Verständnis des CWA-Datenflusses auf einem Client

Inhalt

Einleitung

In diesem Dokument wird der Datenfluss für den Endclient beim Herstellen einer Verbindung mit einem CWA-WLAN beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller (WLC) der Serie 9800
- Allgemeine Kenntnisse der zentralen Webauthentifizierung (CWA) und ihrer Konfiguration auf der Identity Services Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

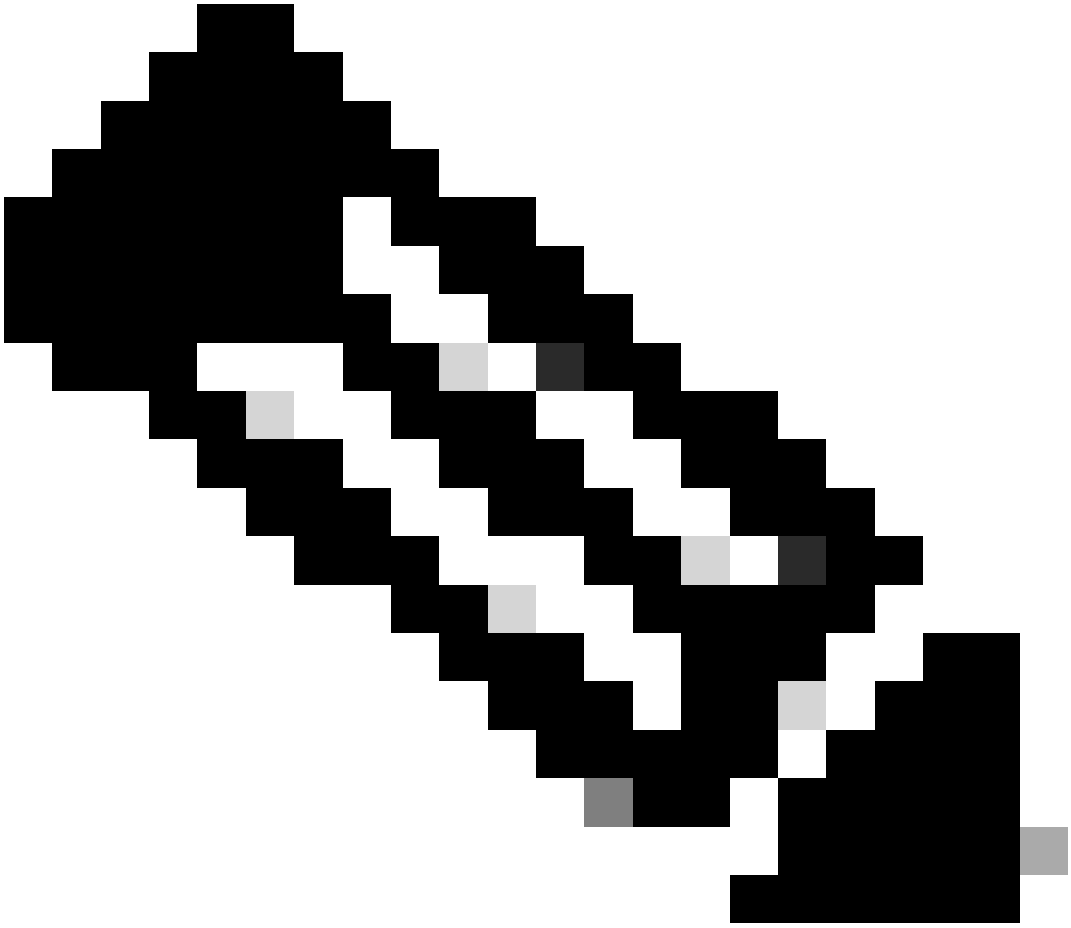
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

CWA ist eine Art von SSID-Authentifizierung, die auf dem WLC konfiguriert werden kann, wenn der Endclient, der eine Verbindung herstellen möchte, aufgefordert wird, seinen Benutzernamen und sein Kennwort in einem Webportal einzugeben, das ihm angezeigt wird. Kurz gesagt: Der Fluss für den Endclient verläuft bei der Verbindung mit dem WLAN wie folgt:

1. Der Endclient stellt eine Verbindung mit der auf seinem Gerät angezeigten SSID her.
2. Der Endclient wird zur Eingabe seiner Anmeldeinformationen an das Webportal weitergeleitet.
3. Der Endclient wird von der ISE mit den eingegebenen Anmeldeinformationen authentifiziert.
4. Die ISE antwortet dem WLC, dass der Endclient authentifiziert wurde. ISE kann einige zusätzliche Attribute bereitstellen, die der Client beim Zugriff auf das Netzwerk erfüllen muss (z. B. bestimmte ACLs)
5. Der End-Client wird neu zugeordnet und authentifiziert, um schließlich Zugriff auf das Netzwerk zu erhalten.



Hinweis: Beachten Sie, dass der Endclient, der zweimal authentifiziert wird, für den Endclient transparent ist.

Der zugrunde liegende Prozess, den der Client durchlaufen muss, ist im Wesentlichen in zwei unterteilt: eine Verbindung vom Client zum ISE-Server und eine einmal authentifizierte Verbindung vom Client zum Netzwerk selbst. Der Controller und die ISE kommunizieren stets über das RADIUS-Protokoll. Im Folgenden eine detaillierte Analyse einer radioaktiven (RA) Spur und einer Embedded Packet Capture (EPC).

CWA-Fluss - radioaktive (RA) Verfolgung

Eine RA-Ablaufverfolgung ist eine Gruppe von Protokollen, die für einen bestimmten Client erfasst werden. Es zeigt den gesamten Prozess an, den der Client während der Verbindung mit einem WLAN durchläuft. Weitere Informationen zu diesen Funktionen und zum Abrufen von RA-Ablaufverfolgungen finden Sie unter Understand Wireless Debugs and Log Collection on Catalyst 9800 Wireless LAN Controllers (Grundlegendes zu Wireless-Debugs und Protokollsammlung auf

Catalyst 9800 Wireless LAN-Controllern).

Erste Verbindung: Client zum ISE-Server

Der WLC lässt keine Verbindung zum Netzwerk zu, wenn der Client zuvor nicht von der ISE autorisiert wurde.

Zuordnung zum WLAN

Der WLC erkennt, dass der Client eine Verbindung zum WLAN "cwa" herstellen möchte, das mit dem Richtlinienprofil "cwa-policy-profile" verknüpft ist und eine Verbindung zum AP "BC-3802" herstellt.

```
<#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-Filterung

Testen der ISE-Serververbindung

Sobald der WLC die Zuordnungsanforderung vom Client erhalten hat, ist der erste Schritt die Durchführung einer MAC-Filterung (auch MAB genannt). Die MAC-Filterung ist eine Sicherheitsmethode, bei der die MAC-Adresse des Clients mit einer Datenbank abgeglichen wird, um zu überprüfen, ob sie dem Netzwerk beitreten dürfen.

```
<#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 attrib
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Session Start event called from SANET-SHIM
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Wireless session sequence, create context w
[auth-mgr-feat_wireless] [17558]: (info): [4203.9522.e682:capwap_90000005] -
```

authc_list: cwa_authz <-- Authentication method list used

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

MAB authentication started for 4203.9522.e682

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

MAB_CONTINUE

```
' on handle 0x8A000002
```

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

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

WLC sendet Anfrage an ISE

Der WLC sendet ein RADIUS-Access-Request-Paket an die ISE, das die MAC-Adresse des Clients enthält, der sich beim WLAN authentifizieren möchte.

<#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

"

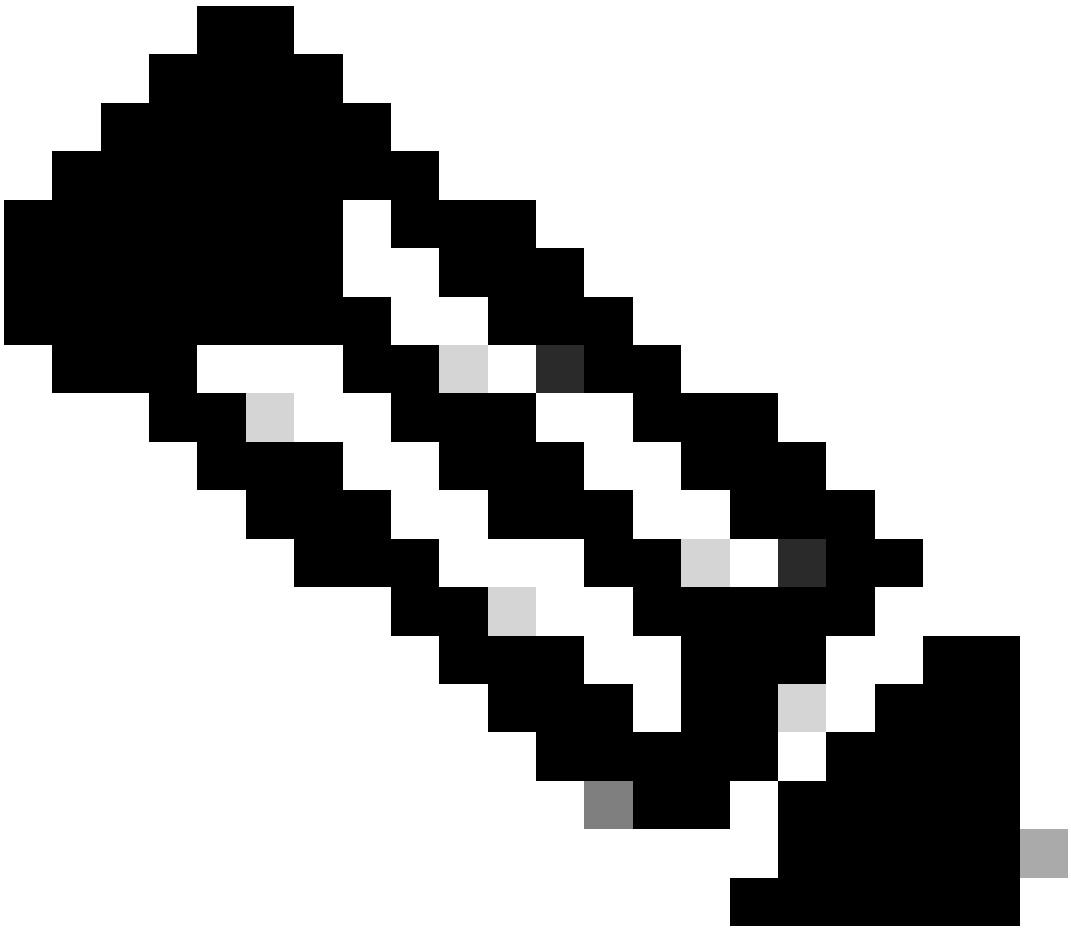
<-- SSID and WLAN the client is attempting to connect

```
[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
```



Hinweis: Ein AV-Paar ist der von der ISE verwendete Attributwert. Hierbei handelt es sich um eine Key-Value-Struktur vordefinierter Informationen, die an den WLC gesendet werden können. Diese Werte werden auf den jeweiligen Client für die jeweilige Sitzung angewendet.

Beispiele für AV-Paare:

- ACL-Name
- URL umleiten
- VLAN-Zuweisung
- Timeout-Timer für Sitzungen
- Timer zur erneuten Authentifizierung

ISE reagiert auf WLC-Anforderung

Wenn die vom WLC gesendete MAC-Adresse von der ISE akzeptiert wird, sendet die ISE ein Access-Accept-RADIUS-Paket. Wenn es sich bei der ISE-Konfiguration um eine unbekannte MAC-Adresse handelt, muss sie diese akzeptieren und den Fluss fortsetzen. Wenn eine Access-Reject (Zugriffs-Ablehnen) angezeigt wird, muss eine nicht ordnungsgemäß konfigurierte Komponente der ISE überprüft werden.

<#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-Prozesse für von der ISE empfangene Informationen

Der WLC verarbeitet alle von der ISE erhaltenen Informationen. Damit wendet sie das Benutzerprofil an, das sie ursprünglich mit den von der ISE gesendeten Daten erstellt hatte. Der WLC weist dem Benutzer beispielsweise eine neue ACL zu. Wenn AAA Override im WLAN nicht aktiviert ist, erfolgt diese Verarbeitung durch den WLC nicht.

<#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-Authentifizierung abgeschlossen

Nachdem das Benutzerprofil für den Client erfolgreich geändert wurde, authentifiziert der WLC die MAC-Adresse des Clients. Wenn die von der ISE empfangene ACL nicht auf dem WLC vorhanden ist, weiß der WLC nicht, wie er mit diesen Informationen umgehen soll. Daher schlägt die Aktion REPLACE fehl, und die MAB-Authentifizierung schlägt ebenfalls fehl. Der Client kann sich nicht authentifizieren.

<#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 sendet Zuordnungsantwort an Client

Nachdem der Client von der ISE authentifiziert und die richtige ACL angewendet wurde, sendet der WLC schließlich eine Assoziationsantwort an den Client. Nun kann der Benutzer die Verbindung mit dem Netzwerk fortsetzen.

<#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-Authentifizierung

Gemäß dem Prozess, den ein Client bei der Verbindung mit einem WLAN durchlaufen muss, "startet" die L2-Authentifizierung. In Wirklichkeit wurde jedoch aufgrund der zuvor durchgeführten MAB-Authentifizierung bereits eine L2-Authentifizierung durchgeführt. Der Client schließt die L2-Authentifizierung sofort ab.

<#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

Daten-Plumb

Der WLC weist dem verbindenden Client Ressourcen zu, damit der Datenverkehr durch das Netzwerk fließen kann.

<#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
```

Dem Benutzer wurde eine IP-Adresse zugewiesen.

Der Endbenutzer benötigt eine IP-Adresse, um durch das Netzwerk zu navigieren. Es durchläuft den DHCP-Prozess. Wenn der Benutzer zuvor eine Verbindung hergestellt hat und sich an seine IP-Adresse erinnert, wird der DHCP-Prozess übersprungen. Wenn der Benutzer keine IP-Adresse empfangen kann, kann der Endbenutzer das Webportal nicht anzeigen. Andernfalls führen Sie die folgenden Schritte aus:

1. Ein DISCOVER-Paket wird vom verbindenden Client als Broadcast gesendet, um alle verfügbaren DHCP-Server zu finden.
2. Wenn ein DHCP-Server verfügbar ist, antwortet der DHCP-Server mit einem ANGEBOT. Das Angebot enthält Informationen wie die dem verbindenden Client zuzuweisende IP-Adresse, Leasedauer usw. Es können viele ANGEBOTE von verschiedenen DHCP-Servern empfangen werden.
3. Der Client nimmt ein ANGEBOT von einem der Server entgegen und antwortet mit einer ANFRAGE für die ausgewählte IP-Adresse
4. Schließlich sendet der DHCP-Server ein BESTÄTIGUNGSPAKET an den Client, dem die neue IP-Adresse zugewiesen wurde.

Der WLC protokolliert die Methode, mit der der Client seine IP-Adresse empfangen hat.

<#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-Authentifizierung beginnt

Nachdem der Endbenutzer eine IP-Adresse erhalten hat, beginnt die L3-Authentifizierung mit der Erkennung von CWA als gewünschte Authentifizierungsmethode.

<#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

Tests von IP-Adressen

Um mit der Verbindung fortzufahren, muss der Client zwei ARP-Anforderungen ausführen:

1. Überprüfen Sie, ob die IP-Adresse aller anderen Personen gültig ist. Wenn für die IP-Adresse des Endbenutzers eine ARP-Antwort vorhanden ist, handelt es sich um eine duplizierte IP-Adresse

2. Überprüfen Sie die Erreichbarkeit zum Gateway. Auf diese Weise wird sichergestellt, dass der Client das Netzwerk verlassen kann. Die ARP-Antwort muss vom Gateway stammen.

<#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
```

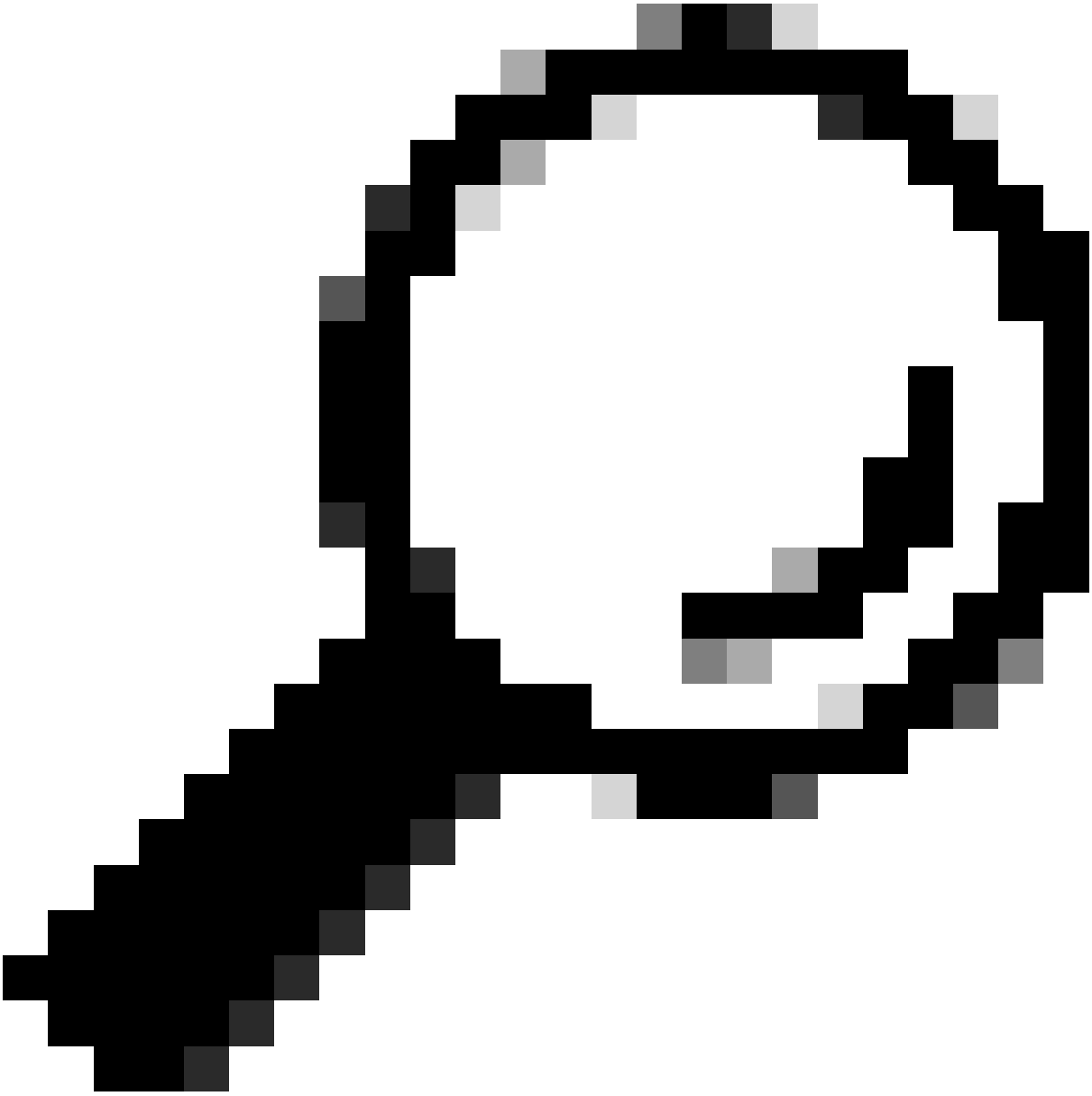
Zweite Verbindung: Client zu Netzwerk

An diesem Punkt wurde der Endbenutzer über seine MAC-Adresse gegenüber der ISE authentifiziert, aber noch nicht vollständig autorisiert. Der WLC muss erneut auf die ISE verweisen, um den Client zur Verbindung mit dem Netzwerk zu autorisieren. An dieser Stelle wird das Portal dem Benutzer angezeigt, in den der Benutzername seinen Benutzernamen und sein Passwort eingeben muss. Auf dem WLC wird der Endbenutzer im Status "Web Auth Pending" (Webauthentifizierung ausstehend) angezeigt.

Autorisierungsänderung (CoA)

An dieser Stelle tritt die "Unterstützung für CoA" in der WLC-Konfiguration in Kraft. Bis zu diesem Zeitpunkt wurde die ACL verwendet. Wenn der Endclient das Portal sieht, wird die ACL nicht mehr verwendet, da der Client lediglich an das Portal weitergeleitet wurde. An diesem Punkt gibt der Client seine Anmeldeinformationen ein, um sich anzumelden und den CoA-Prozess zu starten und den Client erneut zu authentifizieren. Der WLC bereitet das zu sendende Paket vor und leitet es an die ISE weiter

---



Tipp: CoA verwendet Port 1700. Vergewissern Sie sich, dass er nicht von der Firewall blockiert wird.

<#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

Zweite Authentifizierung gegenüber ISE

Die zweite Authentifizierung beginnt nicht bei Null. Das ist die Stärke von CoA. Neue Regeln und/oder AV-Paris können auf den Benutzer angewendet werden. Die ACL und die beim ersten Access-Accept empfangene Umleitungs-URL werden nicht mehr an den Endbenutzer weitergeleitet.

WLC sendet Anfrage an ISE

Der WLC sendet ein neues RADIUSAccess-Requestpaket an die ISE mit der eingegebenen Kombination aus Benutzername und Kennwort. Dies löst eine neue MAB-Authentifizierung aus, und da die ISE den Client bereits kennt, muss ein neuer Richtliniensatz angewendet werden (z. B. Zugriff gewährt).

<#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 reagiert auf WLC-Anforderung

Die ISE führt eine Suche nach ihrer Richtlinie durch. Wenn der empfangene Benutzername mit dem Richtlinienprofil übereinstimmt, antwortet die ISE erneut auf den WLC und akzeptiert die Clientverbindung mit dem WLAN. Es gibt den Benutzernamen des Endbenutzers zurück. Wenn auf der ISE konfiguriert, können zusätzliche Regeln und/oder AV-Paare auf den Benutzer angewendet werden. Diese werden auf "Access-Accept" angezeigt.

<#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-Prozesse für von der ISE empfangene Informationen

Der WLC verarbeitet erneut die von der ISE erhaltenen Informationen. Er führt eine weitere ERSETZUNG-Aktion für den Benutzer mit den neuen Werten aus, die er von der ISE erhält.

<#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-Authentifizierung abgeschlossen

Der Endbenutzer wurde nun mit den angegebenen Daten authentifiziert. L3-Authentifizierung (Webauthentifizierung) ist abgeschlossen.

<#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

Endbenutzer erreicht RUN-Status auf WLC

Schließlich wird der Benutzer authentifiziert und dem WLAN zugewiesen.

<#root>

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

Managed client RUN state

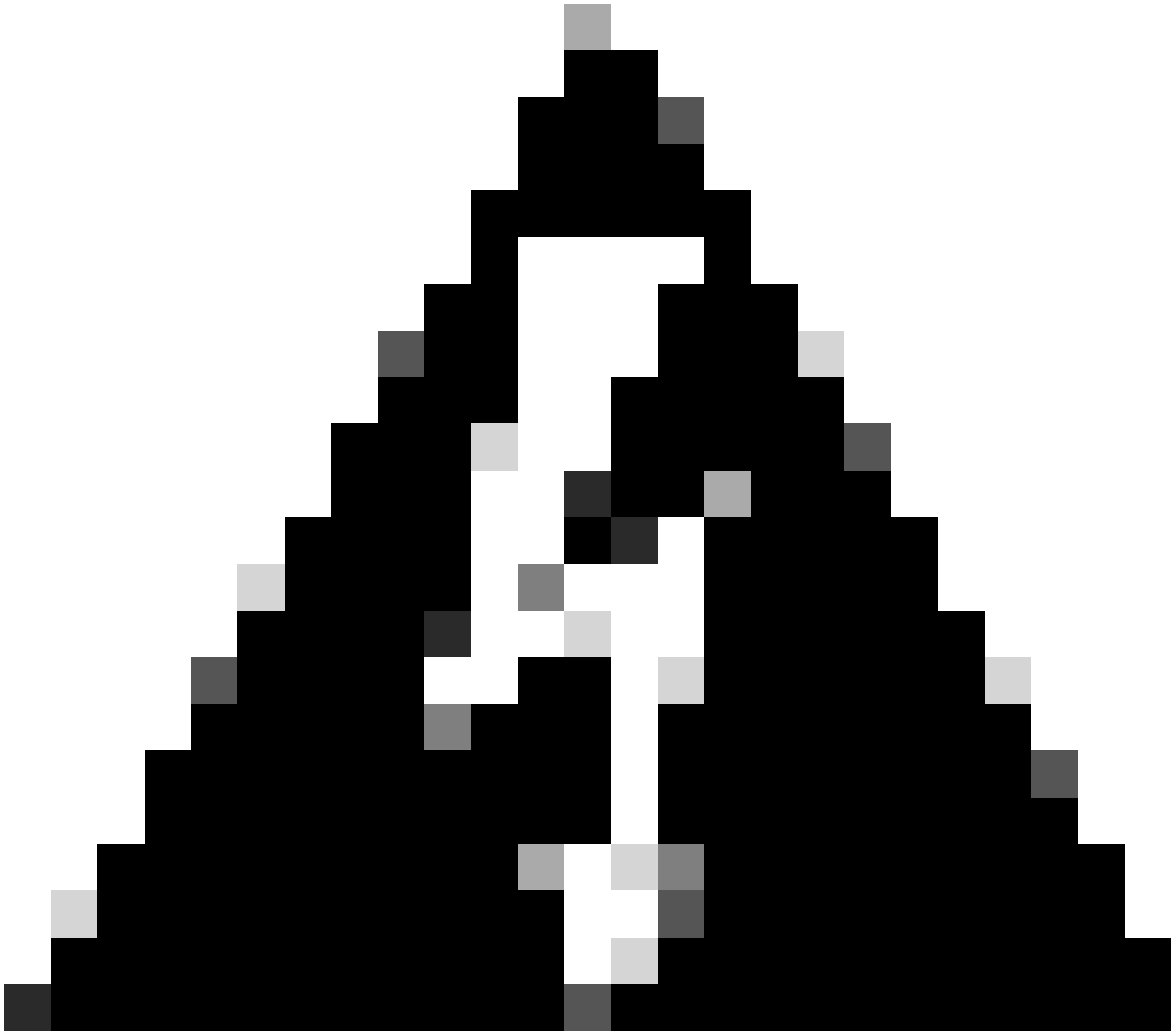
```
 notification: 4203.9522.e682
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
```

S_CO_RUN

CWA-Fluss - Embedded Packet Capture (EPC)

Ein EPC ist eine Paketerfassung, die direkt vom WLC abgerufen werden kann und alle Pakete anzeigt, die entweder den WLC passieren oder von ihm stammen. Weitere Informationen zu diesen Funktionen und zum Abrufen finden Sie unter Verstehen der Wireless-Debugs und der Protokollsammlung auf Catalyst 9800 Wireless LAN-Controllern.

Erste Verbindung: Client zum ISE-Server



Warnung: Die IP-Adressen auf den Bildern der Paketerfassung wurden gelöscht. Sie werden angezeigt als und

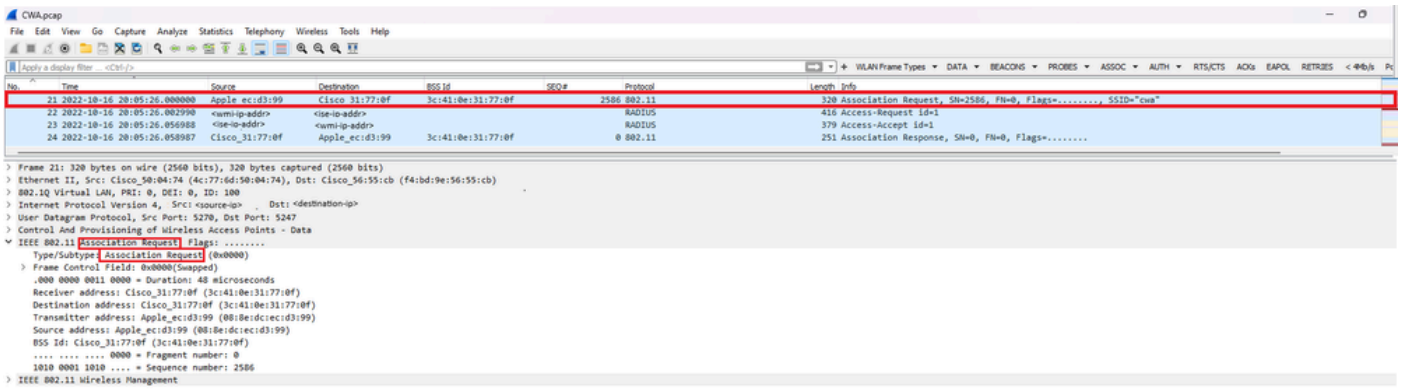
Zuordnung zum WLAN und Anforderung an ISE-Server gesendet

No.	Time	Source	Destination	BSS Id	SEQ#	Protocol	Length	Info
21	2022-10-16 20:05:26.000000	Apple_ec:d3:99	Cisco_31:77:0f	3c:41:0e:31:77:0f	2586	802.11	320	Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
22	2022-10-16 20:05:26.002990	<source-ip-address>	<destination-ip-address>			RADIUS	416	Access-Request id=1
23	2022-10-16 20:05:26.056988	<source-ip-address>	<destination-ip-address>			RADIUS	379	Access-Accept id=1
24	2022-10-16 20:05:26.058987	Cisco_31:77:0f	Apple_ec:d3:99	3c:41:0e:31:77:0f	0	802.11	251	Association Response, SN=0, FN=0, Flags=........

Erste Pakete

Zuordnungsanfrage vom WLC an den Client

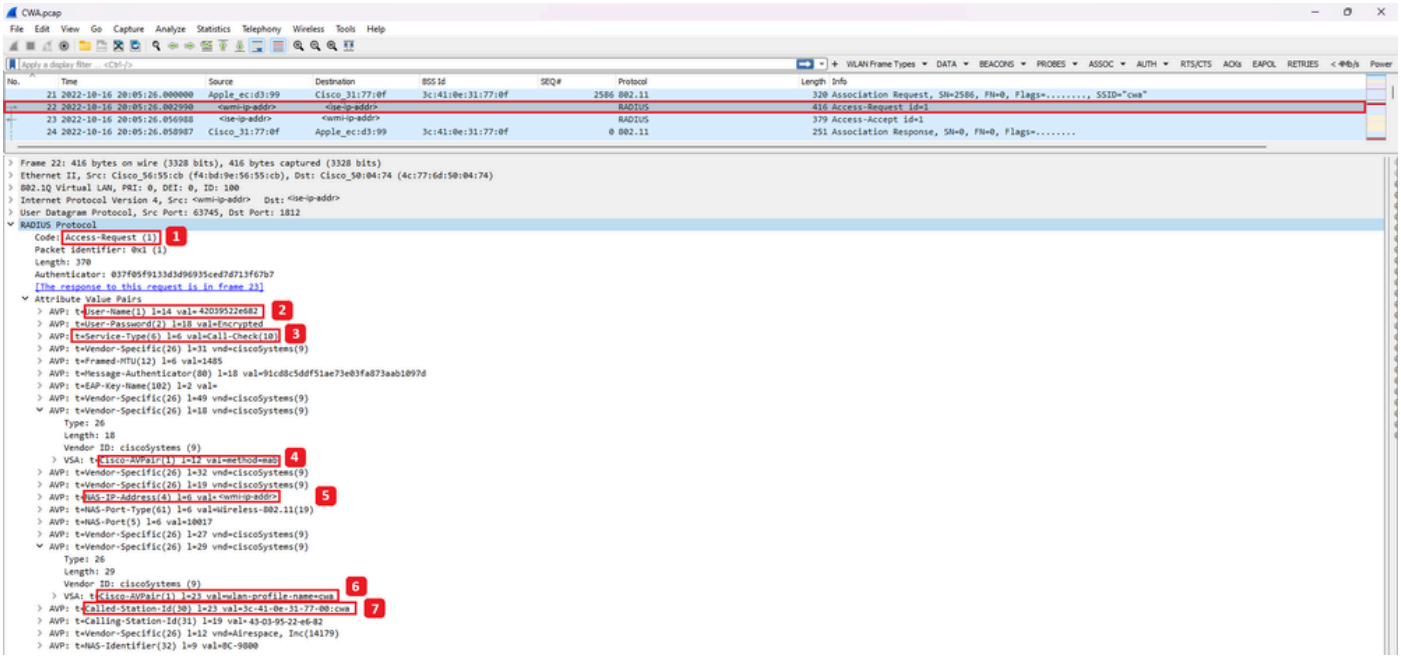
Beim ersten Paket "Association Request" sehen Sie die MAC-Adressen der Geräte, die an diesem Prozess beteiligt sind.



Zuordnungsanforderung

Access-Request-Paket vom WLC an die ISE gesendet

Nachdem die Zuordnungsanforderung vom WLC verarbeitet wurde, sendet der WLC ein Access-Request-Paket an den ISE-Server.



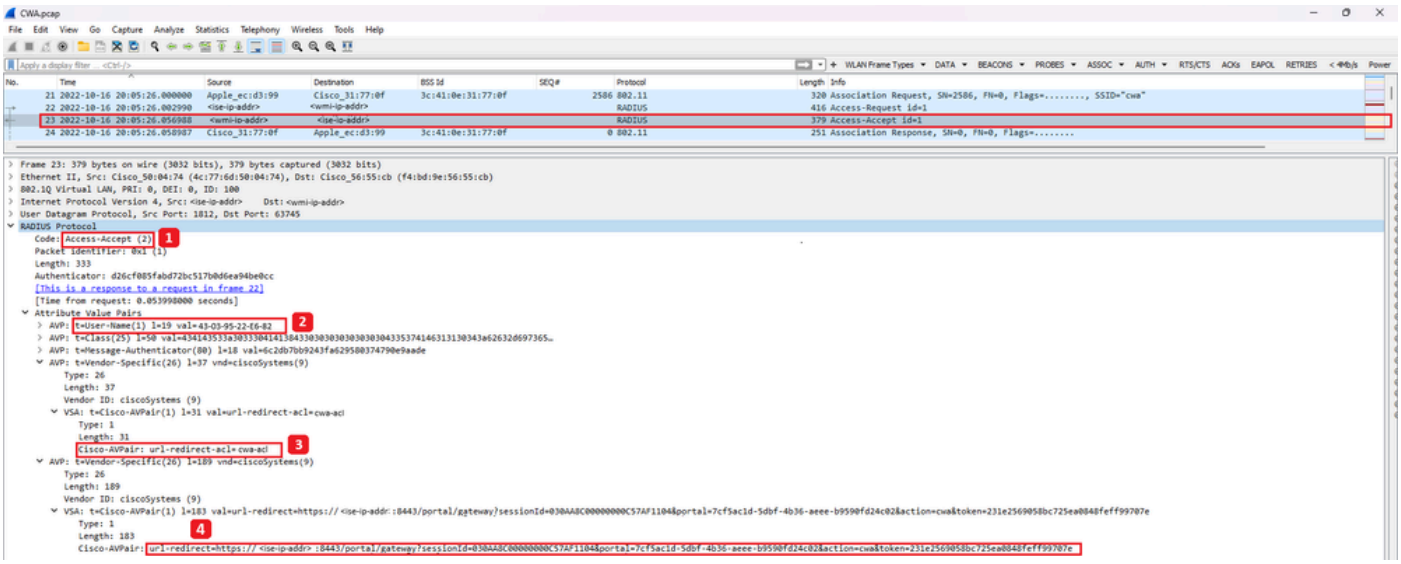
Analyse des Access-Request-Pakets

1. Name des Pakets.
2. Die MAC-Adresse, die authentifiziert werden soll.
3. Dies weist auf eine MAC-Filterung hin.
4. Das AV-Paar, das vom Controller an die ISE gesendet wird, um einen MAC-Filterprozess anzuzeigen.
5. Die WMI-IP-Adresse des WLC
6. Die SSID, die der Client versucht, eine Verbindung herzustellen.
7. Der Name des WLAN, mit dem der Client eine Verbindung herstellen möchte.

Access-Accept-Paket vom WLC an die ISE gesendet

Nachdem die ISE das Access-Accept-Paket verarbeitet hat, antwortet sie bei Erfolg mit einem

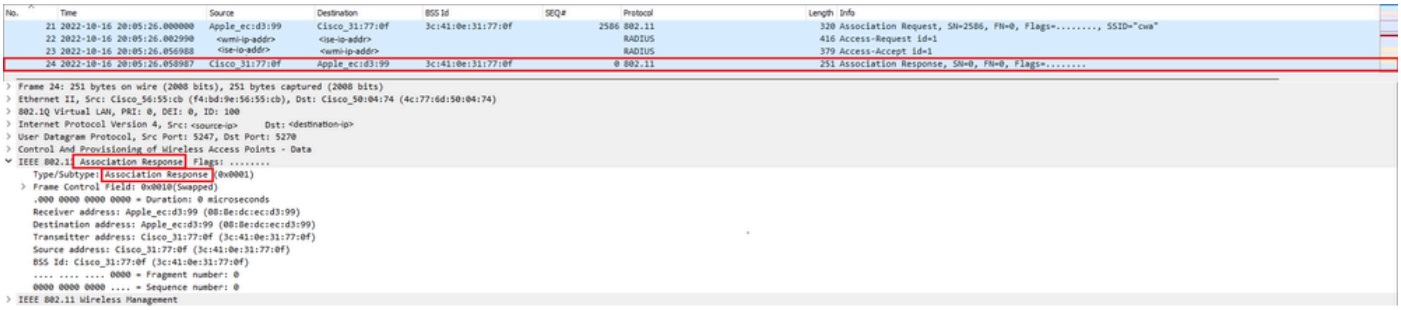
Access-Accept bzw. bei Nichtbestehen mit einem Access-Reject.



Analyse des Access-Accept-Pakets

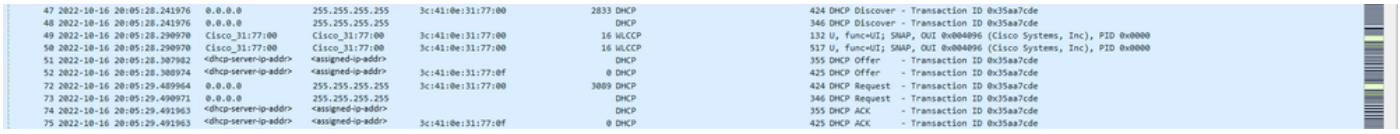
1. Name des Pakets.
2. MAC-Adresse authentifiziert.
3. Die anzuwendende ACL.
4. Die URL, an die der Benutzer umgeleitet werden soll.

Zuordnungsantwort vom WLC zum Client

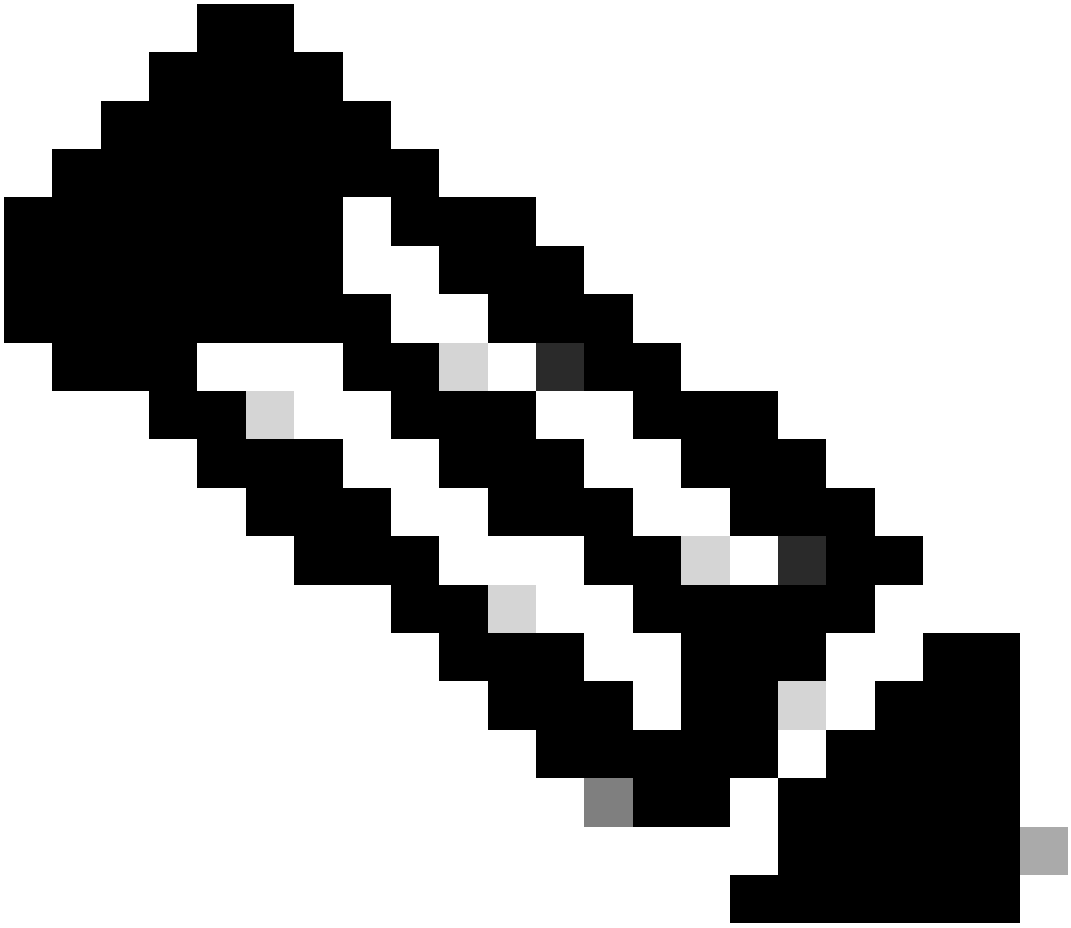


Assoziationsantwort

DHCP-Prozess

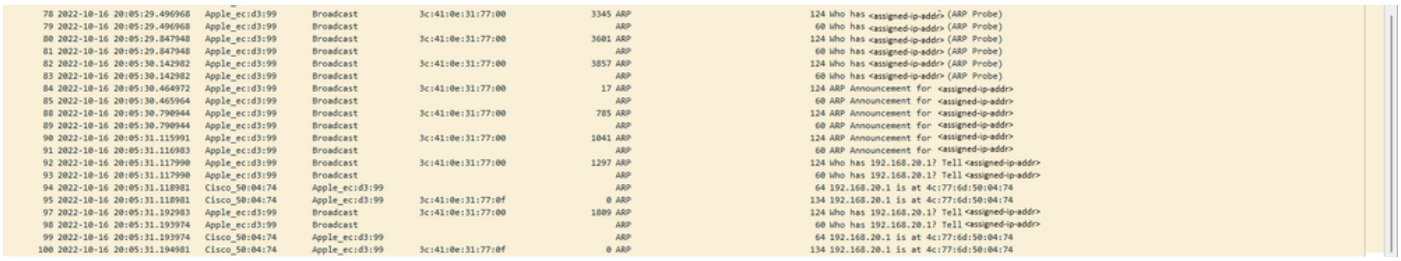


DHCP-Prozess



Hinweis: Ab jetzt werden Pakete als dupliziert angesehen, aber das liegt nur daran, dass das eine CAPWAP-gekapselt ist und das andere nicht.

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-ARP für eigene IP-Adresse und für das Gateway

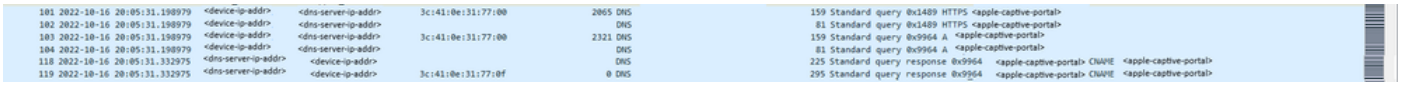
Verbindungstest

Wenn der ARP-Prozess abgeschlossen ist, führt das Gerät, das eine Verbindung herstellen

möchte, eine Überprüfung durch, um zu überprüfen, ob ein Portal ausgelöst wird. Dies wird auch als Sondierung bezeichnet. Wenn das Gerät angibt, dass keine Internetverbindung besteht, bedeutet dies, dass der ARP-Prozess fehlgeschlagen ist (das Gateway hat beispielsweise nie geantwortet) oder das Gerät nicht in der Lage war, die Suche durchzuführen.

Diese Sondierung ist etwas, das nicht auf den RA-Spuren zu sehen ist, nur der EPC ist in der Lage, diese Informationen zur Verfügung zu stellen. Die Sondierungsabfrage hängt von dem Gerät ab, das eine Verbindung herstellen möchte. In diesem Beispiel war das Testgerät ein Apple-Gerät, sodass die Sondierung direkt in Richtung des Captive Portals von Apple durchgeführt wurde.

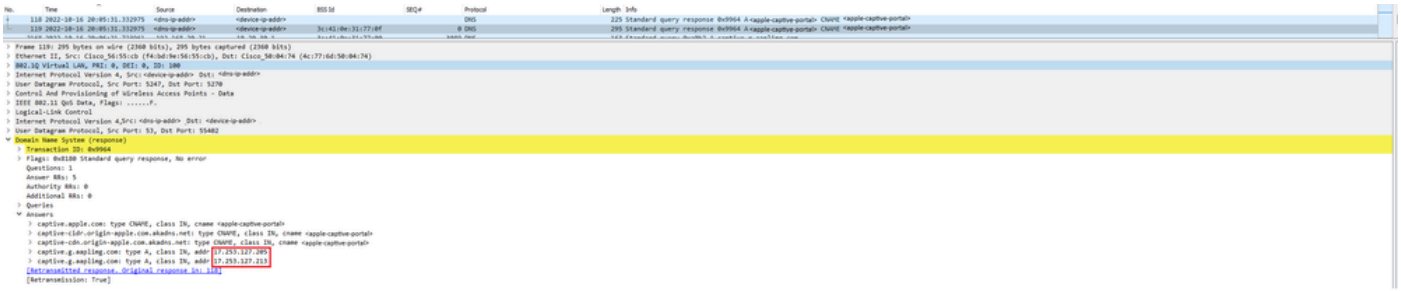
Da die Überprüfung mithilfe einer URL erfolgt, ist DNS erforderlich, um diese URL zu lösen. Wenn der DNS-Server daher nicht in der Lage ist, auf die Abfragen des Clients zu reagieren, fragt der Client weiterhin nach der URL ab, und das Portal wird nie angezeigt. Wenn an diesem Punkt die IP-Adresse des ISE-Servers im Webbrowser des Endgeräts eingegeben wird, muss das Portal sichtbar sein. Wenn dies der Fall ist, liegt ein Problem mit dem DNS-Server vor.



Verbindungstest vom Client - DNS-Abfrage und -Antwort

DNS - aufgelöste IP-Adresse

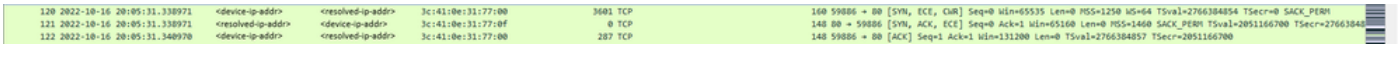
Beim Überprüfen der DNS-Abfrageantwort sehen Sie die IP-Adresse, die vom DNS-Server aufgelöst wurde.



IP-Adresse vom DNS-Server aufgelöst

Drei-Schritte-Handshake

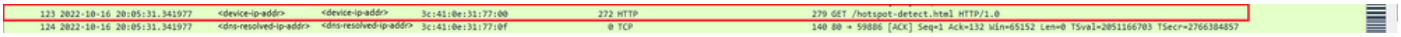
Nachdem die DNS-IP-Adresse aufgelöst wurde, wird ein TCP-3-Wege-Handshake zwischen dem Portal und dem Client eingerichtet. Die verwendete IP-Adresse ist eine aufgelöste IP-Adresse.



Drei-Schritte-Handshake

GET-Hotspot

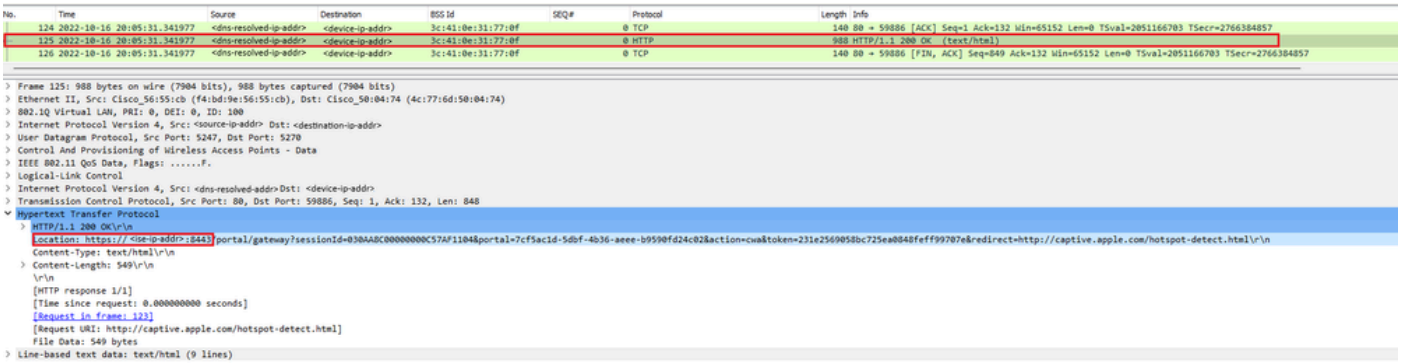
Nachdem die TCP-Sitzung hergestellt wurde, führt der Client eine Überprüfung durch und versucht, auf das Portal zuzugreifen.



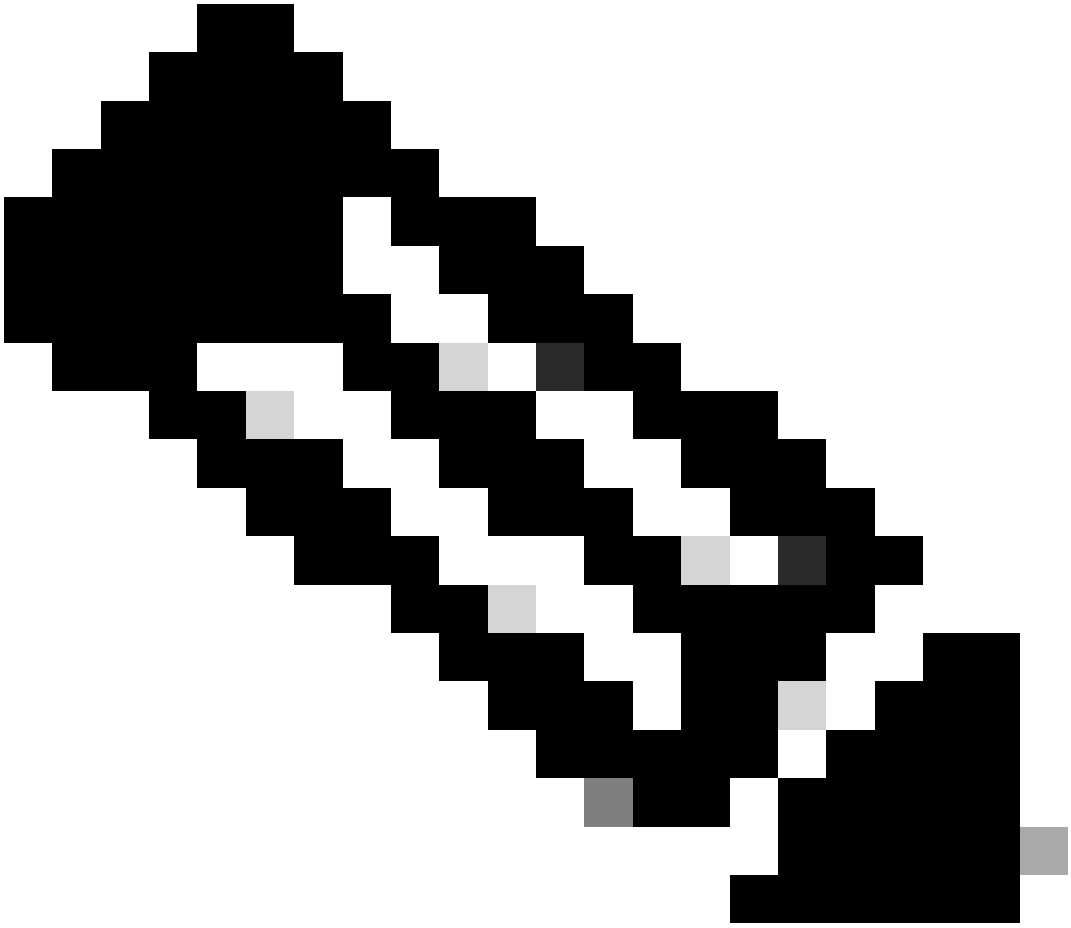
GET-Hotspot

OK-Paket

Das OK-Paket enthält das ISE-Portal, an das der Client umgeleitet werden muss.



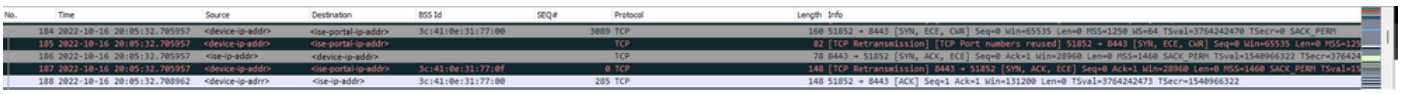
OK-Paket



> Hinweis: Die meisten Leute haben eine andere URL im OK-Paket zurückgegeben. Daher muss eine andere DNS-Abfrage durchgeführt werden, um die endgültige IP-Adresse zu erhalten.

Neue TCP-Sitzung eingerichtet

Nachdem die IP-Adresse des Portals erkannt wurde, werden viele Pakete ausgetauscht, aber am Ende zeigt ein Paket mit der Ziel-IP, die im OK-Paket zurückgegeben wurde (oder durch DNS aufgelöst wurde), welches der IP-Adresse der ISE entspricht, dass eine neue TCP-Sitzung zum Portal aufgebaut wird.



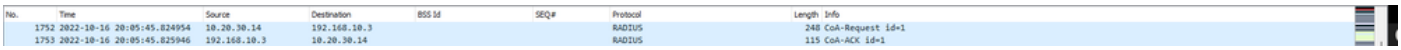
Zweite Verbindung und neue TCP-Sitzung zum ISE-Portal

Portal wird dem Benutzer angezeigt

An dieser Stelle wird schließlich das Portal der ISE im Browser des Client-Browsers angezeigt. Wie zuvor werden viele Pakete zwischen der ISE und dem Gerät ausgetauscht, z. B. ein Client-Hello, ein Server-Hello usw. An dieser Stelle fordert die ISE den Client auf, den Benutzernamen und das Kennwort einzugeben, die Nutzungsbedingungen zu akzeptieren oder die Konfiguration auf dem ISE-Server vorzunehmen.

CoA-Anfrage/CoA-Bestätigung

Nachdem der Benutzer alle angeforderten Daten eingegeben hat, sendet die ISE eine CoA-Anfrage an den Controller, um die Autorisierung des Benutzers zu ändern. Wenn alles auf dem WLC wie erwartet konfiguriert ist, z. B. der NAC-Status, die Unterstützung für CoA usw., sendet der WLC eine CoA-Bestätigung (CoA ACK). Andernfalls kann der WLC eine CoA Non-Acknowledgement (CoA NACK) senden oder er sendet einfach nicht einmal die CoA ACK.

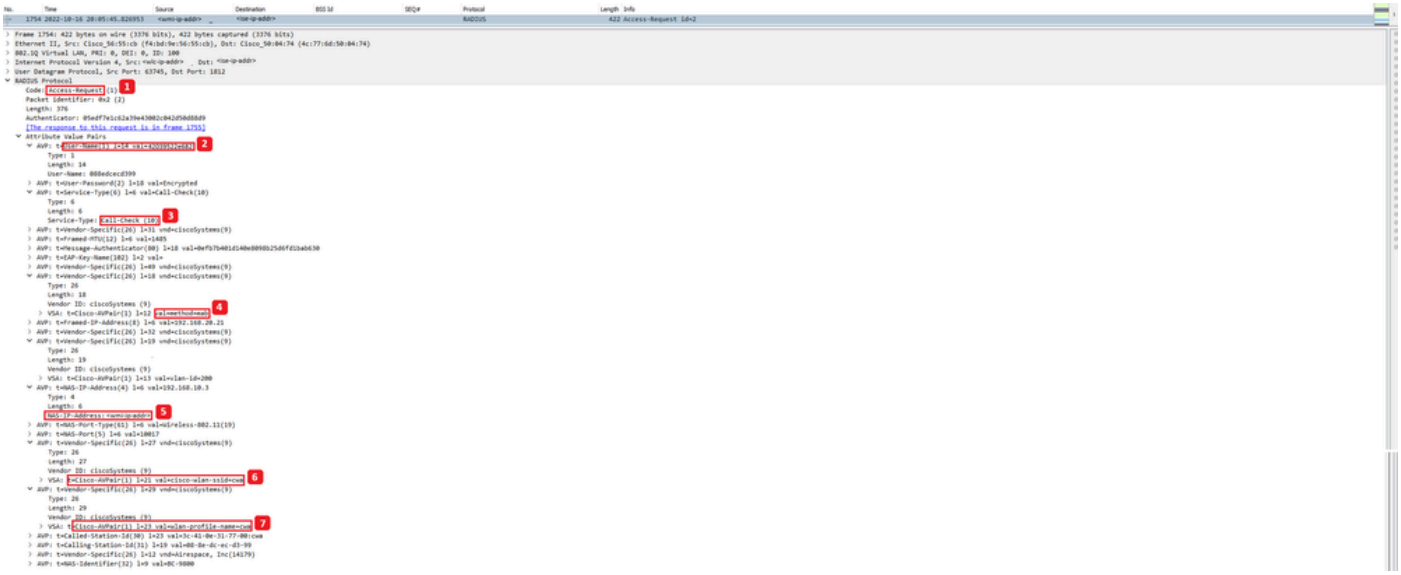


CoA-Antrag und -Anerkennung

Zweite Verbindung: Client zu Netzwerk

Neue Zugriffsanfrage

Der WLC sendet ein neues Access-Request-Paket an die ISE.



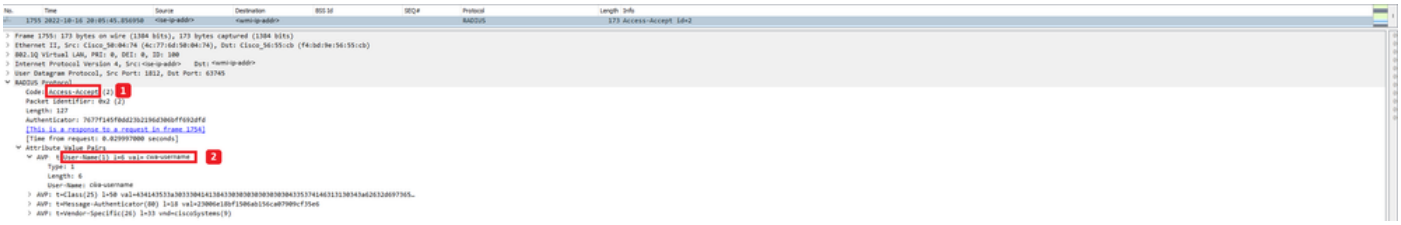
Analyse des neuen Access-Request-Pakets

1. Name des Pakets.
2. Die MAC-Adresse, die authentifiziert werden soll.
3. Dies weist auf eine MAC-Filterung hin.
4. Das AV-Paar, das vom Controller an die ISE gesendet wird, um einen MAC-Filterprozess anzuzeigen.
5. Die WMI-IP-Adresse des WLC
6. Die SSID, die der Client versucht, eine Verbindung herzustellen.

7. Der Name des WLAN, mit dem der Client eine Verbindung herstellen möchte.

Neuer Zugang - Akzeptieren

Der WLC sendet ein neues Access-Request-Paket an die ISE.



Analyse des neuen Access-Accept-Pakets

1. Name des Pakets.
2. Der Benutzername, den der Endclient in das angezeigte Portal eingegeben hat.

Auch hier wird ein neuer Verbindungstest vom Client durchgeführt. Sobald der Client bestätigt hat, dass er über eine Internetverbindung verfügt, kann das Portal geschlossen werden (je nach verwendetem Gerät kann es automatisch geschlossen werden). Der Client ist jetzt mit dem Netzwerk verbunden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.