了解客户端上的CWA流程

目录

简介

本文档介绍连接到CWA WLAN时终端客户端所经历的流程。

先决条件

要求

思科建议您具备以下方面的基础知识：

- 思科无线LAN控制器(WLC) 9800系列
- 对集中Web身份验证(CWA)及其在身份服务引擎(ISE)上的配置的一般了解

使用的组件

本文档中的信息基于以下软件和硬件版本：

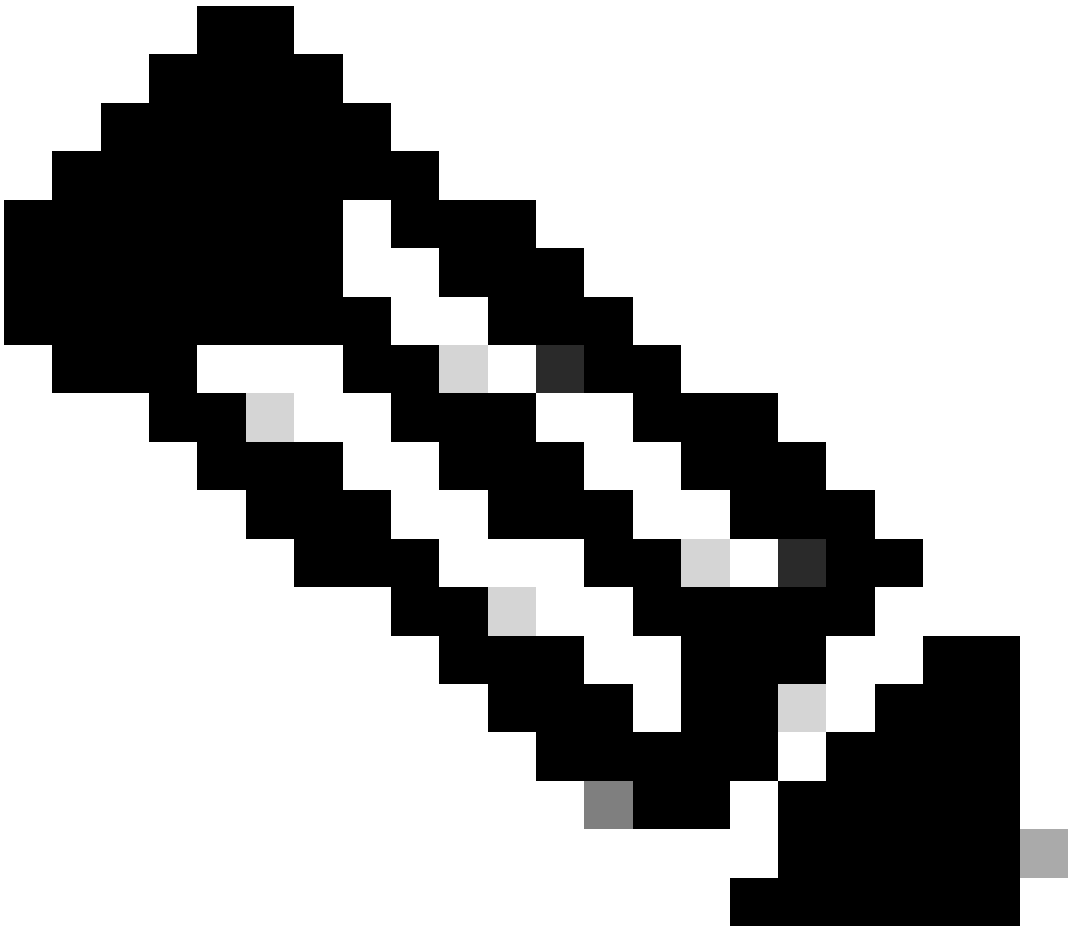
- 9800-CL WLC
- 思科AP 3802
- 9800 WLC Cisco IOS® XE v17.3.6
- 身份服务引擎(ISE) v3.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

CWA是一种SSID身份验证，可在WLC上配置，其中会提示尝试连接的最终客户端将其用户名和密码输入到向其提供的Web门户。简而言之，连接到WLAN时，终端客户端的流程为：

1. 终端客户端连接到其设备上显示的SSID
2. 终端客户端被重定向到Web门户以输入其凭证
3. 终端客户端由ISE使用输入的凭证进行身份验证
4. ISE回复WLC说终端客户端已经过身份验证。 ISE可以推送客户端在访问网络时必须遵守的一些其他属性（例如特定ACL）
5. 最终客户端重新关联并重新进行身份验证，最终获得网络访问权限



注意：请注意，两次身份验证的终端客户端对终端客户端是透明的

客户端必须经过的基本过程大致分为两部分：从客户端到ISE服务器的连接，以及经过身份验证后从客户端到网络本身的另一个连接。控制器和ISE始终通过RADIUS协议相互通信。下面是放射性(RA)跟踪和嵌入式数据包捕获(EPC)的深入分析。

CWA流程-放射性(RA)跟踪

RA跟踪是为特定客户端捕获的一组日志。它显示了客户端在连接到WLAN时经历的整个过程。有关它们是什么以及如何检索RA跟踪的详细信息，请访问[了解Catalyst 9800无线LAN控制器上的无线调试和日志收集。]

第一个连接：客户端到ISE服务器

如果客户端之前未经ISE授权，则WLC不允许连接到网络。

关联到WLAN

WLC检测到客户端要关联到WLAN“cwa”，WLAN“cwa”与策略配置文件“cwa-policy-profile相关联，并且正在连接到AP“BC-3802”

```
<#root>

[client-orch-sm] [17558]: (note): MAC: 4203.9522.e682

Association received.

 BSSID dc8c.37d0.83af,

WLAN cwa

, Slot 1 AP dc8c.37d0.83a0, BC-3802
[client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Received Dot11 association request. Processing s

SSID: cwa

,

Policy profile: cwa-policy-profile

,

AP Name: BC-3802

, Ap Mac Address: dc8c.37d0.83a0 BSSID MAC0000.0000.0000 wlan ID: 1RSSI: -46, SNR: 40
[client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition:

 S_CO_INIT -> S_CO_ASSOCIATING


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

MAC 过滤

测试ISE服务器连接

WLC收到来自客户端的关联请求后，第一步是执行MAC过滤（也称为MAB）。MAC过滤是一种安全方法，它根据数据库检查客户端的MAC地址，以验证是否允许它们加入网络。

```
<#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 und
[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 receiv
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is receiv
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change notification is receiv
[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 0E1E140A0000000C
[auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] Applying policy for WlanId: 1, bssid : dc8c
[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_AWAI
[ewlc-infra-evq] [17558]: (note): Authentication Success. Resolved Policy bitmap:11 for client 4203.9522
[client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transition: S_AUTHIF_MAB_
[mab] [17558]: (info): [4203.9522.e682:capwap_90000005] Received event '

MAB_CONTINUE

' on handle 0x8A000002

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

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

WLC向ISE发送请求

WLC向ISE发送RADIUS Access-Request 数据包，其中包含要向WLAN进行身份验证的客户端的MAC地址。

<#root>

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

Access-Request

to

<ise-ip-addr>:1812

id 0/

28

, len 415

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

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

42039522e682

"

<-- MAC address that is attempting to authenticate

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

service-type=Call Check

"

<-- This indicates a MAC filtering process

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

method=mab

"

<-- Controller sends an AVpair with MAB method

[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 26 "client-iif-id=1392509681"
[radius] [17558]: (info): RADIUS: Cisco AVpair [1] 14 "vlan-id=1000"
[radius] [17558]: (info): RADIUS: NAS-IP-Address [4] 6

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

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

cisco-wlan-ssid=cwa

"

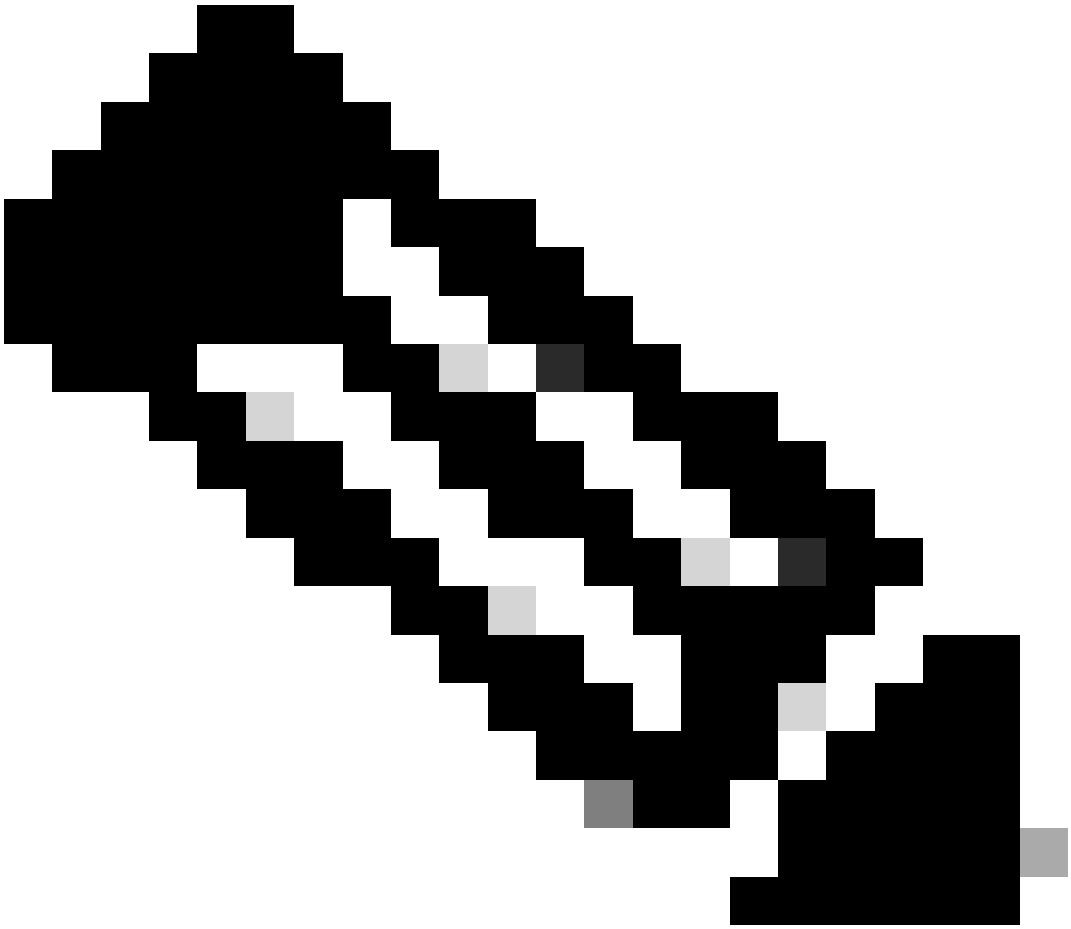
<-- SSID and WLAN the client is attempting to connect

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

wlan-profile-name=cwa

"
[radius] [17558]: (info): RADIUS: Called-Station-Id [30] 32 "dc-8c-37-d0-83-a0:cwa"
[radius] [17558]: (info): RADIUS: Calling-Station-Id [31] 19 "42-03-95-22-e6-82"
[radius] [17558]: (info): RADIUS: Airespace-WLAN-ID [1] 6 1

```
[radius] [17558]: (info): RADIUS: Nas-Identifier       [32]    9  "BC-9800"
[radius] [17558]: (info): RADIUS: Started 5 sec timeout
```



注意：AV对是ISE使用的“属性值”。它是可发送到WLC的预定义信息的Key-Value结构。这些值将应用于该特定会话的特定客户端。

AV对示例：

- ACL 名称
- Redirect URL
- VLAN分配
- 会话超时时间
- 重新身份验证计时器

ISE响应WLC请求

如果WLC发送的MAC地址被ISE接受，则ISE发送Access-Accept RADIUS数据包。根据ISE配置，如果它是未知MAC地址，ISE必须接受该地址并继续处理流量。如果显示Access-Reject，则表明在ISE上没有正确配置需要进行验证。

<#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

从ISE接收信息的WLC进程

WLC处理从ISE接收的所有信息。通过它，它将应用最初创建的用户配置文件与ISE发送的数据的用户配置文件。例如，WLC为用户分配新的ACL。如果在WLAN上未启用AAA Override，则不会发生WLC的此处理。

<#root>

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

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

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

url-redirect-acl 0 "cwa-acl"

>>

<-- Processing ACL redirection received from ISE

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

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

>>

<-- Processing URL redirection received from ISE

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

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

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

User profile is to be applied

. Authz mlist is not present,

Authc mlist cwa_authz

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

Received a request to create a CWA session

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

URL-Redirect-ACL = cwa-acl


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

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


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

User Profile applied



successfully

 for 0x92000002 -

REPLACE



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

MAB身份验证完成

成功修改客户端的用户配置文件后，WLC将完成验证客户端的MAC地址。如果从ISE接收的ACL不存在于WLC上，则WLC不知道如何处理该信息，因此REPLACE操作完全失败，从而也导致MAB身份验证失败。客户端无法进行身份验证。

<#root>

```
{wncd_x_R0-0}{1}: [mm-client] [17558]: (debug): MAC: 0000.0000.0000 Sending pmk_update of XID (0) to (M
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682

 MAB Authentication success

.
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi

S_AUTHIF_MAB_AUTH_DONE
```

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

CO_AUTH_STATUS_SUCCESS

WLC向客户端发送关联响应

现在，客户端已通过ISE的身份验证并已应用正确的ACL，WLC最终会向客户端发送关联响应。现在，用户可以继续连接到网络。

<#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身份验证

根据客户端在与WLAN关联时必须经历的过程，L2身份验证“开始”。但是，实际上，由于以前执行过MAB身份验证，因此已经执行了L2身份验证。客户端立即完成L2身份验证。

<#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

数据插拔

WLC向连接的客户端分配资源，以便流量可以通过网络传输。

<#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
```

为用户分配了IP地址

最终用户需要IP地址才能在网络中导航。它执行DHCP过程。如果用户之前已连接，并且记住了其IP地址，则会跳过DHCP过程。如果用户无法收到IP地址，则最终用户无法查看Web门户。否则，它将执行以下步骤：

1. DISCOVER数据包从连接的客户端以广播形式发送，以查找任何可用的DHCP服务器
2. 如果有可用的DHCP服务器，则DHCP服务器会以OFFER做出响应。该产品包含要分配给连接客户端的IP地址、租用时间等信息。可以从各种DHCP服务器收到许多OFFER
3. 客户端从其中一台服务器接受OFFER，并以REQUEST响应所选择的IP地址
4. 最后，DHCP服务器向客户端发送确认数据包，并分配新的IP地址

WLC记录客户端接收其IP地址的方法。

<#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身份验证开始

现在，最终用户已经收到IP地址，L3身份验证从检测到的所需身份验证方法的CWA开始。

<#root>

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17558]: (debug): MAC: 4203.9522.e682 Triggered L3 authentication. s
{wncd_x_R0-0}{1}: [client-orch-state] [17558]: (note): MAC: 4203.9522.e682 Client state transition: S_C
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682
```

L3 Authentication initiated. CWA

健全性IP地址测试

为了继续连接，客户端必须执行两个ARP请求：

1. 验证其他人没有其IP地址。如果存在最终用户IP地址的ARP应答，则它是重复的IP地址

2. 验证到网关的可达性。这是为了确保客户端可以离开网络。ARP应答必须来自网关

<#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 So

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 So

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 So

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 So

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 So

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 So

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

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

ARP REQUEST,

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP ta
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S

ARP REQUEST,

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

ARP REQUEST,

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 4203.9522.e682 ARP sender IP: <dhcp-server-ip-addr>, AR
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

REPLY,

ARP sender MAC: dca6.32d2.e93f ARP target MAC: 4203.9522.e682 ARP sender IP: <dhcp-server-ip-addr>, AR
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S

ARP REQUEST,

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

ARP REQUEST,

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 64cc.2284.ae10 ARP target MAC: 4203.9522.e682 ARP sender IP: <default-gateway-ip-addr>
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S

ARP REQUEST,

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

ARP REQUEST,

ARP sender MAC: 4203.9522.e682 ARP target MAC: 0000.0000.0000 ARP sender IP: <end-user-ip-addr>, ARP t
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 000c.290e.1c37 ARP target MAC: 4203.9522.e682 ARP sender IP: 10.20.30.17, ARP target I
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REPLY,

ARP sender MAC: 000c.290e.1c37 ARP target MAC: 4203.9522.e682 ARP sender IP: 10.20.30.17, ARP target I
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

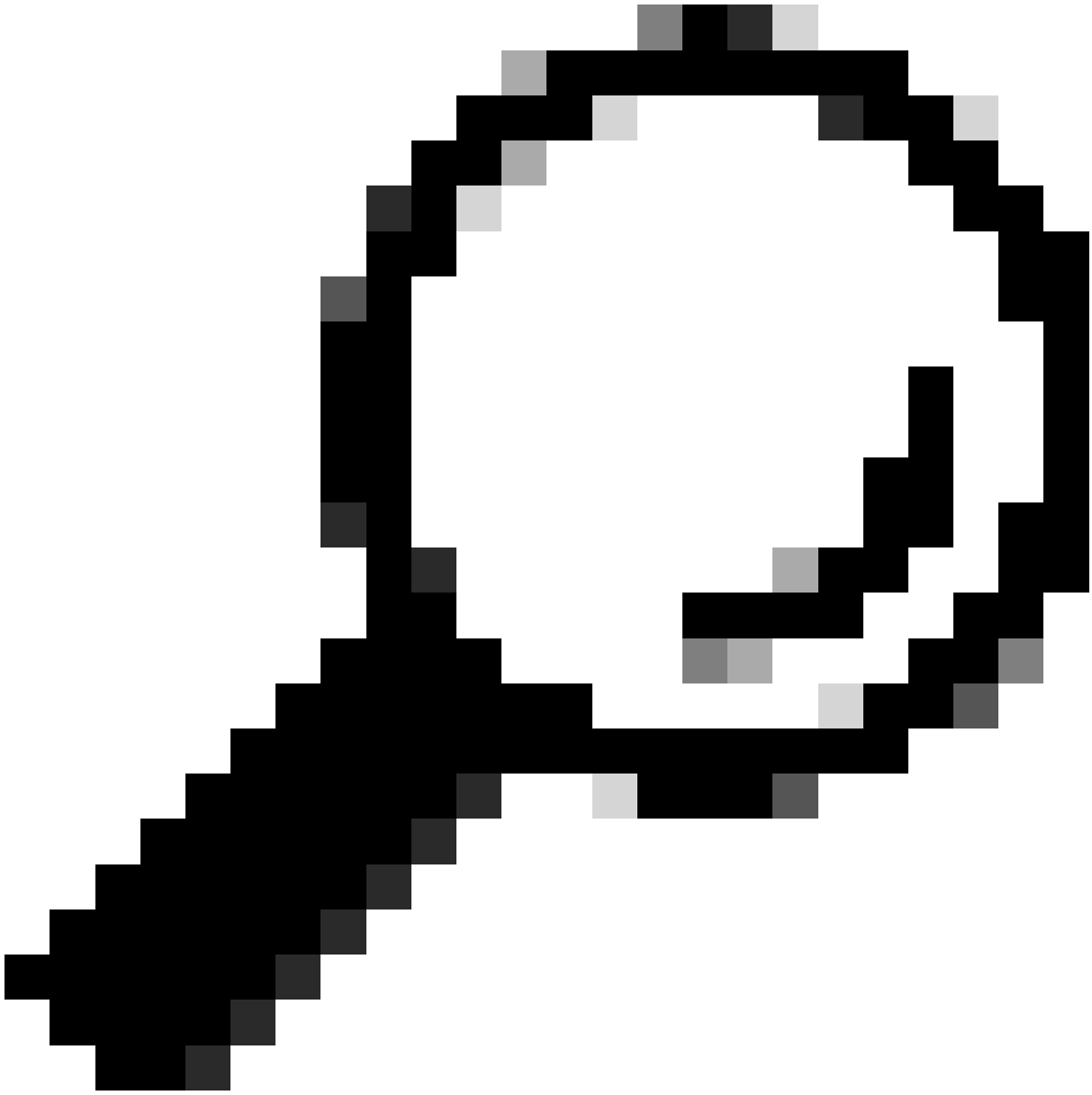
```
ARP REQUEST,

 ARP sender MAC: dca6.32d2.e93f ARP target MAC: 0000.0000.0000 ARP sender IP: <dhcp-server-ip-addr>, AR
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface Tw0/0/0 on vlan 1000 Source MA

ARP REQUEST,

 ARP sender MAC: dca6.32d2.e93f ARP target MAC: 0000.0000.0000 ARP sender IP: <dhcp-server-ip-addr>, AR
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): RX: ARP from interface capwap_90000005 on vlan 1000 S

ARP REPLY,

 ARP sender MAC: 4203.9522.e682 ARP target MAC: dca6.32d2.e93f ARP sender IP: <end-user-ip-addr>, ARP t
{wncd_x_R0-0}{1}: [sisf-packet] [17558]: (debug): TX: ARP from interface capwap_90000005 on vlan 1000 S

ARP REPLY,

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

第二个连接：客户端到网络

此时，最终用户已经通过ISE的MAC地址进行了身份验证，但尚未获得完全授权。WLC必须再次引用ISE以授权客户端连接到网络。此时，门户会呈现给用户，用户必须在其中输入其用户名和密码。在WLC上，最终用户显示为“Web Auth Pending”状态。

授权变更(CoA)

WLC配置中的“CoA支持”在此处生效。在此之前，一直使用该ACL。在终端客户端看到门户后，不再使用ACL，因为仅将客户端重定向到门户。此时，客户端输入其登录凭证，以启动CoA过程并重新验证客户端。WLC准备要发送的数据包并将其转发到ISE



提示：CoA使用端口1700。确保它未被防火墙阻止。

<#root>

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

Processing CoA request

under CH-ctx.

<-- ISE requests the client to reauthenticate

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

MAB re-authentication started

for 2315255810 (4203.9522.e682)

<-- ISE requests the WLC to reauthenciate the CoA

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

CoA Response Details

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

Success

]>>

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

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

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

ISE的第二次身份验证

第二个身份验证不是从零开始。这是CoA的力量。可以对用户应用新规则和/或AV paris。在第一个Access-Accept上收到的ACL和重定向URL将不再推送到最终用户。

WLC向ISE发送请求

WLC使用输入的用户名/密码组合，向ISE发送新的RADIUSAccess-Requestpacket。这将触发新的MAB身份验证，并且由于ISE已经知道客户端，将应用新的策略集（例如，授予访问权限）。

<#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响应WLC请求

ISE会查找其策略，如果收到的用户名与策略配置文件匹配，则ISE会再次响应WLC，接受与WLAN的客户端连接。返回最终用户的用户名。如果在ISE上配置，可以将其他规则和/或AV对应用于用户，这些规则和/或AV对可以在Access-Accept中看到。

<#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

从ISE接收信息的WLC进程

WLC再次处理ISE接收的信息。它使用从ISE接收的新值对用户执行另一REPLACE操作。

<#root>

[aaa-attr-inf] [17558]: (info):

<< username 0 "cwa-username">> <-- Processing username received from ISE

{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< class 0 43 41 43 53 3a 30 45 31 45 31 34 30 41 30 30 30 30 30 30 30 43 38 45 32 44 41 36 34 32 3a 62
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<<Message-Authenticator 0 <hidden>>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< dnis 0 "DC-8C-37-D0-83-A0">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< formatted-clid 0 "42-03-95-22-E6-82">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< audit-session-id 0 "0E1E140A0000000C8E2DA642">>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< method 0 2 [mab]>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< clid-mac-addr 0 42 03 95 22 e6 82 >>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info):
<< intf-id 0 2415919109 (0x90000005)>>
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005] auth mgr attr change not
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]

Received User-Name cwa-username

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

User profile is to be applied.

Authz mlist is not present,

Authc mlist cwa_authz

,session push flag is unset
{wncd_x_R0-0}{1}: [auth-mgr] [17558]: (info): [4203.9522.e682:capwap_90000005]

User Profile applied

successfully

for 0x92000002 -

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

L3身份验证完成

最终用户现在已使用给定数据进行身份验证。L3身份验证（Web身份验证）完成。

<#root>

```
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682

 L3 Authentication Successful

. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [17558]: (info): MAC: 4203.9522.e682 Client auth-interface state transi

 S_AUTHIF_WEBAUTH_DONE


{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS add mobile cb
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 No QoS PM Name or QoS Level re
{wncd_x_R0-0}{1}: [client-auth] [17558]: (note): MAC: 4203.9522.e682 ADD MOBILE sent. Client state flag
{wncd_x_R0-0}{1}: [errmsg] [17558]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entr

cwa-username

) joined with ssid (

cwa

) for device with MAC: 4203.9522.e682 <-- End user "cwa-username" has joined the WLAN "cwa"
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute :               username 0 "

cwa-username

" ]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute :                  class 0 43 41
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute :bsn-vlan-interface-name 0 "MGMT"
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17558]: (info): [ Applied attribute : timeout 0 1800 (0x708) ]
{wncd_x_R0-0}{1}: [ewlc-qos-client] [17558]: (info): MAC: 4203.9522.e682 Client QoS run state handler
```

最终用户在WLC上达到运行状态

最后，对用户进行身份验证并将其与WLAN相关联。

<#root>

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

Managed client RUN state

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

 S_CO_RUN
```

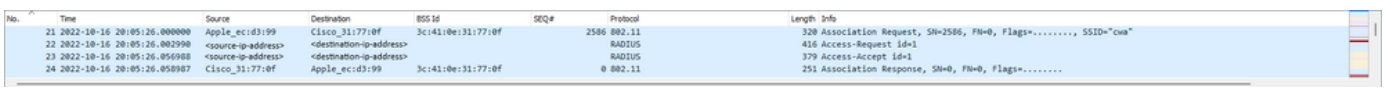
CWA流程-嵌入式数据包捕获(EPC)

EPC是可直接从WLC检索的数据包捕获，显示所有通过WLC或来自该WLC的数据包。有关它们是什么以及如何检索它们的详细信息，请访问[了解Catalyst 9800无线LAN控制器上的无线调试和日志收集。]

第一个连接：客户端到ISE服务器

警告：数据包捕获映像上的IP地址已被删除。它们显示为和

与WLAN的关联和发送到ISE服务器的请求

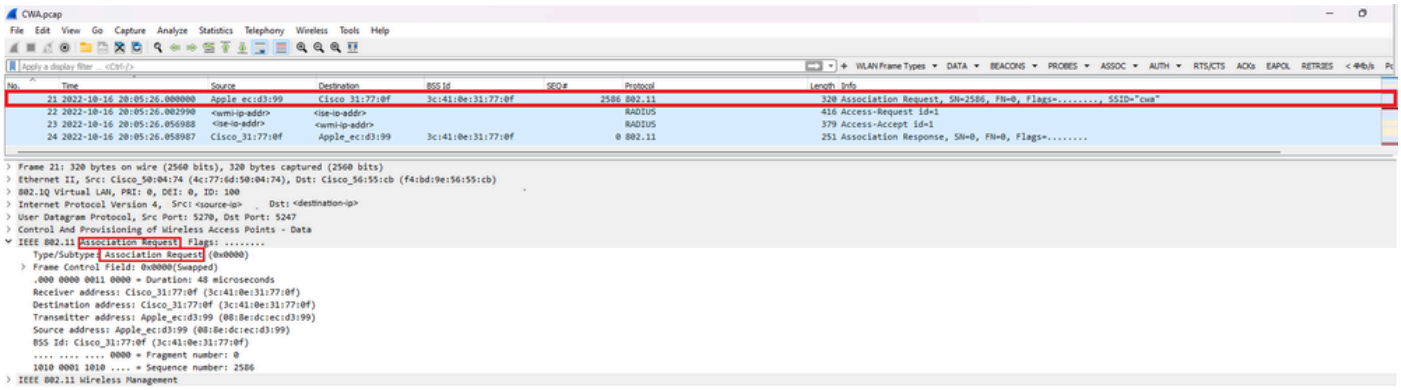


No.	Time	Source	Destination	BSS Id	SEQ#	Protocol	Length	Info
21	2022-10-16 20:05:26.000000	Apple_ec:d3:99	Cisco_31:77:0f	3c:41:0e:31:77:0f	2586	802.11	320	Association Request, SN=2586, FN=0, Flags=........, SSID="cwa"
22	2022-10-16 20:05:26.002990	<source-ip-address>	<destination-ip-address>			RADIUS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

第一个数据包

从WLC到客户端的关联请求

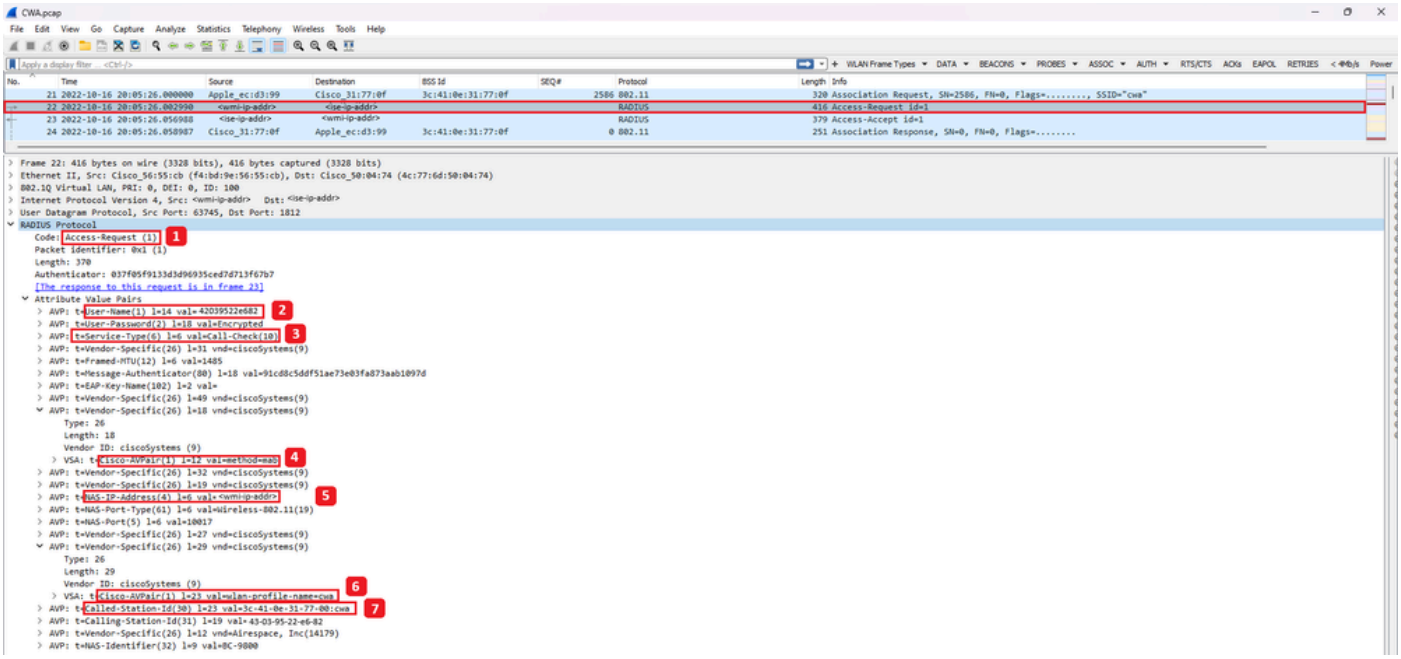
查看第一个数据包“关联请求”，您可以看到此过程中涉及的设备的MAC地址。



关联请求

从WLC发送到ISE的访问请求数据包

WLC处理关联请求后，会向ISE服务器发送Access-Request数据包。

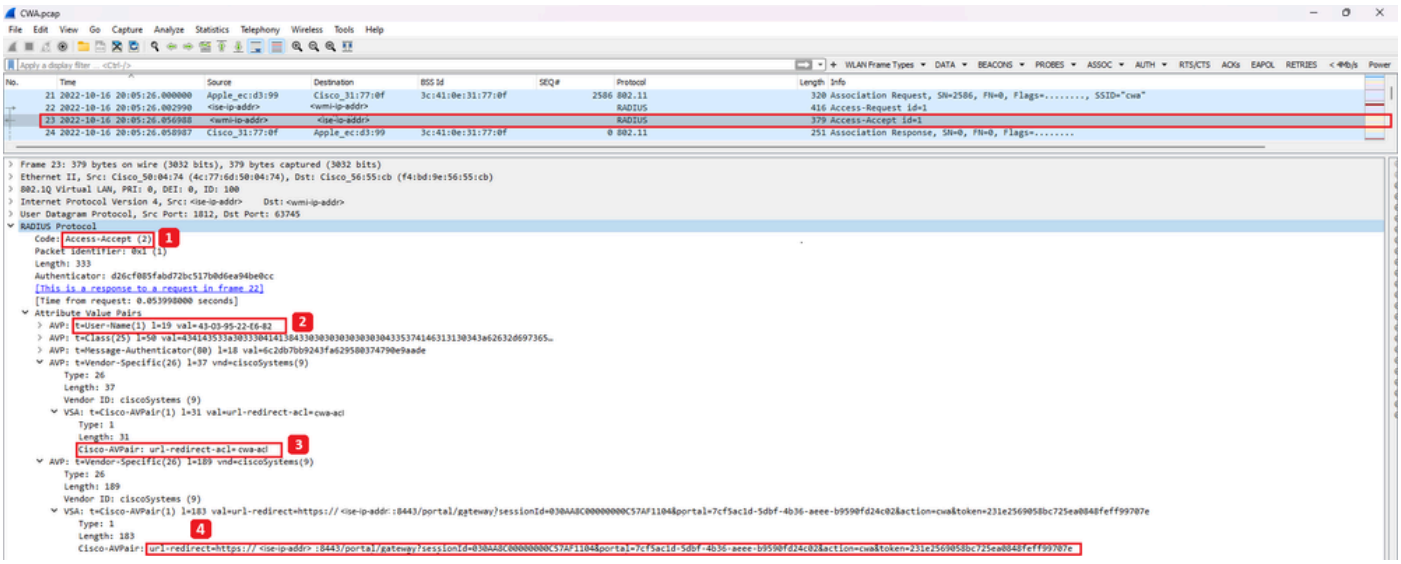


接入请求数据包分析

1. 数据包的名称。
2. 尝试进行身份验证的MAC地址。
3. 这表示MAC过滤。
4. 控制器发送到ISE以指示MAC过滤过程的AV对。
5. WLC的WMI IP地址。
6. 客户端尝试连接的SSID。
7. 客户端尝试连接的WLAN的名称。

从WLC发送到ISE的Access-Accept数据包

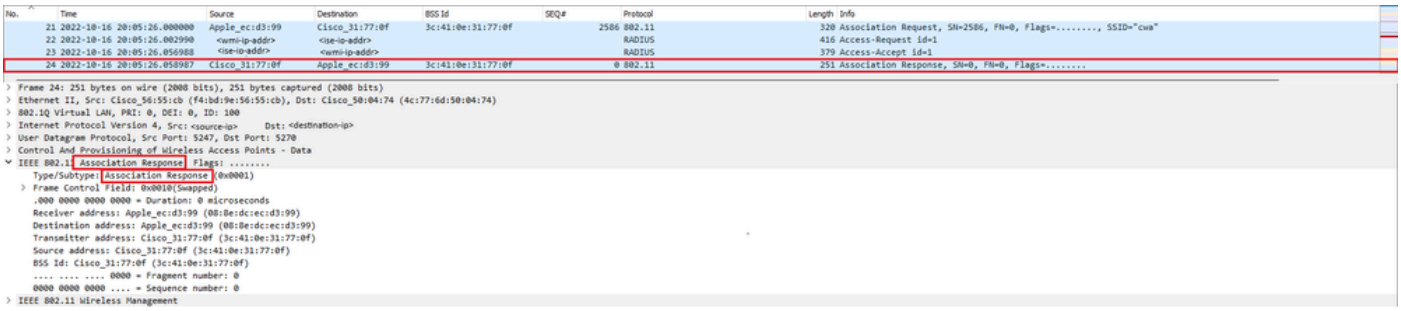
一旦ISE处理了Access-Accept数据包，它将以Access-Accept做出响应（如果成功）或Access-Reject（如果失败）。



Access-Accept数据包分析

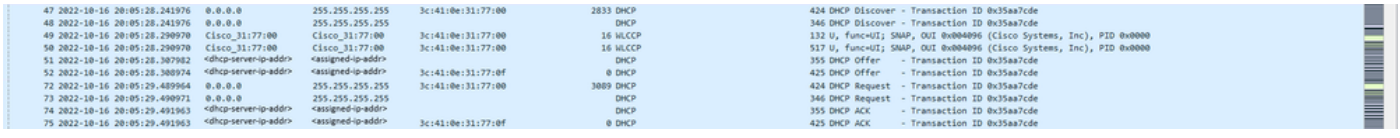
1. 数据包的名称。
2. 经过身份验证的MAC地址。
3. 要应用的ACL。
4. 要将用户重定向到的URL。

从WLC到客户端的关联响应

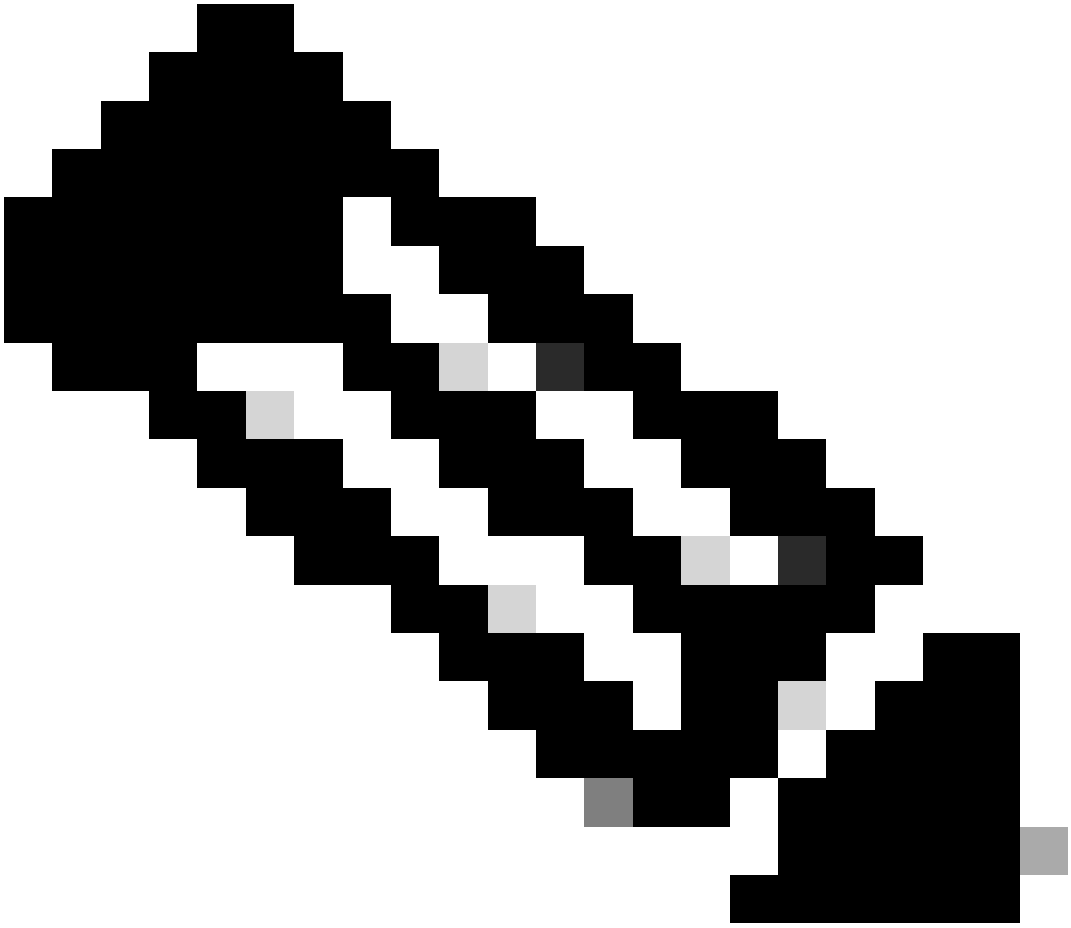


关联响应

DHCP过程



DHCP过程



注意：从现在开始，数据包将被重复，但这只是因为其中一个数据包是CAPWAP封装的，而另一个不是

ARP

78	2022-10-16 20:05:29.496968	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	3345 ARP	124 Who has <assigned-ip-addr> (ARP Probe)
79	2022-10-16 20:05:29.496968	Apple_ec:d3:99	Broadcast		ARP	60 Who has <assigned-ip-addr> (ARP Probe)
80	2022-10-16 20:05:29.847948	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	3601 ARP	124 Who has <assigned-ip-addr> (ARP Probe)
81	2022-10-16 20:05:29.847948	Apple_ec:d3:99	Broadcast		ARP	60 Who has <assigned-ip-addr> (ARP Probe)
82	2022-10-16 20:05:30.142982	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	3857 ARP	124 Who has <assigned-ip-addr> (ARP Probe)
83	2022-10-16 20:05:30.142982	Apple_ec:d3:99	Broadcast		ARP	60 Who has <assigned-ip-addr> (ARP Probe)
84	2022-10-16 20:05:30.464972	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	17 ARP	124 ARP Announcement for <assigned-ip-addr>
85	2022-10-16 20:05:30.465964	Apple_ec:d3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
88	2022-10-16 20:05:30.790944	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	785 ARP	124 ARP Announcement for <assigned-ip-addr>
89	2022-10-16 20:05:30.790944	Apple_ec:d3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
90	2022-10-16 20:05:31.115991	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	1041 ARP	124 ARP Announcement for <assigned-ip-addr>
91	2022-10-16 20:05:31.116983	Apple_ec:d3:99	Broadcast		ARP	60 ARP Announcement for <assigned-ip-addr>
92	2022-10-16 20:05:31.117990	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	1297 ARP	124 Who has 192.168.20.1? Tell <assigned-ip-addr>
93	2022-10-16 20:05:31.117990	Apple_ec:d3:99	Broadcast		ARP	60 Who has 192.168.20.1? Tell <assigned-ip-addr>
94	2022-10-16 20:05:31.118981	Cisco_50:04:74	Apple_ec:d3:99		ARP	64 192.168.20.1 is at 4c:77:6d:50:04:74
95	2022-10-16 20:05:31.118981	Cisco_50:04:74	Apple_ec:d3:99	3c:41:0e:31:77:0f	0 ARP	134 192.168.20.1 is at 4c:77:6d:50:04:74
97	2022-10-16 20:05:31.192983	Apple_ec:d3:99	Broadcast	3c:41:0e:31:77:00	1809 ARP	124 Who has 192.168.20.1? Tell <assigned-ip-addr>
98	2022-10-16 20:05:31.193974	Apple_ec:d3:99	Broadcast		ARP	60 Who has 192.168.20.1? Tell <assigned-ip-addr>
99	2022-10-16 20:05:31.193974	Cisco_50:04:74	Apple_ec:d3:99		ARP	64 192.168.20.1 is at 4c:77:6d:50:04:74
100	2022-10-16 20:05:31.194981	Cisco_50:04:74	Apple_ec:d3:99	3c:41:0e:31:77:0f	0 ARP	134 192.168.20.1 is at 4c:77:6d:50:04:74

客户端ARP获取自己的IP地址和网关

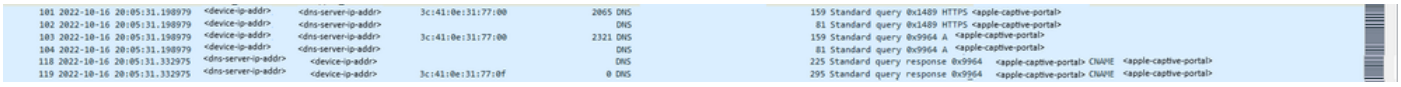
连通性测试

一旦ARP过程完成，尝试连接的设备就会执行检查以验证是否触发了门户，这也称为探测。如果设

备显示没有Internet连接，则表示ARP过程失败（例如，网关从未应答）或设备无法进行探测。

此探测功能在RA跟踪上不可见，只有EPC能够提供此信息。探测查询取决于尝试连接的设备，在本示例中，测试设备是Apple设备，因此探测直接指向Apple的强制网络门户。

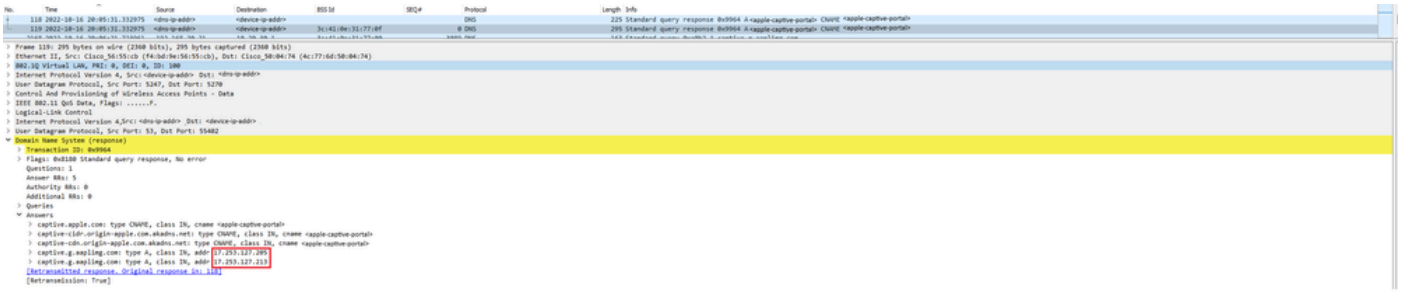
当使用URL进行探测时，需要DNS来解决此URL。因此，如果DNS服务器无法响应客户端的查询，则客户端会继续查询该URL，并且不会看到门户。此时，如果在终端设备Web浏览器上输入ISE服务器的IP地址，门户必须可见。如果是，则DNS服务器存在问题。



来自客户端的连接测试- DNS查询和应答

DNS解析IP地址

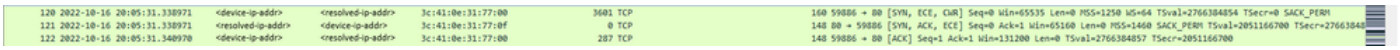
检查DNS查询响应时，您可以看到DNS服务器解析的IP地址。



DNS服务器解析的IP地址

建立三次握手

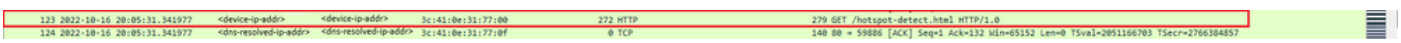
现在，DNS IP地址已经解析，在门户和客户端之间建立TCP三次握手。使用的IP地址是解析的任一IP地址。



三次握手建立

获取热点

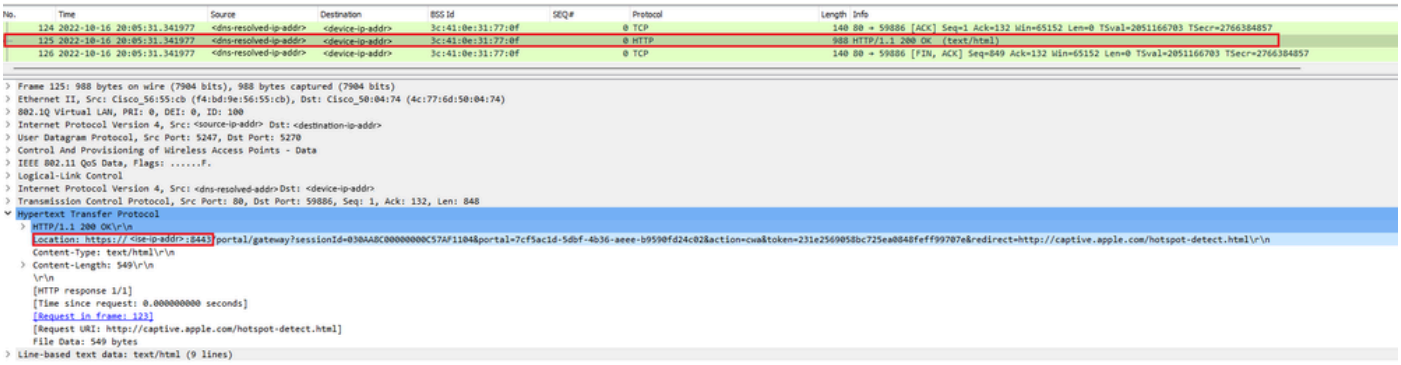
一旦TCP会话建立，客户端就会执行探测并尝试访问门户。



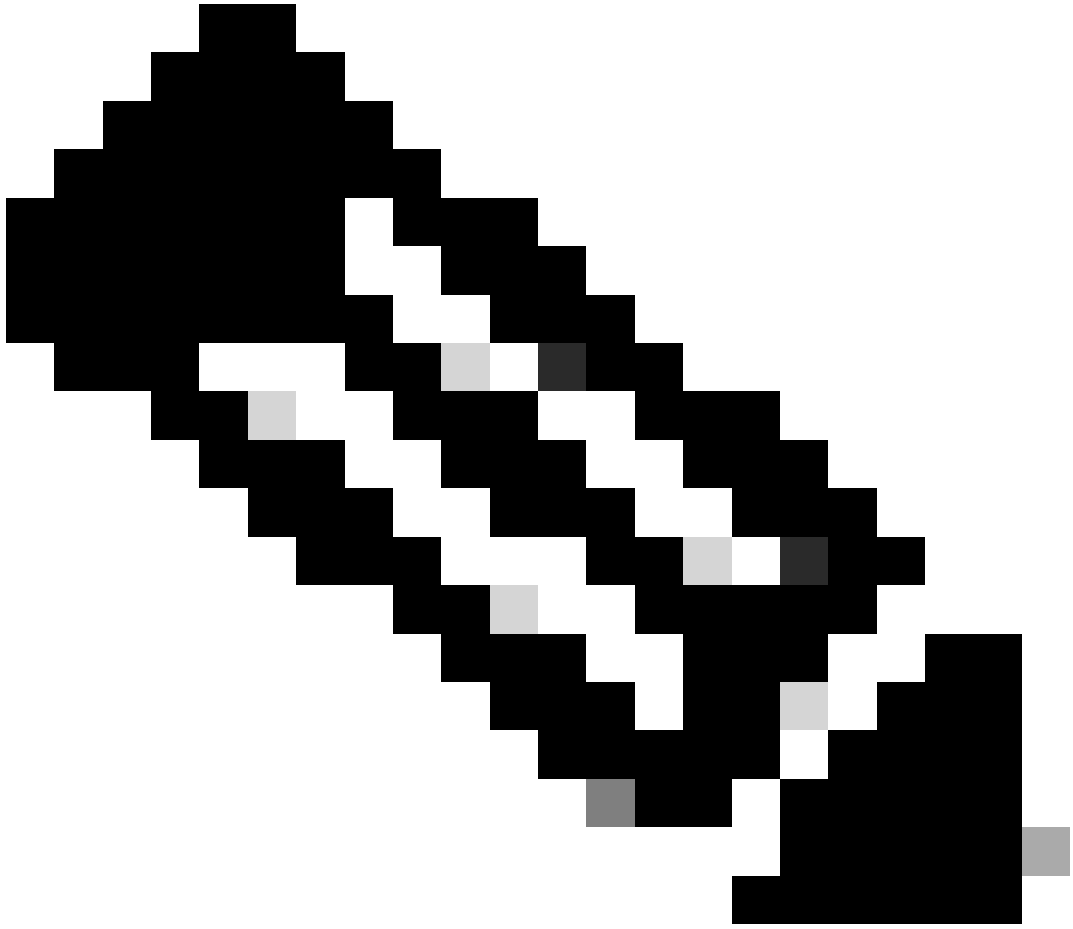
获取热点

正常数据包

OK数据包包含客户端必须重定向到的ISE门户。



正常数据包

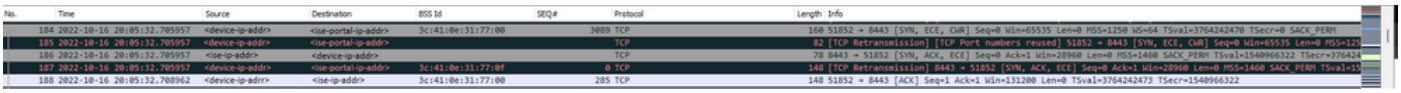


> 注意：大多数人在OK数据包中还返回了另一个URL。因此，需要执行另一个DNS查询以获取最终的IP地址。

已建立新的TCP会话

由于已经发现门户的IP地址，因此会交换许多数据包，但最终在OK数据包（或由DNS解析）中返回

的目标IP与ISE的IP地址对应的数据包显示正在建立到门户的新TCP会话。



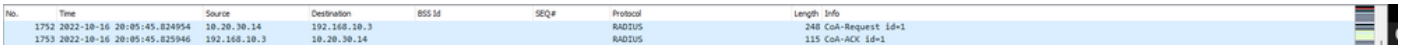
与ISE门户的第二个连接和新TCP会话

向用户显示门户

此时，ISE的门户最终显示在客户端浏览器的浏览器上。与以前一样，ISE和设备之间交换了许多数据包；例如客户端hello和服务器hello等等。在这里，ISE会要求客户端提供用户名和密码、接受条款和条件或在ISE服务器上配置的任何内容。

CoA请求/CoA确认

用户输入所有请求的数据后，ISE会向控制器发送CoA请求以更改用户的授权。如果WLC上的所有内容都已按预期进行配置（例如具有NAC状态、支持CoA等），则WLC将发送CoA确认(CoA ACK)。否则，WLC可能发送CoA非确认(CoA NACK)，或者只是不发送CoA ACK。

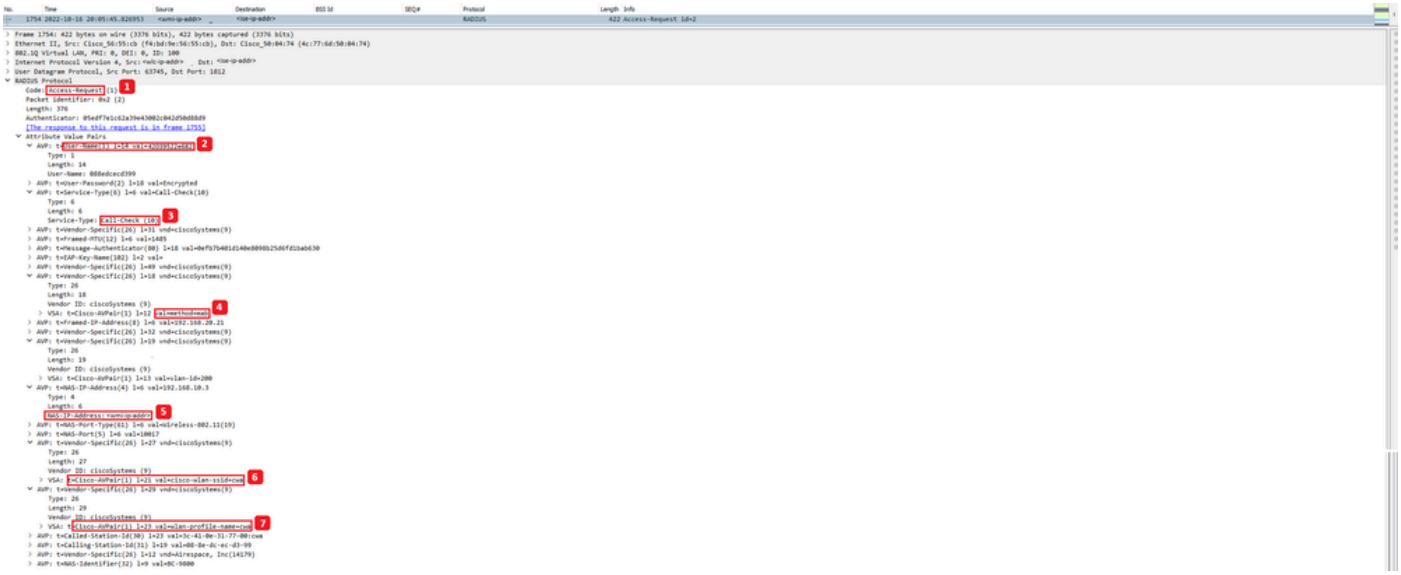


CoA请求和确认

第二个连接：客户端到网络

新访问请求

WLC向ISE发送新的访问请求数据包。



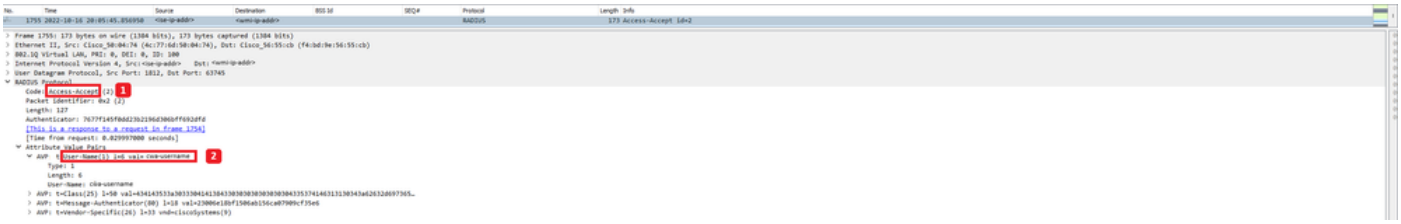
分析新的访问请求数据包

1. 数据包的名称。
2. 尝试进行身份验证的MAC地址。
3. 这表示MAC过滤。

4. 控制器发送到ISE以指示MAC过滤过程的AV对。
5. WLC的WMI IP地址。
6. 客户端尝试连接的SSID。
7. 客户端尝试连接的WLAN的名称。

New Access-Accept

WLC向ISE发送新的访问请求数据包。



分析新的Access-Accept数据包

1. 数据包的名称。
2. 终端客户端在显示的门户上输入的用户名。

同样，从客户端进行新的探测连接测试。一旦客户端确认它具有Internet连接，即可关闭门户（根据使用的设备，可以自动关闭门户）。客户端现在已连接到网络。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。