CWA Flow op een client begrijpen

Inhoud

Inleiding

Dit document beschrijft de stroom voor de eindclient wanneer u verbinding maakt met een CWA WLAN.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van:

- Cisco draadloze LAN-controller (WLC) 9800 Series
- Algemeen begrip van Central Web Verification (CWA) en de configuratie ervan op Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

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

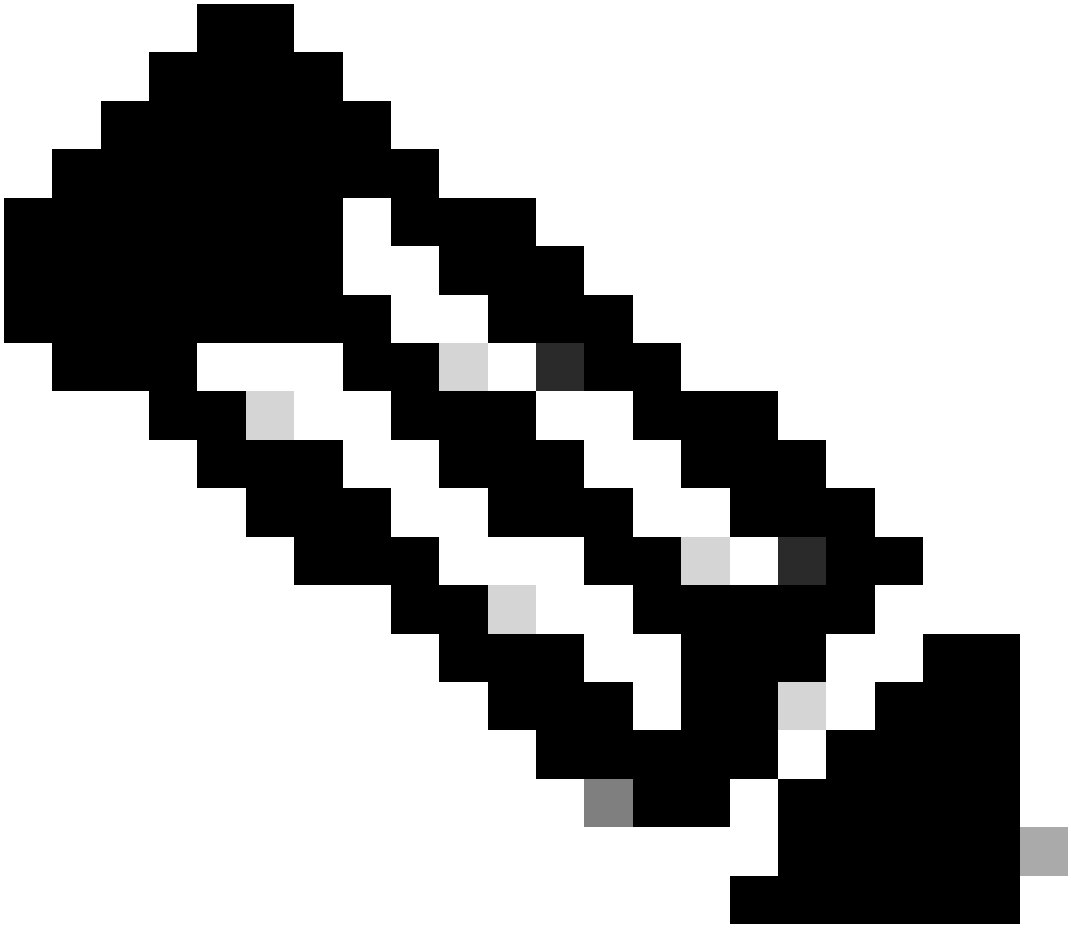
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

CWA is een type van SSID-verificatie dat kan worden geconfigureerd op de WLC waar de eindclient die probeert verbinding te maken wordt gevraagd om zijn gebruikersnaam en wachtwoord in te voeren naar een webportal dat aan hen wordt getoond. Kortom, de stroom voor de eindclient gaat door wanneer u verbinding maakt met het WLAN:

1. De eindclient maakt verbinding met de SSID die op het apparaat wordt weergegeven
2. De eindclient wordt omgeleid naar de webportal om de referenties in te voeren
3. De eindclient wordt geverifieerd door ISE met de ingevoerde referenties
4. ISE antwoordt op de WLC door te zeggen dat de eindclient is geverifieerd. ISE kan bepaalde aanvullende eigenschappen die de client moet naleven bij toegang tot het netwerk (zoals een specifieke ACL) indrukken
5. De eindclient wordt opnieuw gekoppeld en opnieuw geauthenticeerd en krijgt uiteindelijk toegang tot het netwerk

---



Opmerking: het is belangrijk om op te merken dat de eindclient die tweemaal wordt

---

geauthenticeerd transparant is voor de eindclient

Het onderliggende proces dat de client moet doorlopen, is in principe verdeeld in twee processen: een verbinding van de client naar de ISE-server en, eenmaal geverifieerd, een andere verbinding van de client naar het netwerk zelf. De controller en ISE communiceren altijd met elkaar via het RADIUS-protocol. Hieronder een diepgaande analyse van een radioactief (RA) spoor en een ingesloten pakketvastlegging (EPC).

CWA Flow - Radioactive (RA) Trace

Een RA-spoor is een verzameling logboeken die voor een specifieke client zijn opgenomen. Het toont het gehele proces dat de client doormaakt tijdens het verbinden met een WLAN. Ga voor meer informatie over wat ze zijn en hoe u RA-sporen kunt ophalen naar Understand Wireless Debugs and Log Collection op Catalyst 9800 draadloze LAN-controllers.

Eerste verbinding: client naar ISE-server

De WLC staat geen verbinding met het netwerk toe als de client nog niet eerder door ISE is geautoriseerd.

Associatie met het WLAN

De WLC detecteert de client wil associëren met de WLAN "cwa", die ons koppelt aan het beleidsprofiel "cwa-policy-profile" en verbindt met AP "BC-3802"

<#root>

```
[client-orch-sm] [17558]: (note): MAC: 4203.9522.e682
Association received.
 BSSID dc8c.37d0.83af,
WLAN cwa
, Slot 1 AP dc8c.37d0.83a0, BC-3802
[client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Received Dot11 association request. Processing s
SSID: cwa
,
Policy profile: cwa-policy-profile
,
AP Name: BC-3802
, Ap Mac Address: dc8c.37d0.83a0 BSSID MAC0000.0000.0000 wlan ID: 1RSSI: -46, SNR: 40
[client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition:
 S_CO_INIT -> S_CO_ASSOCIATING
```

```
[dot11-validate] [17558]: (info): MAC: 4203.9522.e682 WiFi direct: Dot11 validate P2P IE. P2P IE not pr
```

MAC-filtering

Connectiviteit met Test ISE-servers

Zodra de WLC het associatieverzoek van de client heeft ontvangen, is de eerste stap om MAC-filtering (ook bekend als MAB) uit te voeren. MAC-filtering is een beveiligingsmethode waarbij het MAC-adres van de client wordt gecontroleerd aan de hand van een database die moet worden gevalideerd als ze al dan niet bij het netwerk mogen worden aangesloten.

<#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
```

WLC verzendt aanvraag naar ISE

De WLC stuurt een RADIUS access-request pakket naar ISE met daarin het MAC-adres van de client die wil verifiëren naar het WLAN.

<#root>

```
[radius] [17558]: (info): RADIUS: Send
```

Access-Request

```
 to
```

<ise-ip-addr>:1812

```
 id 0/
```

28

```
, len 415
```

<-- The packet is traveling via RADIUS port 1812. The "28" is the session ID and it is unique for every

```
[radius] [17558]: (info): RADIUS: authenticator e7 85 1b 08 31 58 ee 91 - 17 46 82 79 7d 3b c4 30
[radius] [17558]: (info): RADIUS: User-Name            [1]     14 "
```

42039522e682

```
"
```

<-- MAC address that is attempting to authenticate

```
[radius] [17558]: (info): RADIUS: User-Password        [2]     18 *
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     25 "
```

service-type=Call Check

```
"
```

<-- This indicates a MAC filtering process

```
[radius] [17558]: (info): RADIUS: Framed-MTU           [12]    6  1485
[radius] [17558]: (info): RADIUS: Message-Authenticator[80]    18 ...
[radius] [17558]: (info): RADIUS: EAP-Key-Name         [102]   2  *
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     43 "audit-session-id=0E1E140A0000000C8E2
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     12 "
```

method=mab

```
"
```

<-- Controller sends an AVpair with MAB method

```
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     26 "client-iif-id=1392509681"
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     14 "vlan-id=1000"
```

```
[radius] [17558]: (info): RADIUS: NAS-IP-Address       [4]     6
```

<wmi-ip-addr> <-- WLC WMI IP address

```
[radius] [17558]: (info): RADIUS: NAS-Port-Id          [87]    17 "capwap_90000005"
[radius] [17558]: (info): RADIUS: NAS-Port-Type        [61]    6  802.11 wireless [19]
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     30 "
```

cisco-wlan-ssid=cwa

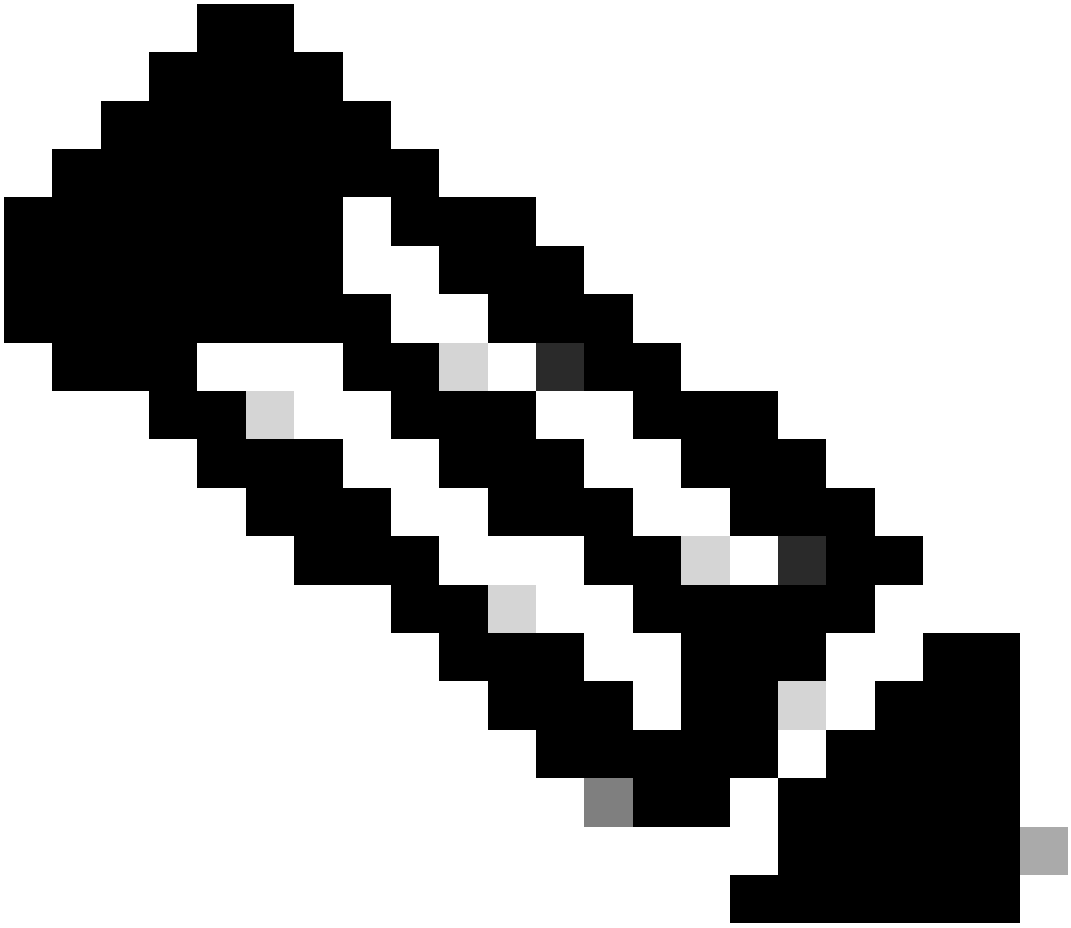
```
"
```

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

```
[radius] [17558]: (info): RADIUS: Cisco AVpair         [1]     32 "
```

wlan-profile-name=cwa

```
"
[radius] [17558]: (info): RADIUS: Called-Station-Id    [30]    32 "dc-8c-37-d0-83-a0:cwa"
[radius] [17558]: (info): RADIUS: Calling-Station-Id   [31]    19 "42-03-95-22-e6-82"
[radius] [17558]: (info): RADIUS: Airespace-WLAN-ID    [1]     6  1
[radius] [17558]: (info): RADIUS: Nas-Identifier       [32]    9  "BC-9800"
[radius] [17558]: (info): RADIUS: Started 5 sec timeout
```



Opmerking: een AV-paar is "Attribute-Value", gebruikt door ISE. Het is een Key-Value structuur van vooraf gedefinieerde informatie die naar de WLC kan worden verzonden. Deze waarden worden toegepast op die specifieke client voor die specifieke sessie.

Voorbeelden van AV-paren:

- ACL-naam
- URL omleiden
- VLAN-toewijzing
- Time-outtimers voor sessies
- Opnieuw verificatietimers

ISE-antwoorden op het WLC-verzoek

Als het MAC-adres dat door de WLC wordt verzonden, door ISE wordt geaccepteerd, wordt er een Access-Accept RADIUS-pakket verzonden. Afhankelijk van de ISE-configuratie, als het een onbekend MAC-adres is, moet ISE het accepteren en doorgaan met de stroom. Als u een Access-

Reject ziet, dan is er iets niet correct geconfigureerd op ISE dat moet worden geverifieerd.

<#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

WLC-informatieprocessen die van ISE worden ontvangen

De WLC verwerkt alle informatie die van ISE is ontvangen. Hiermee past het het gebruikersprofiel toe dat het oorspronkelijk had gemaakt met dat van de door ISE verzonden gegevens. De WLC wijst bijvoorbeeld een nieuwe ACL toe aan de gebruiker. Als AAA Override niet is ingeschakeld op het WLAN, komt deze verwerking door WLC niet voor.

<#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-verificatie voltooid

Nadat het gebruikersprofiel voor de client met succes is gewijzigd, is de WLC klaar met het verifiëren van het MAC-adres van de client. Als de van ISE ontvangen ACL niet bestaat op de WLC, weet de WLC niet wat te doen met die informatie, en daarom faalt de REPLACE actie volledig waardoor de MAB-verificatie faalt. De client kan niet worden geverifieerd.

<#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 stuurt reactie van associatie naar client

Nu de client is geverifieerd door ISE en de juiste ACL is toegepast, stuurt de WLC eindelijk een associatiereactie naar de client. De gebruiker kan nu verbinding met het netwerk blijven maken.

<#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-verificatie

Zoals in het proces moet een client ondergaan wanneer deze wordt gekoppeld aan een WLAN, L2-verificatie "start". In werkelijkheid is L2-authenticatie echter al uitgevoerd door MAB-authenticatie die eerder is uitgevoerd. De client voltooit onmiddellijk de L2-verificatie.

<#root>

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682
```

Starting L2 authentication

```
. Bssid in state machine:dc8c.37d0.83af Bssid in request is:dc8c.37d0.83af
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682 L2 WEBAUTH Authentication Successf
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi
```

S_AUTHIF_L2_WEBAUTH_DONE

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682
```

L2 Authentication of station is successful

., L3 Authentication : 1

Data Plumb

WLC wijst resources toe aan de verbindende client zodat verkeer door het netwerk kan stromen.

<#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
```

De gebruiker heeft een IP-adres toegewezen

De eindgebruiker heeft een IP-adres nodig om door het netwerk te kunnen navigeren. Het ondergaat het DHCP-proces. Als de gebruiker eerder verbonden was en het zijn IP-adres onthoudt, wordt het DHCP-proces overgeslagen. Als de gebruiker geen IP-adres kan ontvangen,

kan de eindgebruiker het webportaal niet bekijken. Anders gaat het door de volgende stappen:

1. Een ONTDEK pakket wordt verzonden van de verbindende cliënt als uitzending om het even welke beschikbare servers van DHCP te vinden
2. Als er een DHCP-server beschikbaar is, reageert de DHCP-server met een OFFER. De aanbieding bevat informatie zoals het IP-adres dat moet worden toegewezen aan de verbindende client, leasetijd, enzovoort. Er kunnen veel OFFERs van verschillende DHCP servers worden ontvangen
3. De client accepteert een AANBOD van een van de servers en reageert met een VERZOEK om het geselecteerde IP-adres
4. Tot slot verzendt de DHCP-server een BEVESTIGingspakket naar de client waaraan het nieuwe IP-adres is toegewezen

De WLC logt de methode in die de client heeft ontvangen.

<#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-verificatie start

Nu de eindgebruiker een IP-adres heeft ontvangen, begint de L3-verificatie met CWA gedetecteerd als de gewenste methode voor verificatie.

<#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-adressen voor tests

Om met de verbinding vooruit te gaan moet de cliënt twee ARP verzoeken uitvoeren:

1. Controleer dat niemand anders zijn IP-adres heeft. Als er een ARP-antwoord is voor het IP-adres van de eindgebruiker, wordt dit gedupliceerd IP-adres

2. Bevestig bereikbaarheid aan de gateway. Dit om ervoor te zorgen dat de client het netwerk kan verlaten. Het ARP antwoord moet van de gateway zijn

<#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,

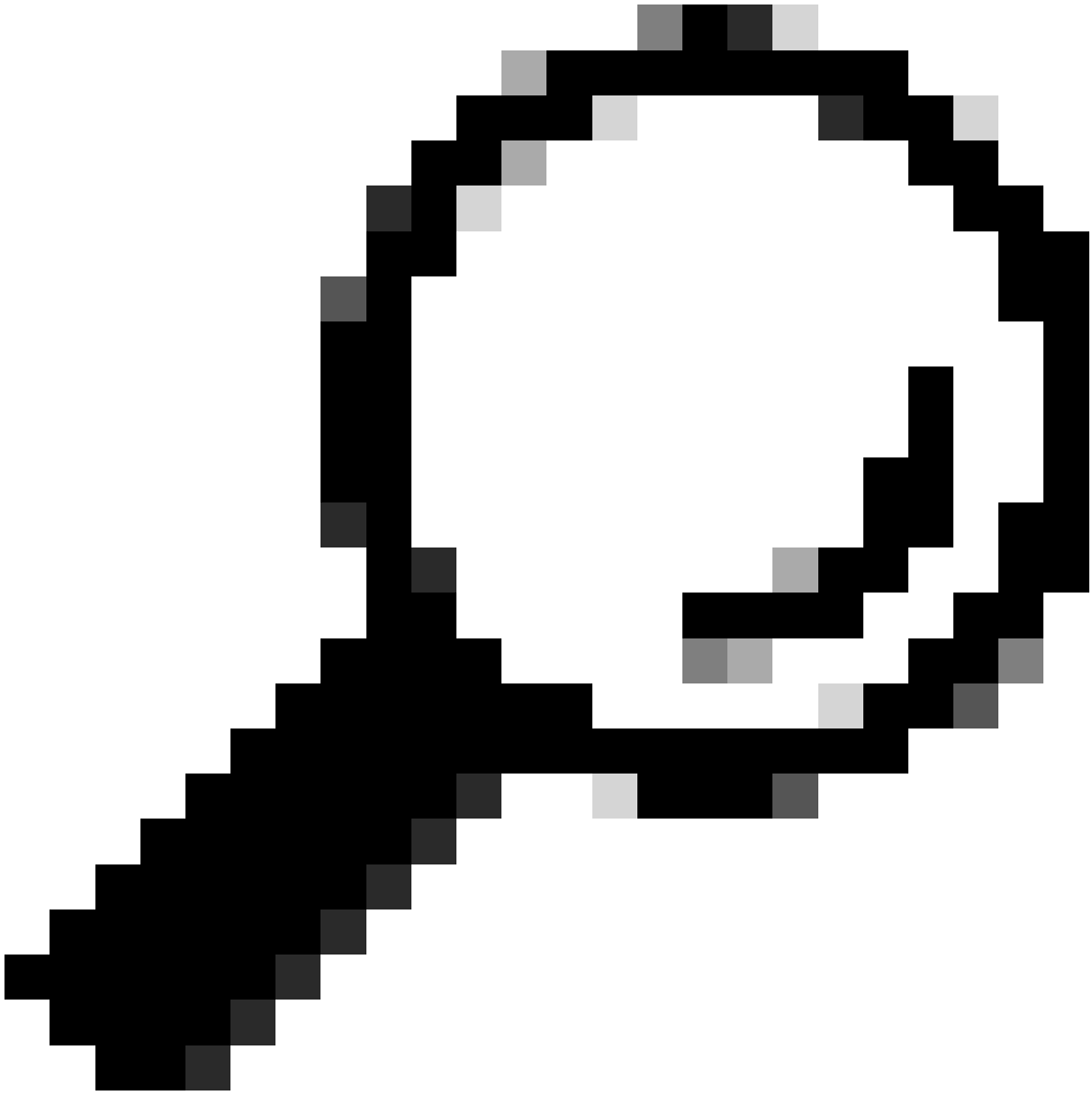
```
 ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t
```

Tweede verbinding: client naar netwerk

Op dit punt is de eindgebruiker nu geauthenticeerd tegen ISE via zijn MAC-adres, maar het is nog niet volledig geautoriseerd. De WLC moet nog eens naar ISE verwijzen om de client toestemming te geven om verbinding te maken met het netwerk. Op dit punt wordt de portal getoond aan de gebruiker waarin de gebruikersnaam zijn gebruikersnaam en wachtwoord moet invoeren. Op de WLC wordt de eindgebruiker gezien in de staat "Web Auth Pending".

Wijziging van de vergunning

Hier wordt "Support for CoA" in de WLC-configuratie van kracht. Tot dit punt werd de ACL gebruikt. Nadat de eindclient het portaal ziet, wordt de ACL niet meer gebruikt, aangezien het enige dat het deed was de client omleiden naar het portaal. Op dit punt voert de client zijn aanmeldingsgegevens in om het CoA-proces te starten en de client opnieuw te verifiëren. De WLC bereidt het pakket voor dat verzonden en doorgestuurd wordt naar ISE



Tip: CoA gebruikt poort 1700. Zorg ervoor dat deze niet wordt geblokkeerd door de firewall.

<#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

Tweede verificatie naar ISE

De tweede verificatie start niet vanaf nul. Dit is de kracht van CoA. Nieuwe regels en/of AV paris kunnen op de gebruiker worden toegepast. De ACL en de omleiding URL die op de eerste Access-Accept ontvangen worden niet meer naar de eindgebruiker gedrukt.

WLC verzendt aanvraag naar ISE

De WLC verzendt een nieuw RADIUSaccess-request naar ISE met de ingevoerde gebruikersnaam/wachtwoordcombinatie. Hierdoor wordt een nieuwe MAB-verificatie geactiveerd en omdat ISE de client al kent, wordt een nieuwe beleidsset toegepast (bijvoorbeeld 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
```

ISE-antwoorden op het WLC-verzoek

ISE voert een raadpleging uit van haar beleid en als de gebruikersnaam die is ontvangen overeenkomt met het beleidsprofiel, dan reageert ISE nogmaals op de WLC, waarbij de clientverbinding met het WLAN wordt geaccepteerd. Het geeft de gebruikersnaam van de eindgebruiker terug. Indien geconfigureerd op ISE, kunnen extra regels en/of AV-paren worden toegepast op de gebruiker en ze worden gezien op Access-Accept.

<#root>

{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Received from id

1812/29

<ise-ip-addr>

:0,

Access-Accept

, len 131

<-- The packet is traveling via RADIUS port 1812 and is has a session ID of 29 (as a response to the abo

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: authenticator a3 b0 45 d6 e5 1e 38 4a - be 15 fa 6b
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS:
```

User-Name

[1] 14 "

cwa-username

"

<-- Username entered by the end client on the portal that was shown

```
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Class                [25] 51 ...
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17558]: (info): RADIUS: Cisco AVpair [1] 22 "profile-name=Unknown"
{wncd_x_R0-0}{1}: [radius] [17558]: (info): Valid Response Packet, Free the identifier
{wncd_x_R0-0}{1}: [eap-auth] [17558]: (info): SUCCESS for EAP method name: Identity on handle 0xEE00003
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005]
```

MAB received an Access-Accept

for 0x8A000002
{wncd_x_R0-0}{1}: [mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '

MAB_RESULT

' on handle 0x8A000002
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Authc success from

MAB, Auth event success

WLC-informatieprocessen die van ISE worden ontvangen

Opnieuw verwerkt de WLC de door ISE ontvangen informatie. Het voert een andere REPLACE actie op de gebruiker met de nieuwe die waarden uit van ISE worden ontvangen.

<#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-verificatie voltooid

De eindgebruiker is nu geverifieerd met de opgegeven gegevens. L3-verificatie (webverificatie) is voltooid.

<#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 4
{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

Eindgebruiker bereikt Run-status op de WLC

Tot slot wordt de gebruiker geverifieerd en gekoppeld aan het WLAN.

<#root>

{wncd_x_R0-0}{1}: [rog-proxy-capwap] [17558]: (debug):

Managed client RUN state

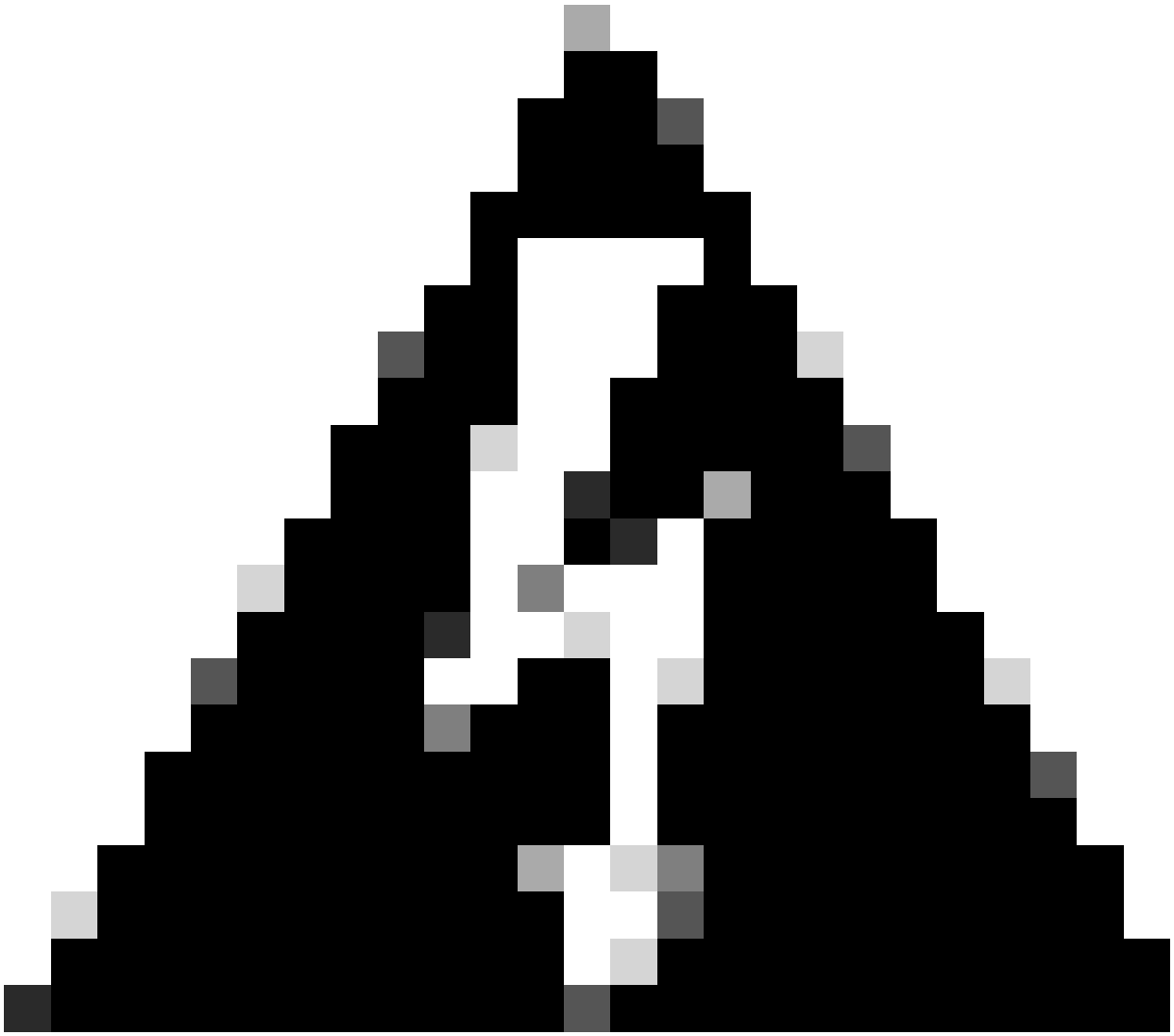
```
 notification: 4203.9522.e682
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

S_CO_RUN

CWA Flow - ingesloten pakketvastlegging (EPC)

Een EPC is een pakketopname die direct uit de WLC kan worden gehaald en die alle pakketten toont die of door de WLC passeren of van de WLC afkomstig zijn. Ga voor meer informatie over wat ze zijn en hoe u ze kunt ophalen naar Understand Wireless Debugs and Log Collection op Catalyst 9800 draadloze LAN-controllers.

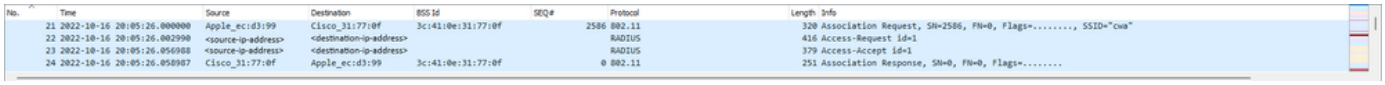
Eerste verbinding: client naar ISE-server



Waarschuwing: de IP-adressen in de afbeeldingen van de pakketopname zijn verwijderd. Ze worden weergegeven als en

---

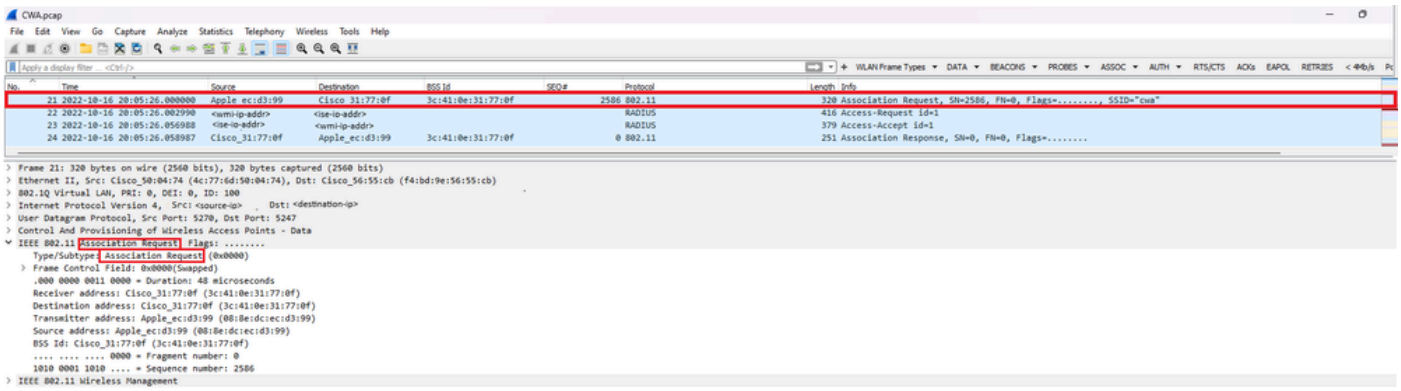
Associatie naar WLAN en verzoek verzonden naar ISE-server



Eerste pakketten

Associatieverzoek Van WLC naar client

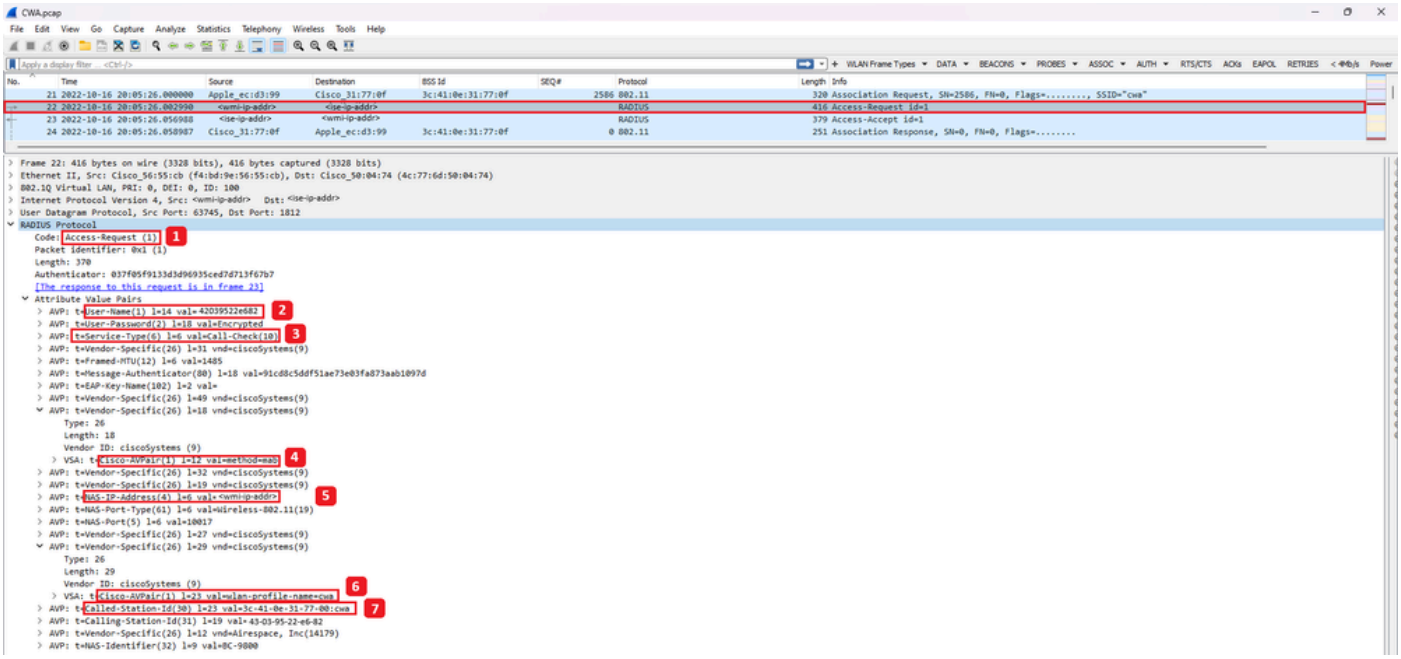
Kijkend naar het eerste pakket "Associatieverzoek" kunt u de MAC-adressen zien van de apparaten die bij dit proces betrokken zijn.



Associatieaanvraag

Packet voor toegangsaanvragen dat van WLC naar ISE wordt verzonden

Zodra het associatieverzoek door WLC is verwerkt, verzendt WLC een access-request pakket naar de ISE-server.



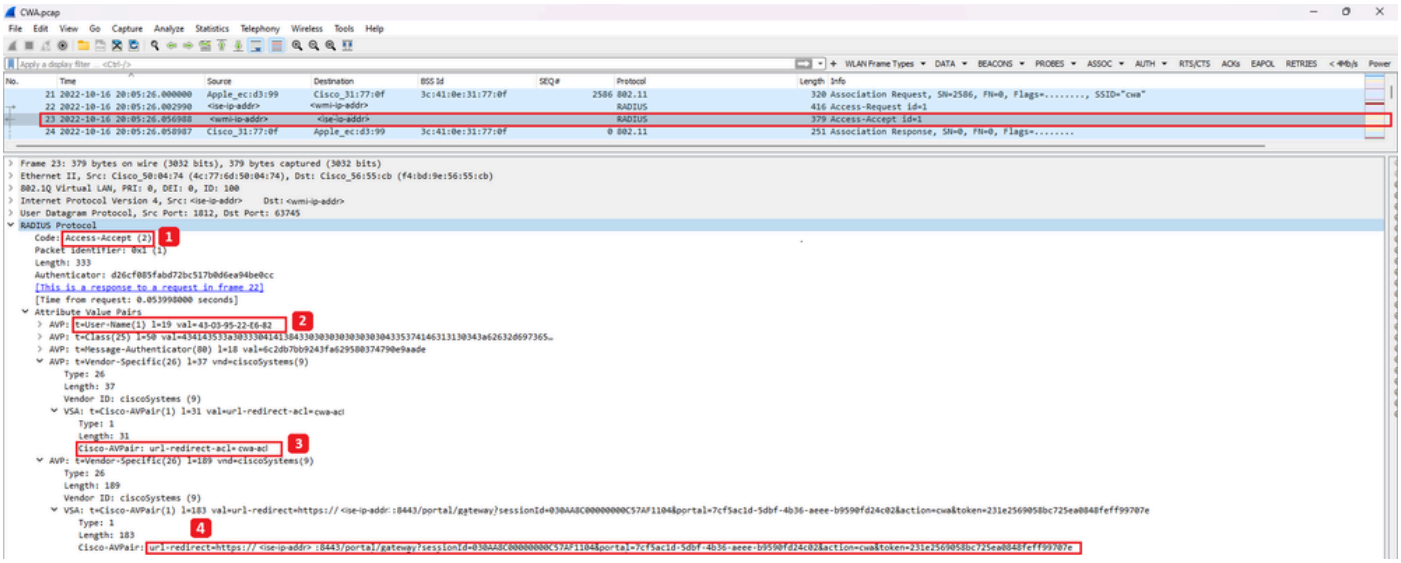
Analyse van access-request

1. Naam van het pakket.

2. Het MAC-adres dat probeert te verifiëren.
3. Dit geeft een MAC-filtering aan.
4. Het AV-paar dat door de controller naar ISE wordt gestuurd om een MAC-filterproces aan te geven.
5. Het WMI IP-adres van de WLC.
6. De SSID die de client probeert te verbinden.
7. De naam van het WLAN dat de client probeert te verbinden.

Access-Accept-pakket verzonden van WLC naar ISE

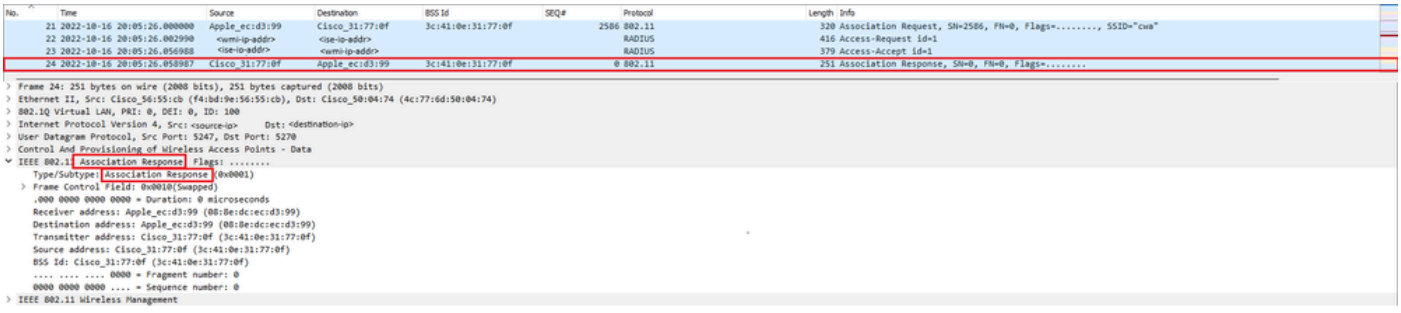
Zodra ISE het access-acceptatiepakket heeft verwerkt, reageert het met een Access-Accept indien geslaagd of met een Access-Reject indien niet.



Analyse van access-acceptatiepakket

1. Naam van het pakket.
2. Het MAC-adres wordt geverifieerd.
3. Toegepaste ACL.
4. De URL om de gebruiker naar te verwijzen.

Reactie van de vereniging van WLC op de client

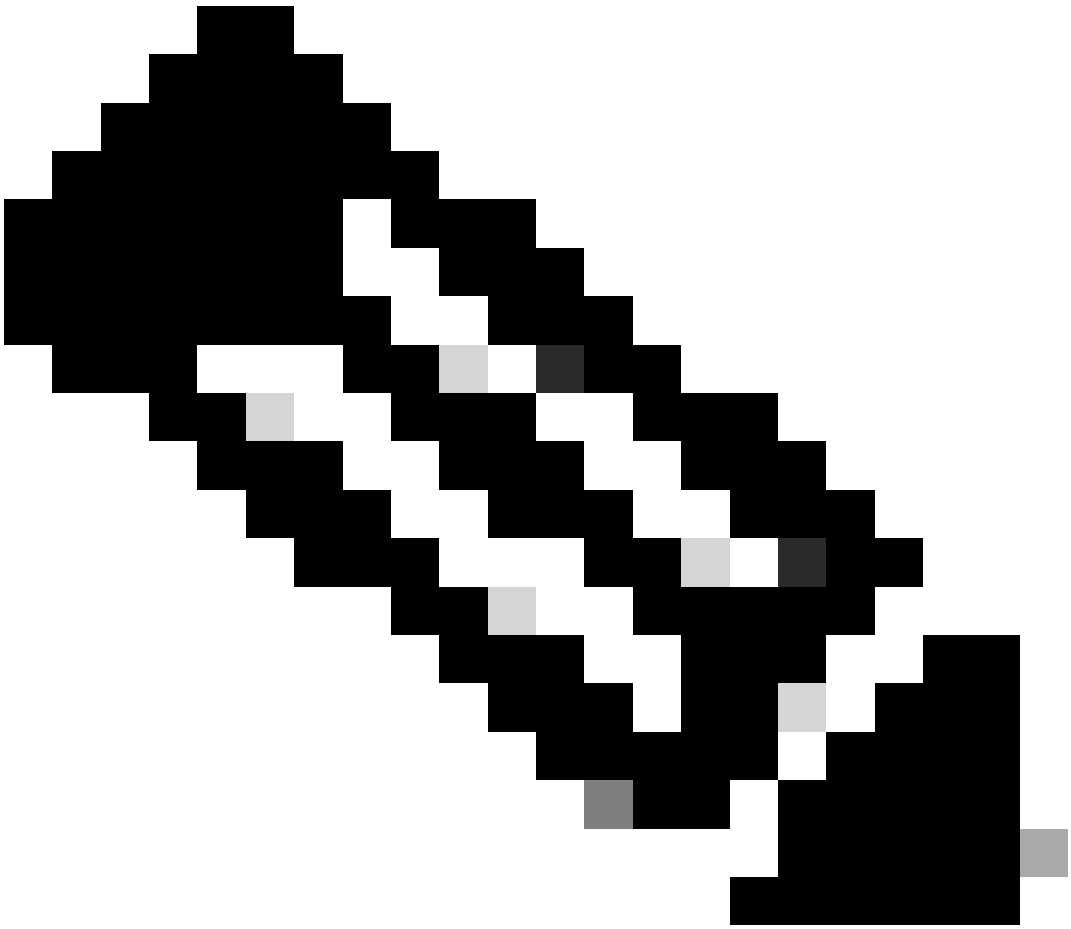


Reactie op associatie

DHCP-proces

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-proces



Opmerking: vanaf nu worden pakketten in twee keer bekeken, maar dat is alleen omdat de ene capwap ingekapseld is en de andere niet

---

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

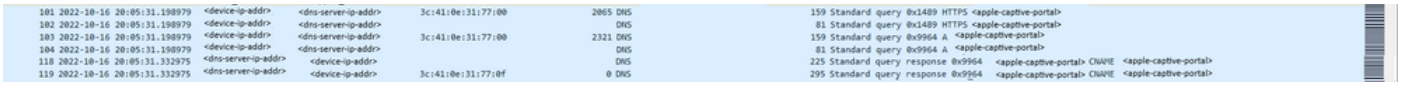
Client ARPing voor zijn eigen IP-adres en voor de gateway

Connectiviteitstest

Als het ARP-proces is voltooid, voert het apparaat dat probeert verbinding te maken een controle uit om te bevestigen of een portal is geactiveerd, dit wordt ook wel saai genoemd. Als het apparaat zegt dat er geen internetverbinding is, betekent dit dat het ARP-proces is mislukt (bijvoorbeeld, de gateway heeft nooit geantwoord) of dat het apparaat de controle niet kon uitvoeren.

Deze controle is iets wat niet te zien is op de RA-sporen, alleen de EPC is in staat deze informatie te verstrekken. De sonderende vraag hangt af van het apparaat dat een verbinding probeert, in dit voorbeeld was het testapparaat een Apple-apparaat, dus de sondering werd direct gemaakt naar de captive portal van Apple.

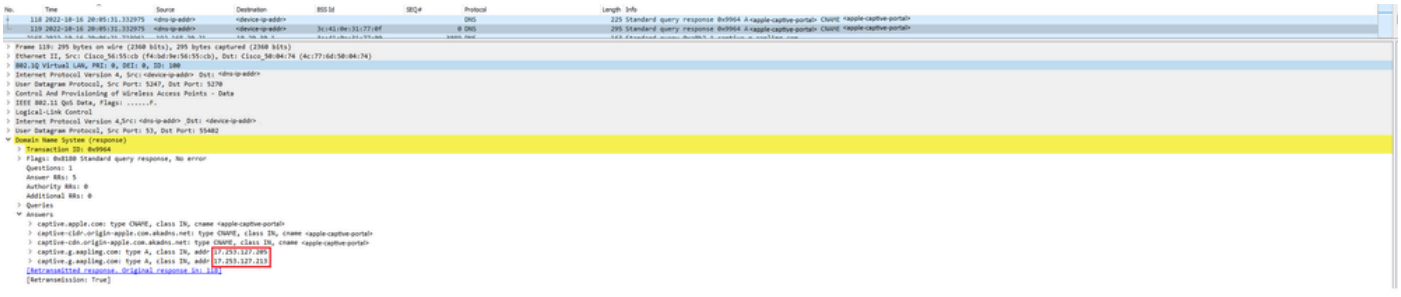
Aangezien de sondering wordt gemaakt met behulp van een URL, is DNS vereist om deze URL op te lossen. Daarom als de DNS server niet in staat is om te reageren op de vragen van de client, dan blijft de client vragen voor de URL en het portaal wordt nooit gezien. Als op dit punt het IP-adres van de ISE-server in de webbrowser van het eindapparaat is ingevoerd, moet het portaal zichtbaar zijn. Als dat zo is, dan is er een probleem met de DNS server.



Connectiviteitstest vanaf client - DNS-query en antwoord

DNS-opgelost IP-adres

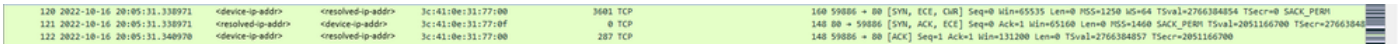
Tijdens het inspecteren van de DNS-query respons, kunt u het IP-adres zien dat werd opgelost door de DNS-server.



IP-adres opgelost door DNS-server

3-voudige handdruk instellen

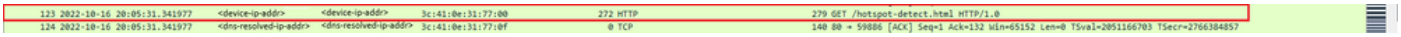
Nu het DNS IP-adres is opgelost, is er een TCP 3-weg handshake ingesteld tussen de portal en de client. Het IP-adres dat wordt gebruikt, is een van de IP-adressen die zijn opgelost.



3-weg handdruk inrichting

GET hotspot

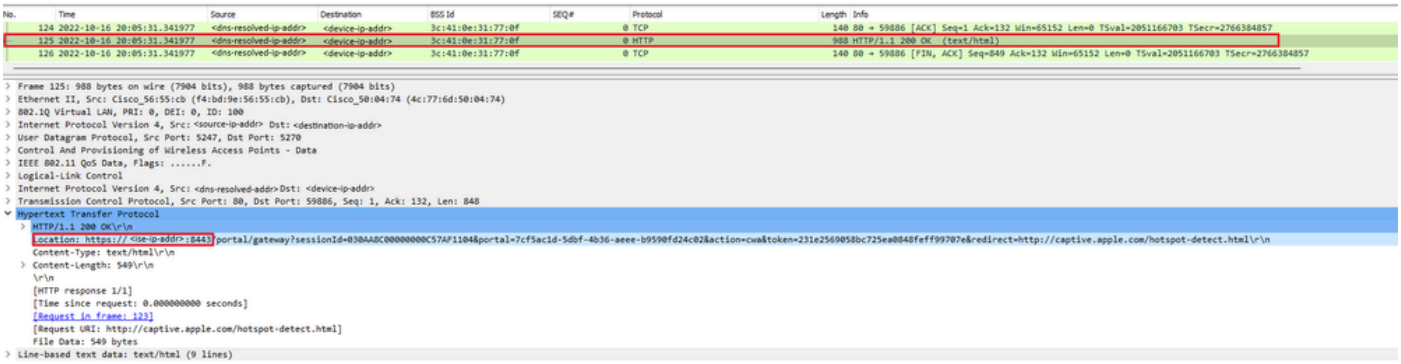
Zodra de TCP sessie is ingesteld, doet de client een sondering en probeert toegang te krijgen tot het portal.



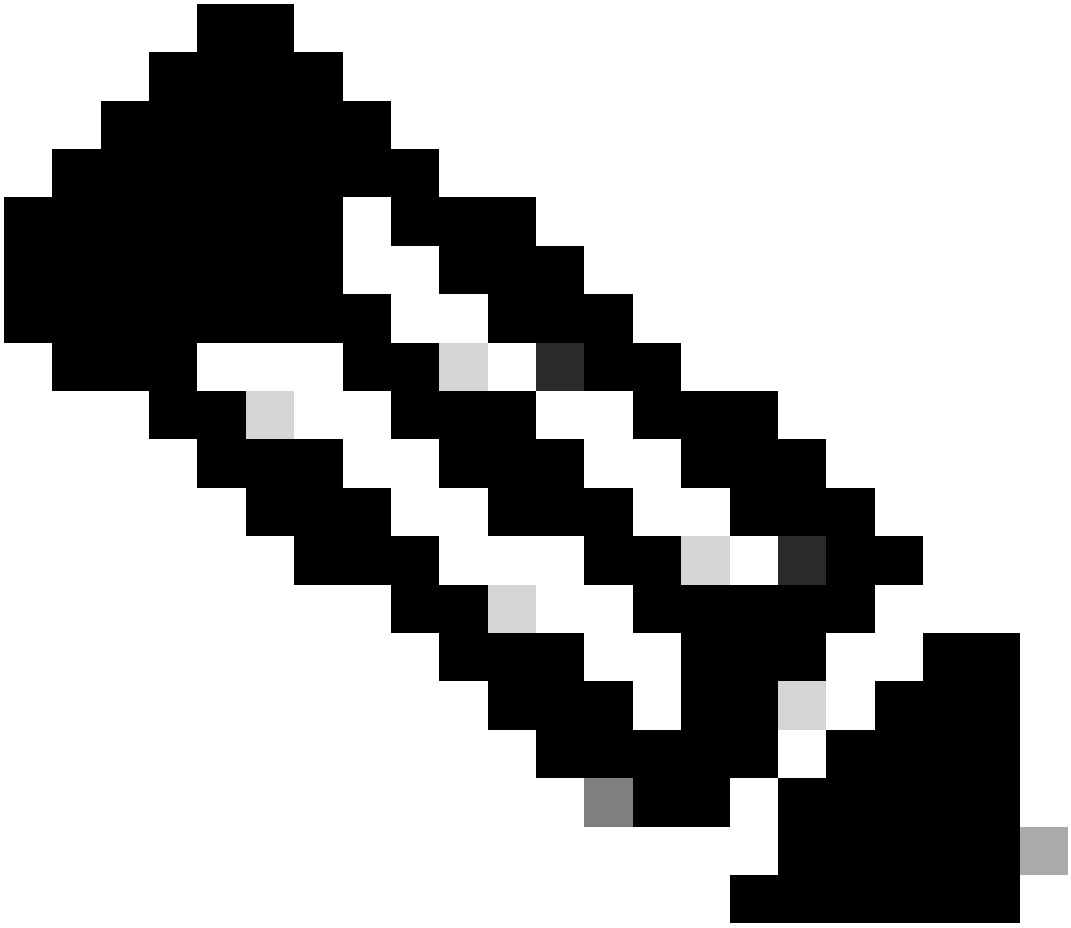
GET hotspot

OK-pakket

Het OK-pakket bevat de portal van ISE waarnaar de client moet worden omgeleid.



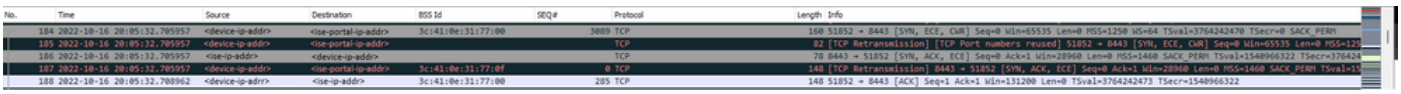
OK-pakket



Opmerking: de meeste mensen hebben een andere URL teruggegeven in het OK pakket. Daarom moet een andere DNS-query worden uitgevoerd om het definitieve IP-adres te verkrijgen.

Nieuwe TCP-sessie ingesteld

Nu het IP-adres van het portal is ontdekt, worden veel pakketten uitgewisseld, maar uiteindelijk toont een pakket met de bestemming IP dat is teruggestuurd in het OK-pakket (of opgelost door DNS) dat overeenkomt met het IP-adres van ISE, een nieuwe TCP-sessie die wordt ingesteld naar het portal.



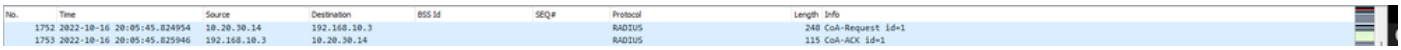
Tweede verbinding en nieuwe TCP-sessie naar ISE-portal

De portal wordt weergegeven aan de gebruiker

Op dit punt wordt de portal van ISE eindelijk weergegeven op de browser van de client browser. Zoals voorheen, worden veel pakketten uitgewisseld tussen ISE en het apparaat; dingen zoals een client hello en een server hello, enzovoort. Hier vraagt ISE de client om de gebruikersnaam en het wachtwoord, accepteert voorwaarden of wat dan ook dat is geconfigureerd op de ISE-server.

CoA-aanvraag / CoA-bevestiging

Zodra de gebruiker alle gevraagde gegevens heeft ingevoerd, stuurt ISE een verzoek van de CoA naar de verwerkingsverantwoordelijke om de autorisatie van de gebruiker te wijzigen. Als alles op de WLC is geconfigureerd zoals verwacht, zoals het hebben van de NAC-staat, ondersteuning voor CoA, enzovoort, stuurt de WLC een CoA-bevestiging (CoA ACK). Anders kan de WLC een CoA Non-Recognition (CoA NACK) sturen of de CoA ACK niet eens sturen.

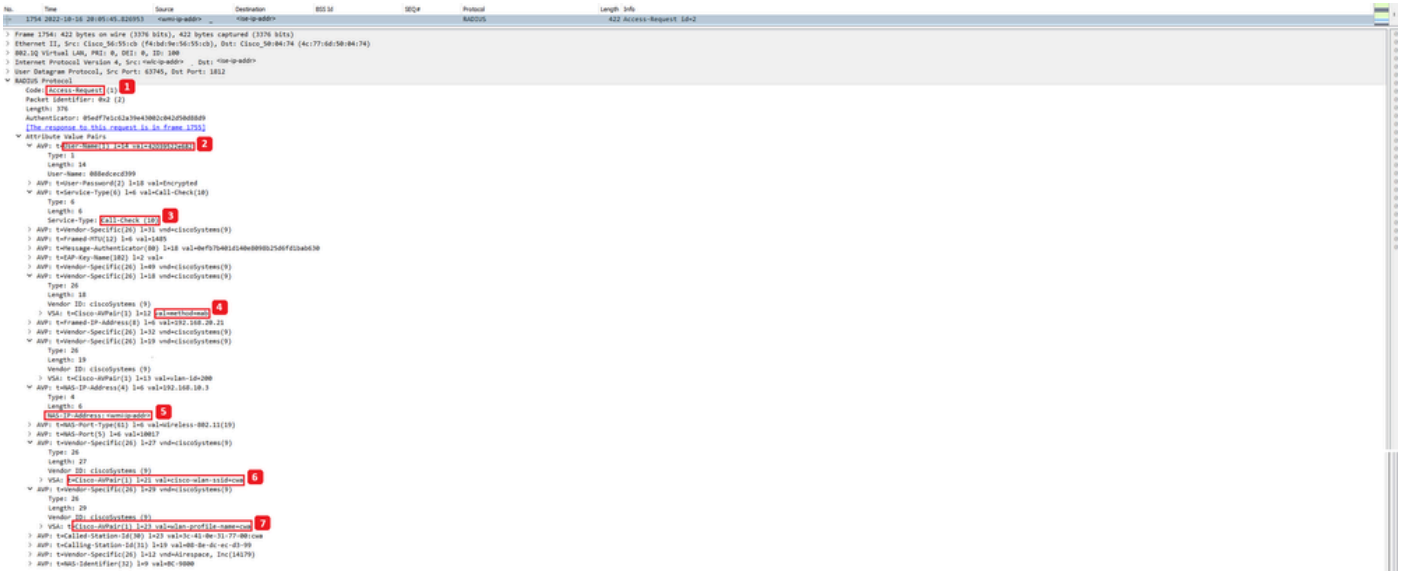


CoA-aanvraag en -bevestiging

Tweede verbinding: client naar netwerk

Nieuw toegangsverzoek

De WLC stuurt een nieuw access-request pakket naar ISE.



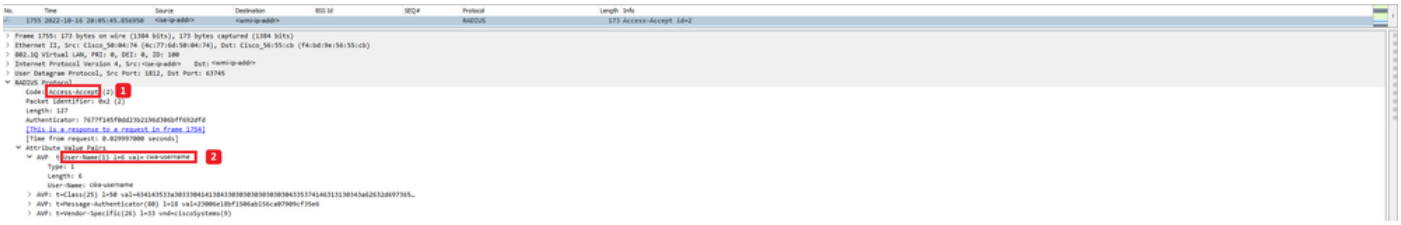
Analyse van nieuw access-request

1. Naam van het pakket.
2. Het MAC-adres dat probeert te verifiëren.
3. Dit geeft een MAC-filtering aan.
4. Het AV-paar dat door de controller naar ISE wordt gestuurd om een MAC-filterproces aan te geven.
5. Het WMI IP-adres van de WLC.
6. De SSID die de client probeert te verbinden.

7. De naam van het WLAN dat de client probeert te verbinden.

Nieuw access-acceptatie

De WLC stuurt een nieuw access-request pakket naar ISE.



Analyse van nieuw access-acceptatiepakket

1. Naam van het pakket.
2. De gebruikersnaam ingevoerd door de eindclient in het portal dat werd getoond.

Opnieuw, wordt een nieuwe het onderzoeken connectiviteitstest gemaakt van de cliënt. Zodra de client heeft bevestigd dat ze internetverbinding heeft, kan het portaal nu worden gesloten (het kan automatisch worden gesloten, afhankelijk van het gebruikte apparaat). De client is nu verbonden met het netwerk.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.