

Comprensión del flujo de tráfico en la configuración de anclaje externo entre el WLC 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción general del escenario de anclaje externo](#)

[Topología](#)

[WLAN con autenticación de capa 2](#)

[Requisito de configuración](#)

[Flujo para SSID basado en anclaje externo de capa 2](#)

[Análisis del Flujo de SSID de Capa 2 en la Configuración de Anclaje Externo a través de Registros](#)

[Registros de controlador externo](#)

[Registros del controlador Anchor 9800](#)

[Estado del cliente en el controlador externo y de anclaje](#)

[WLAN con autenticación de capa 3](#)

[Autenticación web local](#)

[Flujo para SSID de Webauth local en la configuración de anclaje externo](#)

[Análisis del Flujo SSID de Webauth Local en la Configuración de Anclaje Externo a través de Registros](#)

[Registros de controlador externo](#)

[Registros del controlador de anclaje](#)

[Estado del cliente en el controlador externo y de anclaje](#)

[Autenticación web central](#)

[Flujo para SSID de Webauth central en la configuración de anclaje externo](#)

[Análisis del Flujo SSID de Webauth Central en la Configuración de Anclaje Externo a través de Registros](#)

[Registros de controlador externo](#)

[Registros del controlador de anclaje](#)

[Estado del cliente en el controlador externo y de anclaje](#)

[Autenticación web externa](#)

[Flujo para SSID de Webauth externo en la configuración de anclaje externo](#)

[Análisis del Flujo SSID de Webauth Externo en la Configuración de Anclaje Externo a través de Registros](#)

[Registros de controlador externo](#)

[Registros del controlador de anclaje](#)

[Estado del cliente en el controlador externo y de anclaje](#)

[Equilibrio de carga entre varios controladores de anclaje](#)

[Resolución de problemas de conectividad del cliente en escenario de anclaje externo](#)

[Recopilación de registros del controlador externo y de anclaje](#)

Introducción

Este documento describe el flujo de tráfico en la configuración de anclaje externo entre los WLC de Cisco 9800, que cubre la incorporación de clientes L2/L3 y la resolución de problemas.

Prerequisites

Túnel de movilidad entre controlador externo y de anclaje.

Puerto UDP 16666 y 16667 permitidos entre ambos el WLC.

Perfil de política configurado para Central Switching.

Configuration > Wireless > Mobility

Global ConfigurationPeer Configuration

Mobility Peer Configuration

+ Add

× Delete

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
		10.105.60.114	N/A	DMZ	0.0.0.0	::	N/A	N/A	4c7d85dca2ff501a8bf7965fbac811ef66760fa3	N/A
☐		10.107.79.30	10.107.79.30	Bangalore_Site	0.0.0.0	::	Up	1006		Disabled

1

10

1 - 2 of 2 items

Estado del túnel de movilidad en el WLC externo

Configuration > Wireless > Mobility

Global ConfigurationPeer Configuration

Mobility Peer Configuration

+ Add

× Delete

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
		10.105.60.114	N/A	DMZ	0.0.0.0	::	N/A	N/A	4c7d85dca2ff501a8bf7965fbac811ef66760fa3	N/A
☐		10.107.79.30	10.107.79.30	Bangalore_Site	0.0.0.0	::	Up	1006		Disabled

1

10

1 - 2 of 2 items

Estado del túnel de movilidad en el WLC de anclaje

Requirements

Cisco recomienda que conozca estos temas:

- Acceso mediante interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) a los controladores inalámbricos
- Movilidad en los controladores de LAN inalámbrica (WLC) de Cisco
- Controladores inalámbricos 9800
- Rastreo de paquetes y captura de paquetes en el WLC 9800

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Modelo 9800 WLC
- Cisco IOS XE versión 17.15.5
- Modelo AP serie 9100

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

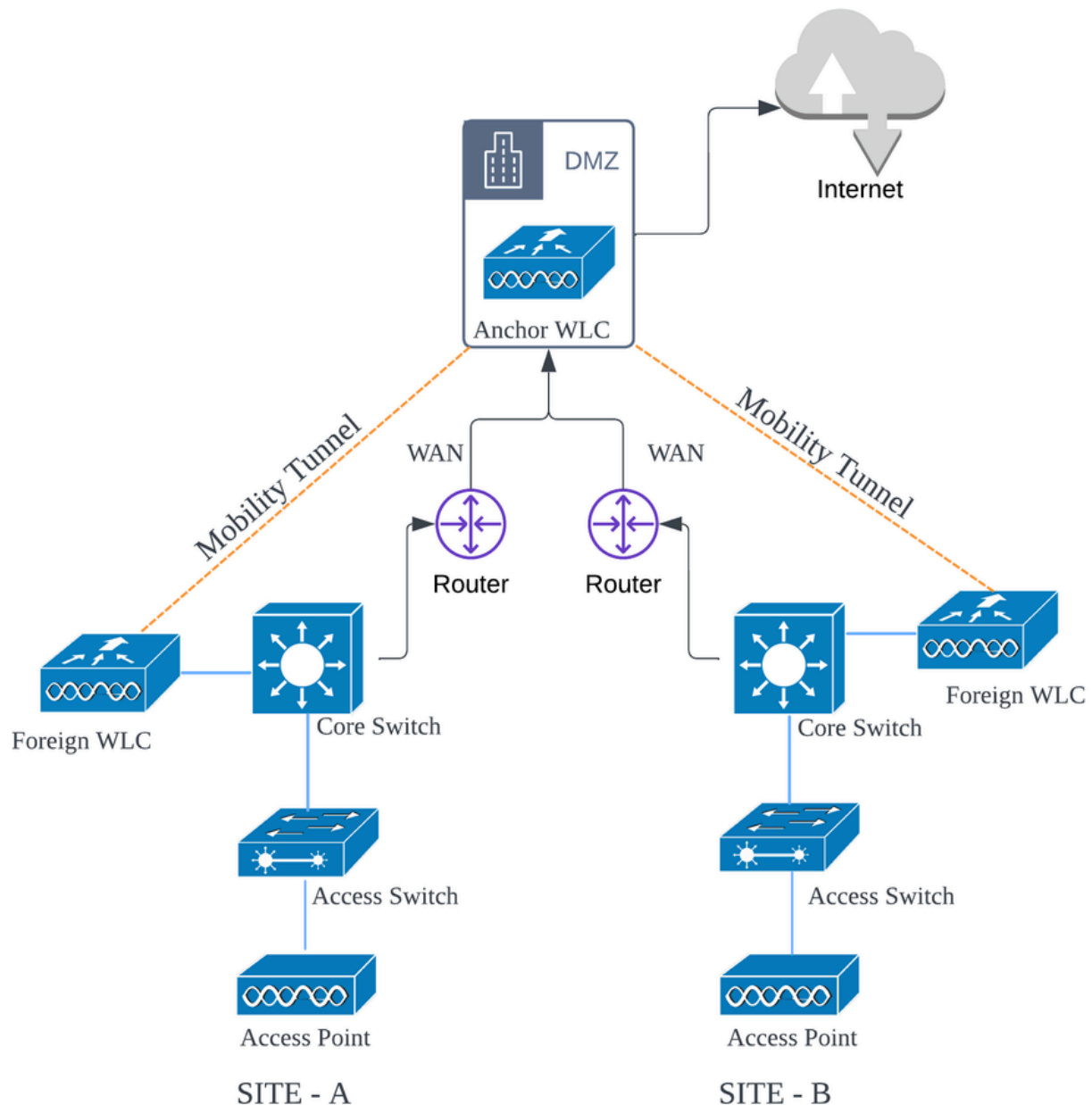
Descripción general del escenario de anclaje externo

- Controlador externo: Este WLC administra la capa 2 o el lado inalámbrico de la red. Tiene puntos de acceso conectados y todo el tráfico de cliente para las WLAN ancladas se encapsula en el túnel de movilidad y se envía al controlador de anclaje. El tráfico no sale localmente en el controlador externo.
- Controlador de anclaje: Sirve como punto de salida de la capa 3. Recibe el tráfico del cliente a través del túnel de movilidad de los controladores externos y desencapsula o termina el tráfico del cliente en el punto de salida (VLAN). Aquí es donde se ven los clientes en la red.

Los puntos de acceso en el WLC externo difunden los SSID de WLAN y tienen una etiqueta de política asignada que enlaza el perfil WLAN con el perfil de política apropiado. Cuando un cliente inalámbrico se conecta a este SSID, el controlador externo envía el nombre SSID y el perfil de política como parte de la información del cliente al WLC de anclaje. Al recibir, el WLC de anclaje verifica su propia configuración para que coincida con el nombre SSID así como el nombre del perfil de política. Una vez que el WLC de anclaje encuentra una coincidencia, aplica la

configuración correspondiente y proporciona un punto de salida para el cliente inalámbrico. Por lo tanto, es obligatorio que los nombres y las configuraciones del perfil de la WLAN y de la política coincidan en los WLCs Foreign y Anchor 9800, con la excepción de la VLAN bajo el perfil de la política.

Topología



Configuración de anclaje externo entre 9800 WLC

WLAN con autenticación de capa 2

Requisito de configuración

1. Asegúrese de que el nombre WLAN y la configuración sean idénticos en los WLCs Foreign y Anchor y que esté configurado para la autenticación de capa 2 (PSK o 802.1x).
2. Cree un perfil de política con el mismo nombre en el WLC externo y de anclaje con la misma configuración.
3. En el WLC externo, configure la asignación de WLC de anclaje dentro del perfil de política respectivo.
4. En el WLC de anclaje, configure el perfil de política para designar al controlador como anclaje de exportación.
5. En el WLC externo, asigne la WLAN al perfil de política apropiado usando una etiqueta de política.

Flujo para SSID basado en anclaje externo de capa 2

1. El cliente inicia una conexión con el SSID transmitido por el WLC extranjero. El WLC externo realiza la autenticación de la capa 2, validando las credenciales localmente o a través de un servidor AAA externo, dependiendo de la política de seguridad configurada.
2. Tras la autenticación exitosa, la sesión del cliente se ancla al WLC de anclaje. Al cliente se le asigna una dirección IP y pasa al estado RUN en el WLC de anclaje.
3. Una vez que se establece la sesión, todo el tráfico de datos del cliente se tuneliza desde el WLC externo al WLC de anclaje, donde se egresa a la red.

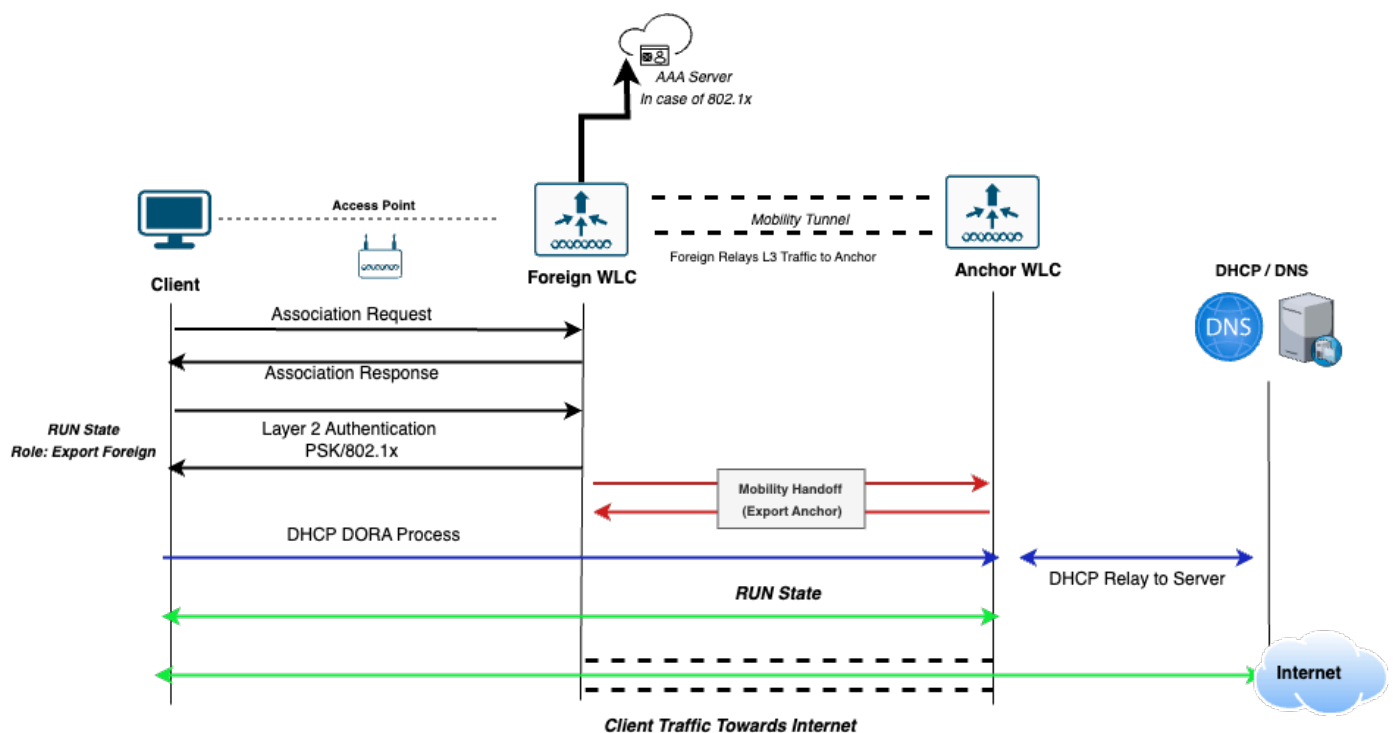


Diagrama de flujo WLAN basado en anclaje externo de capa 2

Análisis del Flujo de SSID de Capa 2 en la Configuración de Anclaje Externo a través de Registros

En esta sección se explica el flujo de conectividad de cliente de capa 2 mediante el uso de seguimiento radioactivo (seguimiento de RA), capturas de paquetes incrustadas (EPC) y el estado del cliente en los controladores externos y de anclaje.

Registros de controlador externo

Trazas radiactivas

!! Client Association started !!

```
[client-orch-sm] Association received. BSSID BSSID-addr, WLAN DMZ_PSK, Slot 1 AP AP_MAC, AP_NAME, Site  
[dot11] [17047] (info) MAC Client-MAC dot11 send association response. Sending assoc response of length  
[dot11] [17047] (info) MAC Client-MAC DOT11 state transition S_DOT11_INIT -> S_DOT11_ASSOCIATED
```

!! Layer 2 Authentication started !!

```
[client-orch-state] Client state transition S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS  
[client-auth] L2 Authentication initiated. method PSK, Policy VLAN 31, AAA override = 0, NAC = 0  
[client-keymgmt] EAP key M1 Sent successfully  
[client-keymgmt] M2 Status EAP key M2 validation success  
[client-keymgmt] EAP key M3 Sent successfully  
[client-keymgmt] M4 Status EAP key M4 validation is successful  
[client-keymgmt] EAP Key management successful. AKMP SK Cipher CCMP WPA Version WPA2 >> !! client successf
```

!! Mobility Handoff !!

```
[mobilityd_R0-0]{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gr  
[mobilityd_R0-0]{1} [mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP [mobilityd_R0-0]{1} [mm-client] [1  
[mobilityd_R0-0]{1} [mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P  
[wncd_x_R0-0]{1} [mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o  
[wncd_x_R0-0]{1} [mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_ANN  
[wncd_x_R0-0]{1} [mm-client] [17047] (debug) MAC Client-MAC Sending export_anchor_req of XID (XID) to (I  
[mobilityd_R0-0]{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_anchor_req, sub type 0 o  
[mobilityd_R0-0]{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE  
[mobilityd_R0-0]{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce  
[mobilityd_R0-0]{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_anchor_req of XID (176282  
[mobilityd_R0-0]{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_anchor_rsp, sub type 0 o  
[mobilityd_R0-0]{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS  
[mobilityd_R0-0]{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc  
[wncd_x_R0-0]{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed [mm-client] [17047] (info) MAC  
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF  
[wncd_x_R0-0]{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_C
```

```
[wncd_x_R0-0]{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEA  
[wncd_x_R0-0]{1} [client-orch-sm] [17047] (debug) MAC Client-MAC Received ip_learn response. method IP
```

```
[wncd_x_R0-0]{1} [client-orch-state] Client state transition S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN >> C
```

Captura de paquete

El cliente envía una solicitud de asociación y realiza la autenticación de la capa 2, gestionada por el controlador externo.

Time	Source Address	Destination Address	Length	Protocol	TID	Info
417	07:36:34.347973	10.107.79.129	272	802.11		Association Request, SN=1680, FN=0, Flags=...R..., SSID="DMZ_PSK"
418	07:36:34.347973	10.107.79.129	268	802.11		Association Request, SN=1680, FN=0, Flags=...R..., SSID="DMZ_PSK"
419	07:36:34.348980	10.107.79.30	211	802.11		Association Response, SN=0, FN=0, Flags=.....
420	07:36:34.348980	10.107.79.30	215	802.11		Association Response, SN=0, FN=0, Flags=.....
421	07:36:34.350979	10.107.79.129	110	LLC		0 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more commo
426	07:36:34.354977	10.107.79.30	203	EAPOL		Key (Message 1 of 4)
427	07:36:34.354977	10.107.79.129	207	EAPOL		Key (Message 1 of 4)
428	07:36:34.360973	10.107.79.129	217	EAPOL		0 Key (Message 2 of 4)
429	07:36:34.361980	10.107.79.30	213	EAPOL		0 Key (Message 2 of 4)
430	07:36:34.361980	10.107.79.30	237	EAPOL		Key (Message 3 of 4)
431	07:36:34.361980	10.107.79.129	241	EAPOL		Key (Message 3 of 4)
432	07:36:34.368968	10.107.79.129	195	EAPOL		0 Key (Message 4 of 4)
433	07:36:34.368968	10.107.79.129	191	EAPOL		0 Key (Message 4 of 4)

Asociación de clientes + tráfico de autenticación de capa 2

Un traspaso de movilidad se dispara entre los controladores externos y de anclaje a través del puerto UDP 16667. Tras un evento de movilidad exitoso, el estado del cliente pasa a EJECUTARSE con una función Externa de exportación.

El controlador externo recibe el tráfico DHCP del cliente a través del túnel CAPWAP y lo reenvía al controlador de anclaje para su procesamiento posterior.

Time	Source Address	Destination Address	Length	Protocol	TID	Info
567	07:36:39.071987	10.107.79.129,0.0.0.0	424	DHCP		0 DHCP Discover - Transaction ID 0x9f36b979
568	07:36:39.071987	10.107.79.30	400	UDP		16667 → 16667 Len=354
752	07:36:41.074993	10.105.60.114	400	UDP		16667 → 16667 Len=354
753	07:36:41.074993	10.107.79.30,10.105.60.69	416	DHCP		0 DHCP Offer - Transaction ID 0x9f36b979
758	07:36:41.111993	10.107.79.129,0.0.0.0	452	DHCP		0 DHCP Request - Transaction ID 0x9f36b979
759	07:36:41.111993	10.105.60.114	428	UDP		16667 → 16667 Len=382
760	07:36:41.113992	10.105.60.114	400	UDP		16667 → 16667 Len=354
761	07:36:41.113992	10.107.79.30,10.105.60.69	416	DHCP		0 DHCP ACK - Transaction ID 0x9f36b979

El tráfico DHCP del cliente recibido en el controlador externo se reenvía al controlador de anclaje mediante el túnel de movilidad

Registros del controlador Anchor 9800

Rastreo de radiactivos desde ancla

!! Mobility Handoff !!

```
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 of
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Number of client is BELOW wlan limit
{mobilityd_R0-0}{1} [mm-transition] [26021] (info) MAC Client-MAC MMFSM transition S_MC_INIT -> S_MC_An
□{wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Roam type changed - None -> L3 Requested
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.
{□wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.>> Client is successf
```

!! Client DHCP Traffic !!

```
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILIT
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_P
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
```

{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [client-iplearn] [24229] (note) MAC Client-MAC Client IP learn successful. Method DHCP
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Sending ipv4_address_update of XID (XID)
{wncd_x_R0-0}{1} [client-iplearn] [24229] (info) MAC Client-MAC IP-learn state transition S_IPLEARN_IN_
Complete

{wncd_x_R0-0}{1} [avc-afc] [24229] (info) ReAnchor [client MAC Client-MAC] Client has Anchor role {wncd_x_R0-0}{1}

Captura de paquetes en anclaje

Después de la transferencia de movilidad, el controlador de anclaje recibe el tráfico DHCP del controlador externo a través del túnel de movilidad.

Una vez finalizado el proceso DORA, el cliente entra en el estado EJECUCIÓN con una función de anclaje de exportación. A partir de este punto, el controlador de anclaje sirve como punto de salida para el tráfico de datos del cliente.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 3, 2025 07:36:39...	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 3, 2025 07:36:39...	0.0.0.0	255.255.255.255	346	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41...	10.105.60.69	10.105.60.226	346	DHCP		DHCP Offer - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354
Jan 3, 2025 07:36:41...	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
Jan 3, 2025 07:36:41...	0.0.0.0	255.255.255.255	374	DHCP		DHCP Request - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41...	10.105.60.69	10.105.60.226	346	DHCP		DHCP ACK - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354

Tráfico DHCP del cliente en controlador de anclaje recibido del controlador externo

Estado del cliente en el controlador externo y de anclaje

Monitoring > Wireless > Clients

Clients

Sleeping Clients

Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐		10.105.60.226	fe80::b77c:b748:ddc:4fc0		1	DMZ_LWA	11	WLAN	Run	11ac		N/A	Export Foreign	No

1 ~ 1 of 1 clients

Estado del cliente en el extranjero

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
		10.105.60.226	fe80::acf2:f7b3:168e:65f2		0	DMZ_PSK	4	WLAN	Run	N/A		N/A	Export Anchor	No

1

10

1 - 1 of 1 clients

Estado del cliente en anclaje

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Client Properties

AP Properties

Security Information

Client Statistics

QOS Properties

Max Client Protocol Capability

802.11 ac Wave 2

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Anchor IP Address

10.105.60.114

Point of Presence

0xA0000003

AuthC Status

False

Move Count

0

Role

Export Foreign

Roam Type

L3 Requested

Complete Timestamp

01/03/2025 13:06:37 India

Propiedades del cliente en Foreign

Client	
360 View	General QOS Statistics ATF Statistics Mobility History Call Statistics
Client Properties AP Properties Security Information Client Statistics QOS Properties	
FlexConnect Authentication	N/A
Number of Tx Total Dropped Packets	0
Client Scan Report Time	Timer not running
Wi-Fi to Cellular Steering	Not implemented
Cellular Capability	N/A
Regular ASR support	DISABLED
Mobility	
Foreign IP Address	10.107.79.30
Point of Presence	0
Move Count	1
Role	Export Anchor
Roam Type	L3 Requested
Complete Timestamp	01/03/2025 07:36:27 UTC

Propiedades del cliente en delimitador

WLAN con autenticación de capa 3

Autenticación web local

Flujo para SSID de Webauth local en la configuración de anclaje externo

1. El cliente inicia una conexión con el SSID anunciado por el WLC extranjero.
2. Como no se realiza ninguna autenticación de Capa 2, el cliente se ancla directamente al WLC de anclaje. El cliente ingresa en el estado RUN en el WLC Externo, con su función de movilidad designada como Export Foreign.
3. El cliente obtiene una dirección IP y es redirigido a una página web. Este tráfico es manejado por el controlador de anclaje.
4. Después de la autenticación exitosa en el portal, el cliente pasa al estado RUN en el WLC de anclaje, con el rol de anclaje de exportación.

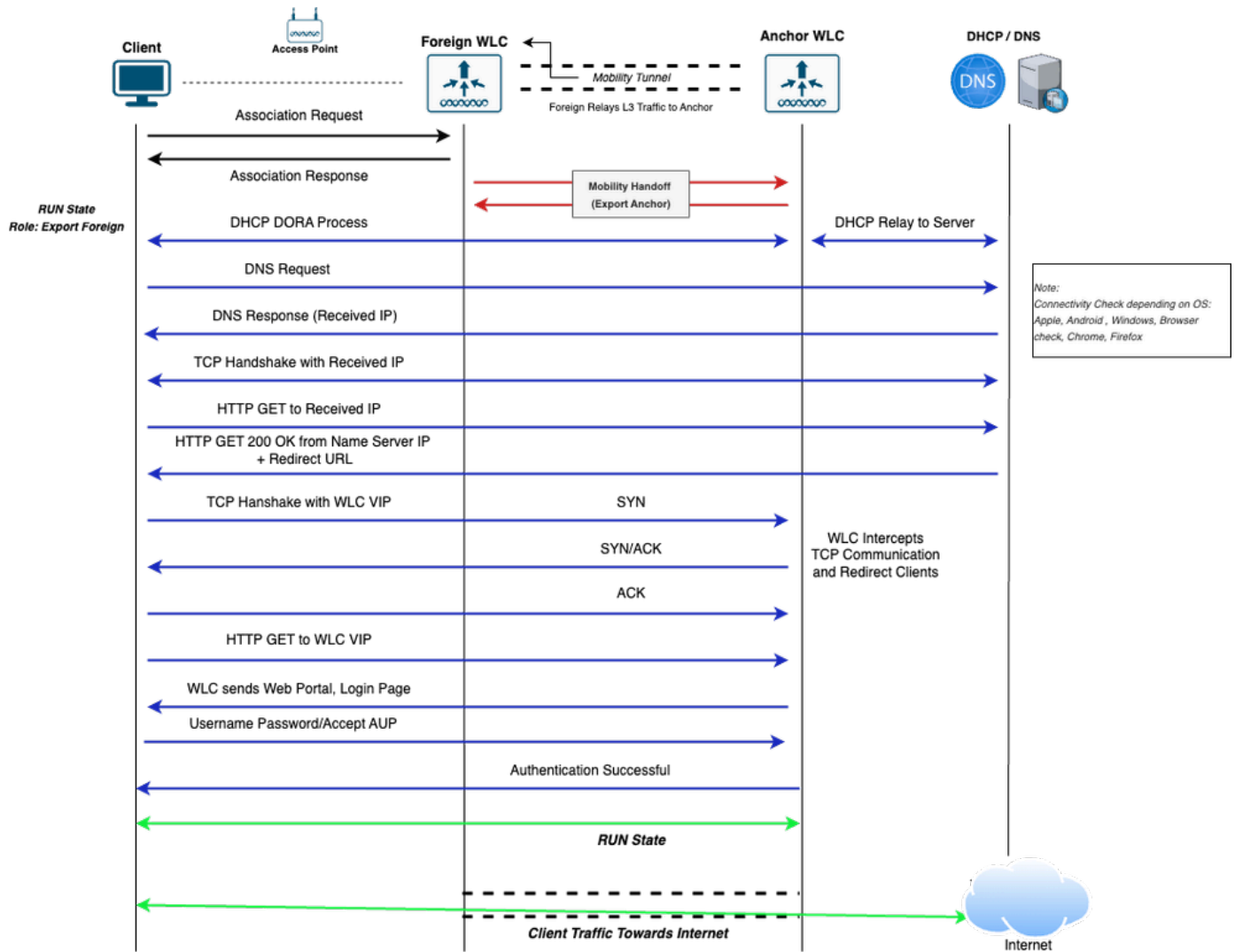


Diagrama de Flujo de Conectividad del Cliente para SSID de Webauth Local en Configuración de Anclaje Externo

Análisis del Flujo SSID de Webauth Local en la Configuración de Anclaje Externo a través de Registros

En esta sección se explica el flujo de conectividad de cliente para el SSID de autenticación web local mediante el uso de seguimiento radioactivo (RA Trace), capturas de paquetes incrustados (EPC) y el estado del cliente en los controladores externos y de anclaje.

Registros de controlador externo

Trazas radiactivas

!! Client Association Phase !!

```
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Association received. BSSID BSSID_M
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_IN
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC dot11 send association response. Sending ass
```

```

!! L2 Auth : None !!
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_L2

!! Mobility Handoff Phase !!
[] {mobilityd_R0-0}{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gr
[] {mobilityd_R0-0}{1} [mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP [] {mobilityd_R0-0}{1} [mm-client] [1
[] {mobilityd_R0-0}{1} [mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P
[] {wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o
[] {wncd_x_R0-0}{1} [mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_ANN
{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Sending export_Anchor_req of XID (XID) to (
[] {mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
[] {mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE
[] {mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce
[] {mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282)
[] {mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o
[] {mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS
[] {mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
[] {wncd_x_R0-0}{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed[] [mm-client] [17047] (info) MAC
[] [mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_IP

!! Client AAA Traffic handling !!
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (10452) to
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of XI
{wncd_x_R0-0}{1}: [mm-transition] [17047]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_Foreign ->
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Mobile AAA Handoff update received.
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC Received username=Guest1
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC IPv6 Client payload is re
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (10452)
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-pmtu] [18401]: (debug): Peer IP: Anchor-WLC-IP PMTU size is 1006 and calculate
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (1045
{wncd_x_R0-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_900000003] auth mgr attr add/change not
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17047]: (info): [Client_MAC:capwap_900000003] SM Notified attrib
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa handoff ack successfully forward

```

Captura de paquete

El cliente envía una solicitud de asociación, que controla el controlador externo.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:21:41	10.107.79.129	10.107.79.30	250	802.11		Association Request, SN=1705, FN=0, Flags=....., SSID="DMZ_LWA"
Jan 5, 2025 12:21:41	10.107.79.129	10.107.79.30	246	802.11		Association Request, SN=1705, FN=0, Flags=....., SSID="DMZ_LWA"
Jan 5, 2025 12:21:41	10.107.79.30	10.107.79.129	211	802.11		Association Response, SN=0, FN=0, Flags=.....
Jan 5, 2025 12:21:41	10.107.79.30	10.107.79.129	215	802.11		Association Response, SN=0, FN=0, Flags=.....

Una transferencia de movilidad se desencadena entre los controladores externos y de anclaje a través del puerto UDP 16667. Tras un evento de movilidad exitoso, el estado del cliente pasa a EJECUTARSE con una función Externa de exportación.

El controlador externo recibe el tráfico DHCP del cliente a través del túnel CAPWAP y lo reenvía al controlador de anclaje para su procesamiento posterior.

Jan 5, 2025 12:21:42...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	424	DHCP	0 DHCP Discover - Transaction ID 0x9f36b979
Jan 5, 2025 12:21:42...	10.107.79.30	10.105.60.114	400	UDP	16667 → 16667 Len=354
Jan 5, 2025 12:21:44...	10.105.60.114	10.107.79.30	400	UDP	16667 → 16667 Len=354
Jan 5, 2025 12:21:44...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0 DHCP Offer - Transaction ID 0x9f36b979
Jan 5, 2025 12:21:44...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	452	DHCP	0 DHCP Request - Transaction ID 0x9f36b979
Jan 5, 2025 12:21:44...	10.107.79.30	10.105.60.114	428	UDP	16667 → 16667 Len=382
Jan 5, 2025 12:21:44...	10.105.60.114	10.107.79.30	400	UDP	16667 → 16667 Len=354
Jan 5, 2025 12:21:44...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0 DHCP ACK - Transaction ID 0x9f36b979

El tráfico DHCP del cliente recibido en el controlador externo se reenvía al controlador de anclaje mediante el túnel de movilidad

De manera similar, el cliente envía el estado de conectividad de red y el tráfico de verificación de acceso a la página web al WLC externo a través del túnel CAPWAP; el WLC extranjero reenvía esto al WLC de anclaje usando el túnel de movilidad, donde el controlador de anclaje intercepta o procesa el tráfico.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:21:46...	10.107.79.129,10.105.60.226	10.107.79.30,DNS Server IP	165	DNS	0	Standard query 0x14e8 Connectivity Check URL
Jan 5, 2025 12:21:46...	10.107.79.30	10.105.60.114	141	UDP		16667 → 16667 Len=95
Jan 5, 2025 12:21:46...	10.105.60.114	10.107.79.30	291	UDP		16667 → 16667 Len=245
Jan 5, 2025 12:21:46...	10.107.79.30, DNS Server IP	10.107.79.129,10.105...	307	DNS	0	Standard query response 0x14e8 Connectivity Check URL raffi
Jan 5, 2025 12:21:46...	10.107.79.129,10.105.60.226	10.107.79.30, Resolved IP	148	TCP	0	52887 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:21:46...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:21:46...	10.105.60.114	10.107.79.30	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:21:46...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	140	TCP	0	80 → 52887 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 5, 2025 12:21:46...	10.107.79.129,10.105.60.226	10.107.79.30, Resolved IP	136	TCP	0	52887 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 5, 2025 12:21:46...	10.107.79.129,10.105.60.226	10.107.79.30, Resolved IP	247	HTTP	0	GET /connecttest.txt HTTP/1.1
Jan 5, 2025 12:21:46...	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:21:46...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	128	TCP	0	80 → 52887 [ACK] Seq=1 Ack=112 Win=64256 Len=0
Jan 5, 2025 12:21:46...	10.105.60.114	10.107.79.30	745	UDP		16667 → 16667 Len=699
Jan 5, 2025 12:21:46...	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:21:46...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	761	HTTP	0	HTTP/1.1 200 OK (text/html)
Jan 5, 2025 12:21:46...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	128	TCP	0	80 → 52887 [FIN, ACK] Seq=634 Ack=112 Win=64256 Len=0

Comprobación del estado de la conectividad de red en el controlador externo

```
> Frame 2176: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits)
> Ethernet II, Src: Cisco_63:8b:8b ( ), Dst: ( )
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: , Dst: 10.105.60.226
> Transmission Control Protocol, Src Port: 80, Dst Port: 52887, Seq: 1, Ack: 112, Len: 633
✓ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://192.0.2.1/login.html?redirect=https://192.0.2.1/login.html\r\n
    Content-Type: text/html\r\n
  > Content-Length: 472\r\n
    \r\n
    [Request in frame: 2169]
    [Time since request: 0.001007000 seconds]
    [Request URI: /connecttest.txt]
    [Full request URI: https://192.0.2.1/login.html?redirect=https://192.0.2.1/login.html]
    File Data: 472 bytes
  > Line-based text data: text/html (9 lines)
```

URL de redirección enviada al cliente

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	148	TCP	0	53024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25	10.105.60.114	10.107.79.30	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25	10.107.79.30, 192.0.2.1	10.107.79.129, 10.105.60.226	140	TCP	0	443 → 53024 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	136	TCP	0	53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	1386	TCP	0	53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 4991]
Jan 5, 2025 12:22:25	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25	10.107.79.30, 192.0.2.1	10.107.79.129, 10.105.60.226	128	TCP	0	443 → 53024 [ACK] Seq=1 Ack=1251 Win=64128 Len=0
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	747	TLSv1		Client Hello
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	148	TCP	0	53025 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25	10.107.79.30, 192.0.2.1	10.107.79.129, 10.105.60.226	128	TCP	0	443 → 53024 [ACK] Seq=1 Ack=1862 Win=64128 Len=0
Jan 5, 2025 12:22:25	10.105.60.114	10.107.79.30	277	UDP		16667 → 16667 Len=231
Jan 5, 2025 12:22:25	10.107.79.30, 192.0.2.1	10.107.79.129, 10.105.60.226	293	TLSv1		Server Hello, Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	143	TLSv1		Alert (Level: Fatal, Description: Certificate Unknown)
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	148	TCP	0	53027 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	211	TLSv1		Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25	10.107.79.30	10.105.60.114	187	UDP		16667 → 16667 Len=141
Jan 5, 2025 12:22:25	10.107.79.129, 10.105.60.226	10.107.79.30, 192.0.2.1	781	TLSv1		Application Data
Jan 5, 2025 12:22:25	10.107.79.30	10.105.60.114	757	UDP		16667 → 16667 Len=711
Jan 5, 2025 12:22:25	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25	10.107.79.30, 192.0.2.1	10.107.79.129, 10.105.60.226	181	TLSv1		Encrypted Alert

Página Acceso de Cliente a Webauth Local para Proporcionar Detalles de Autenticación

Registros del controlador de anclaje

Trazas radiactivas

!! Mobility Handoff !!

```
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Number of client is BELOW wlan limit
{mobilityd_R0-0}{1} [mm-transition] [26021] (info) MAC Client-MAC MMFSM transition S_MC_INIT -> S_MC_Auth
{wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Roam type changed - None -> L3 Requested
```

!! Session Created for Client !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_Auth
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition: S_CO_Auth
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
```

```
{wncd_x_R0-0}{1}: [webauth-ac] [24229]: (info): mobility_a0000001[Client_MAC][ 0.0.0.0]Applying IPv4 i
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_CR
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_INIT -> S_
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.
{wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.>> Client is successf
```

!! Client DHCP Traffic !!

```
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILIT
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_P
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [client-iplearn] [24229] (note) MAC Client-MAC Client IP learn successful. Method DHCP
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Sending ipv4_address_update of XID (XID)
{wncd_x_R0-0}{1} [client-iplearn] [24229] (info) MAC Client-MAC IP-learn state transition S_IPLEARN_IN_
Complete
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC Received ip learn response. method
```

!! Local Web Authentication !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_IP
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication initiated. LWA
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52911/235
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52911/235
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State G
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52911/235
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52911/235
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52911/2
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State G
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52910/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52919/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52919/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52923/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52924/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]52924/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Read co
```

{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State G
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse 1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53008/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse 1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53011/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53011/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53020/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53022/235
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]POST rc
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]get url
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -1526718499,s
{wncd_x_R0-0}{1}: [caaa-authen] [24229]: (info): [CAAA:AUTHEN:4000544] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list 1761615853,sm
{wncd_x_R0-0}{1}: [caaa-author] [24229]: (info): [CAAA:AUTHOR:4000544] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State A
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Unapply I
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template D
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Unapply I
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template D
{wncd_x_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client_MAC Link-local bridging not enabled for
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Authc success from WebAuth
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event APPLY_USER_PRO
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event RX_METHOD_AUT

{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute: username 0 Guest1
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-type 0 1 (0x1)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-service 0 16 (0x10)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : addr 0 0xa693ce2
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : method 0 1 [webauth]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : intf-id 0 2684354561 (0xa0000001)
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [24229]: (info): [Client_MAC:mobility_a0000001] SM Notified attr
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Received User-Name Guest1

{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Method webauth changing st
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event AUTHZ_SUCCESS
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Applying
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Applying Svc Templ IP-Adm-V4-LOGOUT-ACL (ML:NONE)
{wncd_x_R0-0}{1}: [epm] [24229]: (info): [Client_MAC:mobility_a0000001] Feature (EPM URL PLUG-IN) has b
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Response of epm is SYNC with return code Success
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template A
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [24229]: (ERR): authc policy update from SANet vlan 31
{wncd_x_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client_MAC Link-local bridging not enabled for
{wncd_x_R0-0}{1}: [webauth-sess] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State A
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/1
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] SM will not send event Tem
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [rog-proxy-capwap] [24229]: (debug): Managed client RUN state notification: Client_MA
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Client has Anchor role
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Guest client detected. S
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

Captura de paquete

Después de la transferencia de movilidad, el controlador de anclaje recibe el tráfico DHCP del controlador externo a través del túnel de movilidad.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 07:21:49...	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 5, 2025 07:21:49...	0.0.0.0	255.255.255.255	346	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 5, 2025 07:21:51...	10.105.60.69	10.105.60.226	346	DHCP		DHCP Offer - Transaction ID 0x9f36b979
Jan 5, 2025 07:21:51...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354
Jan 5, 2025 07:21:51...	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
Jan 5, 2025 07:21:51...	0.0.0.0	255.255.255.255	374	DHCP		DHCP Request - Transaction ID 0x9f36b979
Jan 5, 2025 07:21:51...	10.105.60.69	10.105.60.226	346	DHCP		DHCP ACK - Transaction ID 0x9f36b979
Jan 5, 2025 07:21:51...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354

Tráfico DHCP de cliente en controlador de anclaje recibido desde controlador externo

El controlador de anclaje recibe comprobaciones de conectividad, solicitudes de acceso a páginas web y detalles de autenticación para seguir procesando.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:21:52...	10.107.79.30	10.105.60.114	141	UDP		16667 → 16667 Len=95
Jan 5, 2025 12:21:52...	10.105.60.226	DNS IP	83	DNS		Standard query 0x14e8 , Connectivity Check URL
Jan 5, 2025 12:21:52...	DNS IP	10.105.60.226	237	DNS		Standard query response 0x14e8 Connectivity Check URL
Jan 5, 2025 12:21:52...	10.105.60.114	10.107.79.30	287	UDP		16667 → 16667 Len=245
Jan 5, 2025 12:21:52...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:21:52...	10.105.60.226	Resolved IP	70	TCP		52887 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:21:52...	Resolved IP	10.105.60.226	66	TCP		80 → 52887 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 5, 2025 12:21:52...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:21:52...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:21:52...	10.105.60.226	Resolved IP	58	TCP		52887 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 5, 2025 12:21:52...	10.107.79.30	10.105.60.114	223	UDP		16667 → 16667 Len=177
Jan 5, 2025 12:21:52...	Resolved IP	10.105.60.226	169	HTTP		GET /connecttest.txt HTTP/1.1
Jan 5, 2025 12:21:52...	Resolved IP	10.105.60.226	54	TCP		80 → 52887 [ACK] Seq=1 Ack=112 Win=64256 Len=0
Jan 5, 2025 12:21:52...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:21:52...	Resolved IP	10.105.60.226	687	HTTP		HTTP/1.1 200 OK (text/html)
Jan 5, 2025 12:21:52...	10.105.60.114	10.107.79.30	741	UDP		16667 → 16667 Len=699
Jan 5, 2025 12:21:52...	Resolved IP	10.105.60.226	54	TCP		80 → 52887 [FIN, ACK] Seq=634 Ack=112 Win=64256 Len=0
Jan 5, 2025 12:21:52...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66

Comprobación del estado de la conectividad de red en el controlador de anclaje

> Frame 604: 687 bytes on wire (5496 bits), 687 bytes captured (5496 bits)
> Ethernet II, Src: [REDACTED], Dst: [REDACTED]
> Internet Protocol Version 4, Src: [REDACTED], Dst: 10.105.60.226
> Transmission Control Protocol, Src Port: 80, Dst Port: 52887, Seq: 1, Ack: 112, Len: 633
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Location: https://192.0.2.1/login.html?redirect=http://[REDACTED]
Content-Type: text/html\r\n
> Content-Length: 472\r\n
\r\n
[Request in frame: 601]
[Time since request: 0.000992000 seconds]
[Request URI: /connecttest.txt]
[Full request URI: http://[REDACTED]]
File Data: 472 bytes
> Line-based text data: text/html (9 lines)

URL de redirección enviada al cliente

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	70	TCP		53024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	66	TCP		443 → 53024 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	58	TCP		53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	450	UDP		16667 → 16667 Len=404
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	1308	TCP		53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 3273]
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53024 [ACK] Seq=1 Ack=1251 Win=64128 Len=0
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	723	UDP		16667 → 16667 Len=677
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	669	TLSv1..		Client Hello
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53024 [ACK] Seq=1 Ack=1862 Win=64128 Len=0
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	219	TLSv1..		Server Hello, Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	273	UDP		16667 → 16667 Len=231
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	65	TLSv1..		Alert (Level: Fatal, Description: Certificate Unknown)
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	58	TCP		53024 → 443 [FIN, ACK] Seq=1869 Ack=166 Win=131072 Len=0
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	187	UDP		16667 → 16667 Len=141
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	133	TLSv1..		Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	757	UDP		16667 → 16667 Len=711
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	703	TLSv1..		Application Data
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	107	TLSv1..		Encrypted Alert
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	161	UDP		16667 → 16667 Len=119
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53027 [FIN, ACK] Seq=219 Ack=2678 Win=64128 Len=0

Página Acceso de Cliente a Webauth Local para Proporcionar Detalles de Autenticación

Después de la autenticación Web local correcta, el cliente entra en el estado EJECUCIÓN con una función de anclaje de exportación. A partir de este punto, el controlador de anclaje sirve como punto de salida para el tráfico de datos del cliente.

Estado del cliente en el controlador externo y de anclaje

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
		10.105.60.226			0	DMZ_LWA	5	WLAN	Run	N/A	Guest1	N/A	Export Anchor	No

1

10

1 - 1 of 1 clients

Estado del cliente en el extranjero

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
		10.105.60.226			0	DMZ_LWA	5	WLAN	Run	N/A	Guest1	N/A	Export Anchor	No

1

10

1 - 1 of 1 clients

Estado del cliente en anclaje

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability

Wi-Fi to Cellular Steering

Cellular Capability

Regular ASR support

802.11ac Wave 2

Not implemented

N/A

DISABLED

Mobility

Anchor IP Address

Point of Presence

AuthC Status

Move Count

Role

Roam Type

10.105.60.114

0xA0000003

True

0

Export Foreign

L3 Requested

Propiedades del cliente en Foreign

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

Propiedades del cliente en delimitador

Autenticación web central

Flujo para SSID de Webauth central en la configuración de anclaje externo

1. El cliente envía una solicitud de asociación para el SSID transmitido por el controlador de LAN inalámbrica externa (WLC).
2. El WLC Externo realiza el filtrado de MAC enviando una petición de acceso al servidor RADIUS. El servidor RADIUS responde con una aceptación de acceso, que incluye la URL de redirección y la lista de control de acceso (ACL) necesarias.
3. El WLC Externo envía la respuesta de asociación al cliente.
4. El cliente está anclado al WLC de anclaje. El cliente ingresa en el estado RUN en el WLC Externo, con el rol de movilidad configurado en Export Foreign.
5. El cliente obtiene una dirección IP. En esta etapa, el WLC de anclaje maneja el tráfico de redirección, dirigiendo al cliente al portal de autenticación.
6. Una vez redirigido, el cliente se comunica directamente con el servidor RADIUS. Este tráfico se tuneliza a través del WLC de anclaje hacia el servidor RADIUS.

7. El cliente introduce las credenciales de autenticación en el servidor RADIUS. Tras una autenticación exitosa, el servidor RADIUS envía una solicitud de cambio de autorización (CoA) al WLC externo.
8. El WLC Externo envía una respuesta CoA al servidor RADIUS. El cliente pasa al estado RUN en el WLC de anclaje, con el rol establecido en Export Anchor.
9. Todo el tráfico subsiguiente del cliente se tuneliza desde el WLC externo al WLC de anclaje, donde sale de la red.

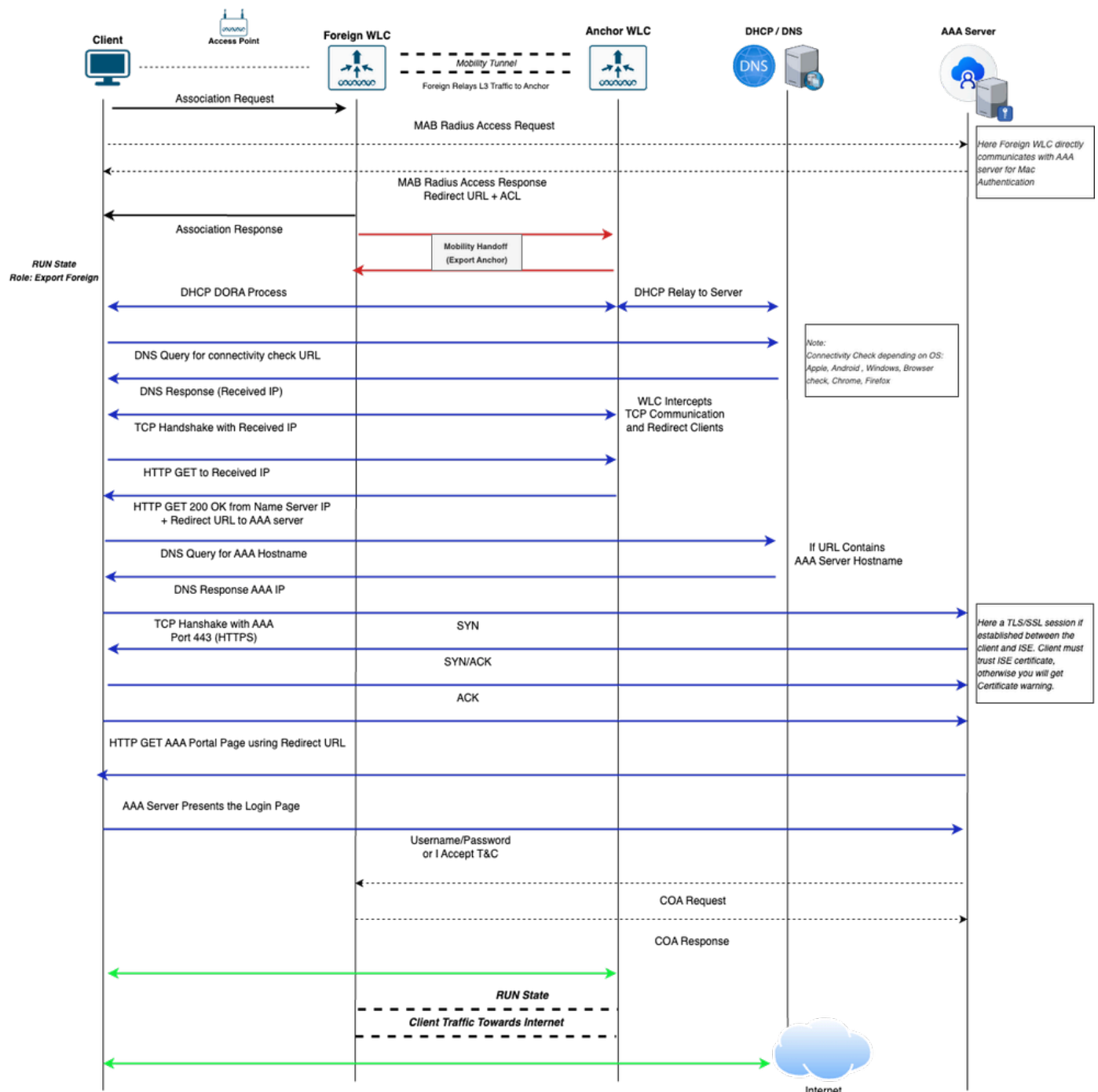


Diagrama de flujo de conectividad de cliente para SSID de Webauth central en configuración de anclaje externo

Análisis del Flujo SSID de Webauth Central en la Configuración de Anclaje Externo a través de

Registros

En esta sección se explica el flujo de conectividad de cliente para SSID de autenticación web central mediante el uso de seguimiento radioactivo (seguimiento de RA), capturas de paquetes incrustados (EPC) y el estado del cliente en los controladores externos y de anclaje.

Registros de controlador externo

Trazas radiactivas

!! Client Association Phase !!

{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Association received. BSSID BSSID_M

{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_IN

!! MAC Authentication !!

{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_INIT -> S_DO

{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS

{wncd_x_R0-0}{1}: [client-auth] [17047]: (note): MAC: Client_MAC MAB Authentication initiated. Policy V

{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authc_list: M

{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authz_list: M

{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition

{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition

{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition

{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] Received event 'MAB_CONTINUE' on

{wncd_x_R0-0}{1}: [caaa-author] [17047]: (info): [CAAA:AUTHOR:a30003a6] NULL ATTR LIST

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Send Access-Request to 10.106.32.130:1812 id 0/245,

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: authenticator

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 14 user-MAC

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Password [2] 18 *

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Service-Type [6] 6 Call Check [10]

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 31

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 25 service-type=Call Check

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Framed-MTU [12] 6 1485

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: EAP-Key-Name [102] 2 *

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 49

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 43 audit-session-id=1E4F6B0A000003

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 18

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 12 method=mab

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 32

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 26 client-iif-id=3556776730

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-IP-Address [4] 6 10.107.79.30

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19]

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-Port [5] 6 141522

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 31

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 25 cisco-wlan-ssid=DMZ_CWA

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 33

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 27 wlan-profile-name=DMZ_CWA

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Called-Station-Id [30] 27 called-station-id

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Calling-Station-Id [31] 19 client-MAC

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Airespace [26] 12

```

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Airespace-WLAN-ID [1] 6 12
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Nas-Identifier [32] 16 ForeignSiteWLC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Started 5 sec timeout
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Received from id 1812/245 10.106.32.130:0, Access-A
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 19 Client_MAC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 37
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 31 url-redirect-ac1=REDIRECT_ACL
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 191
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 185 url-redirect=https://10.106.32
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat

{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB received an Access-Accept for
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC Processing MAB authentication resu
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_MA
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC dot11 send association response. Sending ass
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_MAB_PENDING
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC L2 Authentication of station is su
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Mobility discovery triggered. Clie
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_L2

!! Mobility Handoff !!
[mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gr
[mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP [mm-client] [1
[mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P
[mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o
[mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_ANN
[mm-client] [17047] (debug) MAC Client-MAC Sending export_Anchor_req of XID (XID) to (
[mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
[mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE
[mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce
[mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282
[mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o
[mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS
[mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
[mm-client] [17047] (info) Anchor Vlan-id 31 processed[mm-client] [17047] (info) MAC
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
[client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_C
[client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
[client-orch-sm] [17047] (debug) MAC Client-MAC Received ip learn response. method IP
[client-orch-state] Client state transition S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN >> !

!! Post Successful Web authentication, Change of Authorization !!
[client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Processing CoA request und
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Reauthenticate request (0x
[sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list -50323943,sm_
[mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB re-authentication started for
[auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Context changing state from
[auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Method mab changing state fr
[aaa-coa] [17047]: (info): radius coa proxy relay coa resp(wncd)
[aaa-coa] [17047]: (info): CoA Response Details
[aaa-attr-inf] [17047]: (info): << ssg-command-code 0 32 >>
[aaa-attr-inf] [17047]: (info): << formatted-clid 0 Client_MAC>>
[aaa-attr-inf] [17047]: (info): << error-cause 0 1 [Success]>>
[aaa-coa] [17047]: (info): server:10.107.79.30 cfg_saddr:10.107.79.30 udpport:51304 s

```

```
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER] CoA response sent
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Identity preserved: MAC (C
{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] Received event 'MAB_REAUTHENTICAT
{smd_R0-0}{1}: [aaa-coa] [18867]: (info): ++++++ Received CoA response Attribute List ++++++
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS(00000000): Send CoA Ack Response to 10.106.32.130:51304
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: authenticator
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Vendor, Cisco [26] 9
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: ssg-command-code [252] 3 ...
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Calling-Station-Id [31] 16 Client_MAC
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Dynamic-Author-Error-Cause[101] 6 Success [200]
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Message-Authenticator[80] 18 ...
{smd_R0-0}{1}: [aaa-pod] [18867]: (info): CoA response source port = 0, udpport = 51304,
{wncd_x_R0-0}{1}: [sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list 1627397682,sm
```

Captura de paquete

El cliente envía una solicitud de asociación y realiza la autenticación MAC, este tráfico es manejado por el controlador externo.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:11...	10.107.79.129	10.107.79.30	250	802.11		Association Request, SN=695, FN=0, Flags=....., SSID="DMZ_CWA"
Jan 8, 2025 13:09:11...	10.107.79.129	10.107.79.30	246	802.11		Association Request, SN=695, FN=0, Flags=....., SSID="DMZ_CWA"
Jan 8, 2025 13:09:11...	10.107.79.30	10.106.32.130	412	RADIUS		Access-Request id=245
Jan 8, 2025 13:09:11...	10.107.79.30	10.106.32.130	416	RADIUS		Access-Request id=245, Duplicate Request
Jan 8, 2025 13:09:11...	10.106.32.130	10.107.79.30	429	RADIUS		Access-Accept id=245
Jan 8, 2025 13:09:11...	10.106.32.130	10.107.79.30	425	RADIUS		Access-Accept id=245, Duplicate Response
Jan 8, 2025 13:09:11...	10.107.79.30	10.107.79.129	211	802.11		Association Response, SN=0, FN=0, Flags=.....
Jan 8, 2025 13:09:11...	10.107.79.30	10.107.79.129	215	802.11		Association Response, SN=0, FN=0, Flags=.....

Fase de asociación de cliente en controlador externo con MAB inalámbrico

Una transferencia de movilidad se desencadena entre los controladores externos y de anclaje a través del puerto UDP 16667. Tras un evento de movilidad exitoso, el estado del cliente pasa a EJECUTARSE con una función Externa de exportación.

El controlador externo recibe el tráfico DHCP del cliente a través del túnel CAPWAP y lo reenvía al controlador de anclaje para su procesamiento posterior.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:12...	10.107.79.129,0.0.0.0	10.107.79.30,255.255.255.255	424	DHCP	0	DHCP Discover - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:12...	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.107.79.30,10.105.60.69	10.107.79.129,10.105.60.69	416	DHCP	0	DHCP Offer - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:14...	10.107.79.129,0.0.0.0	10.107.79.30,255.255.255.255	452	DHCP	0	DHCP Request - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:14...	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
Jan 8, 2025 13:09:14...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.107.79.30,10.105.60.69	10.107.79.129,10.105.60.69	416	DHCP	0	DHCP ACK - Transaction ID 0x9f36b979

El tráfico DHCP del cliente recibido en el controlador externo se reenvía al controlador de anclaje mediante el túnel de movilidad

De manera similar, el cliente envía el estado de conectividad de red y el tráfico de verificación de acceso a la página web al WLC externo a través del túnel CAPWAP; el WLC extranjero reenvía esto al WLC de anclaje usando el túnel de movilidad, donde el controlador de anclaje intercepta o procesa el tráfico.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30, DNS IP	165	DNS	0	Standard query 0xd4c8 / Connectivity Check URL
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	100	UDP	16667	→ 16667 Len=54
Jan 8, 2025 13:09:16...	10.105.60.114	10.107.79.30	291	UDP	16667	→ 16667 Len=245
Jan 8, 2025 13:09:16...	10.107.79.30, DNS IP	10.107.79.129,10.105...	307	DNS	0	Standard query response 0xd4c8 / Connectivity Check URL
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30, Resolved IP	148	TCP	0	59484 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	124	UDP	16667	→ 16667 Len=78
Jan 8, 2025 13:09:16...	10.105.60.114	10.107.79.30	124	UDP	16667	→ 16667 Len=78
Jan 8, 2025 13:09:16...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	140	TCP	0	80 → 59484 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30	136	TCP	0	59484 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30, Resolved IP	247	HTTP	0	GET /connecttest.txt HTTP/1.1
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	223	UDP	16667	→ 16667 Len=177
Jan 8, 2025 13:09:16...	10.105.60.114	10.107.79.30	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:16...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	128	TCP	0	80 → 59484 [ACK] Seq=1 Ack=112 Win=64256 Len=0
Jan 8, 2025 13:09:16...	10.105.60.114	10.107.79.30	117	UDP	16667	→ 16667 Len=71
Jan 8, 2025 13:09:16...	10.105.60.114	10.107.79.30	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:16...	10.107.79.30, Resolved IP	10.107.79.129,10.105...	1045	HTTP	0	HTTP/1.1 200 OK (text/html)
Jan 8, 2025 13:09:16...	10.107.79.30	10.107.79.129,10.105...	128	TCP	0	80 → 59484 [FIN, ACK] Seq=918 Ack=112 Win=64256 Len=0
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30	136	TCP	0	59484 → 80 [ACK] Seq=112 Ack=919 Win=130304 Len=0
Jan 8, 2025 13:09:16...	10.107.79.129,10.105.60.249	10.107.79.30, Resolved IP	136	TCP	0	59484 → 80 [FIN, ACK] Seq=112 Ack=919 Win=130304 Len=0
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:16...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66

Comprobación del estado de la conectividad de red en el controlador externo

```
> Frame 2176: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits)
> Ethernet II, Src: Cisco_63:8b:8b..., Dst: Cisco_...
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: ..., Dst: 10.105.60.226
> Transmission Control Protocol, Src Port: 80, Dst Port: 52887, Seq: 1, Ack: 112, Len: 633
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Location: https://192.0.2.1/login.html?redirect=https://www.msftconnecttest.com/connecttest.aspx
  Content-Type: text/html\r\n
> Content-Length: 472\r\n
\r\n
[Request in frame: 2169]
[Time since request: 0.001007000 seconds]
[Request URI: /connecttest.txt]
[Full request URI: ...]
File Data: 472 bytes
> Line-based text data: text/html (9 lines)
```

URL de redirección enviada al cliente

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	124	UDP	16667	→ 16667 Len=78
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	66	TCP	59500	→ 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 8, 2025 13:09:22...	10.106.32.130	10.105.60.249	70	TCP	8443	→ 59500 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	120	UDP	16667	→ 16667 Len=78
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	54	TCP	59501	→ 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	1342	UDP	16667	→ 16667 Len=1296
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	1304	TCP	59500	→ 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 1162]
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	563	UDP	16667	→ 16667 Len=517
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	505	TLSv1...		Client Hello
Jan 8, 2025 13:09:22...	10.106.32.130	10.105.60.249	1308	TCP	8443	→ 59501 [ACK] Seq=1 Ack=1766 Win=33280 Len=1250 [TCP PDU reassembled in 1181]
Jan 8, 2025 13:09:22...	10.106.32.130	10.105.60.249	863	TLSv1...		Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	962	UDP	16667	→ 16667 Len=920
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	446	UDP	16667	→ 16667 Len=404
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	54	TCP	59500	→ 8443 [ACK] Seq=1702 Ack=2056 Win=131072 Len=0
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	119	UDP	16667	→ 16667 Len=73
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	61	TLSv1...		Alert (Level: Fatal, Description: Certificate Unknown)
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	54	TCP	59501	→ 8443 [ACK] Seq=1766 Ack=2056 Win=131072 Len=0
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	180	TLSv1...		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 8, 2025 13:09:22...	10.106.32.130	10.105.60.249	64	TLSv1...		Change Cipher Spec
Jan 8, 2025 13:09:22...	10.106.32.130	10.105.60.249	103	TLSv1...		Encrypted Handshake Message
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	114	UDP	16667	→ 16667 Len=72
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	153	UDP	16667	→ 16667 Len=111
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	54	TCP	59503	→ 8443 [ACK] Seq=1860 Ack=2107 Win=131072 Len=0
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	1095	TLSv1...		Application Data
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	1153	UDP	16667	→ 16667 Len=1107
Jan 8, 2025 13:09:22...	10.105.60.114	10.107.79.30	936	UDP	16667	→ 16667 Len=894
Jan 8, 2025 13:09:22...	10.107.79.30	10.105.60.114	1133	UDP	16667	→ 16667 Len=1087
Jan 8, 2025 13:09:22...	10.105.60.249	10.106.32.130	1075	TLSv1...		Application Data

Página Acceso de Cliente a Webauth Central para Proporcionar Detalles de Autenticación

El controlador externo procesa la solicitud de CoA después de la autenticación Web central correcta.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:33...	10.106.32.130	10.107.79.30	248	RADIUS		CoA-Request id=2
Jan 8, 2025 13:09:33...	10.106.32.130	10.107.79.30	244	RADIUS		CoA-Request id=2, Duplicate Request
Jan 8, 2025 13:09:33...	10.107.79.30	10.106.32.130	111	RADIUS		CoA-ACK id=2
Jan 8, 2025 13:09:33...	10.107.79.30	10.106.32.130	115	RADIUS		CoA-ACK id=2, Duplicate Response

Cambio de autorización (COA) con el controlador externo

Registros del controlador de anclaje

Trazas radiactivas

!! Mobility Handoff !!

```
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Number of client is BELOW wlan limit
{mobilityd_R0-0}{1} [mm-transition] [26021] (info) MAC Client-MAC MMFSM transition S_MC_INIT -> S_MC_Anchor
[wncd_x_R0-0]{1} [mm-client] [24229] (info) MAC Client-MAC Roam type changed - None -> L3 Requested
```

!! Session Created for Client !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_AUTH -> S_CO_AUTH
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition: S_CO_AUTH -> S_CO_AUTH
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition: S_CO_AUTH -> S_CO_AUTH
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC L2 Authentication of station is successful
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_AUTH -> S_CO_AUTH
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MACMMIF FSM transition: S_MA_INIT -> S_MA_AUTH
{wncd_x_R0-0}{1}: [mm-client] [24229]: (info): MAC: Client_MACRoam type changed - None -> L3 Requested
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully processed
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.
[wncd_x_R0-0]{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export Anchor
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.>> Client is successfully anchored
```

!! Central Web Authentication Applied !!

```
{wncd_x_R0-0}{1}: [webauth-dev] [24229]: (info): Central Webauth URL Redirect, Received a request to create session
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]State Invalid State -> INIT
{wncd_x_R0-0}{1}: [epm-redirect] [24229]: (info): [0000.0000.0000:unknown] URL-Redirect = https://10.106.32.130
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: method 0 2 [mab]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: intf-id 0 2415919107 (0x90000000)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: username 0 D0-37-45-88-25-52
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: class 0 43 41 43 53 3a 31 45 34
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: url-redirect-act 0 REDIRECT_ACL
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: url-redirect 0 https://10.106.32.130
```

!! Client DHCP Traffic !!

```
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILITY -> S_CO_MOBILITY
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_P -> S_CO_DPATH_P
```

{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [client-iplearn] [24229] (note) MAC Client-MAC Client IP learn successful. Method DHCP
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Sending ipv4_address_update of XID (XID
{wncd_x_R0-0}{1} [client-iplearn] [24229] (info) MAC Client-MAC IP-learn state transition S_IPLEARN_IN
Complete
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC Received ip learn response. method

!! Central Web Authentication !!

{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): [Client_MAC][10.105.60.249]59494/233 IO state NEW -> R
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): [Client_MAC][10.105.60.249]59495/235 IO state NEW -> R
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): [Client_MAC][10.105.60.249]59494/233 Read event, Messa
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): Captive bypass: No parameter map associated. Falling
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][10.105.60.249]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][10.105.60.249]State GET_REDIRECT -> GE
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): [Client_MAC][10.105.60.249]59494/233 IO state READING
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): [Client_MAC][10.105.60.249]59494/233 IO state WRITING
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): [Client_MAC][10.105.60.249]59494/233 Remove IO ctx
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Sending export_anchor_rsp of XID (18
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

Captura de paquete

Después de la transferencia de movilidad, el controlador de anclaje recibe el tráfico DHCP del controlador externo a través del túnel de movilidad.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:42...	10.107.79.30	10.105.60.114	396	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:42...	0.0.0.0	255.255.255.255	286	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:44...	10.105.60.69	10.105.60.249	286	DHCP		DHCP Offer - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	424	UDP		16667 → 16667 Len=382
Jan 8, 2025 13:09:44...	0.0.0.0	255.255.255.255	286	DHCP		DHCP Request - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:44...	10.105.60.69	10.105.60.249	286	DHCP		DHCP ACK - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354

Tráfico DHCP del cliente en el controlador de anclaje recibido del controlador externo

El controlador de anclaje recibe comprobaciones de conectividad, solicitudes de acceso a páginas web y detalles de autenticación para seguir procesando.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	114	UDP		16667 → 16667 Len=72
Jan 8, 2025 13:09:44...	10.105.60.249	DNS IP	83	DNS		Standard query 0xd4c8 Connectivity Check URL
Jan 8, 2025 13:09:44...	DNS IP	10.105.60.249	237	DNS		Standard query response 0xd4c8 A Connectivity Check URL rafficma
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	287	UDP		16667 → 16667 Len=245
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:44...	10.105.60.249	Resolved IP	70	TCP		59484 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 8, 2025 13:09:44...	Resolved IP	10.105.60.249	66	TCP		80 → 59484 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	223	UDP		16667 → 16667 Len=177
Jan 8, 2025 13:09:44...	10.105.60.249	Resolved IP	58	TCP		59484 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 8, 2025 13:09:44...	10.105.60.249	Resolved IP	169	HTTP		GET /connecttest.txt HTTP/1.1
Jan 8, 2025 13:09:44...	Resolved IP	10.105.60.249	54	TCP		80 → 59484 [ACK] Seq=1 Ack=112 Win=64256 Len=0
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44...	Resolved IP	10.105.60.249	971	HTTP		HTTP/1.1 200 OK (text/html)
Jan 8, 2025 13:09:44...	10.105.60.249	10.105.60.249	54	TCP		80 → 59484 [FIN, ACK] Seq=918 Ack=112 Win=64256 Len=0
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44...	10.105.60.249	Resolved IP	58	TCP		59484 → 80 [ACK] Seq=112 Ack=919 Win=130304 Len=0
Jan 8, 2025 13:09:44...	10.105.60.249	Resolved IP	58	TCP		59484 → 80 [FIN, ACK] Seq=112 Ack=919 Win=130304 Len=0
Jan 8, 2025 13:09:44...	Resolved IP	10.105.60.249	54	TCP		80 → 59484 [ACK] Seq=919 Ack=113 Win=64256 Len=0
Jan 8, 2025 13:09:44...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66

Comprobación del estado de la conectividad de red en el controlador de anclaje

> Frame 864: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits)
> Ethernet II, Src: , Dst:
> Internet Protocol Version 4, Src: Dst: 10.105.60.249
> Transmission Control Protocol, Src Port: 80, Dst Port: 59484, Seq: 1, Ack: 112, Len: 917
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
[...]Location: https://10.106.32.130:8443/portal/gateway?sessionId=1E4F6B0A000003D247203276&portal=d06bc2
Content-Type: text/html\r\n
> Content-Length: 614\r\n
\r\n
[Request in frame: 861]
[Time since request: 0.001007000 seconds]
[Request URI: /connecttest.txt]
[Full request URI:]
File Data: 614 bytes
> Line-based text data: text/html (9 lines)

URL de redirección enviada al cliente

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	148	TCP	0	59501 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	124	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	140	TCP	1	8443 → 59501 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	136	TCP	0	59501 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	1386	TCP	0	59501 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 1420]
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	651	TLSv1...	0	Client Hello
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	627	UDP		16667 → 16667 Len=581
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	1342	UDP		16667 → 16667 Len=1296
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	450	UDP		16667 → 16667 Len=404
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	917	UDP		16667 → 16667 Len=871
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	1378	TCP	0	8443 → 59500 [ACK] Seq=1 Ack=1702 Win=34688 Len=1250 [TCP PDU reassembled in 1432]
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	933	TLSv1...	0	Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	917	UDP		16667 → 16667 Len=871
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	1378	TCP	0	8443 → 59501 [ACK] Seq=1 Ack=1766 Win=33280 Len=1250 [TCP PDU reassembled in 1437]
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	143	TLSv1...	0	Alert (Level: Fatal, Description: Certificate Unknown)
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	136	TCP	0	59501 → 8443 [ACK] Seq=1766 Ack=2056 Win=131072 Len=0
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	119	UDP		16667 → 16667 Len=73
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	262	TLSv1...	0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	118	UDP		16667 → 16667 Len=72
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	157	UDP		16667 → 16667 Len=111
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	134	TLSv1...	0	Change Cipher Spec
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	173	TLSv1...	0	Encrypted Handshake Message
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	1177	TLSv1...	0	Application Data
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	1153	UDP		16667 → 16667 Len=1107
Jan 8, 2025 13:09:21...	10.105.60.114	10.107.79.30	940	UDP		16667 → 16667 Len=894
Jan 8, 2025 13:09:21...	10.107.79.30,10.106.32.130	10.107.79.129,10.105...	956	TLSv1...	0	Application Data
Jan 8, 2025 13:09:21...	10.107.79.129,10.105.60.249	10.107.79.30,10.106.3...	1157	TLSv1...	0	Application Data
Jan 8, 2025 13:09:21...	10.107.79.30	10.105.60.114	1133	UDP		16667 → 16667 Len=1087

Página Acceso de Cliente a Webauth Local para Proporcionar Detalles de Autenticación

Quando la autenticación Web central se realiza correctamente, se activa un cambio de autorización (CoA). Después de una CoA exitosa, el cliente pasa al estado RUN con un rol de anclaje de exportación.

Estado del cliente en el controlador externo y de anclaje

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐		10.105.60.249	fe80::877c:b748:ddc:4fc0		1	DMZ_CWA	14	WLAN	Run	11ac		N/A	Export Foreign	No

1 - 1 of 1 clients

Estado del cliente en el extranjero

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐		10.105.60.249	fe80::877c:b748:ddc:4fc0		0	DMZ_CWA	6	WLAN	Run	N/A	guestuser	N/A	Export Anchor	No

1 - 1 of 1 clients

Estado del cliente en anclaje

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability

802.11ac Wave 2

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Anchor IP Address

10.105.60.114

Point of Presence

0xA0000003

AuthC Status

True

Move Count

0

Role

Export Foreign

Roam Type

L3 Requested

Propiedades del cliente en Foreign

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

Propiedades del cliente en delimitador

Autenticación web externa

Flujo para SSID de Webauth externo en la configuración de anclaje externo

1. El cliente inicia una conexión con el SSID transmitido por el WLC extranjero.
2. Como no se requiere autenticación de Capa 2, el cliente está anclado al WLC de anclaje. El cliente pasa al estado RUN en el WLC Externo, con la función de movilidad designada como Export Foreign.
3. El cliente adquiere una dirección IP. El WLC de anclaje intercepta el tráfico y redirige al cliente al portal del servidor web externo como se define en los parámetros de autenticación web.
4. El cliente envía las credenciales de autenticación a través del portal. Estas credenciales se validan localmente en el WLC o a través de un servidor de autenticación externo, dependiendo de la política de seguridad configurada.
5. Tras la autenticación exitosa, el cliente pasa al estado RUN en el WLC de anclaje, asumiendo el rol de anclaje de exportación.

6. Después de la autenticación exitosa, todo el tráfico subsiguiente del cliente se tuneliza desde el WLC externo al WLC de anclaje, donde egresa de la red.

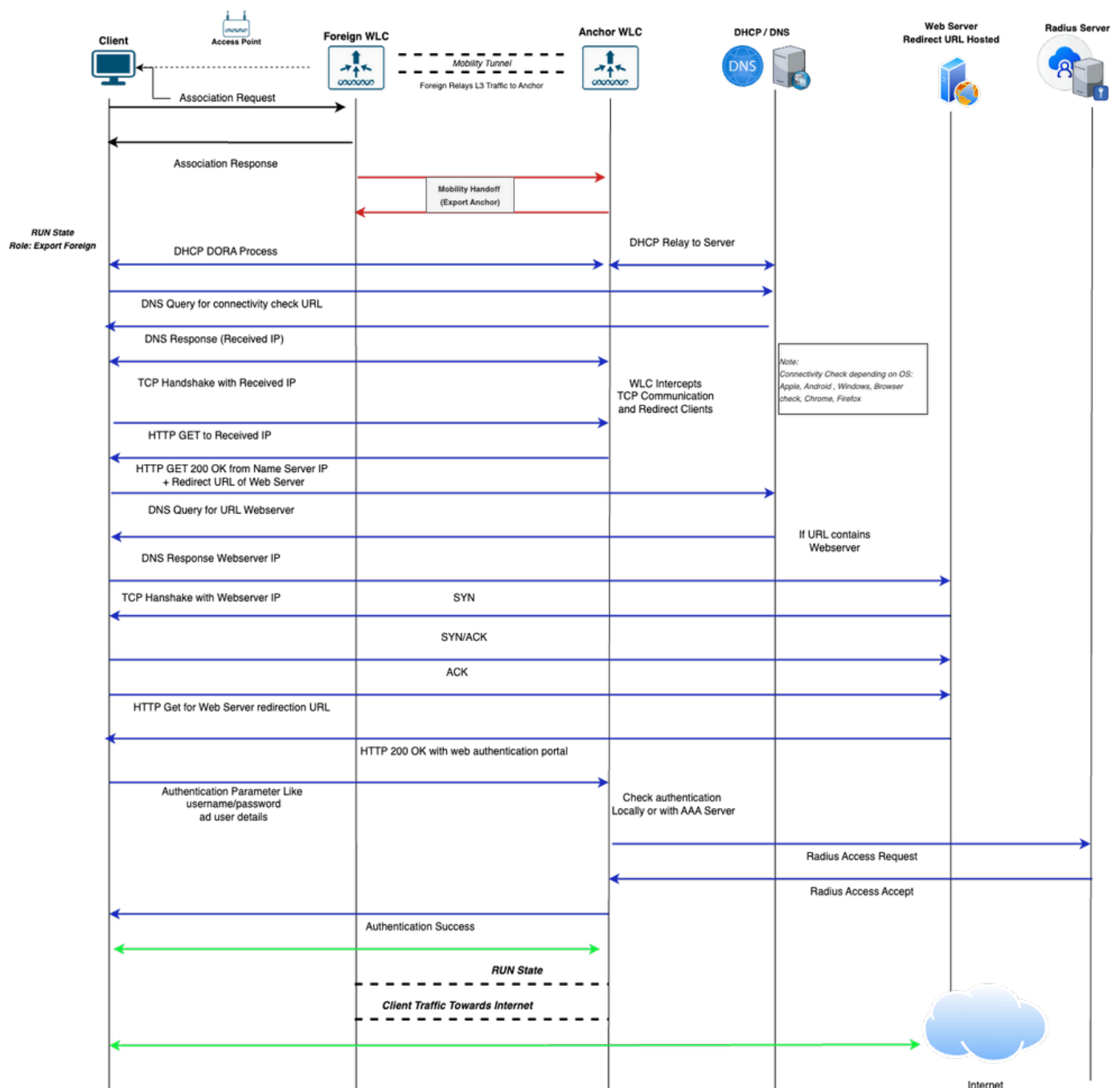


Diagrama de flujo de conectividad del cliente para SSID de Webauth externo en la configuración de anclaje externo

Análisis del Flujo SSID de Webauth Externo en la Configuración de Anclaje Externo a través de Registros

En esta sección se explica el flujo de conectividad de cliente para SSID de autenticación web externa mediante el uso de seguimiento radioactivo (RA Trace), capturas de paquetes incrustados (EPC) y el estado del cliente en los controladores externos y de anclaje.

Registros de controlador externo

Trazas radiactivas

!! Client Association Phase !!

```
{wncd_x_R0-1}{1}: [client-orch-sm] [17162]: (note): MAC: Client_MAC Association received. BSSID BSSID_M
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_IN
{wncd_x_R0-1}{1}: [dot11] [17162]: (info): MAC: Client_MAC dot11 send association response. Sending ass
{wncd_x_R0-1}{1}: [dot11] [17162]: (note): MAC: Client_MAC Association success. AID 1, Roaming = False,
{wncd_x_R0-1}{1}: [dot11] [17162]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_INIT -> S_DO
```

!! Layer 2 Authentication None !!

```
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-1}{1}: [client-auth] [17162]: (note): MAC: Client_MAC L2 Authentication initiated. method WE
{wncd_x_R0-1}{1}: [client-auth] [17162]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-1}{1}: [client-auth] [17162]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-1}{1}: [client-auth] [17162]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-1}{1}: [client-orch-sm] [17162]: (debug): MAC: Client_MAC L2 Authentication of station is su
{wncd_x_R0-1}{1}: [client-orch-sm] [17162]: (note): MAC: Client_MAC Mobility discovery triggered. Client
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_L2
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_MO
```

!! Mobility Handoff !!

```
{mobilityd_R0-0}{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gro
{mobilityd_R0-0}{1} [mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP [mobilityd_R0-0]{1} [mm-client] [1
{mobilityd_R0-0}{1} [mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P
[mobilityd_R0-0]{1} [mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o
[mobilityd_R0-0]{1} [mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_ANN
{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Sending export_Anchor_req of XID (XID) to (
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282)
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
[mobilityd_R0-0]{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed[mobilityd_R0-0]{1} [17047] (info) MAC
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_IP.
```

!! Client AAAA Traffic !!

```
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff base check is VALID
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) t
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of XI
{wncd_x_R0-0}{1}: [mm-transition] [17047]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_FOREIGN ->
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Mobile AAA Handoff update received.
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC Received username=Test321
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC IPv6 Client payload is re
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (38840)
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
```

```
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
```

Captura de paquete

El cliente envía una solicitud de asociación, que controla el controlador externo.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:18:59...	10.107.79.236	10.107.79.30	250	802.11		Association Request, SN=209, FN=0, Flags=....., SSID="DMZ_EWA"
Jan 14, 2025 16:18:59...	10.107.79.236	10.107.79.30	246	802.11		Association Request, SN=209, FN=0, Flags=....., SSID="DMZ_EWA"
Jan 14, 2025 16:18:59...	10.107.79.30	10.107.79.236	211	802.11		Association Response, SN=0, FN=0, Flags=.....
Jan 14, 2025 16:18:59...	10.107.79.30	10.107.79.236	215	802.11		Association Response, SN=0, FN=0, Flags=.....

Fase de asociación de cliente con controlador externo

Una transferencia de movilidad se desencadena entre los controladores externos y de anclaje a través del puerto UDP 16667. Tras un evento de movilidad exitoso, el estado del cliente pasa a EJECUTARSE con una función Externa de exportación.

El controlador externo recibe el tráfico DHCP del cliente a través del túnel CAPWAP y lo reenvía al controlador de anclaje para su procesamiento posterior.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:01...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	424	DHCP	0	DHCP Discover - Transaction ID 0x9f36b979
Jan 14, 2025 16:19:01...	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 14, 2025 16:19:03...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 14, 2025 16:19:03...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0	DHCP Offer - Transaction ID 0x9f36b979
Jan 14, 2025 16:19:03...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	452	DHCP	0	DHCP Request - Transaction ID 0x9f36b979
Jan 14, 2025 16:19:03...	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
Jan 14, 2025 16:19:03...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 14, 2025 16:19:03...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0	DHCP ACK - Transaction ID 0x9f36b979

El tráfico DHCP del cliente recibido en el controlador externo se reenvía al controlador de anclaje mediante el túnel de movilidad

De manera similar, el cliente envía el estado de conectividad de red y el tráfico de verificación de acceso a la página web al WLC externo a través del túnel CAPWAP; el WLC extranjero reenvía esto al WLC de anclaje usando el túnel de movilidad, donde el controlador de anclaje intercepta o procesa el tráfico.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, DNS IP	165	DNS	0	Standard query 0x389b Connectivity Check URL
Jan 14, 2025 16:19:05...	10.107.79.30	10.105.60.114	149	UDP		16667 → 16667 Len=103
Jan 14, 2025 16:19:05...	10.105.60.114	10.107.79.30	291	UDP		16667 → 16667 Len=245
Jan 14, 2025 16:19:05...	10.107.79.30, DNS IP	10.107.79.129,10.105.60.254	307	DNS	0	Standard query response 0x389b A Connectivity Check URL
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, Resolved IP	148	TCP	0	62437 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:05...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:05...	10.105.60.114	10.107.79.30	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:05...	10.107.79.30, Resolved IP	10.107.79.129,10.105.60.254	140	TCP	0	80 → 62437 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, Resolved IP	136	TCP	0	62437 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, Resolved IP	247	HTTP	0	GET /connecttest.txt HTTP/1.1
Jan 14, 2025 16:19:05...	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:05...	10.107.79.30, Resolved IP	10.107.79.129,10.105.60.254	128	TCP	0	80 → 62437 [ACK] Seq=1 Ack=112 Win=64256 Len=0
Jan 14, 2025 16:19:05...	10.105.60.114	10.107.79.30	961	UDP		16667 → 16667 Len=915
Jan 14, 2025 16:19:05...	10.107.79.30, Resolved IP	10.107.79.129,10.105.60.254	977	HTTP	0	HTTP/1.1 200 OK (text/html)
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, Resolved IP	136	TCP	0	62437 → 80 [FIN, ACK] Seq=112 Ack=850 Win=130304 Len=0
Jan 14, 2025 16:19:05...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:05...	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:05...	10.107.79.30, Resolved IP	10.107.79.129,10.105.60.254	128	TCP	0	80 → 62437 [FIN, ACK] Seq=850 Ack=113 Win=64256 Len=0
Jan 14, 2025 16:19:05...	10.107.79.129,10.105.60.254	10.107.79.30, Resolved IP	136	TCP	0	62437 → 80 [ACK] Seq=113 Ack=851 Win=130304 Len=0
Jan 14, 2025 16:19:05...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66

Comprobación del estado de la conectividad de red en el controlador externo

```

> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco (08:00:0c:2c:54:00), Dst: Cisco (08:00:0c:2c:54:00)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.105.60.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 62437, Seq: 1, Ack: 112, Len: 849
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://10.106.32.130:8443/portal/PortalSetup.action?portal=d06bc251-f644-4fc3-b09f-dae9bd8a86
    Content-Type: text/html\r\n
  > Content-Length: 580\r\n
  \r\n
  [Request in frame: 788]
  [Time since request: 0.000991000 seconds]
  [Request URI: /connecttest.txt]
  [Full request URI: ]
  File Data: 580 bytes
> Line-based text data: text/html (9 lines)

```

URL de redirección enviada al cliente

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	148	TCP	0	62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	140	TCP	1	8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	1386	TCP	0	62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 1180]
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	683	TLSv1..	0	Client Hello
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	659	UDP		16667 → 16667 Len=613
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	1342	UDP		16667 → 16667 Len=1296
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	450	UDP		16667 → 16667 Len=404
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	917	UDP		16667 → 16667 Len=871
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	1378	TCP	0	8443 → 62448 [ACK] Seq=1 Ack=1798 Win=33280 Len=1250 [TCP PDU reassembled in 1192]
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	933	TLSv1..	0	Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [ACK] Seq=1798 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	143	TLSv1..	0	Alert (Level: Fatal, Description: Certificate Unknown)
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [FIN, ACK] Seq=1805 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	262	TLSv1..	0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	118	UDP		16667 → 16667 Len=72
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	157	UDP		16667 → 16667 Len=111
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62449 → 8443 [ACK] Seq=1860 Ack=2107 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	1143	TLSv1..	0	Application Data
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	1119	UDP		16667 → 16667 Len=1073
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	1378	TCP	0	8443 → 62449 [ACK] Seq=8357 Ack=2867 Win=37120 Len=1250 [TCP PDU reassembled in 1267]
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62449 → 8443 [ACK] Seq=2867 Ack=10564 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	1168	TLSv1..	0	Application Data
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	1144	UDP		16667 → 16667 Len=1098

Página Acceso de Cliente a Webauth Externo para Proporcionar Detalles de Autenticación

Registros del controlador de anclaje

Trazas radiactivas

!! Mobility Handoff !!

```

{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Number of client is BELOW wlan limit
{mobilityd_R0-0}{1} [mm-transition] [26021] (info) MAC Client-MAC MMFSM transition S_MC_INIT -> S_MC_An

```

!! Session Created for Client !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-ac] [24229]: (info): mobility_a0000001[Client_MAC][ 0.0.0.0]Applying IPv4 i
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_CR
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_INIT -> S_
□{wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Roam type changed - None -> L3 Requested
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.
{□wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.>> Client is successf
```

!! Client DHCP Traffic !!

```
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILIT
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_P
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wncd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA
{wncd_x_R0-0}{1} [client-iplearn] [24229] (note) MAC Client-MAC Client IP learn successful. Method DHCP
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Sending ipv4_address_update of XID (XID)
{wncd_x_R0-0}{1} [client-iplearn] [24229] (info) MAC Client-MAC IP-learn state transition S_IPLEARN_IN_
Complete
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC Received ip learn response. method
```

!! External Web Authentication !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_IP
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62441/235
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Read co
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Read co
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62440/233
{wncd_x_R0-0}{1}: [sisf-packet] [24229]: (info): RX: IPv6 DHCP from intf mobility_a0000001 on vlan 31 S
{wncd_x_R0-0}{1}: [sisf-packet] [24229]: (info): TX: IPv6 DHCP from intf mobility_a0000001 on vlan 31 S
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62480/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62481/239
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]HTTP GE
```

{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Parse G
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -654303708,sm
{wncd_x_R0-0}{1}: [caaa-authen] [24229]: (info): [CAAA:AUTHEN:910007e3] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Send Access-Request to 10.106.32.130:1812 id 0/3, 1
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Calling-Station-Id [31] 19 Client_MAC
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: User-Name [1] 9 Test321
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 49
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 43 audit-session-id=723C690A000007
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Framed-IP-Address [8] 6 10.105.60.254
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 12 vlan-id=31
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-IP-Address [4] 6 10.105.60.114
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-Port-Type [61] 6 Virtual [5]
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-Port [5] 6 0
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 31
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 25 cisco-wlan-ssid=DMZ_EWA
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 33
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 27 wlan-profile-name=DMZ_EWA
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Called-Station-Id [30] 27 Called-Station-ID
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Airespace [26] 12
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Airespace-WLAN-ID [1] 6 7
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Nas-Identifier [32] 12 DMZSiteWLC
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Started 5 sec timeout
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Received from id 1812/3 10.106.32.130:0, Access-Acc
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: User-Name [1] 9 Test321
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat
{wncd_x_R0-0}{1}: [radius] [24229]: (info): Valid Response Packet, Free the identifier
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]State A
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Unapply I
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Unapply I
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : username 0 Test321
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : class 0 43 41 43 53 3a 37 32 33 4
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : Message-Authenticator 0 <hidden>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : method 0 1 [webauth]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 d0 37 45 88 25 5
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : intf-id 0 2684354561 (0xa0000001
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [24229]: (info): [Client_MAC:mobility_a0000001] SM Notified attr
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Received User-Name Test321
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Method webauth changing st
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event AUTHZ_SUCCESS
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [webauth-sess] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]State A
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/2
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]

```
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_ANCHOR -> S_MA_ANCHOR_WAIT
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of 1
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff base check is VALID
{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_MC_ANCHOR_WAIT
{mobilityd_R0-0}{1}: [mm-client] [26021]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 of 1
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) to 10.105.60.114
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type: 0 of 1
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_ANCHOR_WAIT -> S_MC_RUN
```

Captura de paquete

Después de la transferencia de movilidad, el controlador de anclaje recibe el tráfico DHCP del controlador externo a través del túnel de movilidad.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 15:59:04...	10.107.79.30	10.105.60.114	396	UDP		16667 → 16667 Len=354
Jan 14, 2025 15:59:04...	0.0.0.0	255.255.255.255	286	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 14, 2025 15:59:06...	10.105.60.69	10.105.60.254	286	DHCP		DHCP Offer - Transaction ID 0x9f36b979
Jan 14, 2025 15:59:06...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354
Jan 14, 2025 15:59:06...	10.107.79.30	10.105.60.114	424	UDP		16667 → 16667 Len=382
Jan 14, 2025 15:59:06...	0.0.0.0	255.255.255.255	286	DHCP		DHCP Request - Transaction ID 0x9f36b979
Jan 14, 2025 15:59:06...	10.105.60.69	10.105.60.254	286	DHCP		DHCP ACK - Transaction ID 0x9f36b979
Jan 14, 2025 15:59:06...	10.105.60.114	10.107.79.30	396	UDP		16667 → 16667 Len=354

Tráfico DHCP del cliente en controlador de anclaje recibido del controlador externo

El controlador de anclaje recibe comprobaciones de conectividad, solicitudes de acceso a páginas web y detalles de autenticación para seguir procesando.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:06...	10.107.79.30	10.105.60.114	141	UDP		16667 → 16667 Len=95
Jan 14, 2025 16:19:06...	10.105.60.254	DNS IP	83	DNS		Standard query 0x389b Connectivity Check URL
Jan 14, 2025 16:19:06...	DNS IP	10.105.60.254	237	DNS		Standard query response 0x389b A Connectivity Check URL
Jan 14, 2025 16:19:06...	10.105.60.114	10.107.79.30	287	UDP		16667 → 16667 Len=245
Jan 14, 2025 16:19:06...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:06...	10.105.60.254	Resolved IP	70	TCP		62437 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:06...	Resolved IP	10.105.60.254	66	TCP		80 → 62437 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 14, 2025 16:19:06...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:06...	10.107.79.30	10.105.60.114	223	UDP		16667 → 16667 Len=177
Jan 14, 2025 16:19:06...	10.105.60.254	Resolved IP	58	TCP		62437 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:06...	Resolved IP	10.105.60.254	169	HTTP		GET /connecttest.txt HTTP/1.1
Jan 14, 2025 16:19:06...	Resolved IP	10.105.60.254	903	HTTP		HTTP/1.1 200 OK (text/html)
Jan 14, 2025 16:19:06...	10.105.60.114	10.107.79.30	957	UDP		16667 → 16667 Len=915
Jan 14, 2025 16:19:06...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:06...	10.105.60.254	Resolved IP	58	TCP		62437 → 80 [FIN, ACK] Seq=112 Ack=850 Win=130304 Len=0
Jan 14, 2025 16:19:06...	Resolved IP	10.105.60.254	54	TCP		80 → 62437 [FIN, ACK] Seq=850 Ack=113 Win=64256 Len=0
Jan 14, 2025 16:19:06...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:06...	10.105.60.254	Resolved IP	58	TCP		62437 → 80 [ACK] Seq=113 Ack=851 Win=130304 Len=0

Comprobación del estado de la conectividad de red en el controlador de anclaje

```

> Frame 426: 903 bytes on wire (7224 bits), 903 bytes captured (7224 bits)
> Ethernet II, Src: [REDACTED], Dst: [REDACTED]
> Internet Protocol Version 4, Src: [REDACTED], Dst: 10.105.60.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 62437, Seq: 1, Ack: 112, Len: 849
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://10.106.32.130:8443/portal/PortalSetup.action?portal=d06bc251-f644-4fc3-b09f-dae9bd8a86
    Content-Type: text/html\r\n
    Content-Length: 580\r\n
  \r\n
  [Request in frame: 423]
  [Time since request: 0.000000000 seconds]
  [Request URI: /connecttest.txt]
  [Full request URI: [REDACTED]]
  File Data: 580 bytes
> Line-based text data: text/html (9 lines)

```

URL de redirección enviada al cliente

El cliente envía las credenciales de autenticación a través del portal. Estas credenciales se validan localmente en el WLC o a través de un servidor de autenticación externo, dependiendo de la política de seguridad configurada.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	66	TCP		62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	70	TCP		8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	659	UDP		16667 → 16667 Len=613
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1342	UDP		16667 → 16667 Len=1296
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1304	TCP		62449 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 717]
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	537	TLSv1..		Client Hello
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1308	TCP		8443 → 62449 [ACK] Seq=1 Ack=1734 Win=34688 Len=1250 [TCP PDU reassembled in 724]
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	446	UDP		16667 → 16667 Len=404
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	863	TLSv1..		Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	913	UDP		16667 → 16667 Len=871
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62449 → 8443 [ACK] Seq=1734 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	180	TLSv1..		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	64	TLSv1..		Change Cipher Spec
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	103	TLSv1..		Encrypted Handshake Message
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	114	UDP		16667 → 16667 Len=72
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	153	UDP		16667 → 16667 Len=111
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62449 → 8443 [ACK] Seq=1860 Ack=2107 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1119	UDP		16667 → 16667 Len=1073
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1061	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1015	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	962	UDP		16667 → 16667 Len=920
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1144	UDP		16667 → 16667 Len=1098
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1086	TLSv1..		Application Data
Jan 14, 2025 16:19:25...	10.105.60.114	10.106.32.130	460	RADIUS		Access-Request id=3
Jan 14, 2025 16:19:25...	10.105.60.114	10.106.32.130	460	RADIUS		Access-Request id=3, Duplicate Request
Jan 14, 2025 16:19:25...	10.106.32.130	10.105.60.114	191	RADIUS		Access-Accept id=3
Jan 14, 2025 16:19:25...	10.106.32.130	10.105.60.114	187	RADIUS		Access-Accept id=3, Duplicate Response

Página Acceso de Cliente a Webauth Externo para Proporcionar Detalles de Autenticación

Estado del cliente en el controlador externo y de anclaje

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

> Delete



Selected 0 out of 1 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	[REDACTED]	10.105.60.254	fe80::877c:b748:ddc:4fc0	[REDACTED]	1	DMZ_EWA	14	WLAN	Run	11ac		N/A	Export Foreign	No

1 - 1 of 1 clients

Estado del cliente en el extranjero

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
		10.105.60.254	fe80::877c:b748:ddc:4fc0		0	DMZ_EWA	7	WLAN	Run	N/A	Test321	N/A	Export Anchor	No

1 - 1 of 1 clients

Estado del cliente en anclaje

Client

360 ViewGeneralQOS StatisticsATF StatisticsMobility History

Client PropertiesAP PropertiesSecurity InformationClient Statistics

Max Client Protocol Capability	802.11ac Wave 2
Wi-Fi to Cellular Steering	Not implemented
Cellular Capability	N/A
Regular ASR support	DISABLED
Mobility	
Anchor IP Address	10.105.60.114
Point of Presence	0xA0000003
AuthC Status	True
Move Count	0
Role	Export Foreign
Roam Type	L3 Requested

Propiedades del cliente en Foreign

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

Propiedades del cliente en delimitador

Equilibrio de carga entre varios controladores de anclaje

Cuando se asigna más de un controlador de anclaje a una sola WLAN, la distribución del tráfico depende de la prioridad. Se pueden configurar tres niveles de prioridad: Primaria, Secundaria y Superior. La función de prioridad de anclaje de invitado proporciona un mecanismo para la distribución de carga activa/en espera entre los controladores de anclaje. Esto se logra asignando una prioridad fija a cada controlador de anclaje: la carga se distribuye al controlador de mayor prioridad, y de forma rotativa entre los controladores que comparten el mismo valor de prioridad.

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile. There are anchors configured on the policy. Remove anchors before disabling Central Switching.

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

☐

Static IP Mobility

☐ DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

Anchor IP

No anchors available

Selected (1)

Anchor IP

Anchor Priority

 10.105.60.114	Tertiary (3) ▼	←
---	----------------	---

Prioridad de anclaje de asignación



Nota: De forma predeterminada, la prioridad terciaria se configura durante la asignación del controlador de anclaje en el controlador externo.

Resolución de problemas de conectividad del cliente en escenario de anclaje externo

1. Problemas de Onboarding del Cliente

- Estado del túnel: Verifique que el túnel de movilidad entre los controladores externos y de anclaje permanezca activo.
- Discordancia de configuración: Garantice la paridad de la configuración entre ambos controladores. Las discrepancias en los nombres de WLAN, los nombres de perfiles de política o la configuración avanzada (como la anulación de AAA, los requisitos DHCP de IPv4 y NAC) provocan errores de coincidencia de perfil o de denegación de anclaje.
- Otro: Si el túnel está activo sin ningún problema de configuración, el enfoque de troubleshooting es similar al problema de conectividad del cliente normal, asegurándose de verificar en el controlador respectivo que maneja el tráfico afectado.

2. Conectividad intermitente

- i. Aletas del túnel: Si los paquetes keepalive entre los dos controladores no llegan, el túnel se inestabiliza, lo que impide que el cliente mantenga una conexión con el SSID.
- ii. Ancho de banda bajo: Si la MTU de ruta (PMTU) entre los pares de movilidad descende a un valor inferior (576), los clientes experimentan una degradación del rendimiento. Esto sucede generalmente cuando se pierden los mensajes keepalive mtu de la trayectoria entre ambos pares de movilidad



Nota: El controlador con la dirección MAC de movilidad inferior inicia los mensajes keepalive estándar y keepalive de MTU de trayecto.

3. Problemas específicos de acceso al sitio web

- i. Los encabezados de tráfico de movilidad incluyen identificadores de grupos de movilidad, direcciones MAC, direcciones IP y paquetes CAPWAP DTLS cifrados intercambiados a través de los puertos UDP 16666 y 16667. Esta sobrecarga se agrega al encabezado CAPWAP existente. Para el tráfico TCP, ajuste posterior de TCP MSS configurado para AP, si el tamaño del paquete excede la PMTU de movilidad (máximo 1385 bytes) debido a esta sobrecarga adicional, ocurre la fragmentación. Mientras que la fragmentación es generalmente manejada por la red, surgen problemas si los paquetes llegan fuera de orden o tarde. Estas condiciones afectan al reensamblado de paquetes y dan lugar a errores de accesibilidad de datos para sitios web específicos.

Recopilación de registros del controlador externo y de anclaje

1. Habilite term exec prompt timestamp para tener una referencia de tiempo para todos los comandos.
2. Utilice show tech-support wireless !! para revisar la configuración.
3. Puede comprobar el estado del túnel de movilidad show wireless mobility summary !!
4. Estadísticas para el par de movilidad que incluyen el estado del link, los datos y eventos del cliente, las estadísticas de keepalive muestran el ip del par de movilidad inalámbrica <IP>
5. Habilite el seguimiento radioactivo para la dirección IP/MAC del par de movilidad y la dirección MAC del cliente.

A través de CLI:

```
debug wireless {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !!
```

La configuración del tiempo nos permite habilitar seguimientos hasta por 24 días .

```
no debug wireless {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x} !!
```

Para deshabilitar la depuración

WLC genera un archivo de seguimiento de depuración con Client_info, comando para

verificar el archivo de seguimiento de depuración generado por dir bootflash: | i debug !!



Advertencia: La depuración condicional habilita el registro de nivel de depuración que, a su vez, aumenta el volumen de los registros generados. Si deja esta opción en ejecución, reducirá la cantidad de tiempo desde el que puede ver los registros. Por lo tanto, se recomienda desactivar siempre la depuración al final de la sesión de solución de problemas.

6. Para inhabilitar toda la depuración, ejecute estos comandos:

```
# clear platform condition all !!
```

```
# undebg all !!
```

A través de GUI:

Paso 1. Navegue hasta Troubleshooting > Radioactive Trace.

Paso 2. Haga clic en Agregar e ingrese una dirección MAC/IP del par de movilidad o una dirección MAC del cliente que desee resolver.

Paso 3. Cuando esté listo para iniciar el rastreo radiactivo, haga clic en Iniciar. Una vez iniciado, el registro de depuración se escribe en el disco sobre cualquier procesamiento del plano de control relacionado con las direcciones MAC objeto de seguimiento.

Paso 4. Cuando reproduzca el problema que desea resolver, haga clic en Detener.

Paso 5. Para cada dirección MAC depurada, puede generar un archivo de registro que recopile todos los registros pertenecientes a esa dirección MAC haciendo clic en Generar.

Paso 6. Elija cuánto tiempo atrás desea que transcurra el archivo de registro intercalado y haga clic en Aplicar al Dispositivo.

Paso 7. Ahora puede descargar el archivo haciendo clic en el pequeño icono junto al nombre del archivo. Este archivo está presente en la unidad flash de arranque del controlador y también se puede copiar desde el primer momento mediante CLI.

7. Capturas incrustadas

A través de CLI:

```
monitor capture MYCAP clear !!
```

```
monitor capture MYCAP interface Po1 both !!
```

```
monitor capture MYCAP buffer size 100 !!
```

```
monitor capture MYCAP match access-list name !! (si se realiza un seguimiento del tráfico del túnel de movilidad entre el WLC)
```

```
monitor capture MYCAP match any/ipv4/ipv6.MAC !!
```

```
monitor capture MYCAP start !!
```

```
!!Reproducir
```

```
monitor capture MYCAP stop
```

```
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap
```

A través de GUI:

Paso 1. Vaya a Troubleshooting > Packet Capture > +Add.

Paso 2. Defina el nombre de la captura de paquetes. Se permite un máximo de 8 caracteres.

Paso 3. Defina los filtros, si los hay.

Paso 4. Marque la casilla para Monitorear el Tráfico de Control si desea ver el tráfico dirigido a la CPU del sistema e inyectado de nuevo en el plano de datos.

Paso 5. Defina el tamaño del búfer. Se permite un máximo de 100 MB.

Paso 6. Defina el límite, ya sea por la duración que permite un rango de 1 - 1000000 segundos o por el número de paquetes que permite un rango de 1 - 100000 paquetes, según lo deseado.

Paso 7. Elija la interfaz de la lista de interfaces de la columna izquierda y seleccione la flecha para moverla a la columna derecha.

Paso 8. Haga clic en Guardar y aplicar al dispositivo.

Paso 9. Para iniciar la captura, seleccione Iniciar.

Paso 10. Puede dejar que la captura se ejecute hasta el límite definido. Para detener manualmente la captura, seleccione Stop.

Paso 11. Una vez detenido, un botón Exportar está disponible para hacer clic con la opción de descargar el archivo de captura (.pcap) en el escritorio local a través de HTTP o servidor TFTP o servidor FTP o disco duro del sistema local o flash.

Información Relacionada

[Configuración de topologías de movilidad en WLC Catalyst 9800](#)

[Configuración de la función de movilidad de anclaje WLAN en Catalyst 9800](#)

[Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).