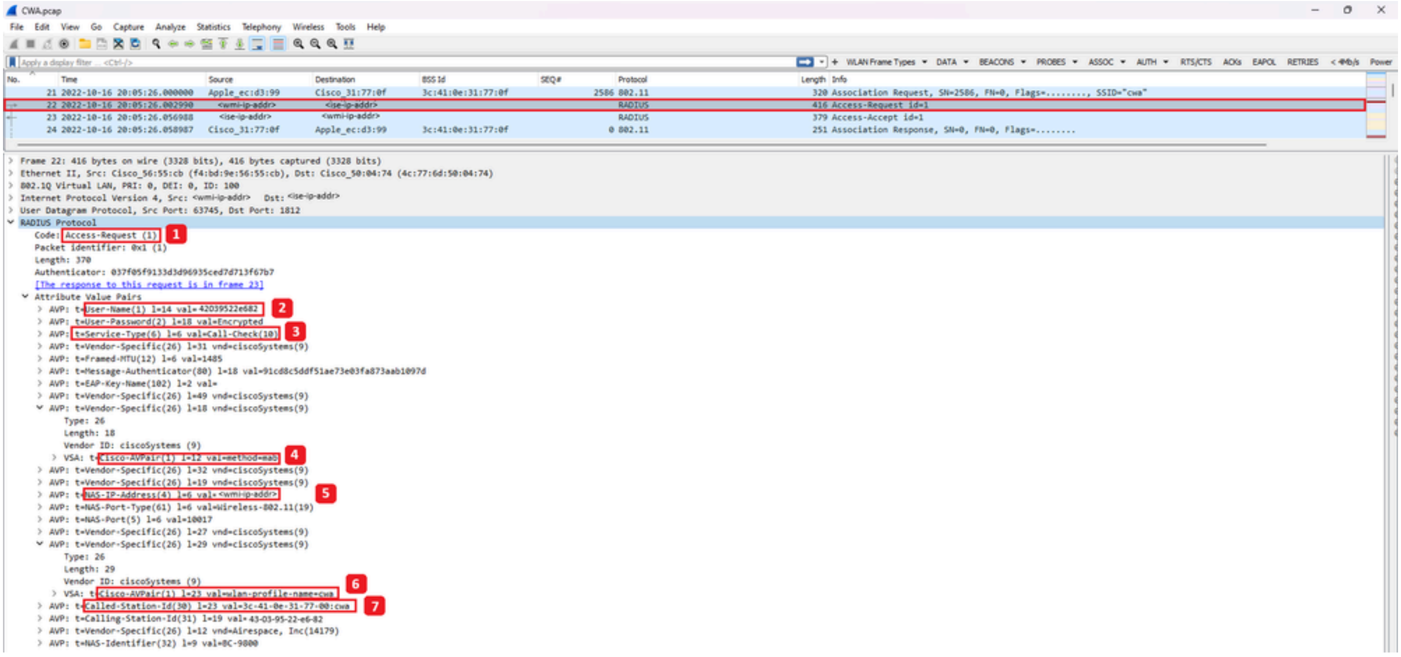
```
No.  Time                        Source          Destination     BSS Id             SEQ#  Protocol  Length Info
  21 2022-10-16 20:05:26.000000  Apple_ec:d3:99  Cisco_31:77:0f  3c:41:0e:31:77:0f  2586 802.11      320 Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
  22 2022-10-16 20:05:26.002990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

```
> Frame 21: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits)
> Ethernet II, Src: Cisco_50:04:74 (4c:77:6d:50:04:74), Dst: Cisco_56:55:cb (f4:bd:9e:56:55:cb)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4,  Src: <source-ip>   Dst: <destination-ip>
> User Datagram Protocol, Src Port: 5270, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
v IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000(Swapped)
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Cisco_31:77:0f (3c:41:0e:31:77:0f)
    Destination address: Cisco_31:77:0f (3c:41:0e:31:77:0f)
    Transmitter address: Apple_ec:d3:99 (08:8e:dc:ec:d3:99)
    Source address: Apple_ec:d3:99 (08:8e:dc:ec:d3:99)
    BSS Id: Cisco_31:77:0f (3c:41:0e:31:77:0f)
    .... .... .... 0000 = Fragment number: 0
    1010 0001 1010 .... = Sequence number: 2586
> IEEE 802.11 Wireless Management
```

關聯請求

從WLC傳送到ISE的訪問請求資料包

WLC處理完關聯請求後，WLC會向ISE伺服器傳送Access-Request資料包。


CWA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
WLAN Frame Types DATA BEACONS PROBES ASSOC AUTH RTS/CTS ACKs EAPOL RETRIES <4Mb/s Power
1
2
3
4
5
6
7

```
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  <wmi-ip-addr>   <ise-ip-addr>                            RADIUS      416 Access-Request id=1
  23 2022-10-16 20:05:26.056988  <ise-ip-addr>   <wmi-ip-addr>                            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=........
```

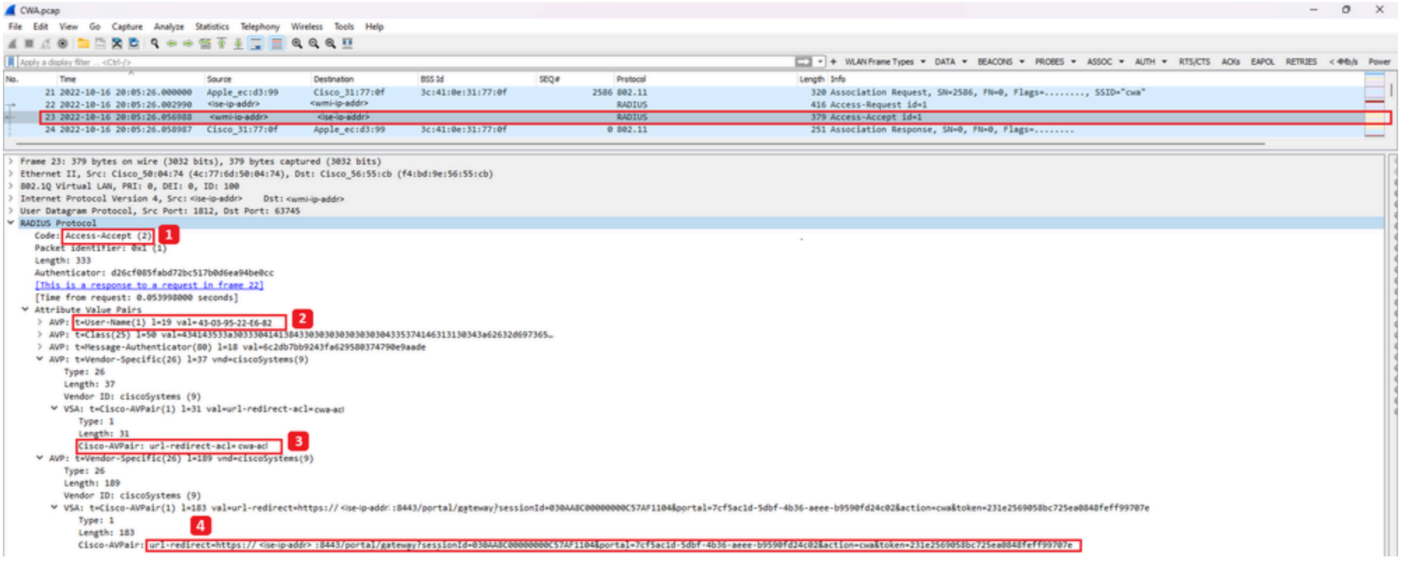
```
> Frame 22: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits)
> Ethernet II, Src: Cisco_56:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_50:04:74 (4c:77:6d:50:04:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <wmi-ip-addr>   Dst: <ise-ip-addr>
> User Datagram Protocol, Src Port: 63745, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1 (1)
    Length: 370
    Authenticator: 037f05f9133d3d96935ced7d713f67b7
    [The response to this request is in frame 23]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=14 val= 42039522e682
    > AVP: t=User-Password(2) l=18 val=Encrypted
    > AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
    > AVP: t=Message-Authenticator(80) l=18 val=91cd8c5ddf51ae73e03fa873aab1097d
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
        Type: 26
        Length: 18
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=12 val=method=mab
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=19 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val= <wmi-ip-addr>
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=10017
    > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
        Type: 26
        Length: 29
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=23 val=wlan-profile-name=cwa
    > AVP: t=Called-Station-Id(30) l=23 val=3c-41-0e-31-77-00:cwa
    > AVP: t=Calling-Station-Id(31) l=19 val= 43-03-95-22-e6-82
    > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    > AVP: t=NAS-Identifier(32) l=9 val=8C-9800
```

訪問請求資料包分析

1. 封包的名稱。
2. 嘗試進行身份驗證的MAC地址。
3. 這表示MAC過濾。
4. 控制器向ISE傳送的AV對，用於指示MAC過濾過程。
5. WLC的WMI IP地址。
6. 客戶端嘗試連線的SSID。
7. 使用者端嘗試連線的WLAN名稱。

從WLC傳送到ISE的Access-Accept資料包

當ISE處理了Access-Accept資料包後，如果成功，它會以Access-Accept做出響應；否則，會以Access-Reject做出響應。


CWA.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
WLAN Frame Types DATA BEACONS PROBES ASSOC AUTH RTS/CTS ACKs EAPOL RETRIES <4Mb/s Power
1
2
3
4

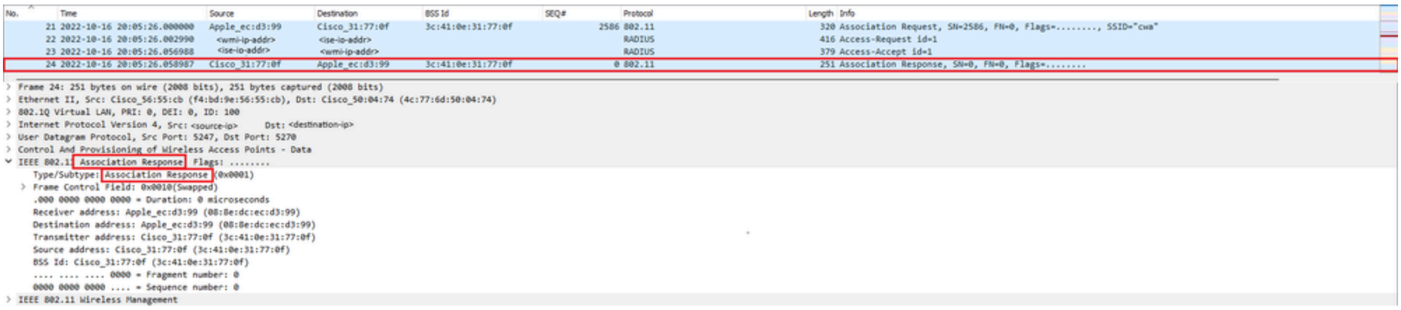
```
No.   Time                        Source          Destination     BSS Id              SEQ#  Protocol  Length  Info
   21 2022-10-16 20:05:26.000000  Apple_ec:d3:99  Cisco_31:77:0f  3c:41:0e:31:77:0f  2586  802.11    320 Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
   22 2022-10-16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

```
> Frame 23: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)
> Ethernet II, Src: Cisco_50:04:74 (4c:77:6d:50:04:74), Dst: Cisco_56:55:cb (f4:bd:9e:56:55:cb)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <ise-ip-addr>     Dst: <wmi-ip-addr>
> User Datagram Protocol, Src Port: 1812, Dst Port: 63745
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1 (1)
    Length: 333
    Authenticator: d26cf085fabd72bc517b0d6ea94be0cc
    [This is a response to a request in frame 22]
    [Time from request: 0.053998000 seconds]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=19 val=43-03-95-22-E6-82
    > AVP: t=Class(25) l=50 val=434143533a30333041413843303030303030303043353741463131303434a62632d697365…
    > AVP: t=Message-Authenticator(80) l=18 val=6c2db7bb9243fa629580374790e9aade
    v AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
        Type: 26
        Length: 37
        Vendor ID: ciscoSystems (9)
      v VSA: t=Cisco-AVPair(1) l=31 val=url-redirect-acl=cwa-acl
          Type: 1
          Length: 31
          Cisco-AVPair: url-redirect-acl= cwa-acl
    v AVP: t=Vendor-Specific(26) l=189 vnd=ciscoSystems(9)
        Type: 26
        Length: 189
        Vendor ID: ciscoSystems (9)
      v VSA: t=Cisco-AVPair(1) l=183 val=url-redirect=https:// <ise-ip-addr :8443/portal/gateway?sessionId=030AA8C00000000C57AF1104&portal=7cf5ac1d-5dbf-4b36-aeee-b9590fd24c02&action=cwa&token=231e2569058bc725ea0848feff99707e
          Type: 1
          Length: 183
          Cisco-AVPair: url-redirect=https:// <ise-ip-addr> :8443/portal/gateway?sessionId=030AA8C00000000C57AF1104&portal=7cf5ac1d-5dbf-4b36-aeee-b9590fd24c02&action=cwa&token=231e2569058bc725ea0848feff99707e
```

Access-Accept資料包分析

1. 封包的名稱。
2. 已驗證的MAC地址。
3. 要應用的ACL。
4. 將使用者重新導向到的URL。

從WLC到客戶端的關聯響應

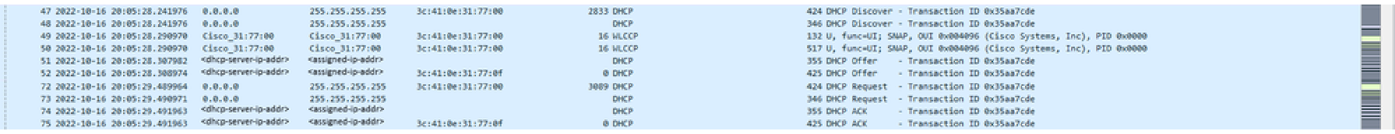


```
No.   Time                        Source          Destination     BSS Id              SEQ#  Protocol  Length  Info
   21 2022-10-16 20:05:26.000000  Apple_ec:d3:99  Cisco_31:77:0f  3c:41:0e:31:77:0f  2586  802.11    320 Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
   22 2022-10-16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

```
> Frame 24: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits)
> Ethernet II, Src: Cisco_56:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_50:04:74 (4c:77:6d:50:04:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <source-ip>     Dst: <destination-ip>
> User Datagram Protocol, Src Port: 5247, Dst Port: 5270
> Control And Provisioning of Wireless Access Points - Data
v IEEE 802.11 Association Response, Flags: ........
    Type/Subtype: Association Response (0x0001)
  > Frame Control Field: 0x0010(Swapped)
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Apple_ec:d3:99 (08:8e:dc:ec:d3:99)
    Destination address: Apple_ec:d3:99 (08:8e: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
```

關聯回應

DHCP進程

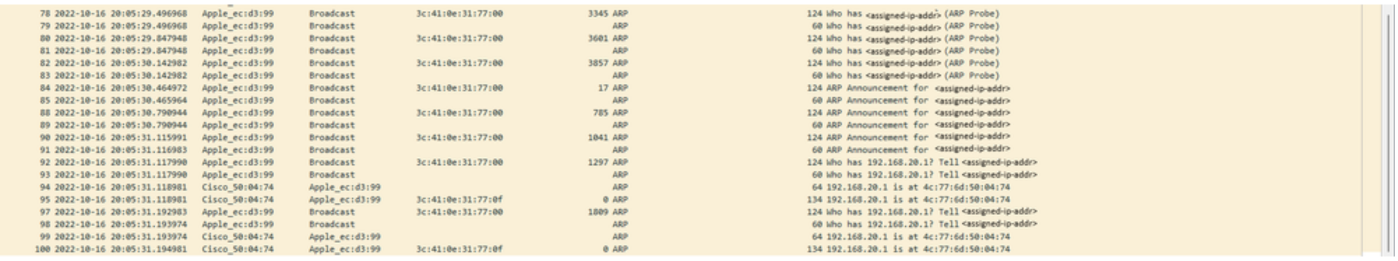


```
   47 2022-10-16 20:05:28.241976  0.0.0.0                 255.255.255.255        3c:41:0e:31:77:00  2833 DHCP   424 DHCP Discover - Transaction ID 0x35aa7cde
   48 2022-10-16 20:05:28.241976  0.0.0.0                 255.255.255.255                                DHCP   346 DHCP Discover - Transaction ID 0x35aa7cde
   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 0x004096 (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 0x004096 (Cisco Systems, Inc), PID 0x0000
   51 2022-10-16 20:05:28.307982  <dhcp-server-ip-addr>   <assigned-ip-addr>                             DHCP   355 DHCP Offer    - Transaction ID 0x35aa7cde
   52 2022-10-16 20:05:28.308974  <dhcp-server-ip-addr>   <assigned-ip-addr>     3c:41:0e:31:77:0f     0 DHCP   425 DHCP Offer    - Transaction ID 0x35aa7cde
   72 2022-10-16 20:05:29.489964  0.0.0.0                 255.255.255.255        3c:41:0e:31:77:00  3089 DHCP   424 DHCP Request  - Transaction ID 0x35aa7cde
   73 2022-10-16 20:05:29.490971  0.0.0.0                 255.255.255.255                                DHCP   346 DHCP Request  - Transaction ID 0x35aa7cde
   74 2022-10-16 20:05:29.491963  <dhcp-server-ip-addr>   <assigned-ip-addr>                             DHCP   355 DHCP ACK      - Transaction ID 0x35aa7cde
   75 2022-10-16 20:05:29.491963  <dhcp-server-ip-addr>   <assigned-ip-addr>     3c:41:0e:31:77:0f     0 DHCP   425 DHCP ACK      - Transaction ID 0x35aa7cde
```

DHCP進程

注意：從現在開始，資料包顯示為重複資料，但這是因為其中有一個是CAPWAP封裝的資料包，而另一個不是

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
```

客戶端ARP用於自己的IP地址和網關

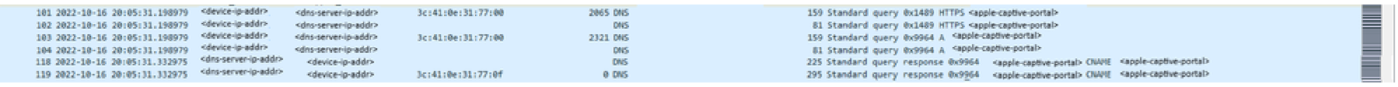
連線測試

ARP過程完成後，嘗試連線的裝置會執行檢查以驗證是否觸發了入口，這也稱為探測。如果裝置顯

示沒有Internet連線，則表示ARP過程失敗（例如，網關從未應答）或裝置無法執行探測。

此探測功能在RA跟蹤中是不可見的，只有EPC能夠提供此資訊。探查查詢取決於嘗試連線的裝置，在本示例中，測試裝置是Apple裝置，因此探查直接指向Apple的強制網路門戶。

當使用URL進行探測時，需要DNS來解決此URL。因此，如果DNS伺服器無法響應客戶端的查詢，則客戶端會繼續查詢該URL，並且門戶從未出現。此時，如果在終端裝置Web瀏覽器上輸入ISE伺服器的IP地址，則必須顯示門戶。如果是，則DNS伺服器發生問題。

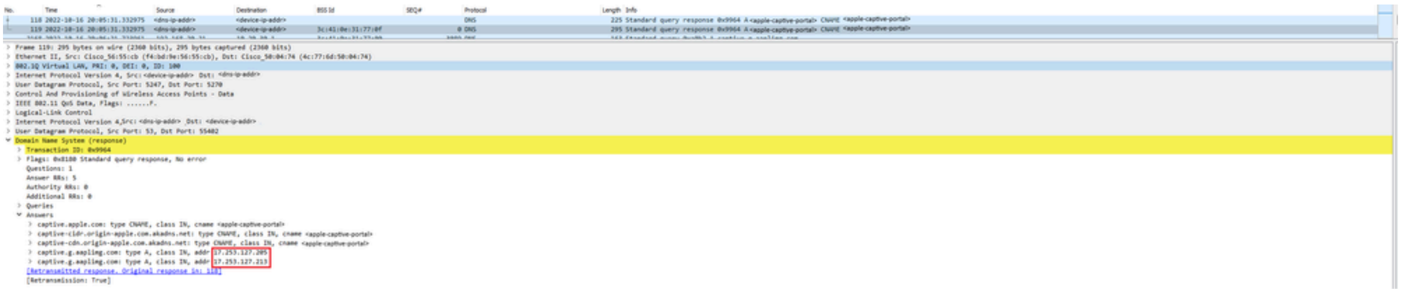


```
101 2022-10-16 20:05:31.198979 <device-ip-addr>     <dns-server-ip-addr>  3c:41:0e:31:77:00  2065 DNS   159 Standard query 0x1489 HTTPS <apple-captive-portal>
102 2022-10-16 20:05:31.198979 <device-ip-addr>     <dns-server-ip-addr>                          DNS    81 Standard query 0x1489 HTTPS <apple-captive-portal>
103 2022-10-16 20:05:31.198979 <device-ip-addr>     <dns-server-ip-addr>  3c:41:0e:31:77:00  2321 DNS   159 Standard query 0x9964 A <apple-captive-portal>
104 2022-10-16 20:05:31.198979 <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>
```

來自客戶端的連線測試- DNS查詢和應答

DNS解析的IP地址

在檢查DNS查詢響應時，您可以看到DNS伺服器解析的IP地址。



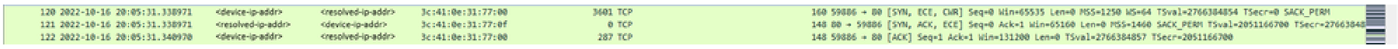
```
No.  Time                       Source          Destination       BSS Id             SEQ#  Protocol  Length Info
118 2022-10-16 20:05:31.332975 <dns-ip-addr>   <device-ip-addr>                             DNS       225 Standard query response 0x9964 A <apple-captive-portal> CNAME <apple-captive-portal>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

> Frame 119: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits)
> Ethernet II, Src: Cisco_56:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_50:04:74 (4c:77:6d:50:04:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <device-ip-addr> Dst: <dns-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-ip-addr> Dst: <device-ip-addr>
> User Datagram Protocol, Src Port: 53, Dst Port: 55402
v Domain Name System (response)
  > Transaction ID: 0x9964
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > captive.apple.com: type CNAME, class IN, cname <apple-captive-portal>
    > captive-cidr.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.aaplimg.com: type A, class IN, addr 17.253.127.205
    > captive.g.aaplimg.com: type A, class IN, addr 17.253.127.213
    [Retransmitted response. Original response in: 118]
    [Retransmission: True]
```

DNS伺服器解析的IP地址

建立三次握手

現在，DNS IP地址已解析，在門戶和客戶端之間建立TCP三次握手。使用的IP地址是解析的任一個IP地址。

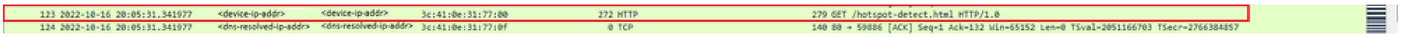


```
120 2022-10-16 20:05:31.338971 <device-ip-addr>    <resolved-ip-addr>  3c:41:0e:31:77:00  3601 TCP  160 59886 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=2766384854 TSecr=0 SACK_PERM
121 2022-10-16 20:05:31.338971 <resolved-ip-addr>  <device-ip-addr>    3c:41:0e:31:77:0f     0 TCP  148 80 → 59886 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2051166700 TSecr=27663848
122 2022-10-16 20:05:31.340970 <device-ip-addr>    <resolved-ip-addr>  3c:41:0e:31:77:00   287 TCP  148 59886 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=2766384857 TSecr=2051166700
```

三次握手建立

取得熱點

一旦TCP會話建立，客戶端就會執行探測並嘗試訪問門戶。

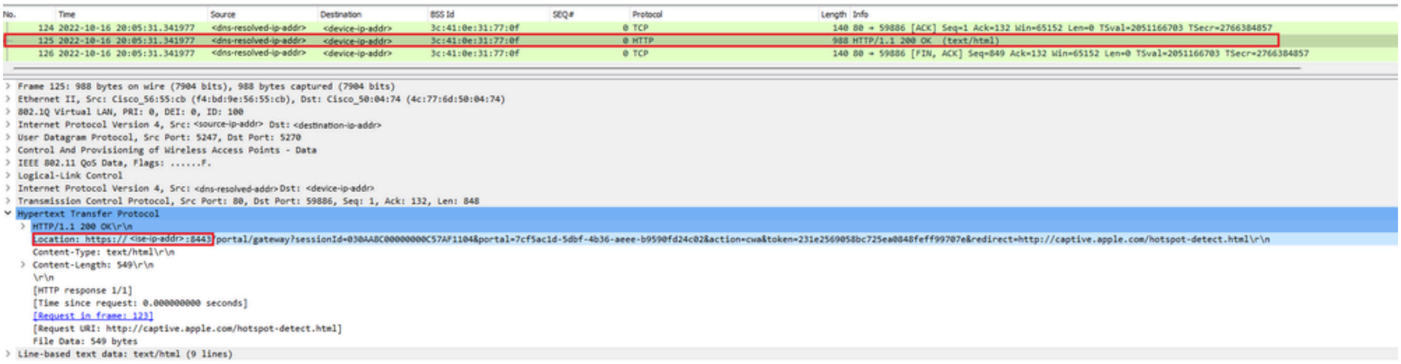


```
123 2022-10-16 20:05:31.341977 <device-ip-addr>        <device-ip-addr>        3c:41:0e:31:77:00  272 HTTP  279 GET /hotspot-detect.html HTTP/1.0
124 2022-10-16 20:05:31.341977 <dns-resolved-ip-addr>  <dns-resolved-ip-addr>  3c:41:0e:31:77:0f    0 TCP   140 80 → 59886 [ACK] Seq=1 Ack=132 Win=65152 Len=0 TSval=2051166703 TSecr=2766384857
```

取得熱點

OK資料包

OK資料包包含客戶端必須重定向到的ISE門戶。



```
No.  Time                        Source                  Destination         BSS Id              SEQ#  Protocol  Length  Info
124 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=65152 Len=0 TSval=2051166703 TSecr=2766384857

> Frame 125: 988 bytes on wire (7904 bits), 988 bytes captured (7904 bits)
> Ethernet II, Src: Cisco_56:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_50:04:74 (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
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https:// <ise-ip-addr>:8443/portal/gateway?sessionId=030AA8C00000000C57AF1104&portal=7cf5ac1d-5dbf-4b36-aeee-b9590fd24c02&action=cwa&token=231e2569058bc725ea0848feff99707e&redirect=http://captive.apple.com/hotspot-detect.html\r\n
    Content-Type: text/html\r\n
  > Content-Length: 549\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000000000 seconds]
    [Request in frame: 123]
    [Request URI: http://captive.apple.com/hotspot-detect.html]
    File Data: 549 bytes
> Line-based text data: text/html (9 lines)
```

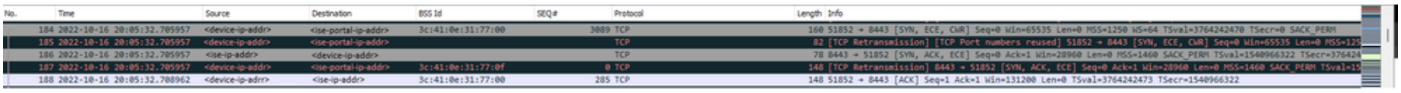
OK資料包

注意：大多數人都在OK資料包中返回了另一個URL。因此，需要執行另一DNS查詢以獲取最終IP地址。

已建立新的TCP作業階段

現在已發現門戶的IP地址，因此會交換許多資料包，但最終在OK資料包（或由DNS解析）中返回的

目標IP與ISE的IP地址對應的資料包顯示正在建立到門戶的新TCP會話。



```
No.   Time                          Source              Destination             BSS Id              SEQ#   Protocol   Length  Info
  184 2022-10-16 20:05:32.705957    <device-ip-addr>    <ise-portal-ip-addr>    3c:41:0e:31:77:00   3089   TCP        160 51852 → 8443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=3764242470 TSecr=0 SACK_PERM
  185 2022-10-16 20:05:32.705957    <device-ip-addr>    <ise-portal-ip-addr>                               TCP        82 [TCP Retransmission] [TCP Port numbers reused] 51852 → 8443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=125
  186 2022-10-16 20:05:32.705957    <ise-ip-addr>       <device-ip-addr>                                   TCP        78 8443 → 51852 [SYN, ACK, ECE] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1540966322 TSecr=376424
  187 2022-10-16 20:05:32.705957    <device-ip-addr>    <ise-portal-ip-addr>    3c:41:0e:31:77:0f      0   TCP        148 [TCP Retransmission] 8443 → 51852 [SYN, ACK, ECE] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=15
  188 2022-10-16 20:05:32.708962    <device-ip-adrr>    <ise-ip-addr>           3c:41:0e:31:77:00    285   TCP        148 51852 → 8443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3764242473 TSecr=1540966322
```

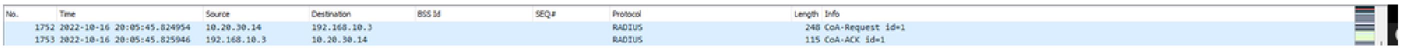
與ISE門戶的第二個連線和新TCP會話

門戶對使用者顯示

此時，ISE的門戶最終顯示在客戶端瀏覽器的瀏覽器上。與以前一樣，許多資料包在ISE和裝置之間交換；例如客戶端Hello和伺服器Hello等。此處，ISE要求客戶端提供使用者名稱和密碼、接受條款和條件或ISE伺服器上配置的任何內容。

CoA請求/CoA確認

使用者輸入所有請求的資料後，ISE會向控制器傳送CoA請求以更改使用者的授權。如果WLC上的所有內容都已按照預期進行配置（例如具有NAC狀態、支援CoA等），則WLC將傳送CoA確認(CoA ACK)。否則，WLC可能會傳送CoA非確認(CoA NACK)，或乾脆不傳送CoA ACK。



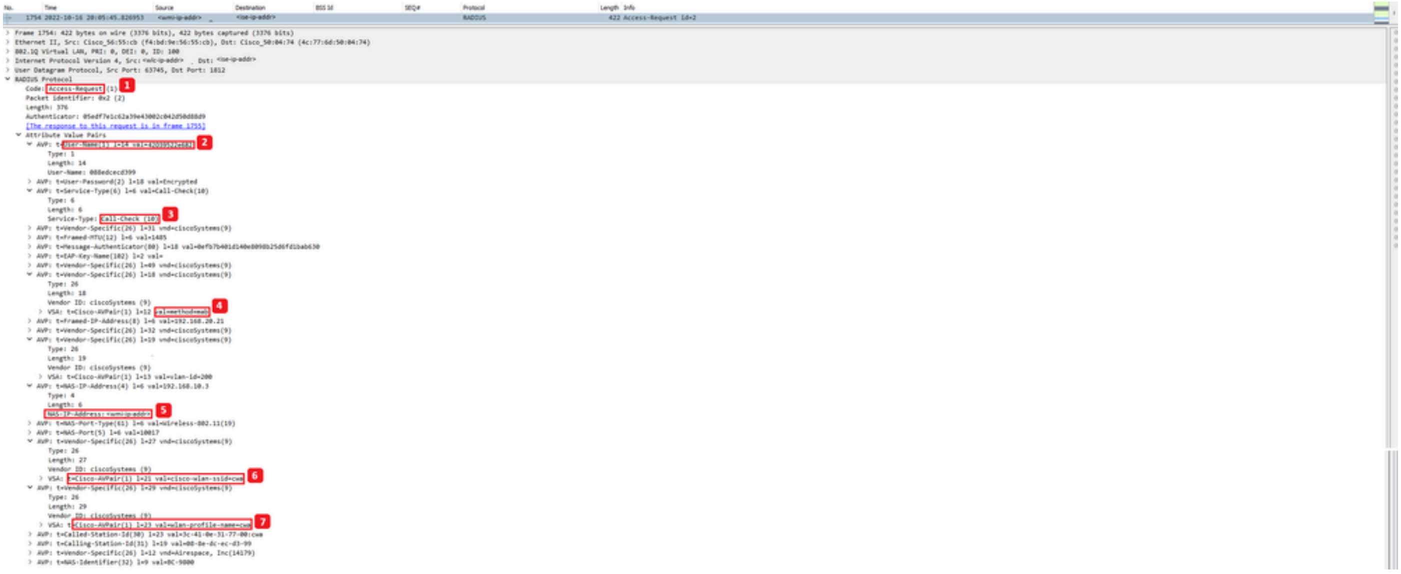
```
No.   Time                          Source          Destination     BSS Id   SEQ#   Protocol   Length  Info
 1752 2022-10-16 20:05:45.824954    10.20.30.14     192.168.10.3                    RADIUS        248 CoA-Request id=1
 1753 2022-10-16 20:05:45.825946    192.168.10.3    10.20.30.14      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

CoA請求和確認

第二個連線：客戶端到網路

新建訪問請求

WLC向ISE傳送新的訪問請求資料包。



```
No.   Time                          Source           Destination     BSS Id   SEQ#   Protocol   Length  Info
 1754 2022-10-16 20:05:45.826953    <wmi-ip-addr>    <ise-ip-addr>                   RADIUS        422 Access-Request id=2
> Frame 1754: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits)
> Ethernet II, Src: Cisco_56:55:cb (f4:bd:9e:56:55:cb), Dst: Cisco_50:04:74 (4c:77:6d:50:04:74)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: <wlc-ip-addr> , Dst: <ise-ip-addr>
> User Datagram Protocol, Src Port: 63745, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet Identifier: 0x2 (2)
    Length: 376
    Authenticator: 05edf7e1c62a39e43002c042d50d88d9
    [The response to this request is in frame 1755]
  v Attribute Value Pairs
    v AVP: t=User-Name(1) l=14 val=4203052e083
        Type: 1
        Length: 14
        User-Name: 088edcecd399
    > AVP: t=User-Password(2) l=18 val=Encrypted
    v AVP: t=Service-Type(6) l=6 val=Call-Check(10)
        Type: 6
        Length: 6
        Service-Type: Call-Check (10)
    > AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
    > AVP: t=Message-Authenticator(80) l=18 val=0efb7b401d140e0090b25d6fd1bab630
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
        Type: 26
        Length: 18
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=12 val=method=mab
    > AVP: t=Framed-IP-Address(8) l=6 val=192.168.20.21
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=19 vnd=ciscoSystems(9)
        Type: 26
        Length: 19
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=13 val=vlan-id=200
    v AVP: t=NAS-IP-Address(4) l=6 val=192.168.10.3
        Type: 4
        Length: 6
        NAS-IP-Address: <wmi-ip-addr>
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=10017
    v AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
        Type: 26
        Length: 27
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=21 val=cisco-wlan-ssid=cwa
    v AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
        Type: 26
        Length: 29
        Vendor ID: ciscoSystems (9)
      > VSA: t=Cisco-AVPair(1) l=23 val=wlan-profile-name=cwa
    > AVP: t=Called-Station-Id(30) l=23 val=3c-41-0e-31-77-00:cwa
    > AVP: t=Calling-Station-Id(31) l=19 val=08-8e-dc-ec-d3-99
    > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    > AVP: t=NAS-Identifier(32) l=9 val=8C-9800
```

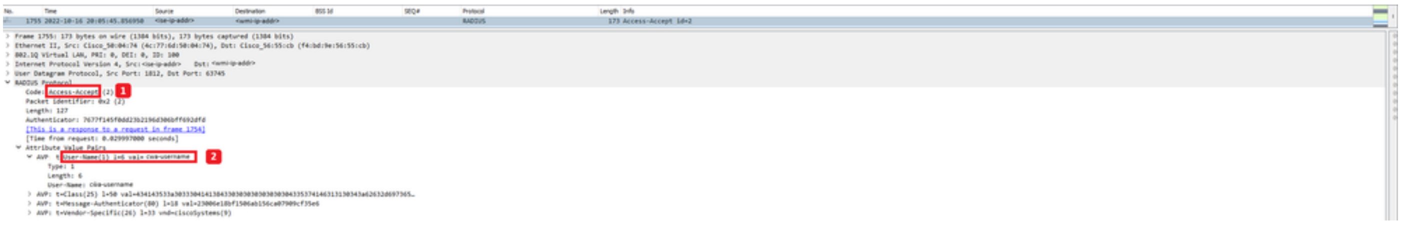
分析新的訪問請求資料包

1. 封包的名稱。
2. 嘗試進行身份驗證的MAC地址。
3. 這表示MAC過濾。

4. 控制器向ISE傳送的AV對，用於指示MAC過濾過程。
5. WLC的WMI IP地址。
6. 客戶端嘗試連線的SSID。
7. 使用者端嘗試連線的WLAN名稱。

新存取-接受

WLC向ISE傳送新的訪問請求資料包。



```
No.    Time                          Source         Destination     BSS Id     SEQ#     Protocol     Length  Info
  1755 2022-10-16 20:05:45.856950    <ise-ip-addr>  <wmi-ip-addr>                       RADIUS          173  Access-Accept id=2

> Frame 1755: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits)
> Ethernet II, Src: Cisco_50:04:74 (4c:77:6d:50:04:74), Dst: Cisco_56:55:cb (f4:bd:9e:56:55:cb)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src:<ise-ip-addr>    Dst: <wmi-ip-addr>
> User Datagram Protocol, Src Port: 1812, Dst Port: 63745
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x2 (2)
    Length: 127
    Authenticator: 7677f145f0dd23b2196d306bff692dfd
    [This is a response to a request in frame 1754]
    [Time from request: 0.029997000 seconds]
  v Attribute Value Pairs
    v AVP: t=User-Name(1) l=6 val= cwa-username
        Type: 1
        Length: 6
        User-Name: cwa-username
    > AVP: t=Class(25) l=50 val=434143533a30333041413843303030303030303030304335374146313130343a62632d697365…
    > AVP: t=Message-Authenticator(80) l=18 val=23006e18bf1506ab156ca07909cf35e6
    > AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
```

新接入接受資料包分析

1. 封包的名稱。
2. 終端客戶端在顯示的門戶上輸入的使用者名稱。

同樣，從客戶端進行新的探測連線測試。一旦客戶端確認它具有Internet連線，即可關閉門戶（根據使用的裝置可自動關閉）。使用者端現在已連線到網路。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。