클라이언트의 CWA 플로우 이해

목차

소개

이 문서에서는 CWA WLAN에 연결할 때 최종 클라이언트가 겪는 흐름에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음에 대한 기본 지식을 갖춘 것을 권장합니다.

- Cisco WLC(Wireless LAN Controller) 9800 시리즈
- ISE(Identity Services Engine)에 대한 CWA(Central Web Authentication) 및 컨피그레이션에 대한 일반적인 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

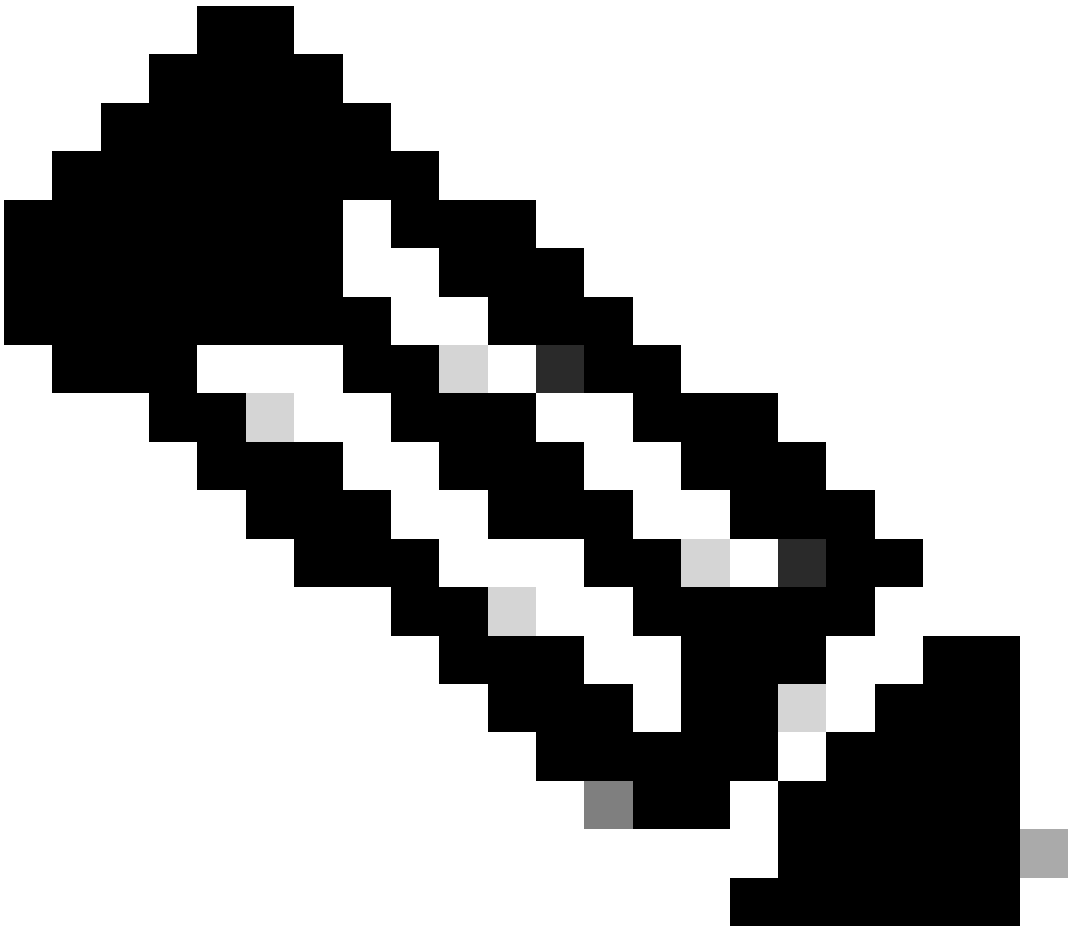
- 9800-CL WLC
- Cisco AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- ISE(Identity Service Engine) v3.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CWA는 WLC에서 구성할 수 있는 SSID 인증 유형으로, 연결을 시도하는 최종 클라이언트에게 웹 포털에 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. 간단히 말해, WLAN에 연결할 때 최종 클라이언트에 대한 흐름은 다음과 같습니다.

1. 최종 클라이언트는 디바이스에 표시되는 SSID에 연결됩니다
2. 최종 클라이언트는 자격 증명을 입력하도록 웹 포털로 리디렉션됩니다
3. 최종 클라이언트는 입력한 자격 증명으로 ISE에서 인증됩니다
4. ISE는 최종 클라이언트가 인증되었음을 WLC에 회신합니다. ISE는 클라이언트가 네트워크에 액세스할 때 준수해야 하는 몇 가지 추가 특성을 푸시할 수 있습니다(예: 특정 ACL)
5. 최종 클라이언트가 다시 연결되고 재인증되며 최종적으로 네트워크에 대한 액세스 권한을 얻습니다



참고: 최종 클라이언트가 두 번 인증될 경우 최종 클라이언트에 대해 투명하다는 점을 유념해야 합니다

클라이언트가 거쳐야 하는 기본 프로세스는 기본적으로 두 가지로 나뉩니다. 클라이언트에서 ISE 서버로의 연결과, 인증된 후 클라이언트에서 네트워크 자체로의 또 다른 연결입니다. 컨트롤러와 ISE는 항상 RADIUS 프로토콜을 통해 서로 통신합니다. 아래에서는 RA(Radioactive) 추적 및 EPC(Embedded Packet Capture)를 심층적으로 분석합니다.

CWA 흐름 - 방사성(RA) 추적

RA 추적은 특정 클라이언트에 대해 캡처된 로그 집합입니다. 클라이언트가 WLAN에 연결하는 동안 거치는 전체 프로세스를 보여 줍니다. RA의 현재 상태와 RA 추적을 검색하는 방법에 대한 자세한 내용은 Informed Wireless Debugs and Log Collection on Catalyst 9800 Wireless LAN Controllers를 참조하십시오.

첫 번째 연결: 클라이언트와 ISE 서버

클라이언트가 이전에 ISE에서 인증되지 않은 경우 WLC는 네트워크에 대한 연결을 허용하지 않습니다.

WLAN에 연결

WLC는 클라이언트가 WLAN "cwa"에 연결하려는 것을 탐지합니다. WLAN은 정책 프로파일 "cwa-policy-profile"에 연결되어 있고 AP "BC-3802"에 연결되어 있습니다

<#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 필터링

ISE 서버 연결 테스트

WLC가 클라이언트로부터 연결 요청을 받으면 첫 번째 단계는 MAC 필터링(MAB라고도 함)을 수행하는 것입니다. MAC 필터링은 클라이언트의 MAC 주소를 데이터베이스와 비교하여 검사하여 네트워크에 가입할 수 있는지 여부를 확인하는 보안 방법입니다.

<#root>

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

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


[client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_CO_ASSOCIATING -> S
[client-auth] [17558]: (note): MAC: 4203.9522.e682 MAB Authentication initiated.

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


[sanet-shim-translate] [17558]: (ERR): 4203.9522.e682 wlan_profile Not Found : Device information attri
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Session Start event called from SANET-SHIM
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wireless session sequence, create context
[auth-mgr-feat_wireless] [17558]: (info): [4203.9522.e682:capwap_90000005] -

authc_list: cwa_authz <-- Authentication method list used


[auth-mgr-feat_wireless] [17558]: (info): [4203.9522.e682:capwap_90000005] - authz_list: Not present un
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_INI
[auth-mgr] [17558]: (info): [4203.9522.e682:unknown] auth mgr attr change notification is received for
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is recei
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Retrieved Client IIF ID 0x530002f1
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Allocated audit session id 0E1E140A0000000
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Applying policy for WlanId: 1, bssid : dc8
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wlan vlan-id from bssid hdl 0
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] SM Reauth Plugin: Received valid timeout =
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005]

MAB authentication started for 4203.9522.e682


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

MAB_CONTINUE

' on handle 0x8A000002

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


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

WLC가 ISE에 요청 전송

WLC는 WLAN에 인증하려는 클라이언트의 MAC 주소가 포함된 RADIUS 액세스 요청 패킷을 ISE에 전송합니다.

<#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

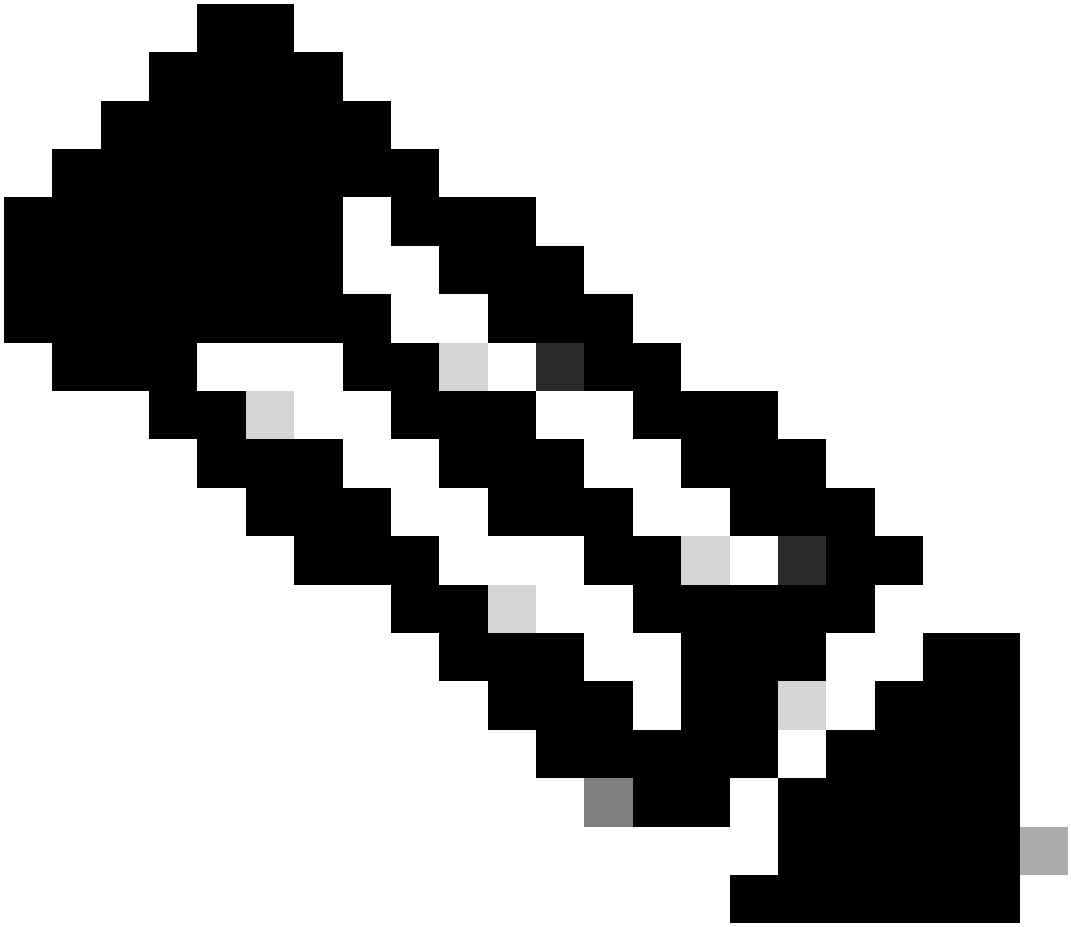
"

<-- 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
```



참고: AV 쌍은 ISE에서 사용하는 "Attribute-Value"입니다. WLC에 전송 할 수 있는 미리 정

의 된 정보의 키 값 구조 입니다. 이러한 값은 해당 특정 세션의 특정 클라이언트에 적용됩니다.

AV 쌍의 예:

- ACL 이름
- 리디렉션 URL
- VLAN 할당
- 세션 시간 초과 시간
- 재인증 타이머

ISE가 WLC 요청에 응답

WLC에서 보낸 MAC 주소가 ISE에서 수락되면 ISE는 Access-Accept RADIUS 패킷을 전송합니다. ISE 컨피그레이션에 따라 알 수 없는 MAC 주소인 경우 ISE는 이를 수락하고 플로우를 계속 진행해야 합니다. Access-Reject(액세스 거부)가 표시되면 ISE에서 올바르게 구성되지 않은 것으로 확인되어야 합니다.

<#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

ISE에서 수신한 정보의 WLC 프로세스

WLC는 ISE에서 받은 모든 정보를 처리합니다. ISE에서 전송한 데이터의 프로필과 함께 원래 생성한 사용자 프로필을 적용합니다. 예를 들어 WLC는 사용자에게 새 ACL을 할당합니다. WLAN에서 AAA Override(AAA 재정의)가 활성화되어 있지 않으면 WLC에서 이러한 처리를 수행하지 않습니다
.

<#root>

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

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

{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< class 0 43 41 43 53 3a 30 45 31 45 31 34 30 41 30 30 30 30 30 30 30 30 43 38 45 32 44 41 36 34 32 3a 62
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<<Message-Authenticator 0 <hidden>>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<<

url-redirect-acl 0 "cwa-acl"

>>

<-- Processing ACL redirection received from ISE

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

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

>>

<-- Processing URL redirection received from ISE

{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< dnis 0 "DC-8C-37-D0-83-A0">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< formatted-clid 0 "42-03-95-22-E6-82">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< audit-session-id 0 "0E1E140A0000000C8E2DA642">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< method 0 2 [mab]>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< clid-mac-addr 0 42 03 95 22 e6 82 >>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< intf-id 0 2415919109 (0x90000005)>>
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]

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

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

User profile is to be applied

. Authz mlist is not present,

Authc mlist cwa_authz

,session push flag is unset
{wncd_x_R0-0}{1}: [webauth-dev] [17558]: (info): Central Webauth URL Redirect,

Received a request to create a CWA session

for a mac [42:03:95:22:e6:82]
{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17558]: (info): [0000.0000.0000:unknown] Retrieved zone id
{wncd_x_R0-0}{1}: [webauth-dev] [17558]: (info): No parameter map is associated with mac 4203.9522.e682
{wncd_x_R0-0}{1}: [epm-redirect] [17558]: (info): [0000.0000.0000:unknown]

URL-Redirect-ACL = cwa-acl

{wncd_x_R0-0}{1}: [epm-redirect] [17558]: (info): [0000.0000.0000:unknown]

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

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

User Profile applied

successfully

for 0x92000002 -

REPLACE

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

MAB 인증 완료

클라이언트의 사용자 프로필이 성공적으로 수정되면 WLC는 클라이언트의 MAC 주소 인증을 완료합니다. ISE에서 받은 ACL이 WLC에 없으면 WLC는 해당 정보로 무엇을 해야 하는지 알지 못하므로 REPLACE 작업이 완전히 실패하여 MAB 인증도 실패합니다. 클라이언트가 인증할 수 없습니다.

<#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

WLC가 클라이언트에 연결 응답을 보냅니다.

이제 클라이언트가 ISE에 의해 인증되고 올바른 ACL이 적용되었으므로 WLC는 클라이언트에 연결 응답을 보냅니다. 이제 사용자는 네트워크에 계속 연결할 수 있습니다.

<#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 인증

클라이언트가 WLAN에 연결할 때 거쳐야 하는 프로세스에 따라 L2 인증이 "시작"됩니다. 그러나 실제로는 이전에 수행된 MAB 인증으로 인해 이미 L2 인증이 수행된 바 있다. 클라이언트는 즉시 L2 인증을 완료합니다.

<#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
```

데이터 플러그

WLC는 트래픽이 네트워크를 통과해 이동할 수 있도록 연결 클라이언트에 리소스를 할당합니다.

<#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

사용자에게 IP 주소가 할당됨

최종 사용자는 네트워크를 탐색하기 위해 IP 주소가 필요합니다. DHCP 프로세스를 거칩니다. 사용자가 이전에 연결되었고 해당 IP 주소를 기억하는 경우 DHCP 프로세스를 건너뜁니다. 사용자가 IP 주소를 수신할 수 없는 경우 최종 사용자는 웹 포털을 볼 수 없습니다. 그렇지 않으면 다음 단계를 거칩니다.

1. DISCOVER 패킷은 사용 가능한 DHCP 서버를 찾기 위해 연결 클라이언트에서 브로드캐스트로 전송됩니다
2. 사용 가능한 DHCP 서버가 있는 경우 DHCP 서버는 OFFER로 응답합니다. 이 서비스에는 연결 클라이언트에 할당할 IP 주소, 리스 시간 등의 정보가 포함됩니다. 다양한 DHCP 서버에서 많은 OFFER를 받을 수 있습니다
3. 클라이언트는 서버 중 하나의 OFFER를 수락하고 선택한 IP 주소에 대한 REQUEST로 응답합니다
4. 마지막으로, DHCP 서버는 새 IP 주소가 할당된 클라이언트에 승인 패킷을 보냅니다

WLC는 클라이언트가 IP 주소를 받은 방법을 로깅합니다.

<#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 인증 시작

최종 사용자가 IP 주소를 받았으므로 L3 인증은 원하는 인증 방법으로 탐지된 CWA로 시작됩니다.

<#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

온전성 IP 주소 테스트

연결을 계속 진행하려면 클라이언트가 2개의 ARP 요청을 수행해야 합니다.

1. 다른 사람이 IP 주소를 가지고 있지 않은지 확인합니다. 최종 사용자의 IP 주소에 대한 ARP 회신이 있는 경우 중복된 IP 주소입니다

2. 게이트웨이에 연결할 수 있는지 확인합니다. 이는 클라이언트가 네트워크에서 나갈 수 있도록 하기 위한 것입니다. ARP 회신은 게이트웨이에서 가져와야 합니다.

<#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 ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{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 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{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 So

ARP REQUEST,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 So

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,

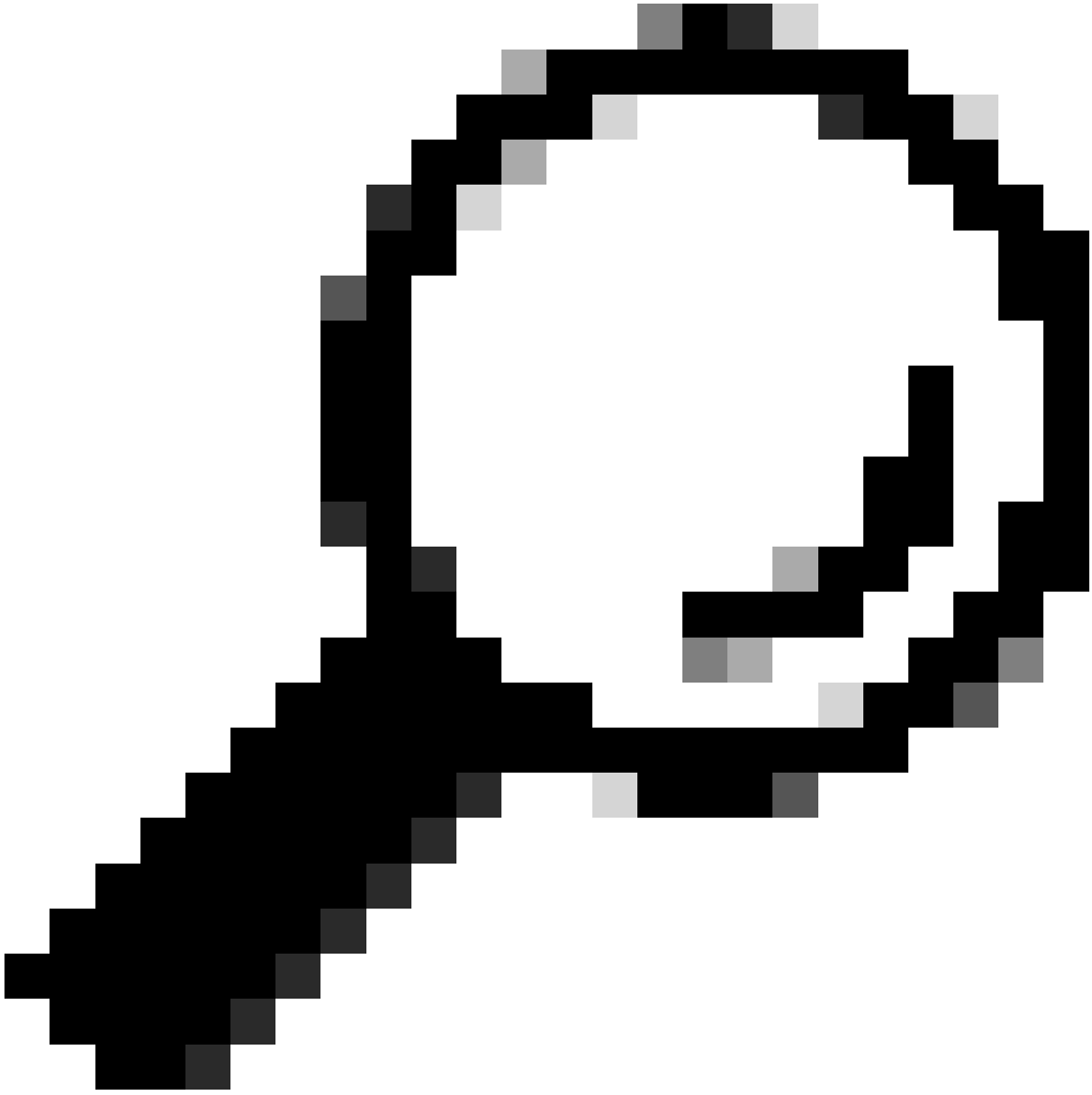
```
 ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t
```

두 번째 연결: 클라이언트와 네트워크

이 시점에서 최종 사용자는 MAC 주소를 통해 ISE에 대해 인증되었지만 아직 완전히 인증되지 않았습니다. WLC는 ISE를 한 번 더 참조하여 클라이언트가 네트워크에 연결하도록 인증해야 합니다. 이때 포털은 사용자에게 표시되며, 여기서 사용자 이름은 사용자 이름과 비밀번호를 입력해야 합니다. WLC에서 최종 사용자는 "웹 인증 보류 중" 상태로 표시됩니다.

CoA(Change of Authorization)

다음은 WLC 구성의 "CoA에 대한 지원"이 적용되는 위치입니다. 이 시점까지는 ACL이 사용되었습니다. 최종 클라이언트가 포털을 본 후에는 ACL이 더 이상 사용되지 않습니다. 이는 클라이언트를 포털로 리디렉션한 것뿐이기 때문입니다. 이때 클라이언트는 CoA 프로세스를 시작하고 클라이언트를 재인증하기 위해 로그인할 때 사용할 자격 증명을 입력합니다. WLC는 전송할 패킷을 준비하고 ISE에 전달합니다



팁: CoA는 포트 1700을 사용합니다. 방화벽에 의해 차단되지 않았는지 확인합니다.

<#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

ISE에 대한 두 번째 인증

두 번째 인증은 0에서 시작하지 않습니다. 이것이 바로 CoA의 힘입니다. 새로운 규칙들 및/또는 AV 파리들이 사용자에게 적용될 수 있다. 첫 번째 Access-Accept에서 받은 ACL 및 리디렉션 URL은 더 이상 최종 사용자에게 푸시되지 않습니다.

WLC가 ISE에 요청 전송

WLC는 입력한 사용자 이름/비밀번호 조합과 함께 ISE에 새 RADIUSAccess-Requestpacket을 전송합니다. 그러면 새 MAB 인증이 트리거되며, ISE가 이미 클라이언트를 알고 있으므로 새 정책 집합이 적용됩니다(예: Access Granted).

<#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

ISE가 WLC 요청에 응답

ISE는 정책 조회를 수행하며, 수신한 사용자 이름이 정책 프로파일과 일치하면 ISE는 WLC에 다시 응답하고 WLAN에 대한 클라이언트 연결을 수락합니다. 최종 사용자의 사용자 이름을 반환합니다. ISE에 구성된 경우 추가 규칙 및/또는 AV 쌍을 사용자에게 적용할 수 있으며 Access-Accept에 표시됩니다.

<#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

ISE에서 수신한 정보의 WLC 프로세스

WLC는 ISE에서 수신한 정보를 다시 처리합니다. ISE에서 받은 새 값으로 사용자에 대해 또 다른 REPLACE 작업을 수행합니다.

<#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 인증 완료

이제 최종 사용자가 지정된 데이터로 인증되었습니다. L3 인증(웹 인증)이 완료되었습니다.

<#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
```

최종 사용자가 WLC에서 RUN 상태에 도달함

마지막으로, 사용자가 인증되고 WLAN에 연결됩니다.

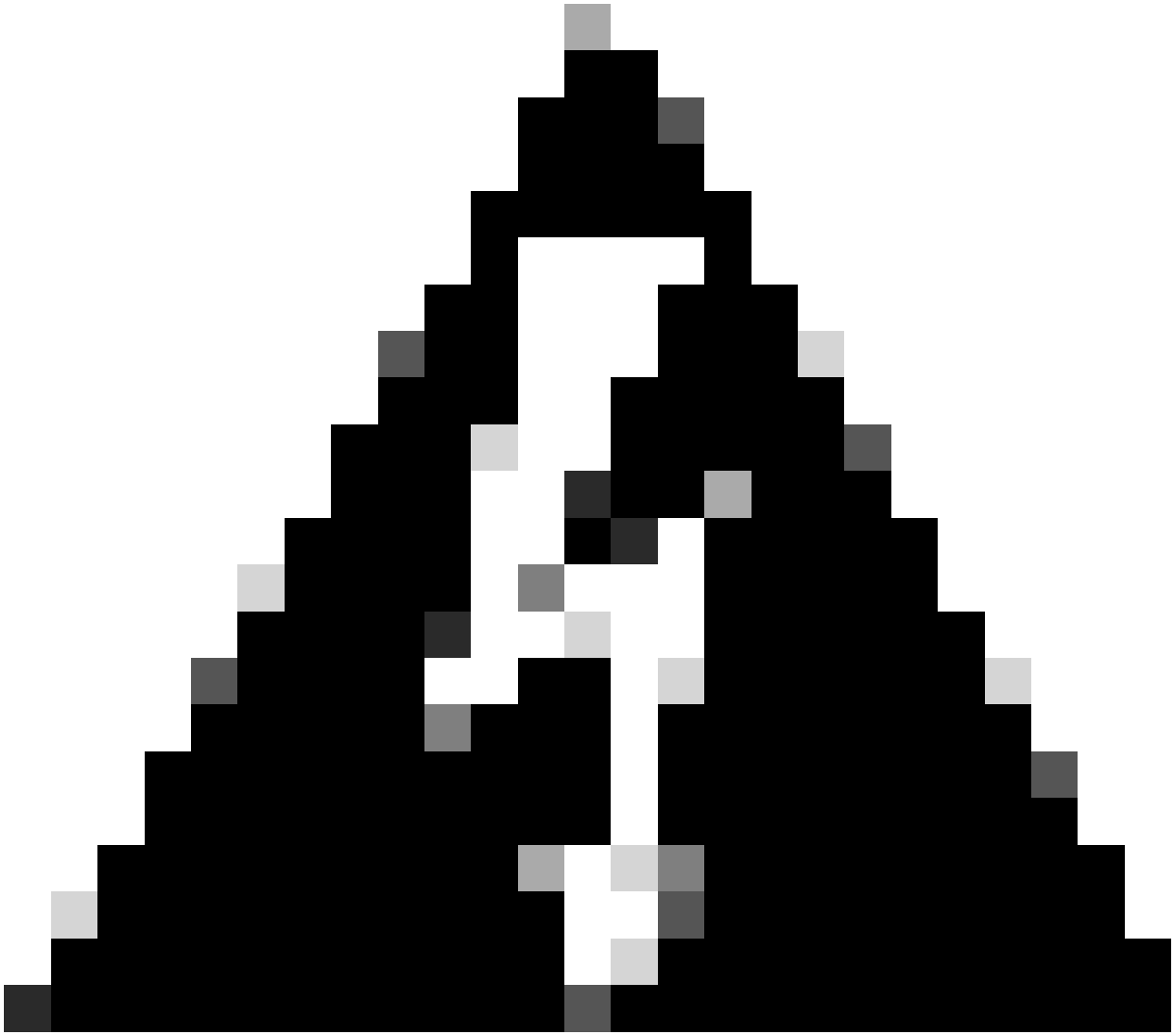
<#root>

```
{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 플로우 - EPC(Embedded Packet Capture)

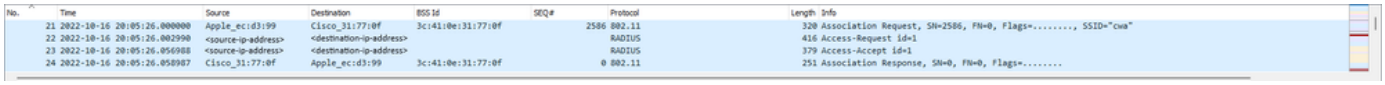
EPC는 WLC에서 직접 검색할 수 있는 패킷 캡처로서 WLC를 통과하거나 WLC에서 소싱되는 모든 패킷을 표시합니다. 현재 상태 및 검색 방법에 대한 자세한 내용은 Cisco Catalyst 9800 Wireless LAN Controller에서 무선 디버깅 및 로그 수집 이해를 참조하십시오.

첫 번째 연결: 클라이언트와 ISE 서버



경고: 패킷 캡처 이미지의 IP 주소가 삭제되었습니다. 및 로 표시됩니다

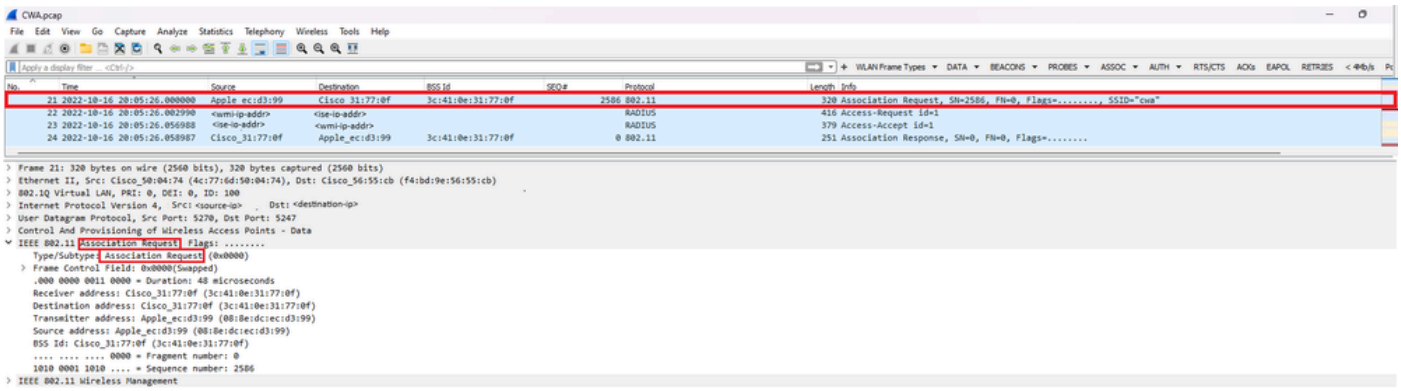
WLAN에 연결 및 ISE 서버로 요청 전송



첫 번째 패킷

WLC에서 클라이언트로 연결 요청

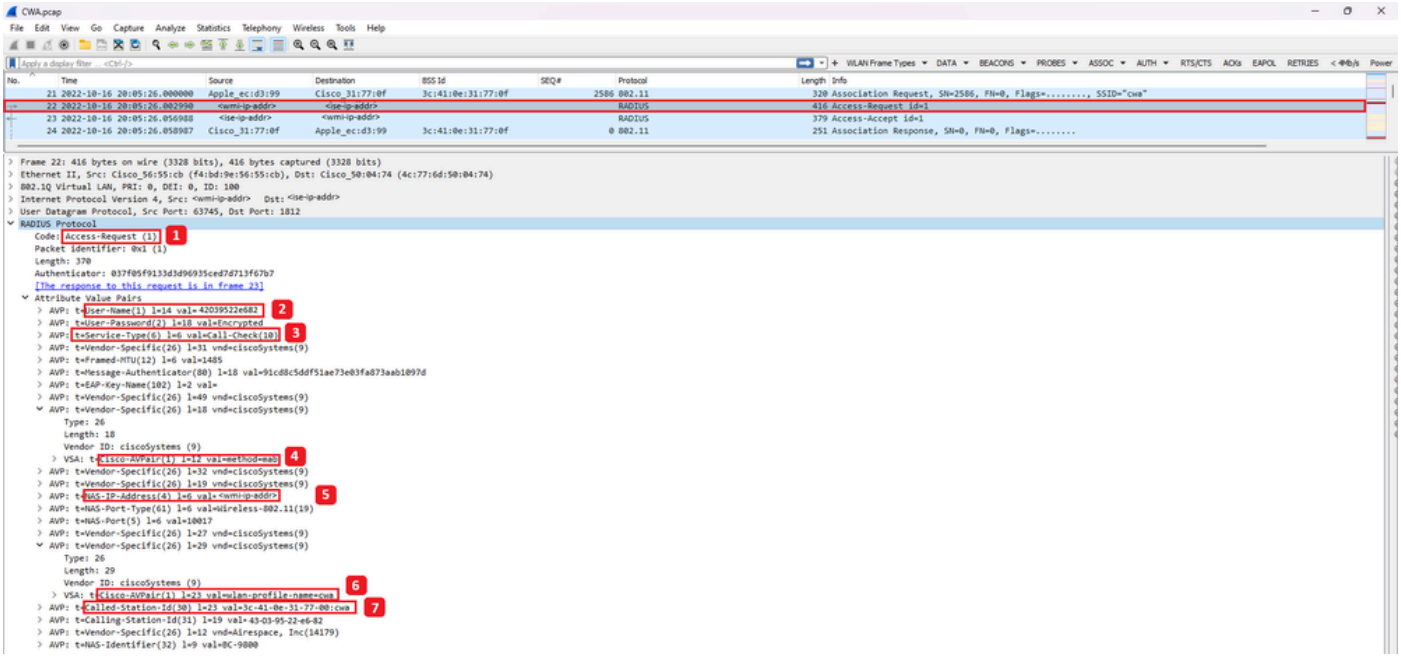
첫 번째 패킷 "Association Request(연결 요청)"를 보면 이 프로세스에 포함된 디바이스의 MAC 주소를 확인할 수 있습니다.



연결 요청

WLC에서 ISE로 전송된 액세스 요청 패킷

연결 요청이 WLC에 의해 처리되면 WLC는 ISE 서버에 Access-Request 패킷을 전송합니다.



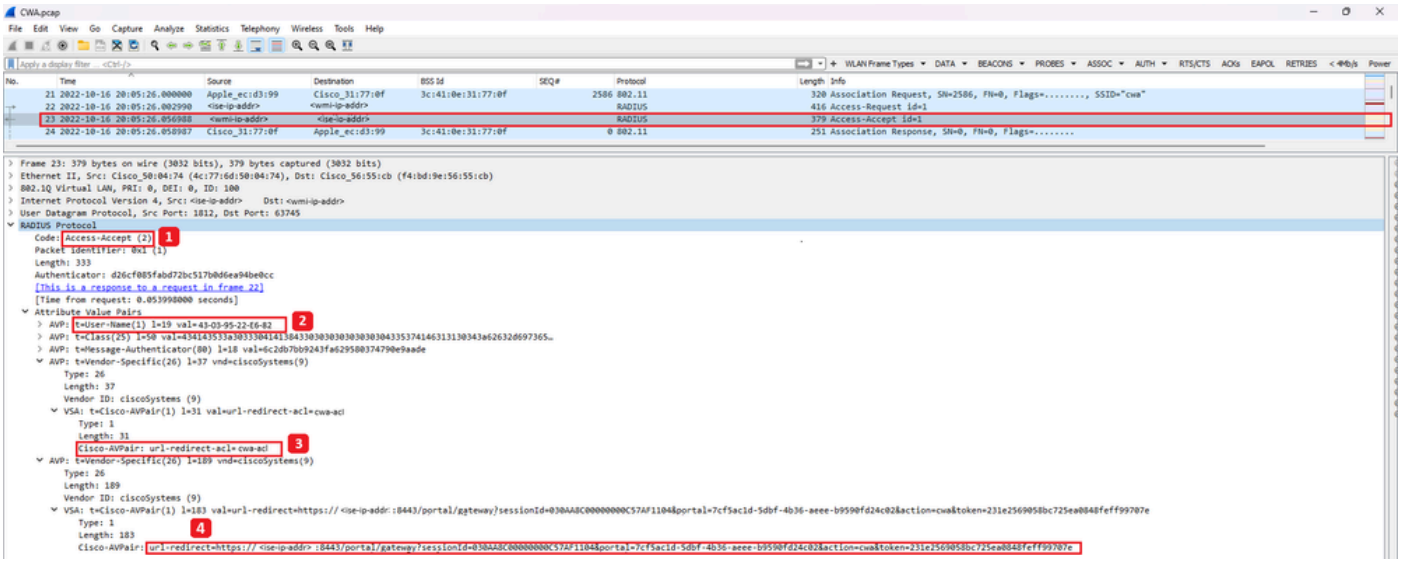
액세스 요청 패킷 분석

1. 패킷의 이름입니다.
2. 인증을 시도하는 MAC 주소.

3. 이는 MAC 필터링을 나타냅니다.
4. 컨트롤러가 MAC 필터링 프로세스를 나타내기 위해 ISE로 보낸 AV 쌍.
5. WLC의 WMI IP 주소입니다.
6. 클라이언트가 연결을 시도하는 SSID입니다.
7. 클라이언트가 연결하려는 WLAN의 이름입니다.

WLC에서 ISE로 전송된 액세스 수락 패킷

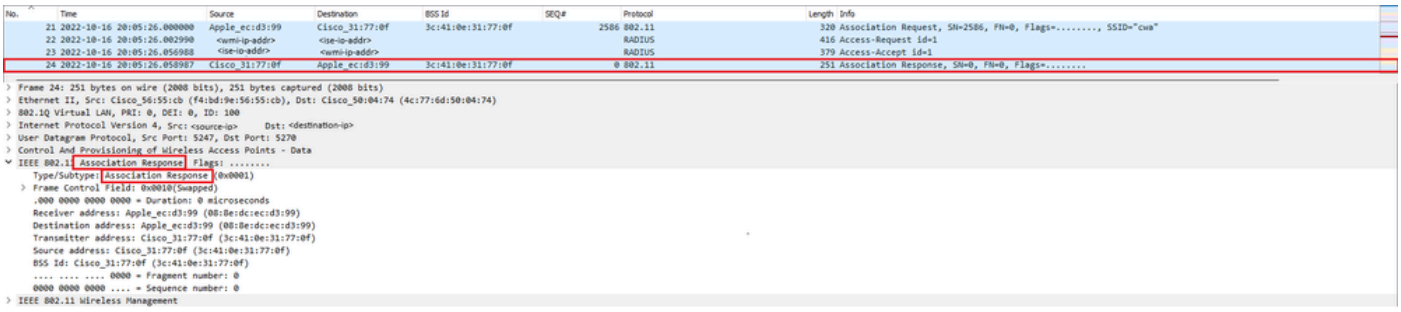
ISE가 Access-Accept 패킷을 처리하면 성공하면 Access-Accept로 응답하고, 성공하지 않으면 Access-Reject로 응답합니다.



Access-Accept 패킷 분석

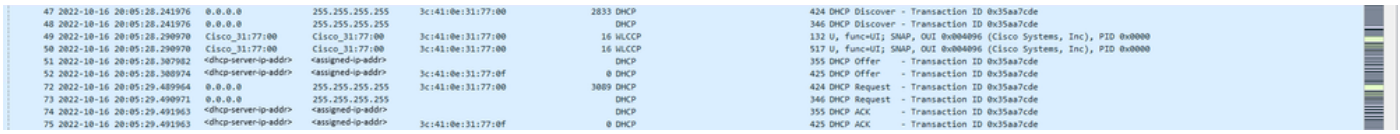
1. 패킷의 이름입니다.
2. 인증된 MAC 주소.
3. 적용할 ACL.
4. 사용자를 리디렉션할 URL입니다.

WLC에서 클라이언트로 연결 응답



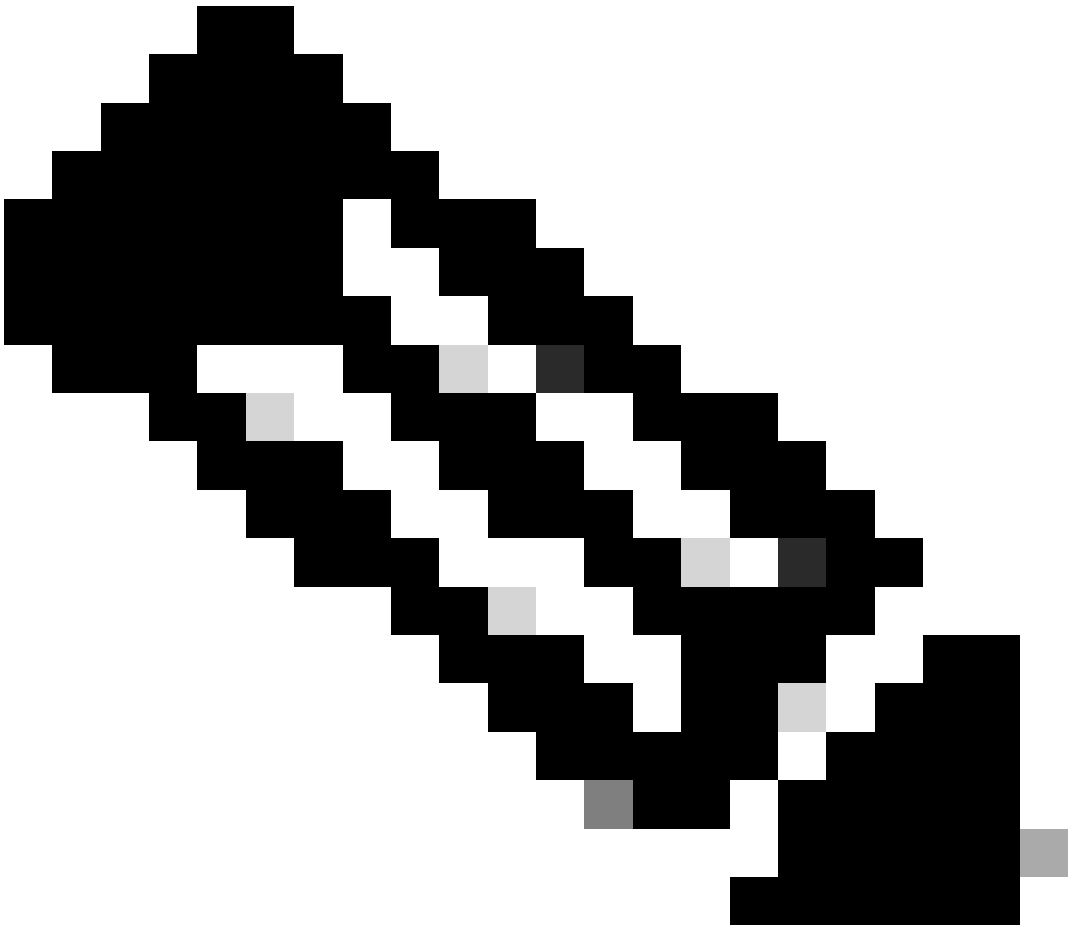
연결 응답

DHCP 프로세스



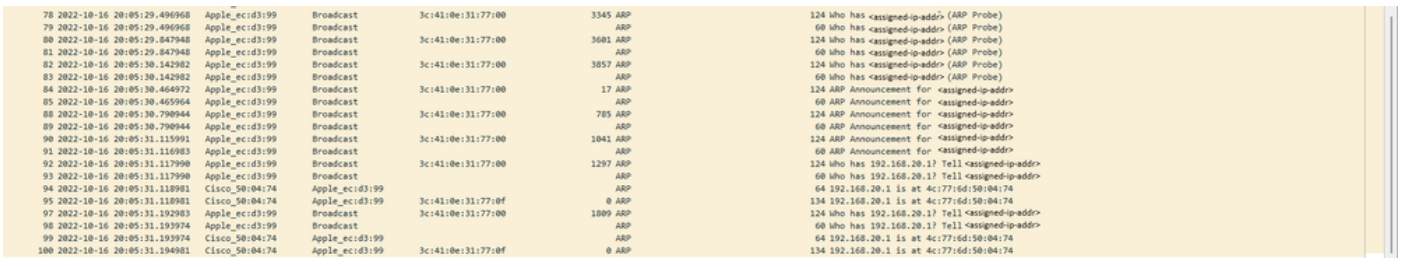
47	2022-10-16 20:05:28.241976	0.0.0.0	255.255.255.255	3c:41:0e:31:77:00	2833 DHCP	424 DHCP Discover - Transaction ID 0x35aa7cde
48	2022-10-16 20:05:28.241976	0.0.0.0	255.255.255.255		DHCP	346 DHCP Discover - Transaction ID 0x35aa7cde
49	2022-10-16 20:05:28.290970	Cisco_31:77:00	Cisco_31:77:00	3c:41:0e:31:77:00	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 프로세스



참고: 이제부터 패킷이 중복된 것으로 표시되지만, 이는 한 패킷은 CAPWAP로 캡슐화되고 다른 패킷은 캡슐화되지 않았기 때문입니다

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

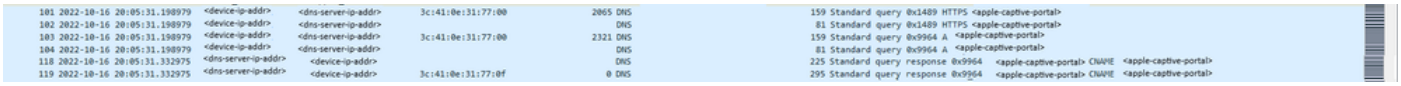
자체 IP 주소 및 게이트웨이에 대한 클라이언트 ARP

연결 테스트

ARP 프로세스가 완료되면 연결을 시도하는 디바이스는 포털이 트리거되었는지 확인하기 위해 검사를 수행합니다. 이를 프로빙이라고도 합니다. 디바이스가 인터넷 연결이 없다고 하면 ARP 프로세스가 실패했거나(예: 게이트웨이가 응답하지 않음) 디바이스가 프로빙을 수행할 수 없음을 의미합니다.

이 프로빙은 RA 추적에서는 보이지 않지만 EPC에서만 이 정보를 제공할 수 있습니다. 프로빙 쿼리는 연결을 시도하는 디바이스에 따라 다릅니다. 이 예에서 테스트 디바이스는 Apple 디바이스이므로 프로빙은 Apple의 종속 포털을 향해 직접 이루어졌습니다.

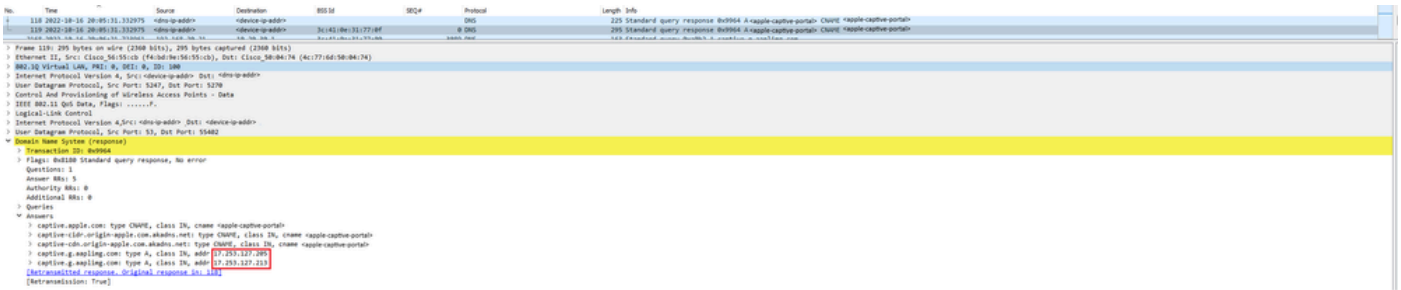
URL을 사용하여 프로빙을 수행하므로 이 URL을 해결하려면 DNS가 필요합니다. 따라서 DNS 서버가 클라이언트의 쿼리에 응답할 수 없는 경우, 클라이언트는 URL에 대한 쿼리를 계속 수행하며 포털이 표시되지 않습니다. 이때 ISE 서버의 IP 주소를 엔드 디바이스 웹 브라우저에 입력하면 포털이 표시되어야 합니다. 그렇다면 DNS 서버에 문제가 있는 것입니다.



클라이언트에서 연결 테스트 - DNS 쿼리 및 응답

DNS 확인 IP 주소

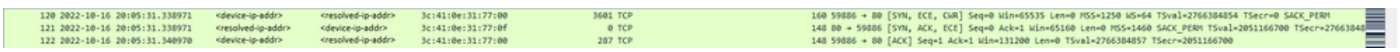
DNS 쿼리 응답을 검사하면 DNS 서버에서 확인된 IP 주소를 확인할 수 있습니다.



DNS 서버에서 확인된 IP 주소

3-Way 핸드셰이크 설정

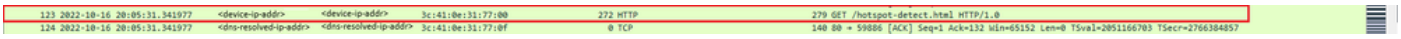
이제 DNS IP 주소가 확인되었으므로 포털과 클라이언트 간에 TCP 3-Way 핸드셰이크가 설정됩니다. 사용된 IP 주소는 확인된 IP 주소 중 하나입니다.



3-Way 핸드셰이크 설정

핫스팟 가져오기

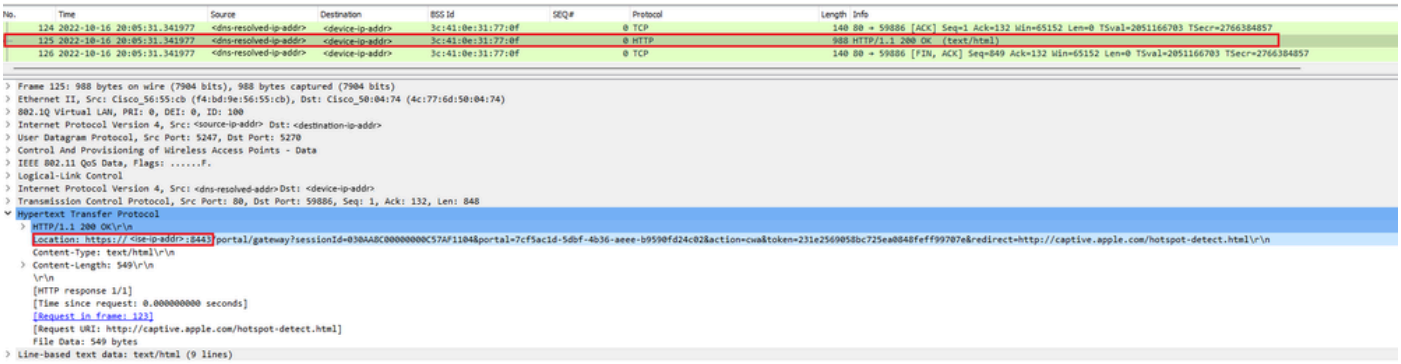
TCP 세션이 설정되면 클라이언트는 프로빙을 수행하고 포털에 액세스를 시도합니다.



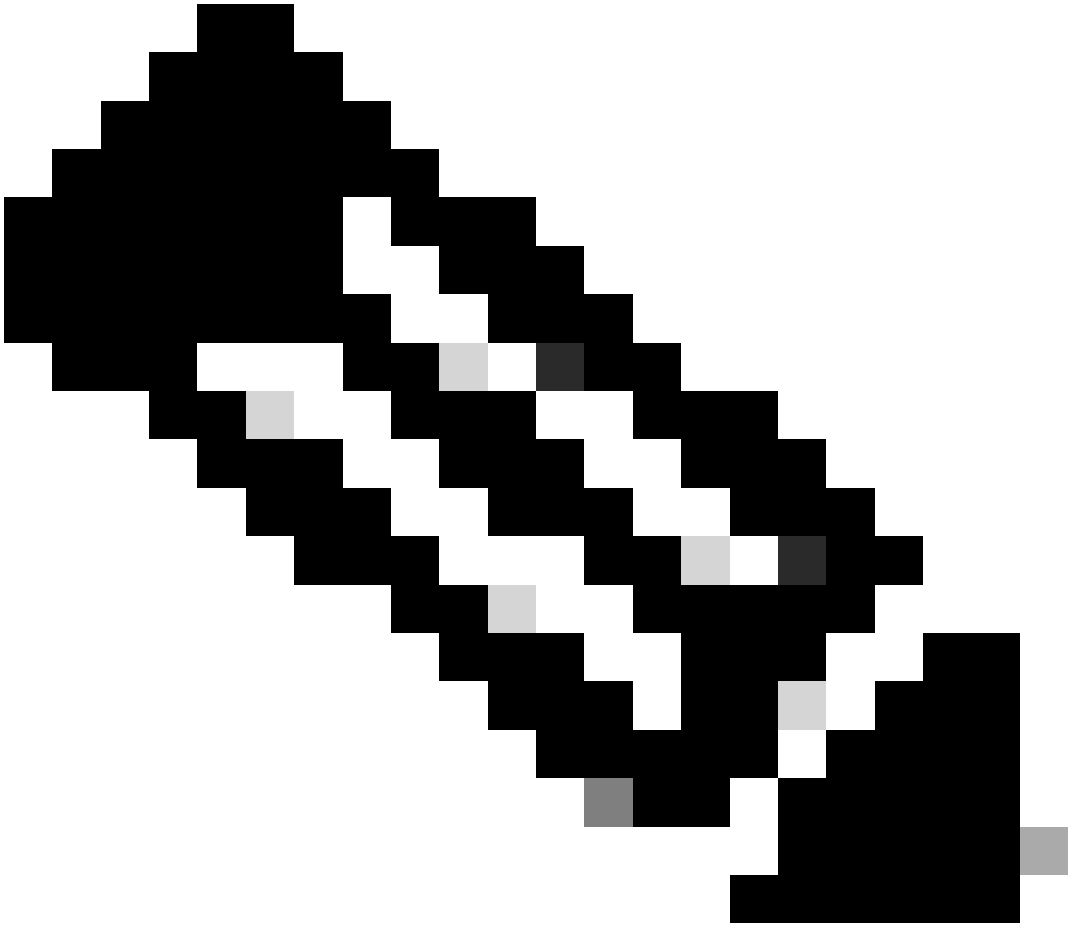
핫스팟 가져오기

OK 패킷

OK 패킷에는 클라이언트가 리디렉션되어야 하는 ISE의 포털이 포함됩니다.



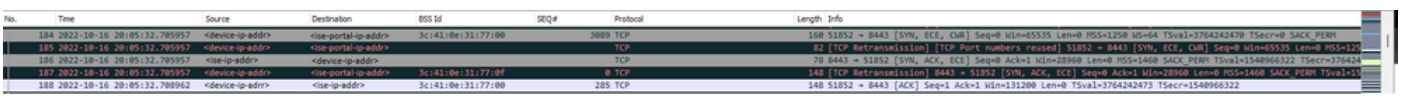
OK 패킷



참고: 대부분의 사용자는 OK 패킷에서 반환된 다른 URL을 가지고 있습니다. 따라서 최종 IP 주소를 얻기 위해 또 다른 DNS 쿼리를 만들어야 합니다.

새 TCP 세션이 설정됨

포털의 IP 주소가 검색되었으므로 많은 패킷이 교환되지만, 결국 ISE의 IP 주소에 해당하는 OK 패킷(또는 DNS로 확인됨)에서 반환된 목적지 IP가 있는 패킷은 포털에 설정되는 새 TCP 세션을 표시합니다.



ISE 포털에 대한 두 번째 연결 및 새 TCP 세션

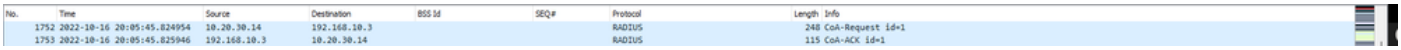
사용자에게 포털 표시

이 시점에서 ISE의 포털은 클라이언트 브라우저의 브라우저에 최종적으로 표시됩니다. 예전처럼

많은 패킷이 ISE와 디바이스 간에 교환됩니다. 클라이언트 hello, 서버 hello 등이 여기에 포함됩니다. 여기서 ISE는 클라이언트에 사용자 이름 및 비밀번호를 요청하고, ISE 서버에서 구성된 약관에 동의합니다.

CoA 요청/CoA 승인

사용자가 요청된 모든 데이터를 입력하면 ISE는 사용자의 권한 부여를 변경하기 위해 컨트롤러에 CoA 요청을 보냅니다. NAC 상태, CoA 지원 등과 같이 WLC의 모든 것이 예상대로 구성된 경우 WLC는 CoA 승인(CoA ACK)을 전송합니다. 그렇지 않으면, WLC는 CoA 비-승인 (CoA NACK) 을 전송할 수 있거나 단순히 CoA ACK 를 전송하지 않는다.

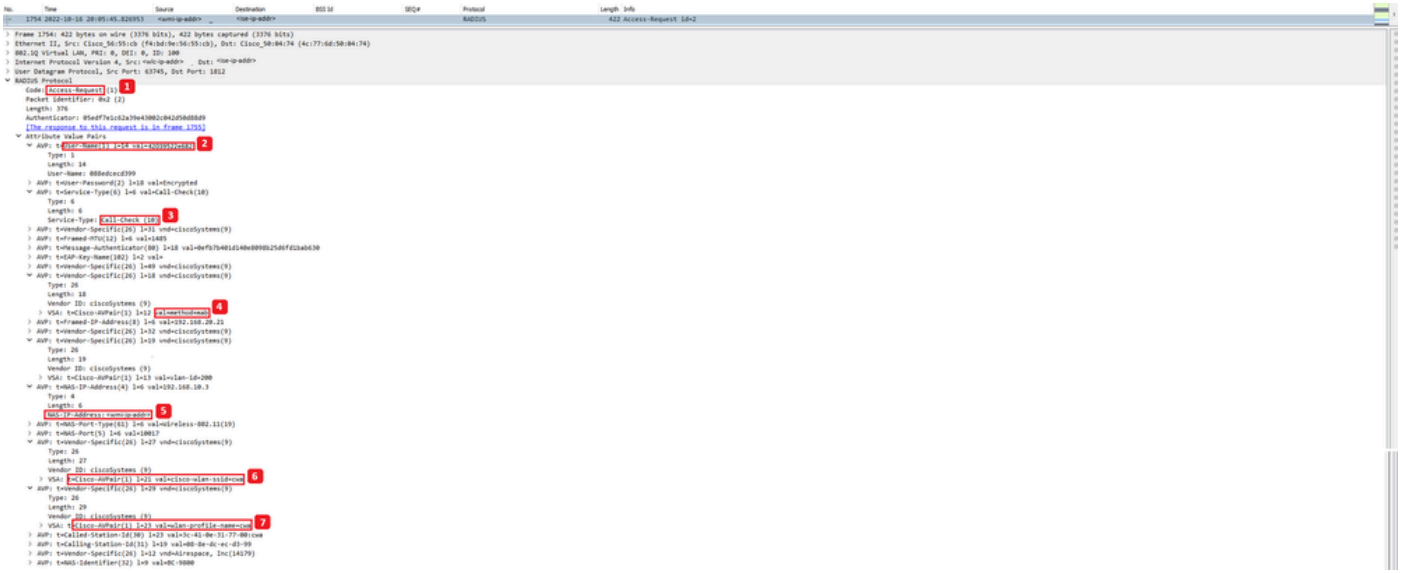


CoA 요청 및 승인

두 번째 연결: 클라이언트와 네트워크

새 액세스 요청

WLC는 새로운 액세스 요청 패킷을 ISE에 전송합니다.

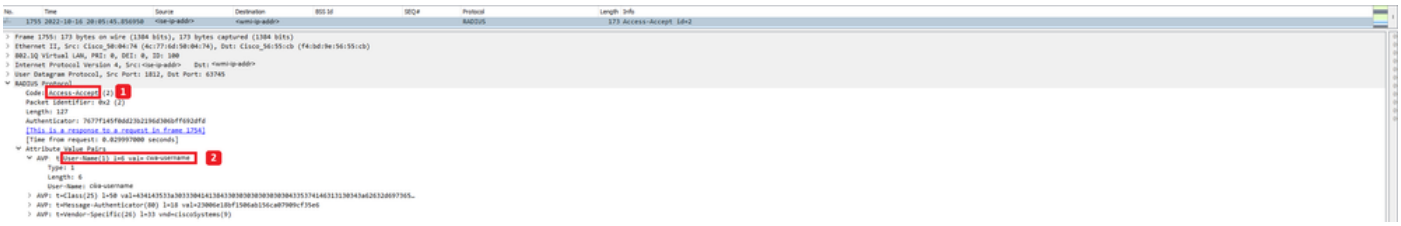


새 액세스 요청 패킷 분석

1. 패킷의 이름입니다.
2. 인증을 시도하는 MAC 주소.
3. 이는 MAC 필터링을 나타냅니다.
4. 컨트롤러가 MAC 필터링 프로세스를 나타내기 위해 ISE로 보낸 AV 쌍.
5. WLC의 WMI IP 주소입니다.
6. 클라이언트가 연결을 시도하는 SSID입니다.
7. 클라이언트가 연결하려는 WLAN의 이름입니다.

새 액세스 수락

WLC는 새로운 액세스 요청 패킷을 ISE에 전송합니다.



새 Access-Accept 패킷 분석

1. 패킷의 이름입니다.
2. 표시된 포털에서 최종 클라이언트가 입력한 사용자 이름.

다시 한 번, 클라이언트에서 새로운 프로빙 연결 테스트가 수행됩니다. 클라이언트가 인터넷 연결을 확인했으면 이제 포털을 닫을 수 있습니다(사용하는 장치에 따라 포털을 자동으로 닫을 수 있음). 이제 클라이언트가 네트워크에 연결됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.