クライアントのCWAフローについて

内容

はじめに

このドキュメントでは、CWA WLANに接続する際にエンドクライアントが受けるフローについて説明します。

前提条件

要件

次の項目に関する基本的な知識があることが推奨されます。

- Cisco Wireless LAN Controller(WLC)9800シリーズ
- Identity Services Engine(ISE)での中央Web認証(CWA)とその設定に関する一般的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

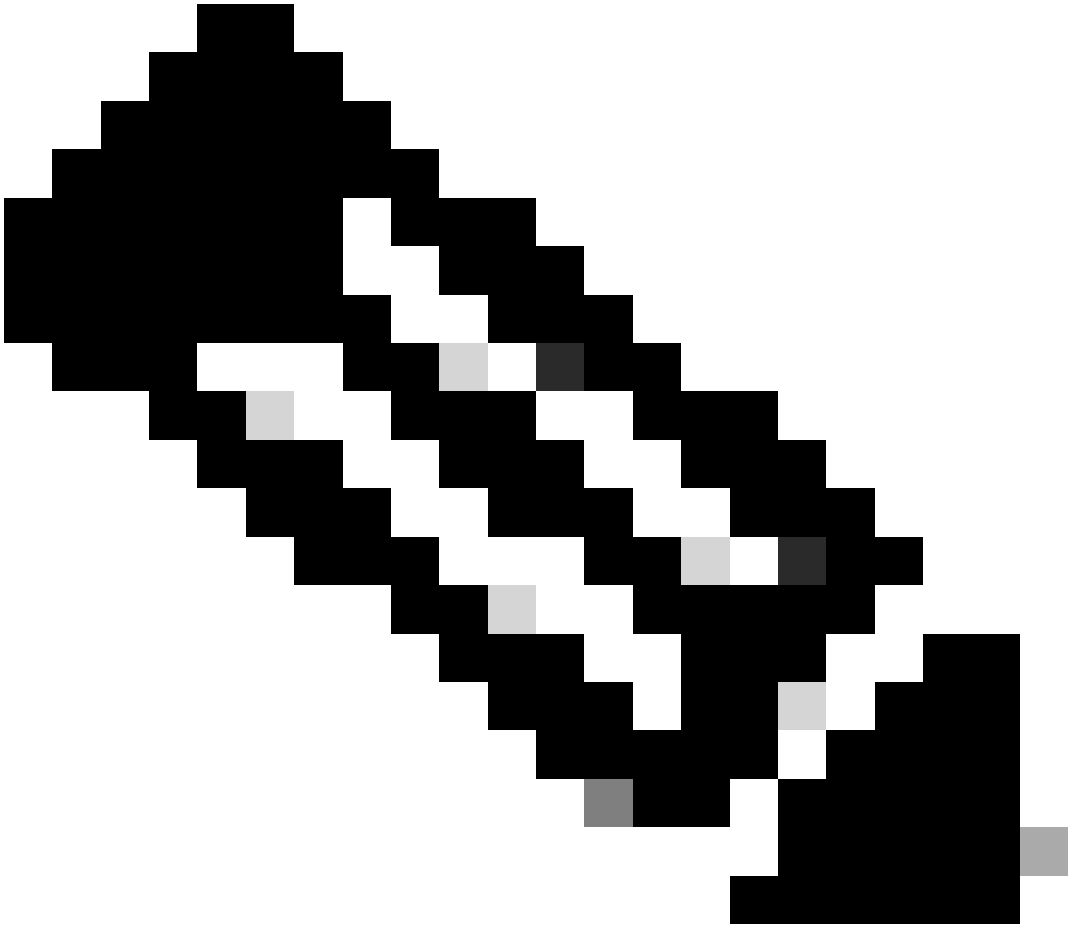
- 9800-CL WLC
- Cisco AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- Identity Service Engine(ISE)v3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CWAは、WLC上で設定できるSSID認証の一種で、接続を試みるエンドクライアントに対して、表示されるWebポータルにユーザ名とパスワードを入力するよう求めるプロンプトを表示します。端的に言うと、WLANに接続するときにエンドクライアントが通過するフローは次のようになります。

1. エンドクライアントは、デバイスに表示されているSSIDに接続します
2. エンドクライアントは、クレデンシャルを入力するためにWebポータルにリダイレクトされます
3. エンドクライアントは、入力されたクレデンシャルでISEによって認証されます
4. ISEは、エンドクライアントが認証されたことを示してWLCに応答します。 ISEは、クライアントがネットワークへのアクセス時に準拠する必要があるいくつかの追加属性（特定のACLなど）をプッシュできます
5. エンドクライアントの関連付けと認証が再度行われ、最終的にネットワークへのアクセスが得られます



注:2回認証されるエンドクライアントは、エンドクライアントに対して透過的です

クライアントが実行する必要がある基本プロセスは、基本的に2つに分けられます。1つはクライアントからISEサーバへの接続で、もう1つは認証が完了した後にクライアントからネットワーク自体への接続です。コントローラとISEは、常にRADIUSプロトコルを介して相互に通信します。次に、放射性(RA)トレースと組み込みパケットキャプチャ(EPC)の詳細分析を示します。

CWAフロー – 放射性(RA)トレース

RAトレースは、特定のクライアント用にキャプチャされたログのセットです。WLANに接続している間にクライアントが実行しているプロセス全体が表示されます。RAトレースの内容とRAトレースの取得方法の詳細については、「Catalyst 9800ワイヤレスLANコントローラでのワイヤレスデバッグとログ収集について」を参照してください。

最初の接続：クライアントからISEサーバ

クライアントが以前にISEによって認可されていない場合、WLCはネットワークへの接続を許可しません。

WLANへの関連付け

WLCは、クライアントがWLAN「cwa」への関連付けを求めていることを検出します。このWLANはポリシープロファイル「cwa-policy-profile」にリンクされ、AP「BC-3802」に接続されています。

<#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 フィルタリング

ISEサーバ接続のテスト

WLCがクライアントからアソシエーション要求を受信したら、最初のステップはMACフィルタリング（MABとも呼ばれる）を実行することです。MACフィルタリングは、クライアントのMACアドレスをデータベースと照合してチェックし、ネットワークへの参加が許可されているかどうかを検証するセキュリティ方式です。

<#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 w
[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 a
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Retrieved Client IIF ID 0x530002f1
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Allocated audit session id 0E1E140A0000000
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Applying policy for WlanId: 1, bssid : dc8
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wlan vlan-id from bssid hdl 0
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] SM Reauth Plugin: Received valid timeout =
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005]

MAB authentication started for 4203.9522.e682

[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_AWA
[ewlc-infra-evq] [17558]: (note): Authentication Success. Resolved Policy bitmap:11 for client 4203.952
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_MAB
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '

MAB_CONTINUE

' on handle 0x8A000002

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

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

WLCがISEに要求を送信

WLCは、WLANでの認証を必要とするクライアントのMACアドレスを含むRADIUS Access-RequestパケットをISEに送信します。

```
<#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

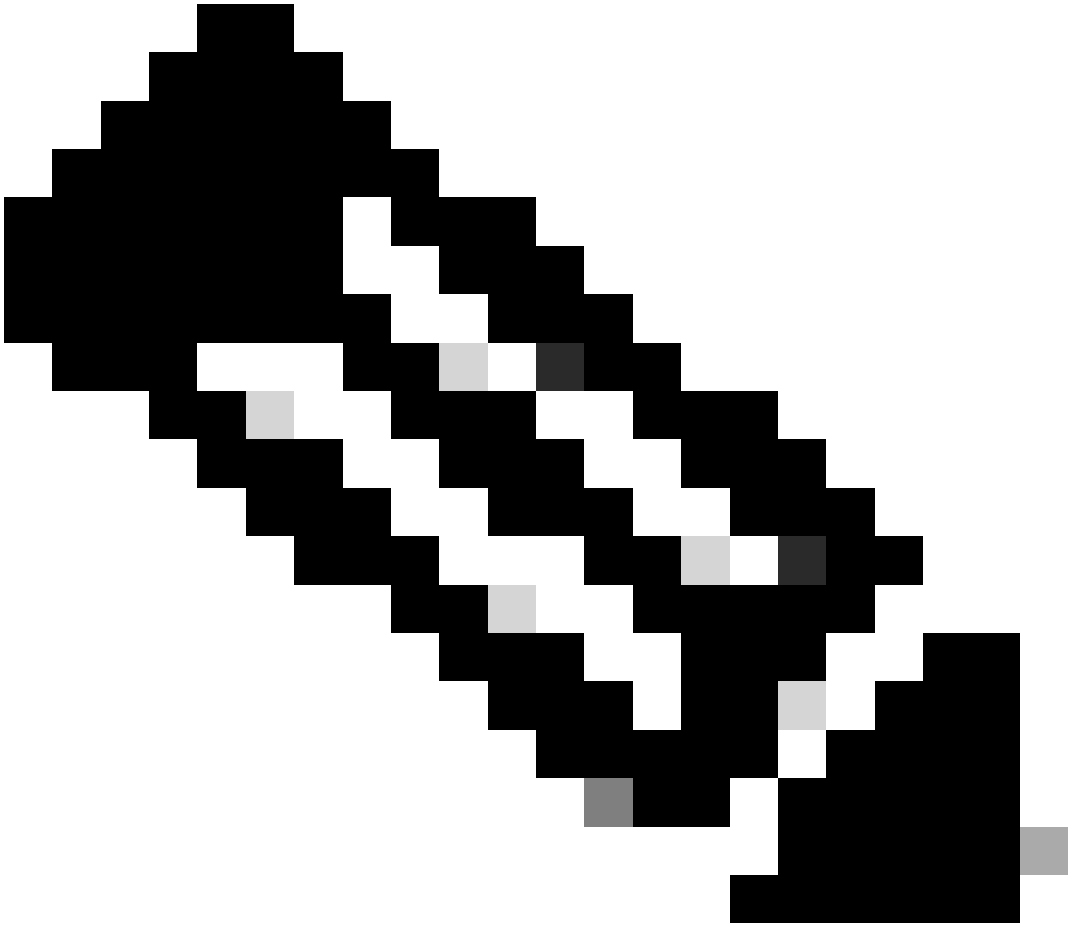
```
"
```

<-- 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:AVペアはISEで使用される「属性値」です。これは、WLCに送信できる事前定義情報のキー値構造です。これらの値は、その特定のセッションのその特定のクライアントに適用されます。

AVペアの例：

- ACL 名
- リダイレクトURL
- VLAN割り当て
- セッションタイムアウト時間
- 再認証タイマー

ISEがWLC要求に応答する

WLCから送信されたMACアドレスがISEで受け入れられる場合、ISEからAccess-Accept RADIUSパケットが送信されます。ISEの設定に応じて、不明なMACアドレスの場合、ISEはそれを受け入れてフローを続行する必要があります。Access-Rejectが表示された場合、ISEで正しく

設定されていない何かを確認する必要があります。

<#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

ISEから受信した情報のWLCプロセス

WLCは、ISEから受信したすべての情報を処理します。これを使用すると、ISEから送信されたデータのユーザプロファイルを使用して作成されたユーザプロファイルが適用されます。たとえば、WLCは新しいACLをユーザに割り当てます。AAA OverrideがWLANで有効になっていない場合、WLCによるこの処理は行われません。

<#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認証の完了

クライアントのユーザプロファイルが正常に変更された後、WLCはクライアントのMACアドレスの認証を終了します。ISEから受信したACLがWLCに存在しない場合、WLCではその情報の処理方法が分かりません。そのため、REPLACEアクションが失敗し、MAB認証も失敗します。クライアントが認証できない。

<#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がクライアントにアソシエーション応答を送信する

クライアントがISEによって認証され、正しいACLが適用されると、WLCは最終的にアソシエーション応答をクライアントに送信します。これで、ユーザはネットワークへの接続を続行できます。

<#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認証

クライアントがWLANにアソシエートするときに実行する必要があるプロセスに従って、L2認証が「開始」されます。ただし、実際には、以前に実行されたMAB認証のために、L2認証がすでに実行されています。クライアントは直ちにL2認証を完了します。

<#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

データの重複

WLCは、接続クライアントにリソースを割り当てて、トラフィックがネットワークを通過できるようにします。

<#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

ユーザにIPアドレスが割り当てられる

エンドユーザがネットワーク内を移動するには、IPアドレスが必要です。DHCPプロセスを実行する。ユーザが以前に接続したことがあり、そのIPアドレスを記憶している場合、DHCPプロセスはスキップされます。ユーザがIPアドレスを受信できない場合、エンドユーザはWebポータルを表示できません。それ以外の場合は、次の手順を実行します。

1. DISCOVERパケットは、接続クライアントからブロードキャストとして送信され、使用可能なDHCPサーバを検出します
2. 使用可能なDHCPサーバがある場合、DHCPサーバはOFFERで応答します。オファーには、接続クライアントに割り当てるIPアドレスやリース時間などの情報が含まれます。さまざまなDHCPサーバから多数のOFFERを受信できます
3. クライアントは、サーバの1つからOFFERを受け入れ、選択したIPアドレスのREQUESTを返します
4. 最後に、DHCPサーバは、新しいIPアドレスが割り当てられたクライアントに確認応答パケットを送信します

WLCは、クライアントがIPアドレスを受信した方法を記録します。

<#root>

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

S_CO_IP_LEARN_IN_PROGRESS

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

SISF_DHCPDISCOVER

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

SISF_DHCPDISCOVER

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

SISF_DHCPDISCOVER

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

SISF_DHCPDISCOVER

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

SISF_DHCPOFFER

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

SISF_DHCPOFFER,

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

SISF_DHCPOFFER

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

SISF_DHCPOFFER

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

SISF_DHCPREQUEST

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

SISF_DHCPREQUEST

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

SISF_DHCPACK

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

SISF_DHCPACK

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

Client IP learn successful. Method: DHCP

IP: <end-user-ip-addr>
{wncd_x_R0-0}{1}: [epm] [17558]: (info): [0000.0000.0000:unknown] HDL = 0x0 vlan 1000 fail count 0 dirty
{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

L3認証の開始

エンドユーザがIPアドレスを受信したので、L3認証は、認証の目的の方式として検出された
CWAで開始されます。

<#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

Sanity IP Addressesテスト

接続を続行するには、クライアントが2つのARP要求を実行する必要があります。

1. そのIPアドレスを持つユーザーが他にいないことを確認します。エンドユーザのIPアドレスに対するARP応答が存在する場合は、IPアドレスが重複しています

2. ゲートウェイへの到達可能性を検証する。これは、クライアントがネットワークから発信できることを確認するためです。ARP応答はゲートウェイから送信される必要があります

<#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,

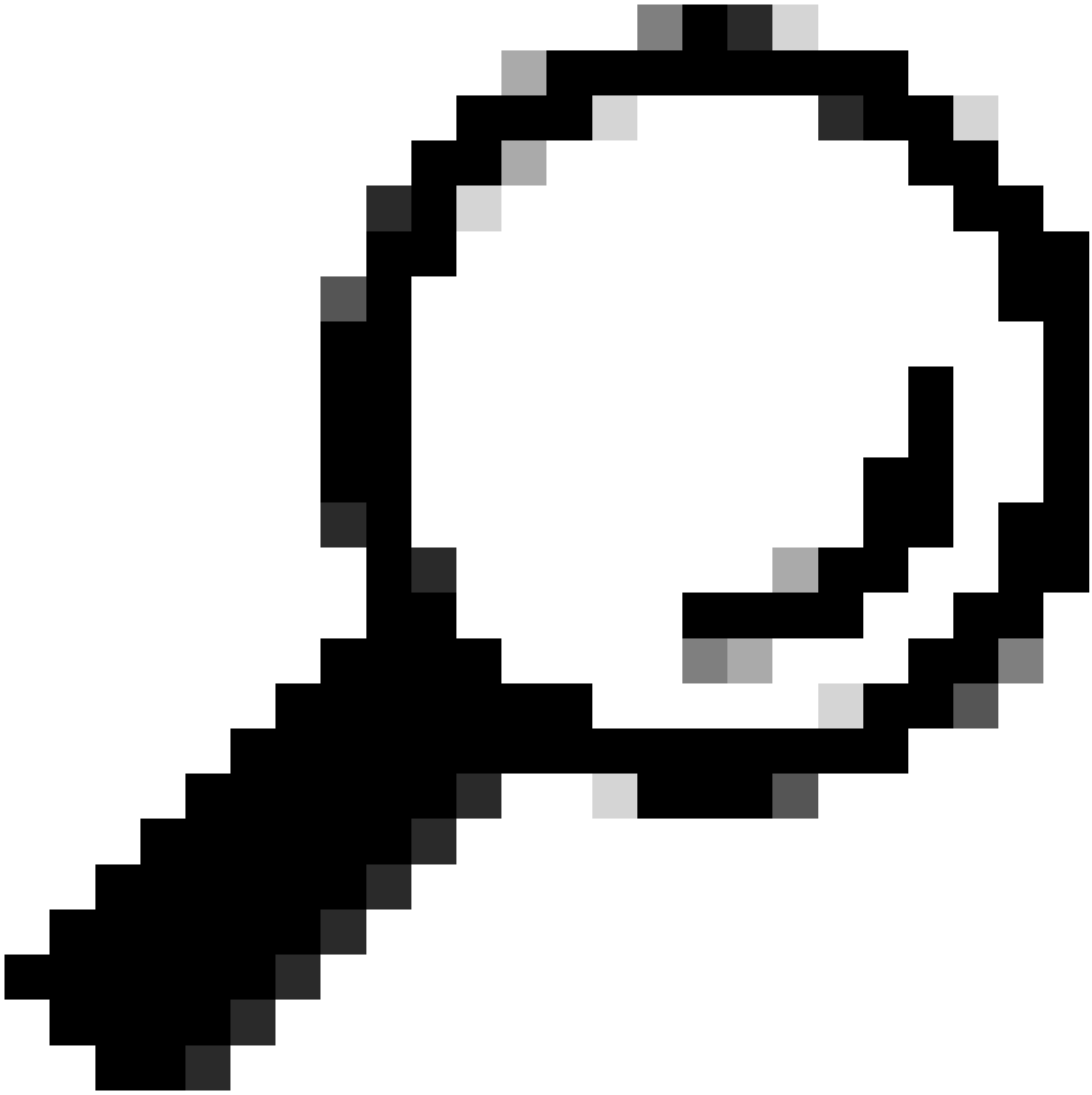
```
 ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t
```

2番目の接続：クライアントからネットワーク

この時点で、エンドユーザはMACアドレスを使用してISEに対して認証されていますが、まだ完全には認証されていません。WLCは、クライアントがネットワークに接続することを許可するために、ISEを再度参照する必要があります。この時点で、ユーザ名がユーザ名とパスワードを入力する必要があるポータルがユーザに表示されます。WLCでは、エンドユーザが「Web Auth Pending」状態として表示されます。

認可変更(CoA)

ここで、WLC設定の「CoAのサポート」が有効になります。この時点まで、ACLが使用されていました。エンドクライアントがポータルを認識した後、ACLは使用されなくなります。これは、エンドクライアントがポータルにリダイレクトしただけであるためです。この時点で、クライアントはログイン用のクレデンシャルを入力してCoAプロセスを開始し、クライアントを再認証します。WLCは、送信するパケットを準備し、ISEに転送します



ヒント:CoAはポート1700を使用します。ファイアウォールでブロックされていないことを確認します。

<#root>

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

Processing CoA request

```
 under CH-ctx.
```

<-- ISE requests the client to reauthenticate

```
{wncd_x_R0-0}{1}: [caaa-ch] [17558]: (info): [CAAA:COMMAND HANDLER:92000002] Reauthenticate request (0x
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

MAB re-authentication started

```
 for 2315255810 (4203.9522.e682)
```

<-- ISE requests the WLC to reauthenciate the CoA

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

CoA Response Details

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << ssg-command-code 0 32 >>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << formatted-clid 0 "4203.9522.e682">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): << error-cause 0 1 [
```

Success

```
]>>
```

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

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

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

ISEへの2番目の認証

2番目の認証はゼロから始まりません。これはCoAの力です。新しいルールやAV parisをユーザに適用できます。最初のAccess-Acceptで受信されたACLとリダイレクションURLは、エンドユーザにプッシュされなくなります。

WLCがISEに要求を送信

WLCは、入力されたユーザ名/パスワードの組み合わせを使用して、新しいRADIUSAccess-RequestpacketをISEに送信します。これにより、新しいMAB認証がトリガーされます。ISEはすでにクライアントを認識しているため、新しいポリシーセット（Access Grantedなど）が適用されます。

<#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がWLC要求に応答する

ISEはポリシーのルックアップを実行し、受信したユーザ名がポリシープロファイルと一致する場合、ISEはWLANへのクライアント接続を受け入れて、WLCに再度応答します。エンドユーザのユーザ名を返します。ISEで設定されている場合、追加のルールやAVペアをユーザに適用でき、それらはAccess-Acceptに表示されます。

<#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

ISEから受信した情報のWLCプロセス

WLCは、ISEが受信した情報を再度処理します。ISEから受信した新しい値を使用して、ユーザに対して別のREPLACEアクションを実行します。

<#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認証の完了

これで、エンドユーザは指定されたデータで認証されました。L3認証（Web認証）が終了します。

```
<#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
```

エンドユーザがWLCでRUN状態になる

最後に、ユーザが認証され、WLANに関連付けられます。

```
<#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

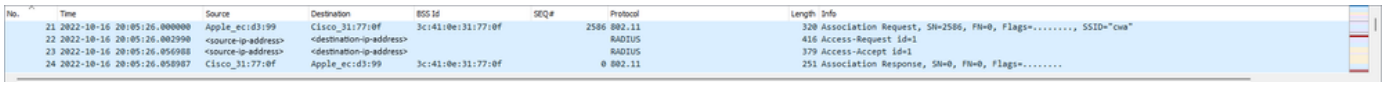
CWAフロー – 組み込みパケットキャプチャ(EPC)

EPCは、WLCから直接取得できるパケットキャプチャで、WLCを通過するすべてのパケット、またはWLCから送信されるすべてのパケットを示します。これらのコマンドの概要と取得方法の詳細については、「Catalyst 9800ワイヤレスLANコントローラでのワイヤレスデバッグとログ収集について」を参照してください。

最初の接続：クライアントからISEサーバ

警告：パケットキャプチャのイメージ上のIPアドレスが削除されました。およびとして表示されます。

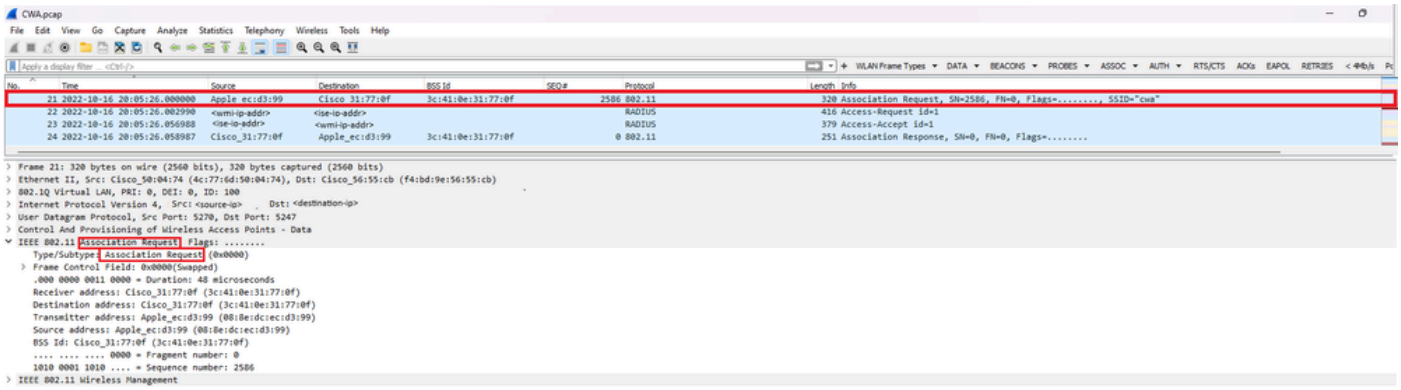
WLANへの関連付けとISEサーバへの要求の送信



最初のパケット

WLCからクライアントへのアソシエーション要求

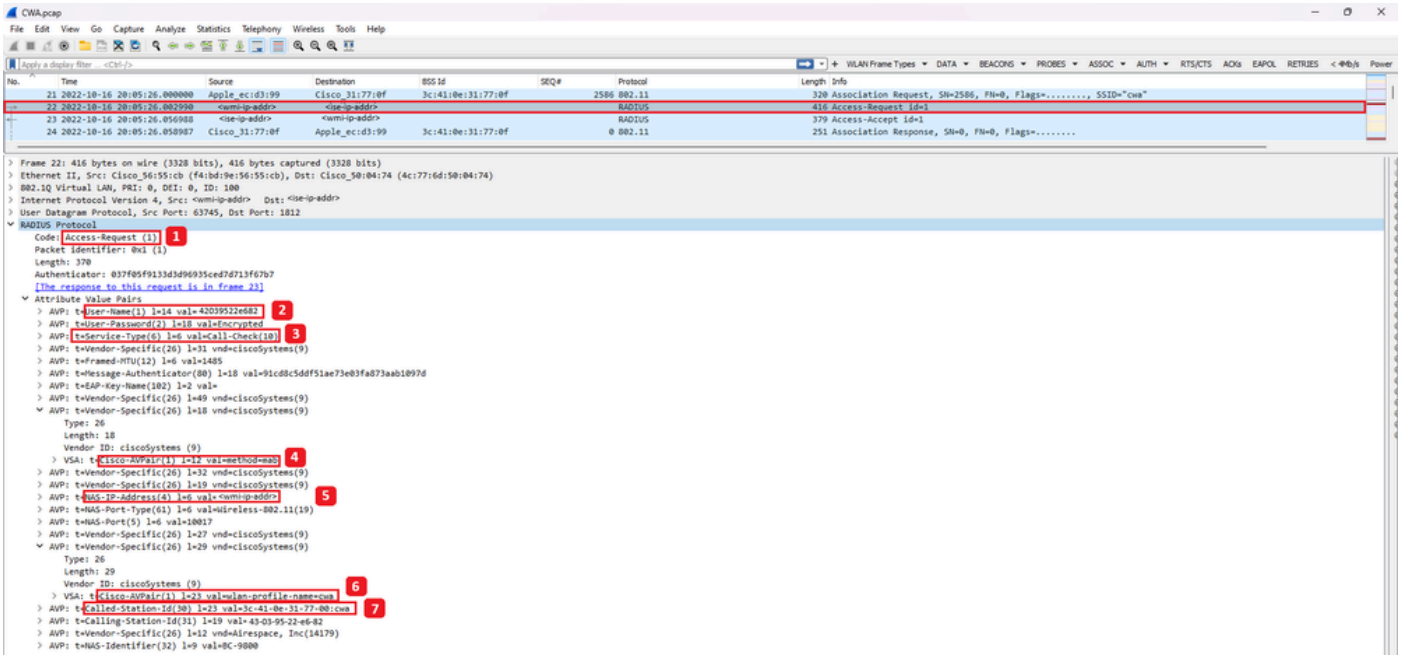
最初のパケット「アソシエーション要求」を見ると、このプロセスに関与するデバイスのMACアドレスがわかります。



関連付け要求

WLCからISEに送信されるアクセス要求パケット

アソシエーション要求がWLCで処理されると、WLCはAccess-RequestパケットをISEサーバに送信します。



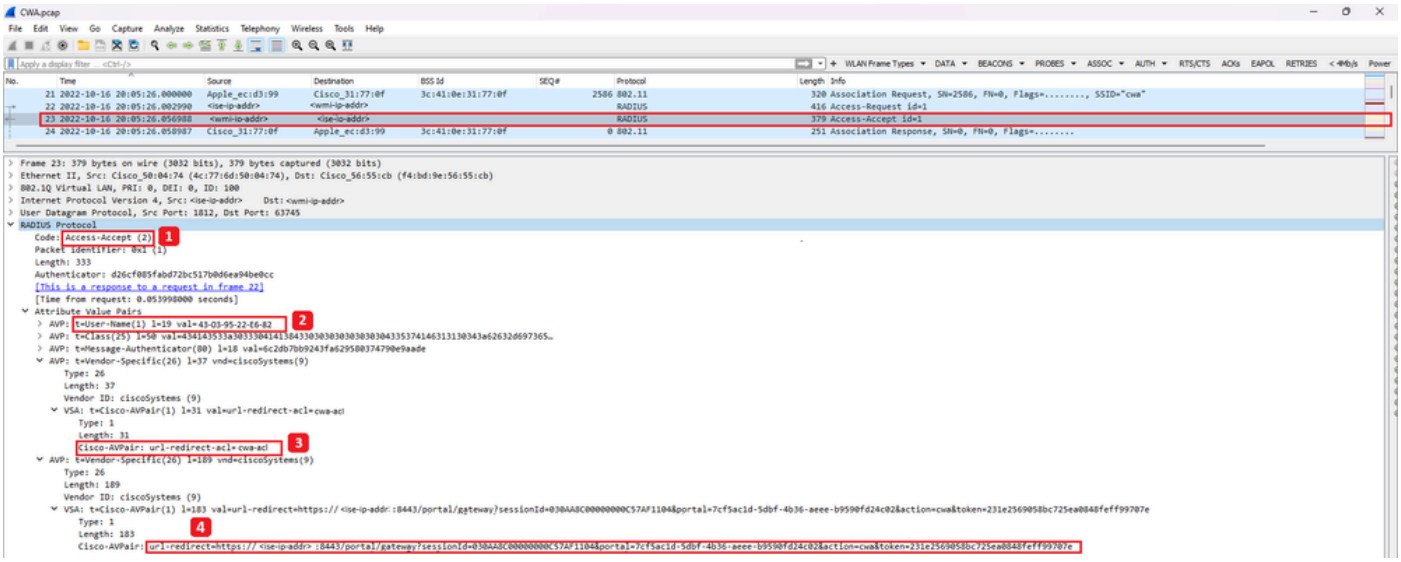
アクセス要求パケットの分析

1. パケット名。
2. 認証を試みているMACアドレス。
3. これは、MACフィルタリングを示します。

4. MACフィルタリングプロセスを示すためにコントローラからISEに送信されるAVペア。
5. WLCのWMI IPアドレス。
6. クライアントが接続しようとしているSSID。
7. クライアントが接続しようとしているWLANの名前。

WLCからISEに送信されるAccess-Acceptパケット

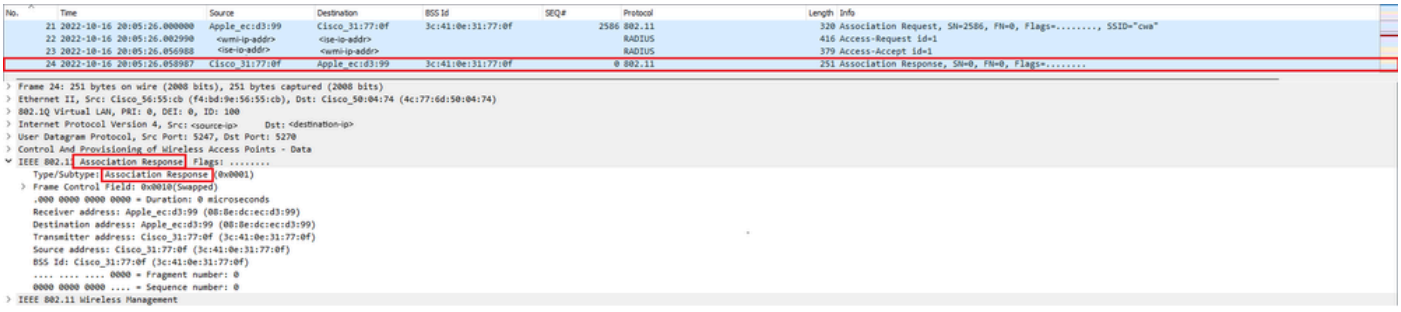
ISEがAccess-Acceptパケットを処理すると、成功の場合はAccess-Acceptで応答し、失敗の場合はAccess-Rejectで応答します。



Access-Acceptパケットの分析

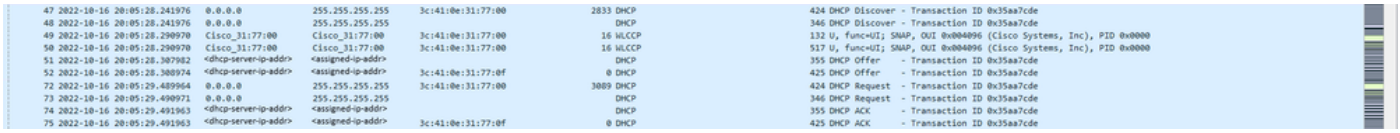
1. パケット名。
2. 認証されたMACアドレス。
3. 適用されるACL。
4. ユーザーのリダイレクト先のURL。

WLCからクライアントへのアソシエーション応答

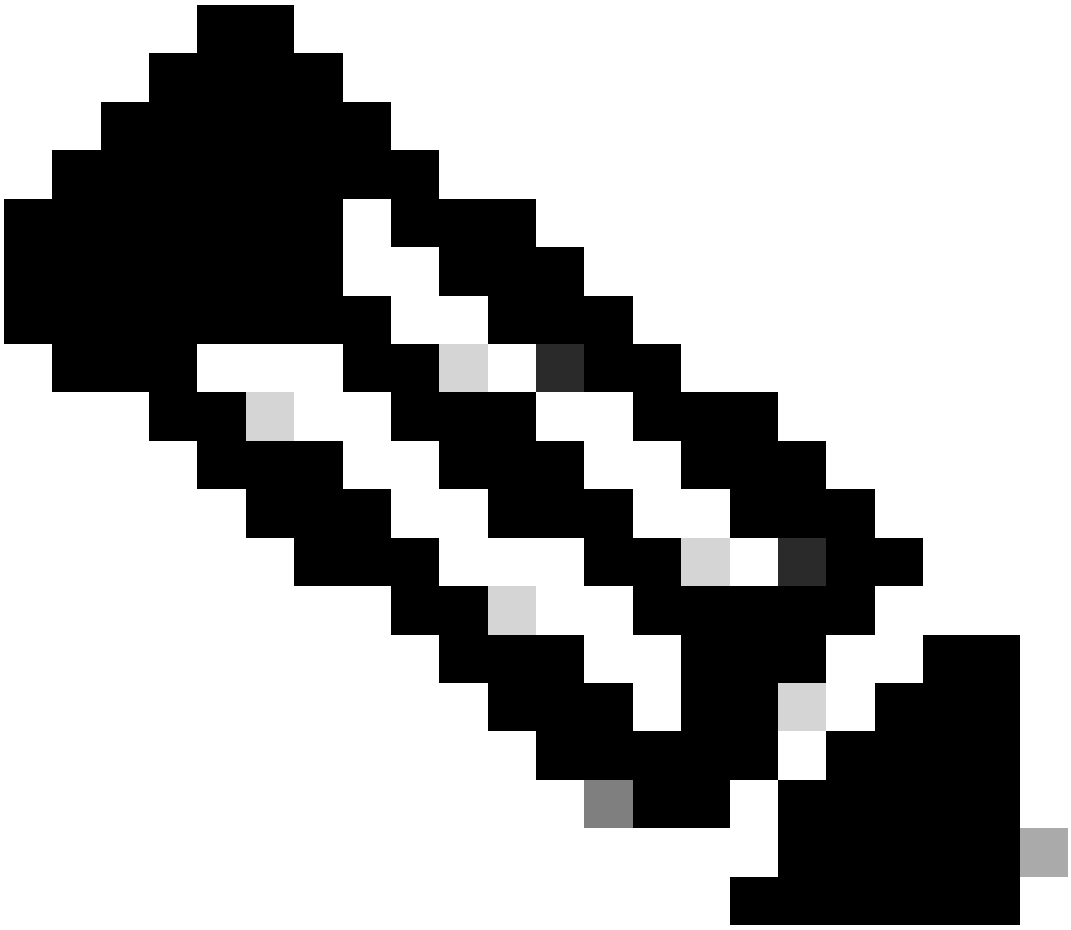


関連付け応答

DHCPプロセス

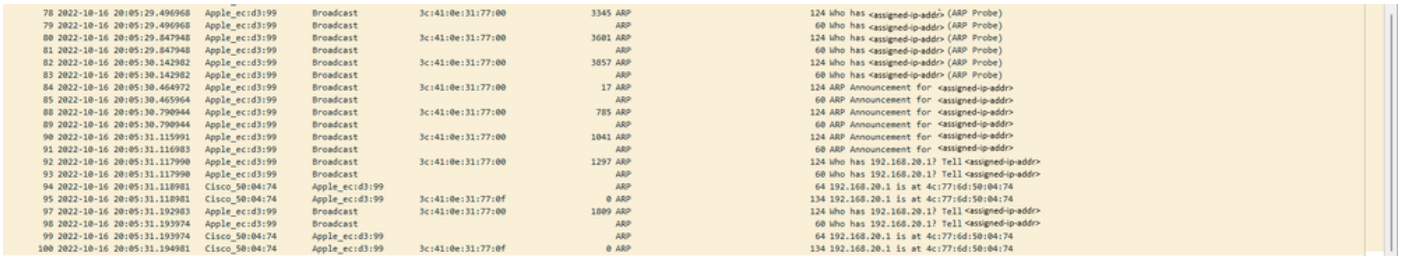


DHCPプロセス



注：これ以降、パケットが重複して表示されますが、これは一方がCAPWAPカプセル化され、他方がCAPWAPカプセル化されていないためです

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

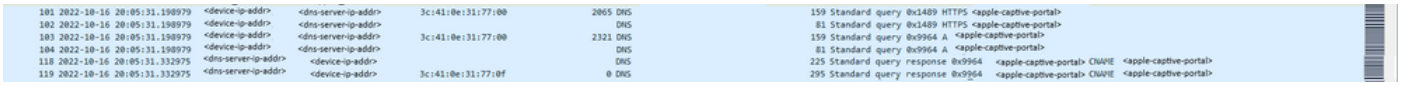
自身のIPアドレスとゲートウェイのクライアントARP

接続テスト

ARPプロセスが終了すると、接続を試みているデバイスはポータルがトリガーされているかどうかを検証するチェックを実行します。これはプローブとも呼ばれます。デバイスにインターネット接続がないと表示される場合は、ARPプロセスが失敗したか（ゲートウェイが応答しなかったなど）、デバイスがプローブを実行できなかったことを意味します。

このプローブはRAトレースでは確認できず、EPCのみがこの情報を提供できます。プローブのクエリは、接続を試行しているデバイスによって異なります。この例では、テストデバイスはAppleデバイスであったため、プローブはAppleのキャプティブポータルに直接向けて行われました。

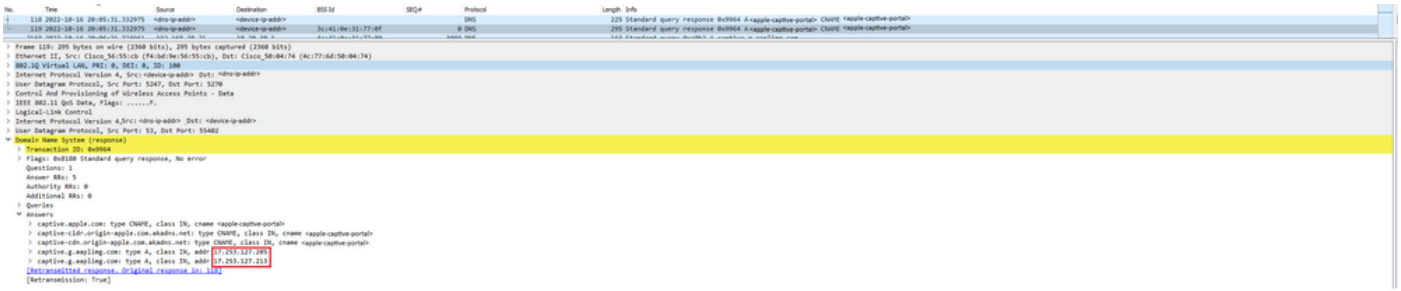
URLを使用してプローブが行われるため、このURLを解決するにはDNSが必要です。そのため、DNSサーバがクライアントのクエリに応答できない場合、クライアントはURLのクエリを続行し、ポータルは表示されません。この時点で、エンドデバイスのWebブラウザでISEサーバのIPアドレスを入力すると、ポータルが表示されます。存在する場合は、DNSサーバに問題があります。



クライアントからの接続テスト – DNSクエリーおよび応答

DNSで解決されたIPアドレス

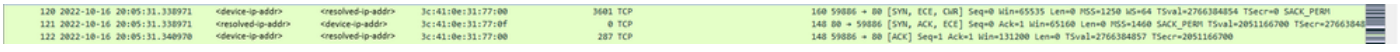
DNSクエリー応答を調べると、DNSサーバによって解決されたIPアドレスを確認できます。



DNSサーバによって解決されるIPアドレス

3ウェイハンドシェイクを確立する

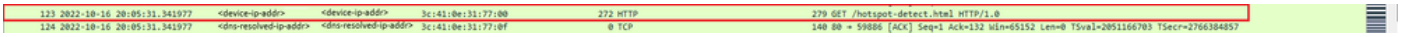
DNS IPアドレスが解決されたので、ポータルとクライアントの間でTCP 3ウェイハンドシェイクが確立されます。使用されるIPアドレスは、解決されたIPアドレスのいずれかです。



3ウェイハンドシェイクの確立

ホットスポットの取得

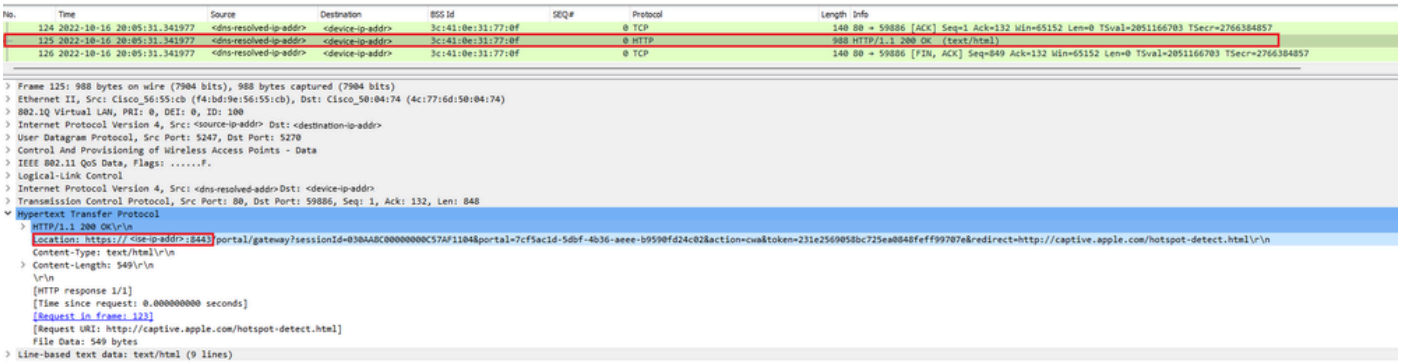
TCPセッションが確立されると、クライアントはプローブを実行し、ポータルへのアクセスを試みます。



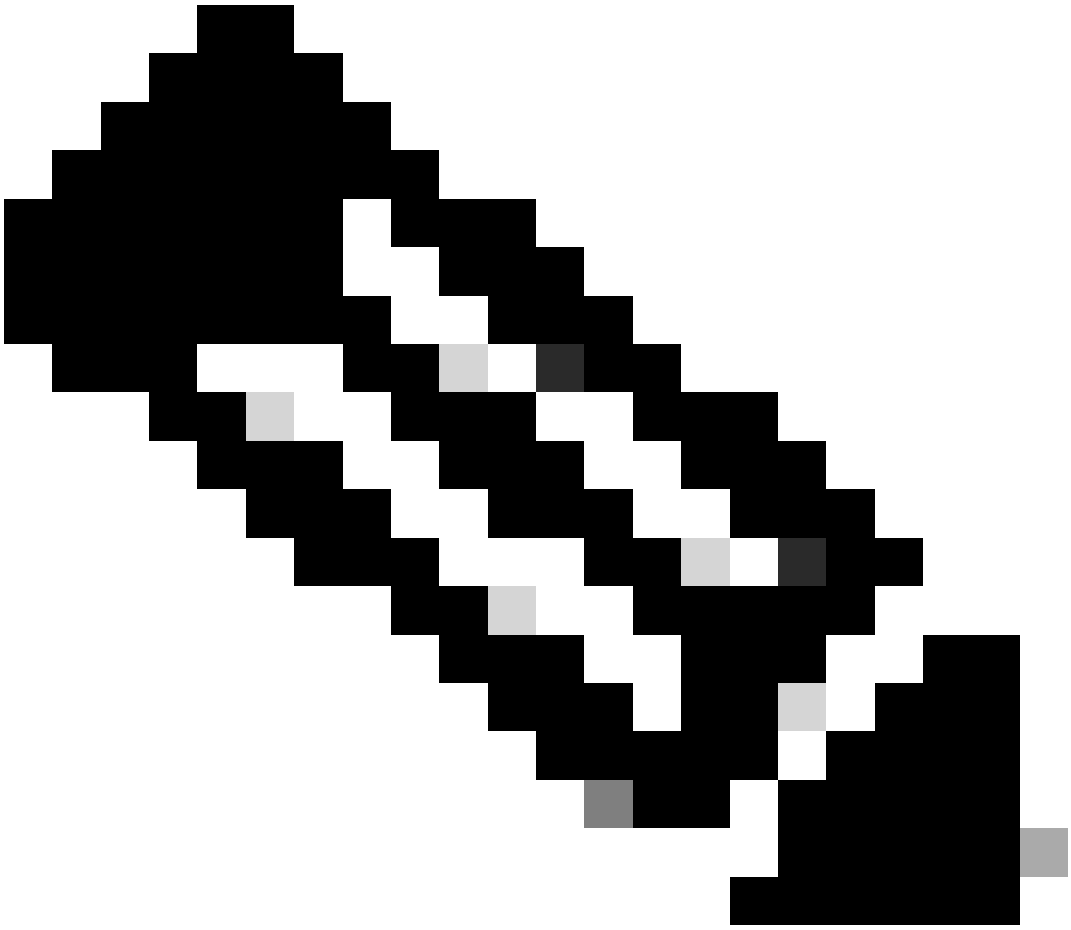
ホットスポットの取得

OKパケット

OKパケットには、クライアントのリダイレクト先となるISEのポータルが含まれています。



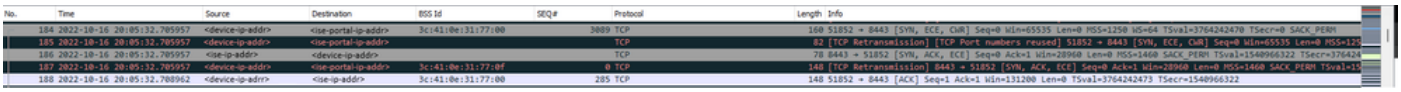
OKパケット



> 注：ほとんどの場合、OKパケットには別のURLが返されます。したがって、最終的なIPアドレスを取得するために別のDNSクエリを実行する必要があります。

新しいTCPセッションの確立

ポータルのIPアドレスが検出されたため、多くのパケットが交換されますが、最後に、ISEのIPアドレスに対応するOKパケット（またはDNSによって解決されたIP）で返された宛先IPを持つパケットは、ポータルに新しいTCPセッションが確立されていることを示します。



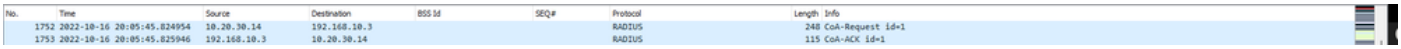
ISEポータルへの2番目の接続と新しいTCPセッション

ポータルがユーザに表示される

この時点で、ISEのポータルが最終的にクライアントブラウザのブラウザに表示されます。前と同様に、多くのパケットがISEとデバイスの間で交換されます。たとえば、client helloやserver helloなどです。ここでは、ISEがクライアントにユーザ名とパスワードを要求し、利用条件を受け入れるか、またはISEサーバ上で設定されているものに何かを要求します。

CoA要求/CoA確認応答

ユーザが要求されたすべてのデータを入力すると、ISEはCoA要求をコントローラに送信して、ユーザの許可を変更します。NAC状態の設定やCoAのサポートなど、WLC上のすべてが想定どおりに設定されている場合、WLCはCoA確認応答(CoA ACK)を送信します。そうしないと、WLCはCoA非確認応答(CoA NACK)を送信するか、単にCoA ACKを送信しないことさえできます。

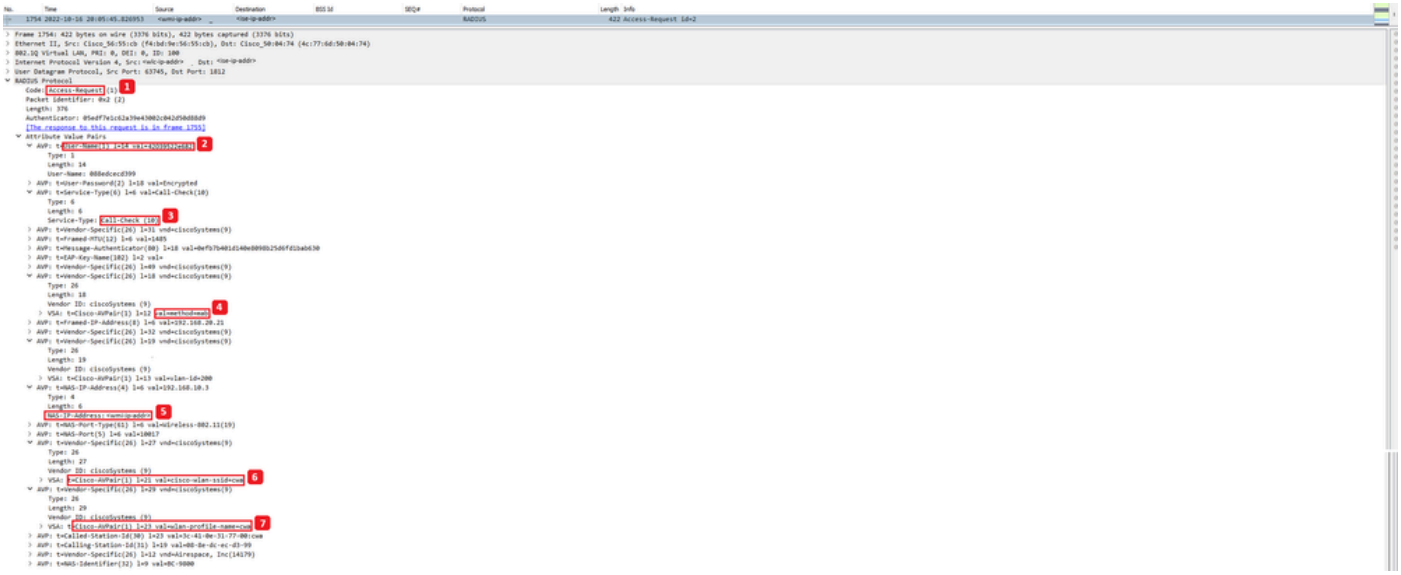


CoA要求および確認応答

2番目の接続：クライアントからネットワーク

新しいアクセス要求

WLCが新しいアクセス要求パケットをISEに送信します。

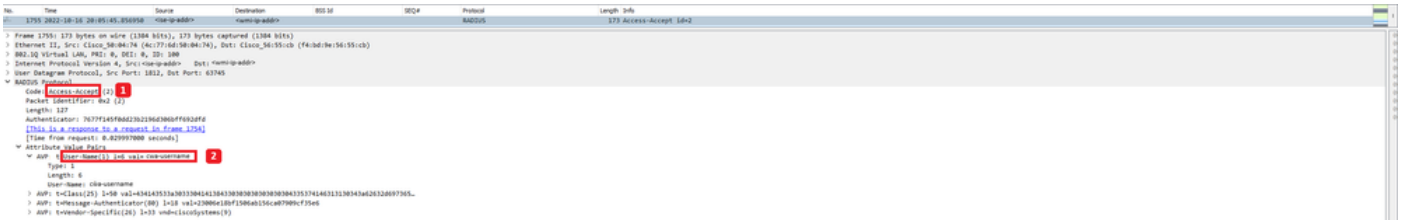


新しいアクセス要求パケットの分析

1. パケット名。
2. 認証を試みているMACアドレス。
3. これは、MACフィルタリングを示します。
4. MACフィルタリングプロセスを示すためにコントローラからISEに送信されるAVペア。
5. WLCのWMI IPアドレス。
6. クライアントが接続しようとしているSSID。
7. クライアントが接続しようとしているWLANの名前。

新しいアクセス許可

WLCが新しいアクセス要求パケットをISEに送信します。



新しいAccess-Acceptパケットの分析

1. パケット名。
2. 表示されたポータルでエンドクライアントが入力したユーザ名。

ここでも、クライアントから新しいプローブ接続テストが行われます。クライアントがインターネットに接続できることを確認したら、ポータルを閉じることができます（使用するデバイスに応じて自動的に閉じることができます）。これで、クライアントがネットワークに接続されました。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。