

Comprendre le flux de trafic dans une configuration d'ancrage étranger entre un WLC 9800

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation du scénario d'ancrage étranger](#)

[Topologie](#)

[WLAN avec authentification de couche 2](#)

[Configuration requise](#)

[Flux pour le SSID basé sur l'ancrage étranger de couche 2](#)

[Analyse du flux SSID de couche 2 dans la configuration d'ancrage étranger via les journaux](#)

[Journaux du contrôleur étranger](#)

[Journaux du contrôleur Anchor 9800](#)

[État du client sur le contrôleur étranger et le contrôleur d'ancrage](#)

[WLAN avec authentification de couche 3](#)

[Authentification Web locale](#)

[Flux pour SSID Webauth local dans la configuration d'ancrage étranger](#)

[Analyse du flux SSID Webauth local dans la configuration d'ancrage étranger via les journaux](#)

[Journaux du contrôleur étranger](#)

[Journaux du contrôleur d'ancrage](#)

[État du client sur le contrôleur étranger et le contrôleur d'ancrage](#)

[Authentification Web centralisée](#)

[Flux pour le SSID Webauth central dans la configuration d'ancrage étranger](#)

[Analyse du flux SSID Webauth central dans la configuration d'ancrage étranger via les journaux](#)

[Journaux du contrôleur étranger](#)

[Journaux du contrôleur d'ancrage](#)

[État du client sur le contrôleur étranger et le contrôleur d'ancrage](#)

[Authentification Web externe](#)

[Flux pour le SSID Webauth externe dans la configuration d'ancrage étranger](#)

[Analyse du flux SSID Webauth externe dans la configuration d'ancrage étranger via les journaux](#)

[Journaux du contrôleur étranger](#)

[Journaux du contrôleur d'ancrage](#)

[État du client sur le contrôleur étranger et le contrôleur d'ancrage](#)

[Équilibrage De Charge Entre Contrôleur D'Ancrage Multiple](#)

[Dépannage de la connectivité client dans un scénario d'ancrage étranger](#)

[Collecte des journaux à partir du contrôleur étranger et d'ancrage](#)

[Informations connexes](#)

Introduction

Ce document décrit le flux de trafic dans la configuration Foreign-Anchor entre les WLC Cisco 9800, couvrant l'intégration et le dépannage des clients L2/L3.

Conditions préalables

Tunnel de mobilité entre contrôleur étranger et contrôleur d'ancrage.

Les ports UDP 16666 et 16667 sont autorisés entre les deux WLC.

Profil de stratégie configuré pour la commutation centrale.

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

État du tunnel de mobilité sur le WLC étranger

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

État du tunnel de mobilité sur le WLC d'ancrage

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Accès aux contrôleurs sans fil via l'interface de ligne de commande ou l'interface utilisateur graphique
- Mobilité sur les contrôleurs LAN sans fil (WLC) Cisco
- Contrôleurs sans fil 9800
- Traces radioactives et capture de paquets sur le WLC 9800

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Modèle WLC 9800
- Cisco IOS XE 17.15.5 version
- Modèle AP gamme 9100

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

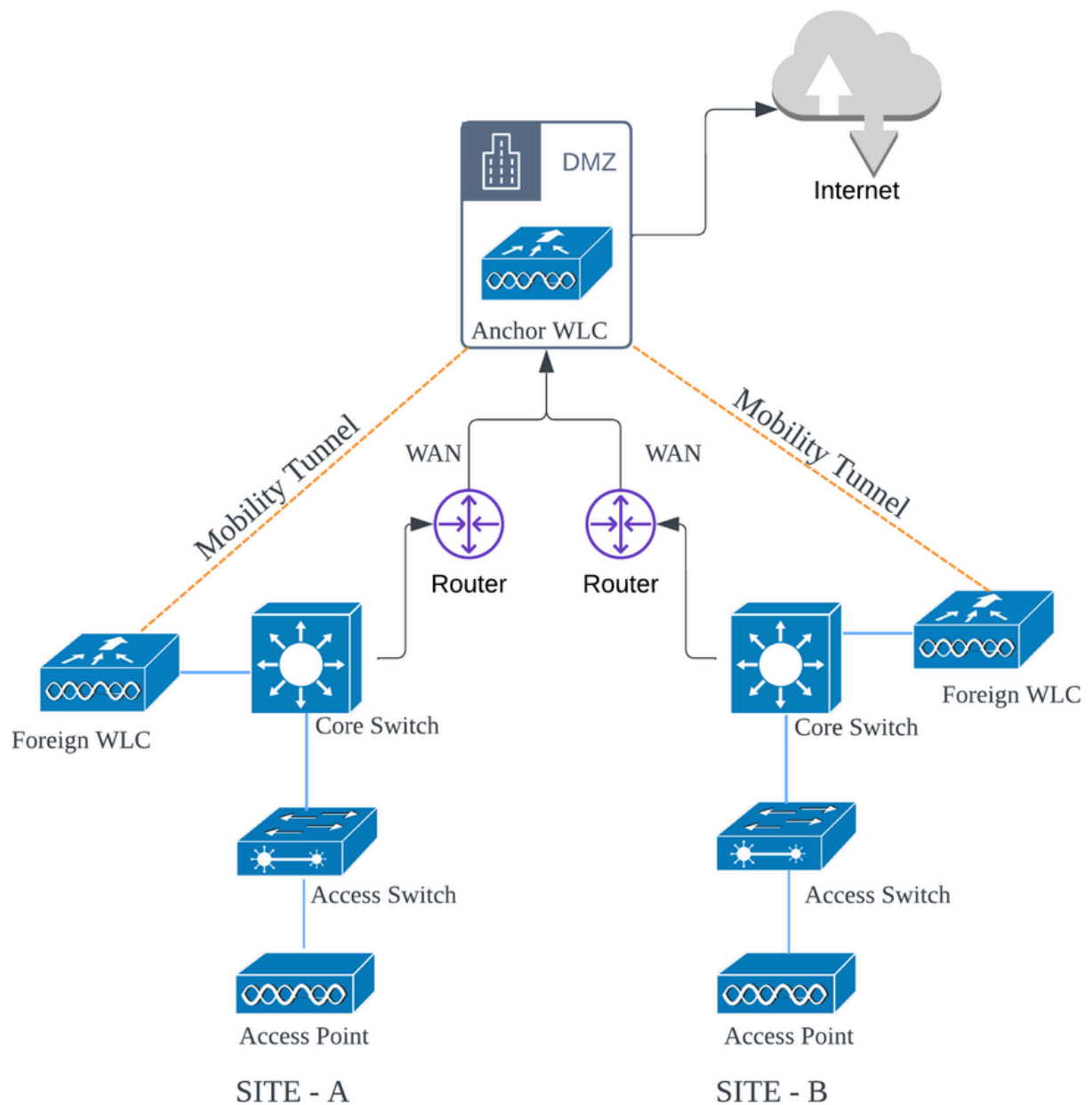
Présentation du scénario d'ancrage étranger

- Contrôleur étranger : Ce WLC gère la couche 2 ou le côté sans fil du réseau. Des points d'accès lui sont connectés et tout le trafic client des WLAN ancrés est encapsulé dans le tunnel de mobilité et envoyé au contrôleur d'ancrage. Le trafic ne sort pas localement sur le contrôleur étranger.
- Contrôleur d'ancrage : Il sert de point de sortie de la couche 3. Il reçoit le trafic client via le tunnel de mobilité des contrôleurs étrangers et décapsule ou termine le trafic client dans le point de sortie (VLAN). C'est là que les clients sont visibles sur le réseau.

Les points d'accès sur le WLC étranger diffusent les SSID WLAN et ont une balise de stratégie attribuée qui lie le profil WLAN au profil de stratégie approprié. Lorsqu'un client sans fil se connecte à ce SSID, le contrôleur étranger envoie le nom SSID et le profil de stratégie dans les informations du client au WLC d'ancrage. À la réception, le WLC d'ancrage vérifie sa propre configuration pour correspondre au nom SSID ainsi qu'au nom du profil de stratégie. Une fois que le WLC d'ancrage a trouvé une correspondance, il applique la configuration correspondante et fournit un point de sortie pour le client sans fil. Par conséquent, il est obligatoire que les noms et

configurations du WLAN et du profil de stratégie correspondent sur les WLC étrangers et d'ancrage 9800, à l'exception du VLAN sous le profil de stratégie.

Topologie



Configuration d'ancrage étranger entre WLC 9800

WLAN avec authentification de couche 2

Configuration requise

1. Assurez-vous que le nom et la configuration du WLAN sont identiques sur les WLC étrangers et d'ancrage et qu'ils sont configurés pour l'authentification de couche 2 (PSK ou 802.1x).
2. Créez un profil de stratégie avec le même nom sur les WLC étrangers et d'ancrage avec la même configuration.
3. Sur le WLC étranger, configurez le mappage du WLC d'ancrage dans le profil de stratégie respectif.
4. Sur le WLC d'ancrage, configurez le profil de stratégie pour désigner le contrôleur en tant qu'ancrage d'exportation.
5. Sur le WLC étranger, mappez le WLAN au profil de stratégie approprié à l'aide d'une balise de stratégie.

Flux pour le SSID basé sur l'ancrage étranger de couche 2

1. Le client initie une connexion au SSID diffusé par le WLC étranger. Le WLC étranger effectue l'authentification de couche 2, en validant les informations d'identification localement ou via un serveur AAA externe, selon la stratégie de sécurité configurée.
2. Une fois l'authentification réussie, la session client est ancrée au WLC d'ancrage. Le client reçoit une adresse IP et passe à l'état RUN sur le WLC d'ancrage.
3. Une fois la session établie, tout le trafic de données client est tunnelisé du WLC étranger au WLC d'ancrage, où il sort dans le réseau.

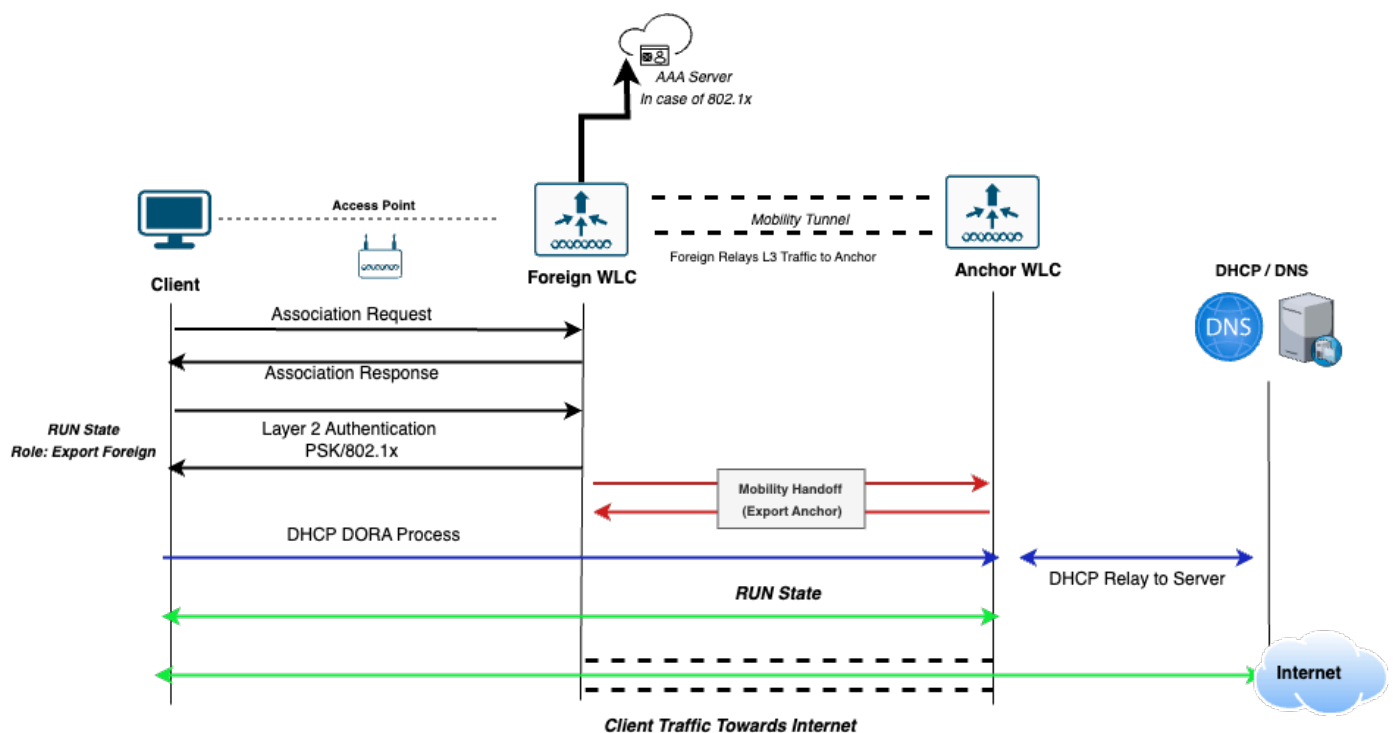


Diagramme de flux WLAN basé sur des ancrages étrangers de couche 2

Analyse du flux SSID de couche 2 dans la configuration d'ancrage étranger via les journaux

Cette section explique le flux de connectivité du client de couche 2 à l'aide de la trace radioactive (RA Trace), des captures de paquets intégrées (EPC) et de l'état du client sur les contrôleurs Foreign et Anchor.

Journaux du contrôleur étranger

Traces radioactives

!! 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 (C  
[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
```

Capture de paquets

Le client envoie une demande d'association et effectue l'authentification de couche 2, gérée par le contrôleur étranger.

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

Association client + trafic d'authentification de couche 2

Un transfert de mobilité se déclenche entre les contrôleurs étranger et d'ancrage via le port UDP 16667. Lors d'un événement de mobilité réussi, l'état du client passe à EXÉCUTER avec un rôle Exporter étranger.

Le contrôleur étranger reçoit le trafic DHCP client via le tunnel CAPWAP et le transfère au contrôleur d'ancrage pour un traitement ultérieur.

Time	Source Address	Destination Address	Length	Protocol	TID	Info
567 07:36:39.071987	10.107.79.129,0.0.0.0	10.107.79.30,255.255.255.255	424	DHCP		0 DHCP Discover - Transaction ID 0x9f36b979
568 07:36:39.071987	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
752 07:36:41.074993	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
753 07:36:41.074993	10.107.79.30,10.105.60.69	10.107.79.129,10.105.60.226	416	DHCP		0 DHCP Offer - Transaction ID 0x9f36b979
758 07:36:41.111993	10.107.79.129,0.0.0.0	10.107.79.30,255.255.255.255	452	DHCP		0 DHCP Request - Transaction ID 0x9f36b979
759 07:36:41.111993	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
760 07:36:41.113992	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
761 07:36:41.113992	10.107.79.30,10.105.60.69	10.107.79.129,10.105.60.226	416	DHCP		0 DHCP ACK - Transaction ID 0x9f36b979

Le trafic DHCP client reçu sur le contrôleur étranger est transféré au contrôleur d'ancrage à l'aide du tunnel de mobilité

Journaux du contrôleur Anchor 9800

Traces radioactives de l'ancre

!! 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
{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
```

!! Client DHCP Traffic !!

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

Capture de paquets sur l’ancre

Après le transfert de mobilité, le contrôleur d'ancrage reçoit le trafic DHCP du contrôleur étranger via le tunnel de mobilité.

Une fois le processus DORA terminé, le client passe à l'état EXÉCUTÉ avec un rôle d'ancrage d'exportation. À partir de ce point, le contrôleur d’ancrage sert de point de sortie pour le trafic de données client.

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

Trafic DHCP client sur le contrôleur d'ancrage reçu du contrôleur étranger

État du client sur le contrôleur étranger et le contrôleur d'ancrage

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::877c:b748:ddc:4fc0		1	DMZ_LWA	11	WLAN	Run	11ac		N/A	Export Foreign	No

1 ~ 1 of 1 clients

État du client sur étranger

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

État du client au point d'ancrage

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

Propriétés du client sur les

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

Propriétés du client sur l'ancre

WLAN avec authentification de couche 3

Authentification Web locale

Flux pour SSID Webauth local dans la configuration d'ancrage étranger

1. Le client initie une connexion au SSID annoncé par le WLC étranger.
2. Comme aucune authentification de couche 2 n'est effectuée, le client est immédiatement ancré au WLC d'ancrage. Le client passe à l'état EXÉCUTÉ sur le WLC étranger, avec son rôle de mobilité désigné comme Exportation étrangère.
3. Le client obtient une adresse IP et est redirigé vers une page Web. Ce trafic est géré par le contrôleur d'ancrage.
4. Une fois l'authentification réussie sur le portail, le client passe à l'état d'exécution sur le WLC d'ancrage, avec le rôle d'ancrage d'exportation.

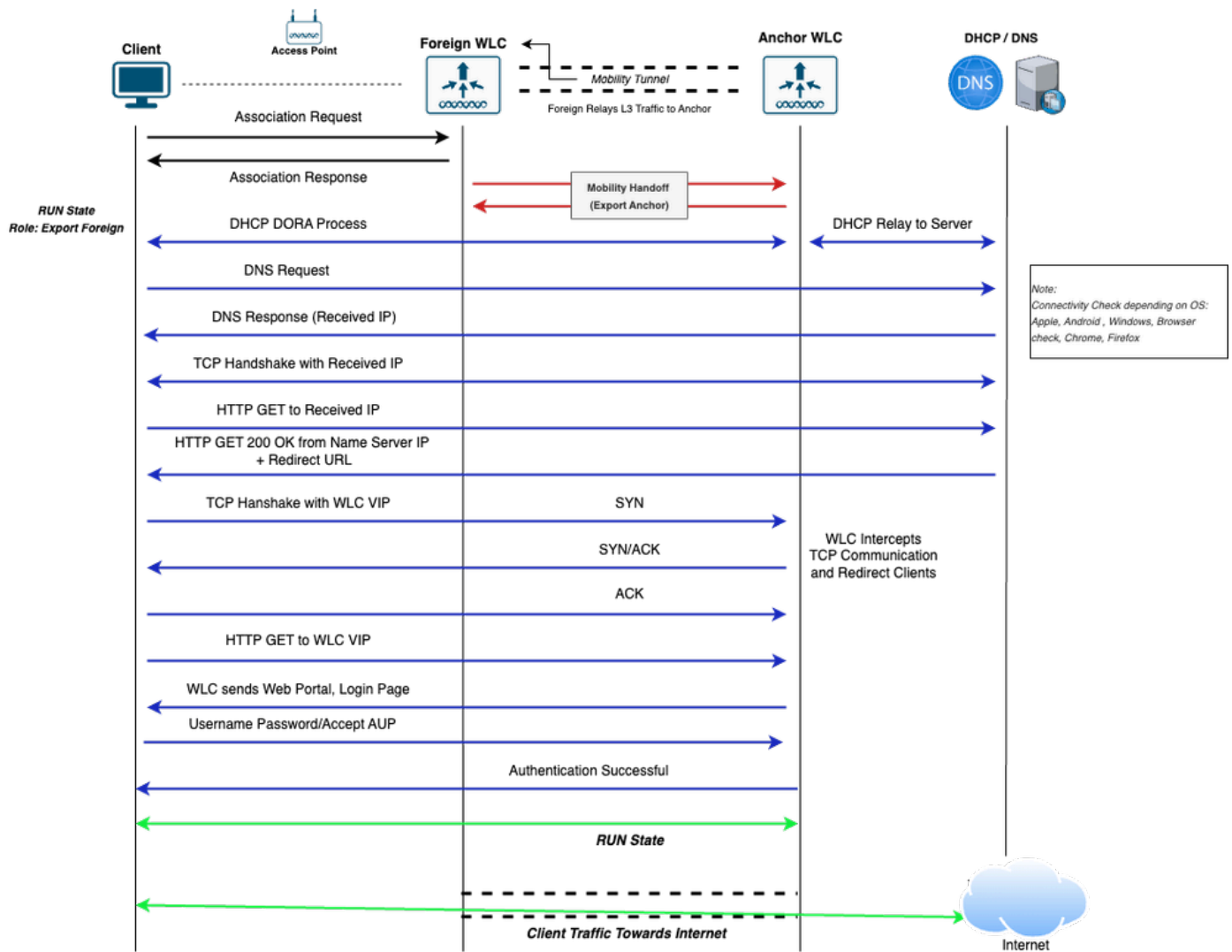


Diagramme de flux de connectivité client pour SSID Webauth local dans la configuration d'ancrage étranger

Analyse du flux SSID Webauth local dans la configuration d'ancrage étranger via les journaux

Cette section explique le flux de connectivité client pour le SSID d'authentification Web locale à l'aide de la trace radioactive (RA Trace), des captures de paquets intégrées (EPC) et de l'état du client sur les contrôleurs étranger et d'ancrage.

Journaux du contrôleur étranger

Traces radioactives

!! 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 !!
[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
[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 (
[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
[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 !!
[mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
[mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
[mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (10452) t
[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.
[sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC Received username=Guest1
[sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC IPv6 Client payload is re
[mm-client] [17047]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (10452)
[mm-client] [18401]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type:
[mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
[mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
[mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
[mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
[mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
[mm-pmtu] [18401]: (debug): Peer IP: Anchor-WLC-IP PMTU size is 1006 and calculate
[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
[mm-client] [18401]: (debug): MAC: Client_MAC aaa handoff ack successfully forward
```

Capture de paquets

Le client envoie une demande d'association que le contrôleur étranger traite.

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=.....

Phase d'association client avec contrôleur étranger

Un transfert de mobilité se déclenche entre les contrôleurs étranger et d'ancrage via le port UDP 16667. Lors d'un événement de mobilité réussi, l'état du client passe à EXÉCUTER avec un rôle Exporter étranger.

Le contrôleur étranger reçoit le trafic DHCP client via le tunnel CAPWAP et le transfère au contrôleur d'ancrage pour un traitement ultérieur.

Jan 5, 2025 12:21:42...	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 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	10.107.79.129,10.105.60.69	416	DHCP	0 DHCP Offer - Transaction ID 0x9f36b979
Jan 5, 2025 12:21:44...	10.107.79.129,0.0.0.0	10.107.79.30,255.255.255.255	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	10.107.79.129,10.105.60.69	416	DHCP	0 DHCP ACK - Transaction ID 0x9f36b979

Le trafic DHCP client reçu sur le contrôleur étranger est transféré au contrôleur d'ancrage à l'aide du tunnel de mobilité

De même, le client envoie l'état de connectivité réseau et le trafic de vérification d'accès à la page Web au WLC étranger via le tunnel CAPWAP ; le WLC étranger transfère ceci au WLC d'ancrage à l'aide du tunnel de mobilité, où le contrôleur d'ancrage intercepte ou traite le trafic.

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	10.107.79.129,10.105.60.226	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	10.107.79.129,10.105.60.226	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	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	10.107.79.129,10.105.60.226	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	10.107.79.129,10.105.60.226	761	HTTP	0	HTTP/1.1 200 OK (text/html)
Jan 5, 2025 12:21:46...	10.107.79.30	10.107.79.129,10.105.60.226	128	TCP	0	80 → 52887 [FIN, ACK] Seq=634 Ack=112 Win=64256 Len=0

Vérification de l'état de la connectivité réseau sur le contrôleur étranger

> Frame 2176: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits)
> Ethernet II, Src: Cisco_63:8b:8b (08:00:06:35:8b:8b), Dst: (08:00:06:35:8b:8b)
> 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: (08:00:06:35:8b:8b), 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)

Rediriger l'URL envoyée au client

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...	148	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...	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...		0 Client Hello
Jan 5, 2025 12:22:25...	10.107.79.129,10.105.60.226	10.107.79.30,142.250...	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...	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...	293	TLSv1...		0 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...		0 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...		0 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...		0 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...	181	TLSv1...		0 Encrypted Alert

Page Client Access to Local Webauth pour fournir les détails d'authentification

Journaux du contrôleur d'ancrage

Traces radioactives

!! 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_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-ac1] [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_MA_Anchor
{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 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 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
```

```
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC Received ip learn response. method
```

```
{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][ 10.105.60.226]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-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]Read co
```

```
{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]52910/195
```

```
{wncd x B0-0}{11}: [webauth-httpd] [24229]: (info): mobility a0000001[Client MAC][ 10.105.60.226]HTTP GE
```

```
{wncd x B0-0}{11}: [webauth-httpd] [24229]: (info): mobility a0000001[Client MAC][ 10.105.60.226]Read co
```

```
{wncd x R0-0}{1}: [webauth-state] [24229]: (info): mobility a00000001[Client MAC][ 10.105.60.226]State G
```

```
{wncid=x_R0=0}{1}: [webauth-io] [24229]: (info): mobility a00000001[Client MAC][ 10.105.60.226]52910/195
```

```
{wncid=x_R0-0}{11}: [webauth-httpd] [24225]: (info): mobility a00000001[Client MAC][ 10.105.60.226]52919/195
```

```
{wired_x_R0-0}{1}: [webauth-httpd] [24225]: (info): mobility_a00000001[Client-MAC][ 10:105:60:220]52919/1
{wired_x_R0-0}{13}: [webauth-httpd] [34338]: (info): mobility_a00000001[Client-MAC][ 10:105:60:336]53933/195
```

```
{wired_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a00000001[Client-MAC][ 10.105.60.226]52924/195
```

```
{wined_x_R0=0}{1}: [webauth-httpd] [24229]: (info): mobility_a00000001[Client MAC][ 10.105.60.226]GET /CV
{wined_x_R0=0}{1}: [webauth-httpd] [24230]: (info): mobility_a00000001[Client MAC][ 10.105.60.226]HTTP GET
```

```
{wined_x_R0=0}{1}: [webauth-httpd] [24229]: (info): mobility_a00000001[Client_MAC][ 10.105.60.226]Parse G
```

```
{wncd_x_R0-0}{1}: [webauth:state] [24229]: (info): mobility_a00000001[Client_MAC][ 10.105.60.226]Param=...
```

```
{whcd_x_RU-0}{1}: [webauth-page] [24229]: (Info): mobility_a0000001[Client_MAC][ 10.105.60.226]Sending
```

```
{whcd_x_RU=0}{1}: [webauth-to] [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_a00000001[Client_MAC][ 10.105.60.226]Parse G
```

```
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a00000001[Client_MAC][ 10.105.60.226]Parse 1
```

```
{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]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]Parse G
```

```
{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-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53009/1
```

```
{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_PR
{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 [cclient MAC: Client_MAC] Guest client detected. S
{wncd_x_R0-0}{1}: [cclient-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

Capture de paquets

Après le transfert de mobilité, le contrôleur d'ancrage reçoit le trafic DHCP du contrôleur étranger via le tunnel de mobilité.

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

Trafic DHCP client sur le contrôleur d'ancrage reçu du contrôleur étranger

Le contrôleur d'ancrage reçoit les vérifications de connectivité, les demandes d'accès aux pages Web et les détails d'authentification pour poursuivre le traitement.

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...	10.105.60.226	Resolved IP	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

Vérification de l'état de la connectivité réseau sur le contrôleur d'ancrage

> Frame 604: 687 bytes on wire (5496 bits), 687 bytes captured (5496 bits)

> Ethernet II, Src: , Dst:

> 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\nLocation: https://192.0.2.1/login.html?redirect=http://\r\nContent-Type: text/html\r\nContent-Length: 472\r\n\r\n[Request in frame: 601]\r\n[Time since request: 0.000992000 seconds]\r\n[Request URI: /connecttest.txt]\r\n[Full request URI:]\r\nFile Data: 472 bytes

> Line-based text data: text/html (9 lines)

Rediriger l'URL envoyée au client

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

Page Client Access to Local Webauth pour fournir les détails d'authentification

Une fois l'authentification Web locale réussie, le client passe à l'état EXÉCUTÉ avec un rôle d'ancrage d'exportation. À partir de ce point, le contrôleur d'ancrage sert de point de sortie pour le trafic de données client.

État du client sur le contrôleur étranger et le contrôleur d'ancrage

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			0	DMZ_LWA	5	WLAN	Run	N/A	Guest1	N/A	Export Anchor	No

1

10

1 - 1 of 1 clients



État du client sur étranger

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			0	DMZ_LWA	5	WLAN	Run	N/A	Guest1	N/A	Export Anchor	No

1

10

1 - 1 of 1 clients

État du client au point d'ancrage

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

Propriétés du client sur les

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

Propriétés du client sur l'ancre

Authentification Web centralisée

Flux pour le SSID Webauth central dans la configuration d'ancrage étranger

1. Le client envoie une demande d'association pour le SSID diffusé par le contrôleur de réseau local sans fil étranger (WLC).
2. Le WLC étranger effectue le filtrage MAC en envoyant une requête d'accès au serveur RADIUS. Le serveur RADIUS répond avec un Access-Accept, qui inclut l'URL de redirection et la liste de contrôle d'accès (ACL) nécessaires.
3. Le WLC étranger envoie la réponse d'association au client.
4. Le client est ancré au WLC d'ancrage. Le client passe à l'état d'exécution sur le WLC étranger, avec le rôle de mobilité défini sur Exporter étranger.
5. Le client obtient une adresse IP. À ce stade, le WLC d'ancrage gère le trafic de redirection, dirigeant le client vers le portail d'authentification.
6. Une fois redirigé, le client communique directement avec le serveur RADIUS. Ce trafic est tunnelisé via le WLC d'ancrage vers le serveur RADIUS.

7. Le client saisit les informations d'authentification sur le serveur RADIUS. Une fois l'authentification réussie, le serveur RADIUS envoie une demande de modification d'autorisation (CoA) au WLC étranger.
8. Le WLC étranger envoie une réponse CoA au serveur RADIUS. Le client passe à l'état EXÉCUTÉ sur le WLC d'ancrage, avec le rôle défini sur Exporter l'ancrage.
9. Tout le trafic client suivant est tunnelisé du WLC étranger au WLC d'ancrage, où il sort du réseau.

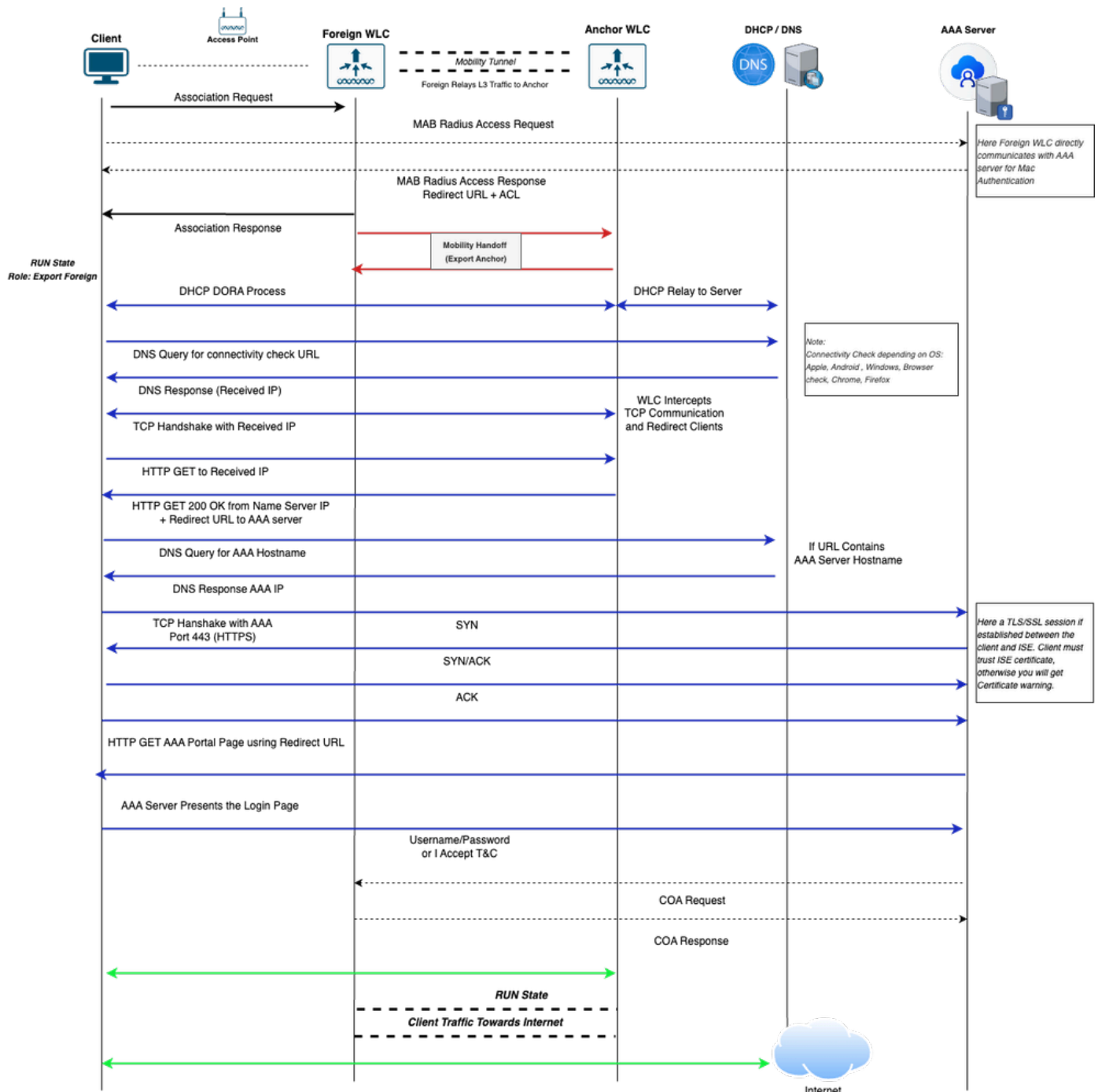


Diagramme de flux de connectivité client pour le SSID Webauth central dans la configuration d'ancrage étranger

Analyse du flux SSID Webauth central dans la configuration d'ancrage étranger via les journaux

Cette section explique le flux de connectivité client pour le SSID d'authentification Web centrale à l'aide de la trace radioactive (RA Trace), des captures de paquets intégrées (EPC) et de l'état du client sur les contrôleurs Foreign et Anchor.

Journaux du contrôleur étranger

Traces radioactives

!! 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. Client
{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
[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
[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
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER] CoA response sent
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Identity preserved: MAC (C
[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
```

Capture de paquets

Le client envoie une demande d'association et effectue l'authentification MAC, ce trafic est géré par le contrôleur étranger.

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=.....

Phase d'association client sur contrôleur étranger avec MAB sans fil

Un transfert de mobilité se déclenche entre les contrôleurs étranger et d'ancrage via le port UDP 16667. Lors d'un événement de mobilité réussi, l'état du client passe à EXÉCUTER avec un rôle Exporter étranger.

Le contrôleur étranger reçoit le trafic DHCP client via le tunnel CAPWAP et le transfère au contrôleur d'ancrage pour un traitement ultérieur.

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

Le trafic DHCP client reçu sur le contrôleur étranger est transféré au contrôleur d'ancrage à l'aide du tunnel de mobilité

De même, le client envoie l'état de connectivité réseau et le trafic de vérification d'accès à la page Web au WLC étranger via le tunnel CAPWAP ; le WLC étranger transfère ceci au WLC d'ancrage à l'aide du tunnel de mobilité, où le contrôleur d'ancrage intercepte ou traite le trafic.

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

Vérification de l'état de la connectivité réseau sur le contrôleur étranger

```
> 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)
```

Rediriger l'URL envoyée au client

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

Page Client Access to Central Webauth pour fournir les détails d'authentification

Le contrôleur étranger traite la demande CoA après une authentification Web centrale réussie.

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

Changement d'autorisation (COA) avec contrôleur étranger

Journaux du contrôleur d'ancrage

Traces radioactives

!! 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_CR
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC L2 Authentication of station is su
{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_MACMMIF FSM transition: S_MA_INIT -> S_MA
{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 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
```

!! Central Web Authentication Applied !!

```
{wncd_x_R0-0}{1}: [webauth-dev] [24229]: (info): Central Webauth URL Redirect, Received a request to cr
{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://10.10
{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-ac1 0 REDIRECT_ACL
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: url-redirect 0 https://10.106.3
```

!! 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

!! 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

Capture de paquets

Après le transfert de mobilité, le contrôleur d'ancrage reçoit le trafic DHCP du contrôleur étranger via le tunnel de mobilité.

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

Trafic DHCP client sur le contrôleur d'ancrage reçu du contrôleur étranger

Le contrôleur d'ancrage reçoit les vérifications de connectivité, les demandes d'accès aux pages Web et les détails d'authentification pour poursuivre le traitement.

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

Vérification de l'état de la connectivité réseau sur le contrôleur d'ancrage

> 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)

Rediriger l'URL envoyée au client

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

Page Client Access to Local Webauth pour fournir les détails d'authentification

Lorsque l'authentification Web centrale réussit, un changement d'autorisation (CoA) se déclenche. Après une CoA réussie, le client passe à l'état EXÉCUTÉ avec un rôle Ancre d'exportation.

État du client sur le contrôleur étranger et le contrôleur d'ancrage

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

État du client sur étranger

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

État du client au point d'ancrage

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

Propriétés du client sur les

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

Propriétés du client sur l'ancrage

Authentification Web externe

Flux pour le SSID Webauth externe dans la configuration d'ancrage étranger

1. Le client initie une connexion au SSID diffusé par le WLC étranger.
2. Comme aucune authentification de couche 2 n'est requise, le client est ancré au WLC d'ancrage. Le client passe à l'état EXÉCUTER sur le WLC étranger, avec le rôle de mobilité désigné comme Exporter étranger.
3. Le client acquiert une adresse IP. Le WLC d'ancrage intercepte le trafic et redirige le client vers le portail du serveur Web externe comme défini dans les paramètres d'authentification Web.
4. Le client envoie les informations d'authentification via le portail. Ces informations d'identification sont validées localement sur le WLC ou via un serveur d'authentification externe, selon la stratégie de sécurité configurée.
5. Une fois l'authentification réussie, le client passe à l'état RUN sur le WLC d'ancrage, en assumant le rôle d'ancrage d'exportation.

6. Après une authentification réussie, tout le trafic client suivant est tunnelisé du WLC étranger au WLC d'ancrage, où il sort du réseau.

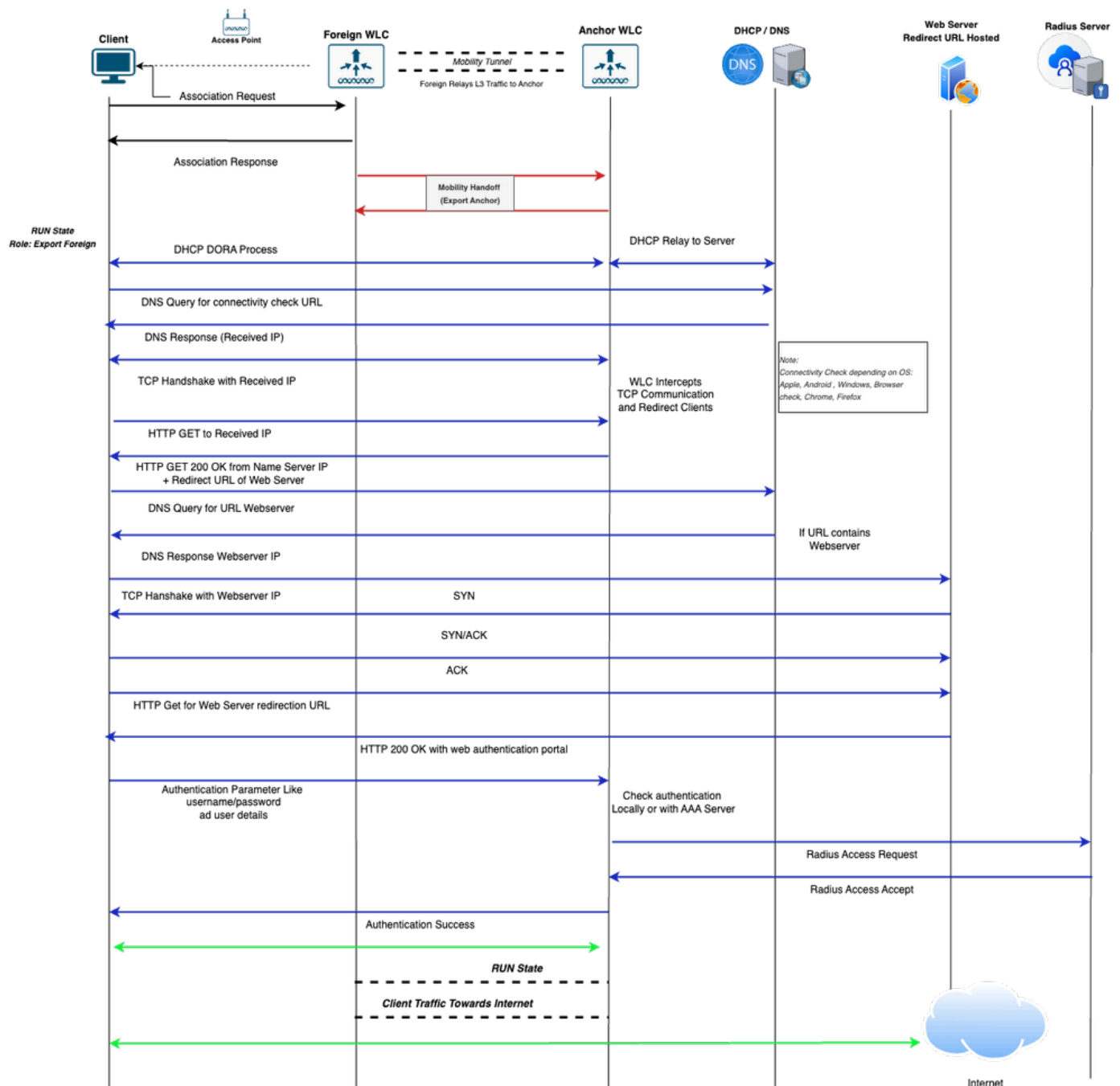


Diagramme de flux de connectivité client pour SSID Webauth externe dans la configuration d'ancrage étranger

Analyse du flux SSID Webauth externe dans la configuration d'ancrage étranger via les journaux

Cette section explique le flux de connectivité client pour le SSID d'authentification Web externe à l'aide de la trace radioactive (RA Trace), des captures de paquets intégrées (EPC) et de l'état du client sur les contrôleurs Foreign et Anchor.

Journaux du contrôleur étranger

Traces radioactives

!! 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:
```

Capture de paquets

Le client envoie une demande d'association que le contrôleur étranger traite.

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=.....

Phase d'association client avec contrôleur étranger

Un transfert de mobilité se déclenche entre les contrôleurs étranger et d'ancrage via le port UDP 16667. Lors d'un événement de mobilité réussi, l'état du client passe à EXÉCUTER avec un rôle Exporter étranger.

Le contrôleur étranger reçoit le trafic DHCP client via le tunnel CAPWAP et le transfère au contrôleur d'ancrage pour un traitement ultérieur.

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 16:19:05...	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

Le trafic DHCP client reçu sur le contrôleur étranger est transféré au contrôleur d'ancrage à l'aide du tunnel de mobilité

De même, le client envoie l'état de connectivité réseau et le trafic de vérification d'accès à la page Web au WLC étranger via le tunnel CAPWAP ; le WLC étranger transfère ceci au WLC d'ancrage à l'aide du tunnel de mobilité, où le contrôleur d'ancrage intercepte ou traite le trafic.

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

Vérification de l'état de la connectivité réseau sur le contrôleur étranger

```

> 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: (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: 788]
  [Time since request: 0.000991000 seconds]
  [Request URI: /connecttest.txt]
  [Full request URI: (redacted)]
  File Data: 580 bytes
> Line-based text data: text/html (9 lines)

```

Rediriger l'URL envoyée au client

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

Accès client à la page WebAuth externe pour fournir les détails d'authentification

Journaux du contrôleur d'ancrage

Traces radioactives

!! 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
```

Capture de paquets

Après le transfert de mobilité, le contrôleur d'ancrage reçoit le trafic DHCP du contrôleur étranger via le tunnel de mobilité.

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

Trafic DHCP client sur le contrôleur d'ancrage reçu du contrôleur étranger

Le contrôleur d'ancrage reçoit les vérifications de connectivité, les demandes d'accès aux pages Web et les détails d'authentification pour poursuivre le traitement.

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

Vérification de l'état de la connectivité réseau sur le contrôleur d'ancrage

```

> 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)

```

Rediriger l'URL envoyée au client

Le client envoie les informations d'authentification via le portail. Ces informations d'identification sont validées localement sur le WLC ou via un serveur d'authentification externe, selon la stratégie de sécurité configurée.

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	10.107.79.30	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

Accès client à la page WebAuth externe pour fournir les détails d'authentification

État du client sur le contrôleur étranger et le contrôleur d'ancrage

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

État du client sur étranger

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

État du client au point d'ancrage

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

Propriétés du client sur les

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

Propriétés du client sur l'ancre

Équilibrage De Charge Entre Contrôleur D'Ancrage Multiple

Lorsque plusieurs contrôleurs d'ancrage sont mappés à un seul WLAN, la distribution du trafic dépend de la priorité. Trois niveaux de priorité peuvent être configurés : Primaire, secondaire et tertiaire. La fonction de priorité d'ancrage invité fournit un mécanisme de distribution de charge active/en veille entre les contrôleurs d'ancrage. Pour ce faire, attribuez une priorité fixe à chaque contrôleur d'ancrage : La charge est distribuée au contrôleur de priorité la plus élevée, et de manière circulaire parmi les contrôleurs qui partagent la même valeur de priorité.

⚠ 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)



Mappage de priorité d'ancrage



Remarque : Par défaut, la priorité tertiaire est configurée lors du mappage du contrôleur d'ancrage sur le contrôleur étranger.

Dépannage de la connectivité client dans un scénario d'ancrage étranger

1. Problèmes d'intégration client

- i. État du tunnel : Vérifiez que le tunnel de mobilité entre les contrôleurs étranger et d'ancrage reste actif.
- ii. Non-concordance de configuration : Assurez la parité de configuration entre les deux contrôleurs. Des différences dans les noms de WLAN, les noms de profil de stratégie ou les paramètres avancés (tels que le remplacement AAA, les exigences DHCP IPv4 et NAC) entraînent des erreurs de non-correspondance de profil ou de refus d'ancrage.
- iii. Divers : Si le tunnel est activé sans problème de configuration, l'approche de dépannage est similaire à un problème de connectivité client normal en s'assurant de vérifier le contrôleur respectif qui gère le trafic affecté.

2. Connectivité intermittente

- i. Volets du tunnel : Si les paquets keepalive entre les deux contrôleurs ne parviennent pas, le tunnel s'affole, empêchant le client de maintenir une connexion au SSID.
- ii. Bande passante faible : Si la valeur de la MTU de chemin (PMTU) entre homologues de mobilité diminue (576), les clients subissent une dégradation des performances. Cela se produit généralement lorsque des messages de test d'activité mtu de chemin sont manqués entre les deux homologues de mobilité



Remarque : Le contrôleur avec l'adresse MAC de mobilité inférieure lance les messages de keepalive standard et de MTU de chemin.

3. Problèmes spécifiques d'accès au site Web

- i. Les en-têtes de trafic de mobilité incluent les identificateurs de groupe de mobilité, les adresses MAC, les adresses IP et les paquets DTLS CAPWAP chiffrés échangés sur les ports UDP 16666 et 16667. Cette surcharge s'ajoute à l'en-tête CAPWAP existant. Pour le trafic TCP, après l'ajustement de TCP MSS configuré pour AP, si la taille du paquet dépasse la PMTU de mobilité (maximum 1385 octets) en raison de cette surcharge supplémentaire, la fragmentation se produit. Bien que la fragmentation soit généralement gérée par le réseau, des problèmes surviennent si les paquets arrivent dans le désordre ou en retard. Ces conditions ont un impact sur le réassemblage des paquets et entraînent des échecs d'accessibilité des données pour des sites Web spécifiques.

Collecte des journaux à partir du contrôleur étranger et d'ancrage

1. Activez term exec prompt timestamp pour avoir une référence temporelle pour toutes les commandes.
2. Utilisez la commande show tech-support wireless !! pour vérifier la configuration.
3. Vous pouvez vérifier l'état du tunnel de mobilité show wireless mobility summary !!
4. Statistiques de Mobility Peer qui incluent l'état de la liaison, les données et les événements client, les statistiques de maintien de la connexion montrent la mobilité sans fil peer ip <IP>
5. Activez le suivi radioactif pour l'adresse IP/MAC de l'homologue de mobilité et l'adresse MAC du client.

Via CLI :

debug wireless {MAC | ip} {aaaa.bbb.cccc | x.x.x.x } {monitor-time} {N secondes} !! Le réglage du temps nous permet d'activer les traces pendant 24 jours .

no debug wireless {MAC | ip} {aaaa.bbb.cccc | x.x.x.x } !! Pour désactiver le débogage

WLC génère un fichier de trace de débogage avec Client_info, commande pour vérifier le fichier de trace de débogage généré dir bootflash: | i debug !!



Avertissement : Le débogage conditionnel active la journalisation au niveau du débogage qui à son tour augmente le volume des journaux générés. Laisser cette opération en cours réduit le retard dans le temps à partir duquel vous pouvez afficher les journaux. Il est donc recommandé de toujours désactiver le débogage à la fin de la session de dépannage.

6. Afin de désactiver tous les débogages, exécutez ces commandes :

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

```
# undebug all !!
```

Via l'interface utilisateur :

Étape 1. Accédez à Troubleshooting > Radioactive Trace.

Étape 2. Cliquez sur Add et entrez une adresse MAC/IP d'homologue de mobilité ou une adresse MAC de client que vous souhaitez dépanner.

Étape 3. Lorsque vous êtes prêt à démarrer le suivi radioactif, cliquez sur Start. Une fois démarré, la journalisation de débogage est écrite sur le disque à propos de tout traitement du plan de contrôle lié aux adresses MAC suivies.

Étape 4. Lorsque vous reproduisez le problème que vous souhaitez résoudre, cliquez sur Stop.

Étape 5. Pour chaque adresse MAC déboguée, vous pouvez générer un fichier journal rassemblant tous les journaux relatifs à cette adresse MAC en cliquant sur Générer.

Étape 6. Choisissez le délai de retour du fichier journal que vous souhaitez conserver et cliquez sur Apply to Device (Appliquer au périphérique).

Étape 7. Vous pouvez maintenant télécharger le fichier en cliquant sur la petite icône en regard du nom du fichier. Ce fichier est présent dans le lecteur flash d'amorçage du contrôleur et peut également être copié à partir de la boîte via CLI.

7. Captures intégrées

Via CLI :

```
capture de moniteur MYCAP clear !!
```

```
capture de moniteur MYCAP interface Po1 les deux !!
```

```
Taille de la mémoire tampon MYCAP de capture de moniteur 100 !!
```

```
monitor capture MYCAP match access-list name !! (si suivi du trafic du tunnel de mobilité entre WLC)
```

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

```
capture de moniteur MYCAP start !!
```

```
!!Reproduire
```

```
capture de moniteur arrêt MYCAP
```

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

Via l'interface utilisateur :

Étape 1. Accédez à Troubleshooting > Packet Capture > +Add.

Étape 2 : définition du nom de la capture de paquets Un maximum de 8 caractères est autorisé.

Étape 3. Définissez les filtres, le cas échéant.

Étape 4. Cochez la case pour surveiller le trafic de contrôle si vous voulez voir le trafic envoyé au processeur du système et réinjecté dans le plan de données.

Étape 5 : définition de la taille de la mémoire tampon Un maximum de 100 Mo est autorisé.

Étape 6. Définissez la limite, soit par la durée qui autorise une plage de 1 à 1000000 secondes, soit par le nombre de paquets qui autorise une plage de 1 à 100000 paquets, selon les besoins.

Étape 7. Choisissez l'interface dans la liste des interfaces de la colonne de gauche et sélectionnez la flèche pour la déplacer vers la colonne de droite.

Étape 8. Cliquez sur Save and Apply to Device.

Étape 9. Pour démarrer la capture, sélectionnez Start.

Étape 10. Vous pouvez laisser la capture s'exécuter jusqu'à la limite définie. Pour arrêter manuellement la capture, sélectionnez Arrêter.

Étape 11. Une fois arrêté, un bouton Export (Exporter) devient disponible et vous permet de cliquer sur l'option permettant de télécharger le fichier de capture (.pcap) sur le bureau local via le serveur HTTP ou TFTP, le serveur FTP ou le disque dur ou la mémoire flash du système local.

Informations connexes

[Configuration des topologies de mobilité sur les WLC Catalyst 9800](#)

[Configuration de la fonction WLAN Anchor Mobility sur Catalyst 9800](#)

[Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.