

# Comprendere il flusso del traffico nella configurazione di una porta esterna tra 9800 WLC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica sullo scenario di ancoraggio esterno](#)

[Topologia](#)

[WLAN con autenticazione di layer 2](#)

[Requisiti di configurazione](#)

[Flusso per SSID basato su ancoraggio esterno di livello 2](#)

[Analisi del flusso SSID di layer 2 nella configurazione dell'ancoraggio esterno tramite i log](#)

[Registri da controller esterno](#)

[Registri dal controller Anchor 9800](#)

[Stato client su controller esterno e ancoraggio](#)

[WLAN con autenticazione di layer 3](#)

[Autenticazione Web locale](#)

[Flusso per SSID autenticazione Web locale nell'installazione dell'ancoraggio esterno](#)

[Analisi del flusso SSID dell'autenticazione Web locale nell'impostazione dell'ancoraggio esterno tramite log](#)

[Registri da controller esterno](#)

[Registri da controller di ancoraggio](#)

[Stato client su controller esterno e ancoraggio](#)

[Autenticazione Web centrale](#)

[Flusso per SSID autenticazione Web centrale nell'impostazione dell'ancoraggio esterno](#)

[Analisi del flusso SSID Webauth centrale nella configurazione dell'ancoraggio esterno tramite i log](#)

[Registri da controller esterno](#)

[Registri da controller di ancoraggio](#)

[Stato client su controller esterno e ancoraggio](#)

[Autenticazione Web esterna](#)

[Flusso per SSID Webauth esterno nell'installazione di una porta esterna](#)

[Analisi del flusso SSID Webauth esterno nell'impostazione dell'ancoraggio esterno tramite i log](#)

[Registri da controller esterno](#)

[Registri da controller di ancoraggio](#)

[Stato client su controller esterno e ancoraggio](#)

[Bilanciamento del carico tra più controller di ancoraggio](#)

[Risoluzione dei problemi di connettività dei client nello scenario di ancoraggio esterno](#)

[Raccolta registri da controller esterno e ancoraggio](#)

[Informazioni correlate](#)

---

# Introduzione

Questo documento descrive il flusso del traffico nell'impostazione Foreign-Anchor tra i WLC di Cisco 9800, includendo l'onboarding e la risoluzione dei problemi dei client L2/L3.

## Prerequisiti

Tunnel di mobilità tra controller esterno e ancoraggio.

Le porte UDP 1666 e 1667 sono consentite tra due WLC.

Profilo criteri configurato per la commutazione centrale.

Configuration > Wireless > Mobility

Global Configuration Peer 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                  |
| <input type="checkbox"/> |             | 10.107.79.30  | 10.107.79.30 | Bangalore_Site | 0.0.0.0        | ::             | Up     | 1006 |                                          | Disabled             |

1

10

1 - 2 of 2 items

Stato tunnel Mobility su WLC esterno

Configuration > Wireless > Mobility

Global Configuration Peer 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                  |
| <input type="checkbox"/> |             | 10.107.79.30  | 10.107.79.30 | Bangalore_Site | 0.0.0.0        | ::             | Up     | 1006 |                                          | Disabled             |

1

10

1 - 2 of 2 items

Stato tunnel mobilità su WLC ancorato

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso ai controller wireless tramite interfaccia a riga di comando (CLI) o interfaccia grafica utente (GUI)
- Mobilità sui Cisco Wireless LAN Controller (WLC)
- 9800 Wireless Controller
- Tracce radioattive e acquisizione di pacchetti su 9800 WLC

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 9800 modello WLC
- Cisco IOS XE versione 17.15.5
- Serie 9100 AP Model

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

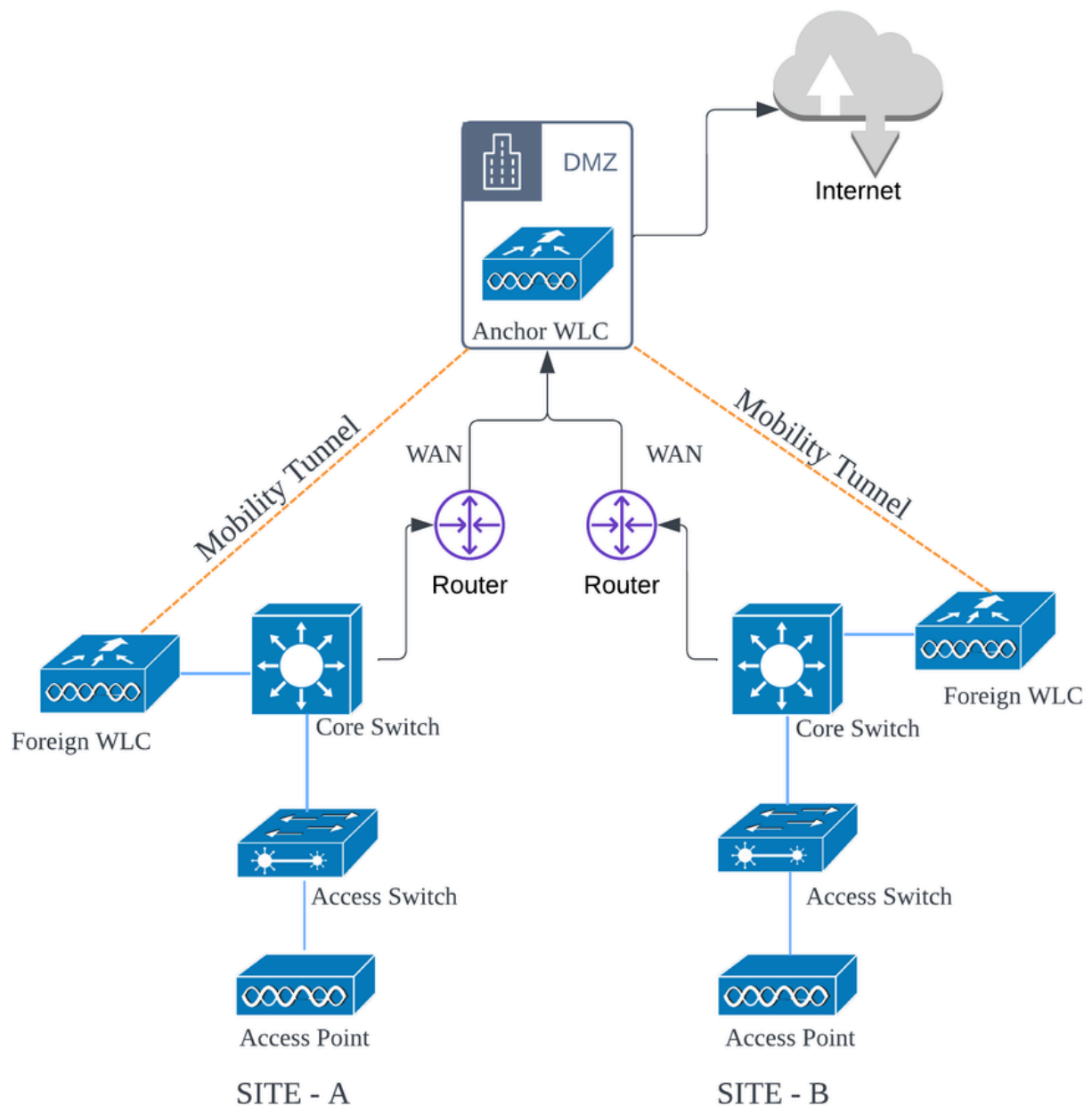
## Panoramica sullo scenario di ancoraggio esterno

- Controller esterno: Questo WLC gestisce il layer 2 o il lato wireless della rete. Ha dei punti di accesso connessi e tutto il traffico dei client per le WLAN ancorate viene incapsulato nel tunnel della mobilità e inviato al controller di ancoraggio. Il traffico non esiste localmente nel controller esterno.
- Controller di ancoraggio: Questo serve come punto di uscita di livello 3. Riceve il traffico del client tramite il tunnel della mobilità dai controller esterni e decapsula o termina il traffico del client nel punto di uscita (VLAN). In questa posizione i client vengono visualizzati nella rete.

I punti di accesso sul WLC esterno trasmettono gli SSID WLAN e hanno un tag di policy assegnato che collega il profilo WLAN al profilo di policy appropriato. Quando un client wireless si connette a questo SSID, il controller esterno invia sia il nome SSID che il profilo dei criteri come parte delle informazioni client al WLC di ancoraggio. Al momento della ricezione, il WLC di ancoraggio controlla la propria configurazione in modo che corrisponda al nome dell'SSID e al nome del profilo dei criteri. Quando Anchor WLC trova una corrispondenza, applica la

configurazione corrispondente e fornisce un punto di uscita per il client wireless. Pertanto, è obbligatorio che i nomi e le configurazioni del profilo della WLAN e delle policy corrispondano sui WLC esteri e ancorati alla WLC 9800, con l'eccezione della VLAN in Policy Profile.

## Topologia



Configurazione di un'ancora esterna tra 9800 WLC

## WLAN con autenticazione di layer 2

## Requisiti di configurazione

1. Verificare che il nome e la configurazione della WLAN siano identici sui WLC esterni e di ancoraggio e che sia configurata per l'autenticazione di layer 2 (PSK o 802.1x).
2. Creare un profilo criteri con lo stesso nome sui WLC esterni e ancorati con la stessa configurazione.
3. Sul WLC esterno, configurare il mapping del WLC di ancoraggio all'interno del rispettivo profilo criteri.
4. Sul WLC di ancoraggio, configurare il profilo dei criteri per designare il controller come ancoraggio di esportazione.
5. Sul WLC esterno, mappare la WLAN al profilo della policy appropriato utilizzando un codice di matricola.

## Flusso per SSID basato su ancoraggio esterno di livello 2

1. Il client avvia una connessione al SSID trasmesso dal WLC esterno. Il WLC esterno esegue l'autenticazione di layer 2, convalidando le credenziali localmente o tramite un server AAA esterno, a seconda dei criteri di sicurezza configurati.
2. Una volta completata l'autenticazione, la sessione client viene ancorata al WLC di ancoraggio. Al client viene assegnato un indirizzo IP e viene eseguita la transizione allo stato RUN sul WLC di ancoraggio.
3. Una volta stabilita la sessione, tutto il traffico di dati dei client viene tunneling dal WLC esterno al WLC di ancoraggio, dove viene reindirizzato alla rete.

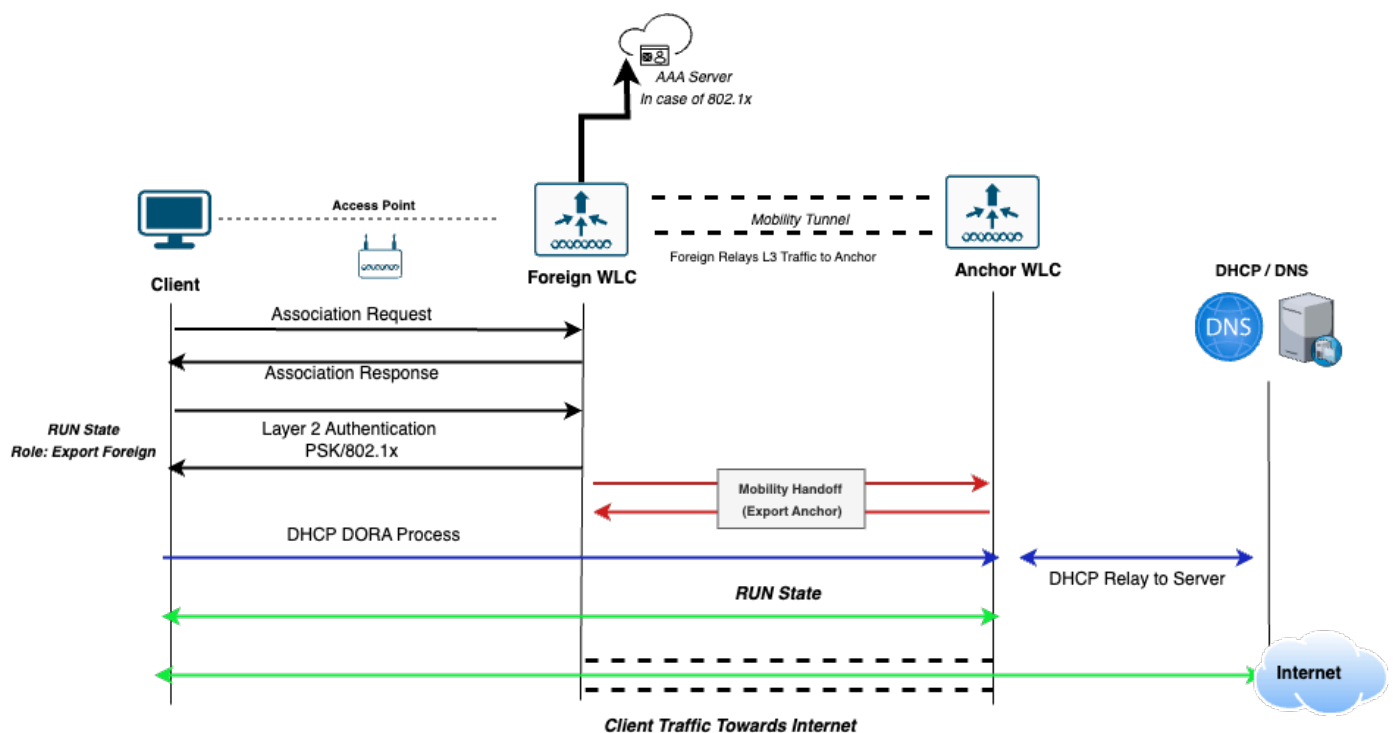


Diagramma di flusso WLAN basata su ancoraggio esterno di layer 2

## Analisi del flusso SSID di layer 2 nella configurazione dell'ancoraggio esterno tramite i log

In questa sezione viene illustrato il flusso della connettività del client di layer 2 tramite l'utilizzo di Traccia radioattiva (RSA Trace), di EPC (Embedded Packet Capture) e dello stato del client sui controller esterno e di ancoraggio.

### Registri da controller esterno

#### Tracce radioattive

!! Client Association started !!

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

!! Layer 2 Authentication started !!

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

!! Mobility Handoff !!

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

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

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

#### Acquisizione pacchetti

Il client invia una richiesta di associazione ed esegue l'autenticazione di layer 2, gestita dal controller esterno.

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

Associazione client + traffico di autenticazione di livello 2

Viene attivato un handoff di mobilità tra i controller esteri e ancorati tramite la porta UDP 16667. Se un evento di mobilità ha esito positivo, lo stato del client passa a ESEGUI con un ruolo Esporta esterno. Il controller esterno riceve il traffico DHCP del client tramite il tunnel CAPWAP e lo inoltra al controller di ancoraggio per un'ulteriore elaborazione.

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

Il traffico DHCP client ricevuto sul controller esterno viene inoltrato al controller di ancoraggio tramite il tunnel della mobilità

## Registri dal controller Anchor 9800

## Tracce radioattive dall'ancoraggio

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

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

{wncd\_x\_R0-0}{1} [sisf-packet] TX DHCPv4 from interface mobility\_a0000001 on vlan 31 Src MAC Client-MAC  
{wncd\_x\_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA  
{wncd\_x\_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MA  
{wncd\_x\_R0-0}{1} [client-iplearn] [24229] (note) MAC Client-MAC Client IP learn successful. Method DHCP  
{mobilityd\_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Sending ipv4\_address\_update of XID (XID)  
{wncd\_x\_R0-0}{1} [client-iplearn] [24229] (info) MAC Client-MAC IP-learn state transition S\_IPLEARN\_IN\_ Complete  
  
{wncd\_x\_R0-0}{1} [avc-afc] [24229] (info) ReAnchor [client MAC Client-MAC] Client has Anchor role {wncd\_x\_R0-0}{1}

Acquisizione pacchetto su ancoraggio

Dopo il passaggio della mobilità, il controller di ancoraggio riceve il traffico DHCP dal controller esterno tramite il tunnel della mobilità.  
Al completamento del processo DORA, il client entra in stato RUN con un ruolo Export Anchor. Da questo punto in avanti, il controller di ancoraggio funge da punto di uscita per il traffico di dati del 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                     |

Traffico DHCP client su controller di ancoraggio ricevuto da controller esterno

Stato client su controller esterno e ancoraggio

Monitoring > Wireless > Clients

Clients

Sleeping Clients

Excluded Clients

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 |
|--------------------------|--------------------|---------------|--------------------------|---------|---------|---------|---------|-------------|-------|----------|-----------|-------------|----------------|------------|
| <input type="checkbox"/> |                    | 10.105.60.226 | fe80::b77c:b748:ddc:4fc0 |         | 1       | DMZ_LWA | 11      | WLAN        | Run   | 11ac     |           | N/A         | Export Foreign | No         |

1 ~ 1 of 1 clients

Stato client all'esterno

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

Stato client su ancoraggio

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

Proprietà client su esterno

| Client                                                                                                                                                                |                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 360 View                                                                                                                                                              | <a href="#">General</a> <a href="#">QOS Statistics</a> <a href="#">ATF Statistics</a> <a href="#">Mobility History</a> <a href="#">Call Statistics</a> |
| <a href="#">Client Properties</a> <a href="#">AP Properties</a> <a href="#">Security Information</a> <a href="#">Client Statistics</a> <a href="#">QOS Properties</a> |                                                                                                                                                        |
| 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                                                                                                                                               |
| <b>Mobility</b>                                                                                                                                                       |                                                                                                                                                        |
| 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                                                                                                                                |

Proprietà client su ancoraggio

## WLAN con autenticazione di layer 3

### Autenticazione Web locale

Flusso per SSID autenticazione Web locale nell'installazione dell'ancoraggio esterno

1. Il client avvia una connessione al SSID annunciato dal WLC esterno.
2. Poiché non viene eseguita alcuna autenticazione di layer 2, il client viene immediatamente ancorato al WLC di ancoraggio. Il client entra in stato RUN sul WLC esterno, con il ruolo di mobilità designato come Esporta esterno.
3. Il client ottiene un indirizzo IP e viene reindirizzato a una pagina Web. Questo traffico viene gestito dal controller di ancoraggio.
4. Una volta completata l'autenticazione sul portale, il client passa allo stato RUN sul WLC di ancoraggio, con il ruolo di ancoraggio di esportazione.

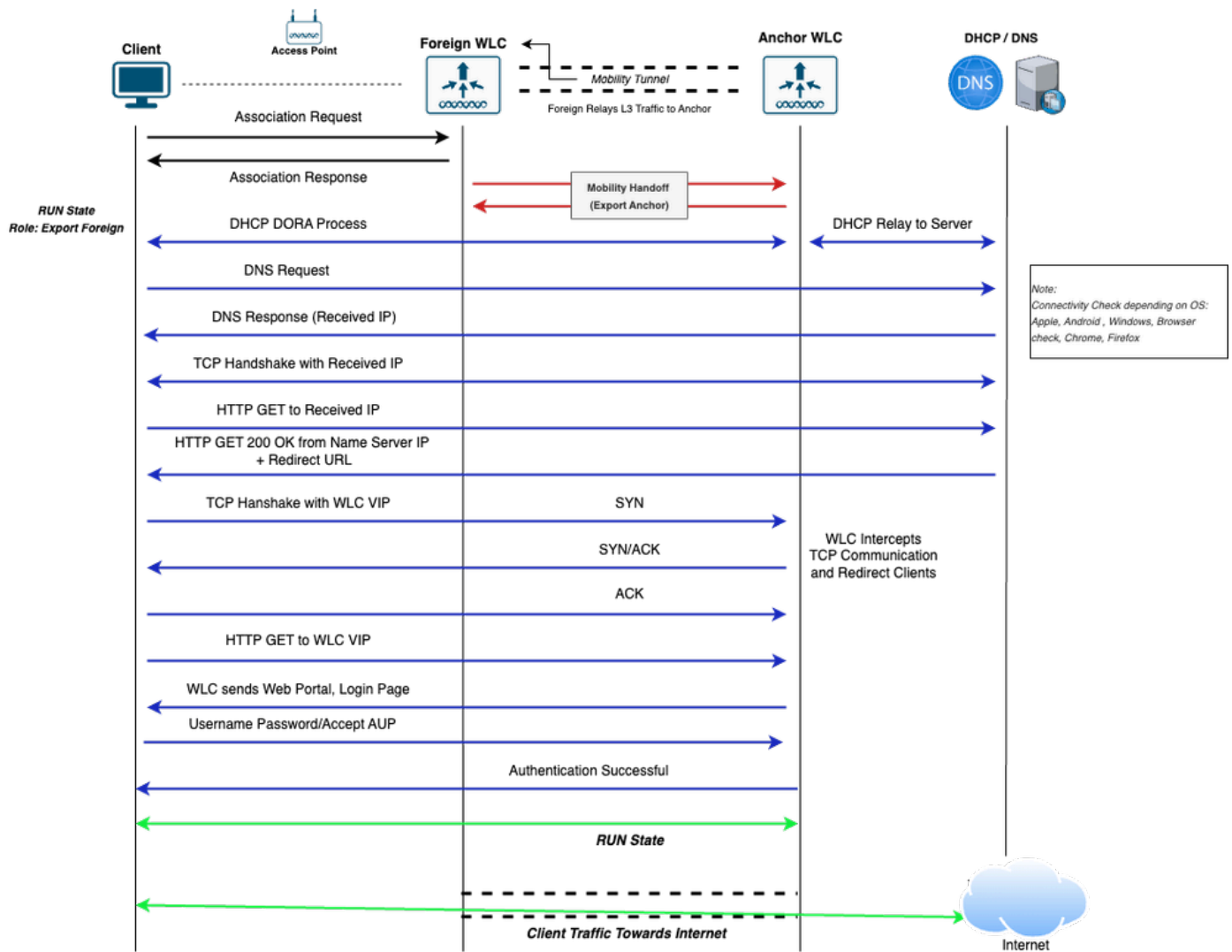


Diagramma di flusso della connettività client per SSID autenticazione Web locale in configurazione ancoraggio esterno

## Analisi del flusso SSID dell'autenticazione Web locale nell'impostazione dell'ancoraggio esterno tramite log

In questa sezione viene illustrato il flusso della connettività client per l'SSID dell'autenticazione Web locale tramite la traccia radioattiva (RA Trace), l'EPC (Embedded Packet Capture) e lo stato del client sui controller esterno e di ancoraggio.

### Registri da controller esterno

### Tracce radioattive

!! Client Association Phase !!

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

```

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

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

!! Client AAA Traffic handling !!
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (10452) to
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of XI
{wncd_x_R0-0}{1}: [mm-transition] [17047]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_Foreign ->
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Mobile AAA Handoff update received.
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC Received username=Guest1
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [17047]: (info): MAC: Client_MAC IPv6 Client payload is re
{wncd_x_R0-0}{1}: [mm-client] [17047]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (10452)
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-pmtu] [18401]: (debug): Peer IP: Anchor-WLC-IP PMTU size is 1006 and calculate
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (1045
{wncd_x_R0-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] auth mgr attr add/change not
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17047]: (info): [Client_MAC:capwap_90000003] SM Notified attrib
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa handoff ack successfully forward

```

## Acquisizione pacchetti

Il client invia una richiesta di associazione, che viene gestita dal controller esterno.

| 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=.....                   |

Viene attivato un handoff di mobilità tra i controller esteri e ancorati tramite la porta UDP 16667. Se un evento di mobilità ha esito positivo, lo stato del client passa a ESEGUI con un ruolo Esporta esterno.

Il controller esterno riceve il traffico DHCP del client tramite il tunnel CAPWAP e lo inoltra al controller di ancoraggio per un'ulteriore elaborazione.

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

Il traffico DHCP client ricevuto sul controller esterno viene inoltrato al controller di ancoraggio tramite il tunnel della mobilità

Analogamente, il client invia lo stato della connettività di rete e il traffico di controllo dell'accesso alla pagina Web al WLC esterno tramite il tunnel CAPWAP; il WLC esterno lo inoltra al WLC di ancoraggio utilizzando il tunnel per la mobilità, dove il controller di ancoraggio intercetta o elabora il traffico.

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

Controllo stato connettività di rete su controller esterno

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

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

Pagina Accesso client a autenticazione Web locale per fornire i dettagli di autenticazione

Registri da controller di ancoraggio

Tracce radioattive

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

## !! Client DHCP Traffic !!

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

## !! Local Web Authentication !!

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

{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Param-m  
{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]State G  
{wncd\_x\_R0-0}{1}: [webauth-page] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Sending V  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53007/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53007/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53007/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]GET rcv  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]HTTP GE  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Parse G  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Read co  
{wncd\_x\_R0-0}{1}: [webauth-error] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Parse 1  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53007/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53007/1  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53008/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53009/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53009/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]GET rcv  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]HTTP GE  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Parse G  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Read co  
{wncd\_x\_R0-0}{1}: [webauth-error] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Parse 1  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53009/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53009/1  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53011/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53011/1  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53020/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53022/235  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53023/195  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53023/195  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]POST rc  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]get url  
{wncd\_x\_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Read co  
{wncd\_x\_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -1526718499,s  
{wncd\_x\_R0-0}{1}: [caaa-authen] [24229]: (info): [CAAA:AUTHEN:4000544] NULL ATTR LIST  
{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Param-m  
{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]State L  
{wncd\_x\_R0-0}{1}: [webauth-io] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]53023/195  
{wncd\_x\_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list 1761615853,sm  
{wncd\_x\_R0-0}{1}: [caaa-author] [24229]: (info): [CAAA:AUTHOR:4000544] NULL ATTR LIST  
{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Param-m  
{wncd\_x\_R0-0}{1}: [webauth-state] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]State A  
{wncd\_x\_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Unapply I  
{wncd\_x\_R0-0}{1}: [auth-mgr] [24229]: (info): [Client\_MAC:mobility\_a0000001] Raising ext evt Template D  
{wncd\_x\_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility\_a0000001[Client\_MAC][ 10.105.60.226]Unapply I  
{wncd\_x\_R0-0}{1}: [auth-mgr] [24229]: (info): [Client\_MAC:mobility\_a0000001] Raising ext evt Template D  
{wncd\_x\_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client\_MAC Link-local bridging not enabled for  
{wncd\_x\_R0-0}{1}: [auth-mgr] [24229]: (info): [Client\_MAC:mobility\_a0000001] Authc success from WebAuth  
{wncd\_x\_R0-0}{1}: [auth-mgr] [24229]: (info): [Client\_MAC:mobility\_a0000001] Raised event APPLY\_USER\_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 [client MAC: Client_MAC] Guest client detected. S
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

```

## Acquisizione pacchetti

Dopo il passaggio della mobilità, il controller di ancoraggio riceve il traffico DHCP dal controller esterno tramite il tunnel della mobilità.

| 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                     |

Traffico DHCP client su controller di ancoraggio ricevuto da controller esterno

Il controller di ancoraggio riceve i controlli di connettività, le richieste di accesso alle pagine Web e i dettagli di autenticazione per continuare l'elaborazione.

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

Controllo dello stato della connettività di rete sul controller di ancoraggio

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

Reindirizza URL inviato al 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                         |

Pagina Accesso client a autenticazione Web locale per fornire i dettagli di autenticazione

Una volta completata correttamente l'autenticazione Web locale, il client passa allo stato RUN con un ruolo di ancoraggio di esportazione. Da questo punto in avanti, il controller di ancoraggio funge da punto di uscita per il traffico di dati del client.

Stato client su controller esterno e ancoraggio

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

Stato client all'esterno

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

Stato client su ancoraggio

Client

360 ViewGeneralQOS StatisticsATF StatisticsMobility History

Client PropertiesAP PropertiesSecurity InformationClient Statistics

Max Client Protocol Capability802.11ac Wave 2

Wi-Fi to Cellular SteeringNot implemented

Cellular CapabilityN/A

Regular ASR supportDISABLED

Mobility

Anchor IP Address10.105.60.114

Point of Presence0xA0000003

AuthC StatusTrue

Move Count0

RoleExport Foreign

Roam TypeL3 Requested

Proprietà client su esterno

## 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

Proprietà client su ancoraggio

## Autenticazione Web centrale

Flusso per SSID autenticazione Web centrale nell'impostazione dell'ancoraggio esterno

1. Il client invia una richiesta di associazione per il SSID trasmesso dal controller WLC (Foreign Wireless LAN Controller).
2. Il WLC esterno esegue il filtro MAC inviando una richiesta di accesso al server RADIUS. Il server RADIUS risponde con un comando Access-Accept, che include l'URL di reindirizzamento e l'elenco di controllo di accesso (ACL) necessari.
3. Il WLC esterno invia la risposta dell'associazione al client.
4. Il client è ancorato al WLC di ancoraggio. Il client entra nello stato RUN sul WLC esterno, con il ruolo mobility impostato su Export Foreign.
5. Il client ottiene un indirizzo IP. In questa fase, il WLC di ancoraggio gestisce il traffico di reindirizzamento, indirizzando il client al portale di autenticazione.
6. Una volta reindirizzato, il client comunica direttamente con il server RADIUS. Il traffico viene tunneling attraverso il WLC di ancoraggio verso il server RADIUS.

7. Il client immette le credenziali di autenticazione nel server RADIUS. Una volta completata l'autenticazione, il server RADIUS invia una richiesta di modifica dell'autorizzazione (CoA) al WLC esterno.
8. Il WLC esterno invia una risposta di CoA al server RADIUS. Il client passa allo stato RUN sul WLC di ancoraggio, con il ruolo impostato su Export Anchor.
9. Tutto il traffico client successivo viene tunneling dal WLC esterno al WLC di ancoraggio, dove esce dalla rete.

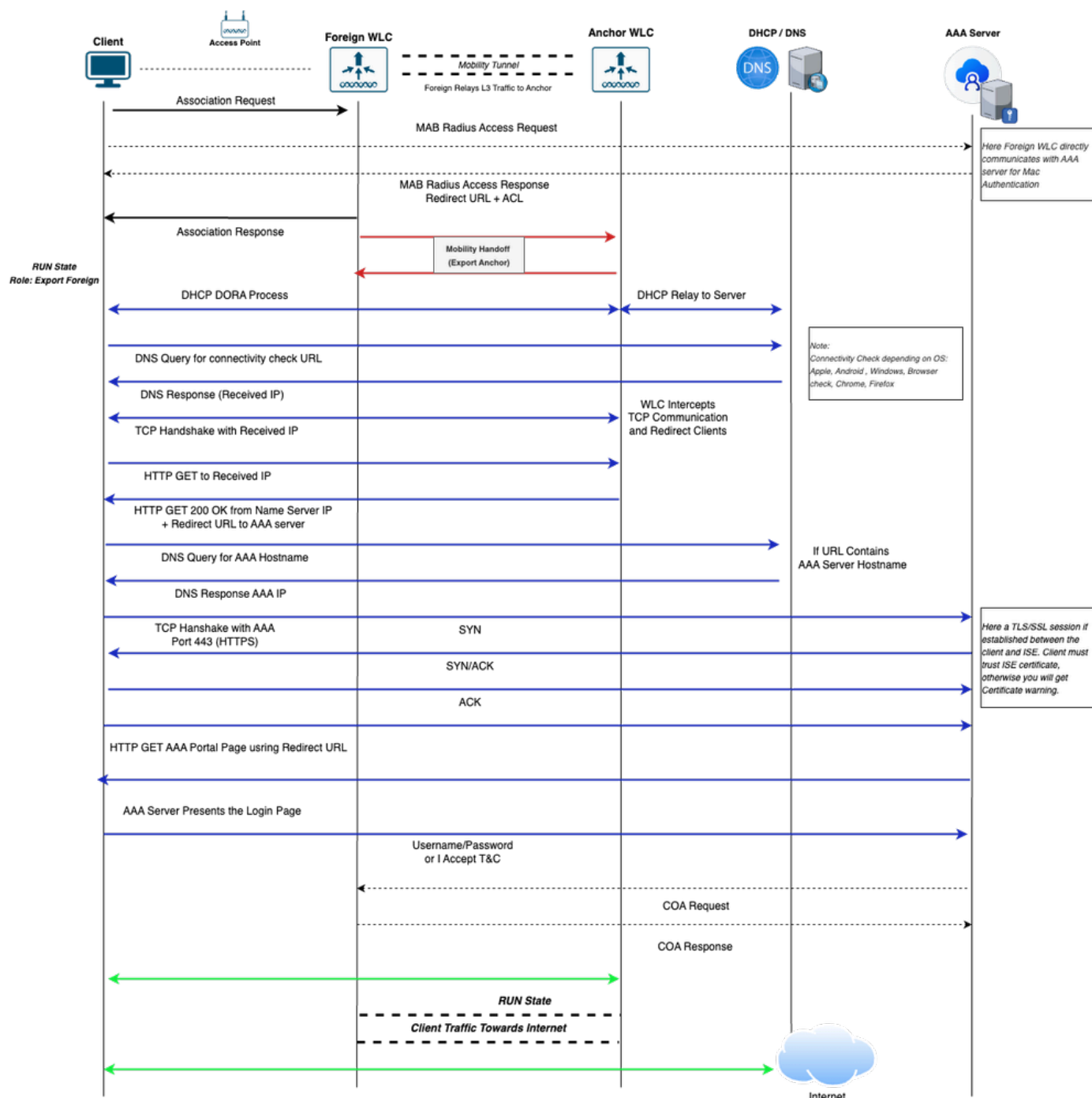


Diagramma di flusso della connettività client per SSID autenticazione Web centrale in configurazione ancoraggio esterno

Analisi del flusso SSID Webauth centrale nella configurazione dell'ancoraggio esterno tramite i log

In questa sezione viene illustrato il flusso della connettività client per l'SSID di autenticazione Web centrale tramite la traccia radioattiva (RA Trace), l'EPC (Embedded Packet Capture) e lo stato del client sia sul controller esterno che sul controller di ancoraggio.

## Registri da controller esterno

### Tracce radioattive

!! 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
[mm-client] [17047] (info) Anchor Vlan-id 31 processed[mm-client] [17047] (info) MAC
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
[client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_C
[client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
[client-orch-sm] [17047] (debug) MAC Client-MAC Received ip learn response. method IP
[client-orch-state] Client state transition S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN >> !

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

## Acquisizione pacchetti

Il client invia una richiesta di associazione ed esegue l'autenticazione MAC. Questo traffico viene gestito dal controller esterno.

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

Fase associazione client su controller esterno con MAB wireless

Viene attivato un handoff di mobilità tra i controller esteri e ancorati tramite la porta UDP 16667. Se un evento di mobilità ha esito positivo, lo stato del client passa a ESEGUI con un ruolo Esporta esterno.

Il controller esterno riceve il traffico DHCP del client tramite il tunnel CAPWAP e lo inoltra al controller di ancoraggio per un'ulteriore elaborazione.

| 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      |

Il traffico DHCP client ricevuto sul controller esterno viene inoltrato al controller di ancoraggio tramite il tunnel della mobilità

Analogamente, il client invia lo stato della connettività di rete e il traffico di controllo dell'accesso alla pagina Web al WLC esterno tramite il tunnel CAPWAP; il WLC esterno lo inoltra al WLC di ancoraggio utilizzando il tunnel per la mobilità, dove il controller di ancoraggio intercetta o elabora il traffico.

| 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                                                              |

Controllo stato connettività di rete su controller esterno

```
> 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: ...: 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.ms.com/connecttest.htm/connecttest.htm
  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)
```

Reindirizza URL inviato al 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                                                              |

Accesso client alla pagina WebAuth centrale per fornire i dettagli di autenticazione

Il controller esterno elabora la richiesta CoA dopo la riuscita autenticazione Web centrale.

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

Cambio di autorizzazione (COA) con controller esterno

Registri da controller di ancoraggio

Tracce radioattive

!! 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

Acquisizione pacchetti

Dopo il passaggio della mobilità, il controller di ancoraggio riceve il traffico DHCP dal controller esterno tramite il tunnel della mobilità.

| 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                     |

Traffico DHCP client su controller di ancoraggio ricevuto da controller esterno

Il controller di ancoraggio riceve i controlli di connettività, le richieste di accesso alle pagine Web e i dettagli di autenticazione per continuare l'elaborazione.

| 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                                                        |

Controllo dello stato della connettività di rete sul controller di ancoraggio

```
> Frame 864: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits)
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: [redacted] 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: [redacted]]
    File Data: 614 bytes
> Line-based text data: text/html (9 lines)
```

Reindirizza URL inviato al 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                                                             |

Pagina Accesso client a autenticazione Web locale per fornire i dettagli di autenticazione

Quando l'autenticazione Web centrale ha esito positivo, viene attivato il processo di modifica dell'autorizzazione (CoA). Dopo un'operazione di CoA riuscita, il client passa allo stato RUN con un ruolo di ancoraggio di esportazione.

Stato client su controller esterno e ancoraggio

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 |
|--------------------------|--------------------|---------------|--------------------------|---------|---------|---------|---------|-------------|-------|----------|-----------|-------------|----------------|------------|
| <input type="checkbox"/> |                    | 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

Stato client all'esterno

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 |
|--------------------------|--------------------|---------------|--------------------------|---------|---------|---------|---------|-------------|-------|----------|-----------|-------------|---------------|------------|
| <input type="checkbox"/> |                    | 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

Stato client su ancoraggio

## 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

Proprietà client su esterno

## 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

Proprietà client su ancoraggio

## Autenticazione Web esterna

Flusso per SSID Webauth esterno nell'installazione di una porta esterna

1. Il client avvia una connessione al SSID trasmesso dal WLC esterno.
2. Poiché non è richiesta l'autenticazione di layer 2, il client è ancorato al WLC di ancoraggio. Il client passa allo stato RUN sul WLC esterno, con il ruolo di mobilità designato come Esporta esterno.
3. Il client acquisisce un indirizzo IP. Il WLC di ancoraggio intercetta il traffico e reindirizza il client al portale del server Web esterno, come definito nei parametri di autenticazione Web.
4. Il client invia le credenziali di autenticazione tramite il portale. Queste credenziali vengono convalidate localmente sul WLC o tramite un server di autenticazione esterno, a seconda dei criteri di sicurezza configurati.
5. Una volta completata l'autenticazione, il client passa allo stato RUN sul WLC di ancoraggio, assumendo il ruolo di ancoraggio di esportazione.

6. Dopo aver completato l'autenticazione, tutto il traffico client successivo viene tunneling dal WLC esterno al WLC di ancoraggio, dove esce dalla rete.

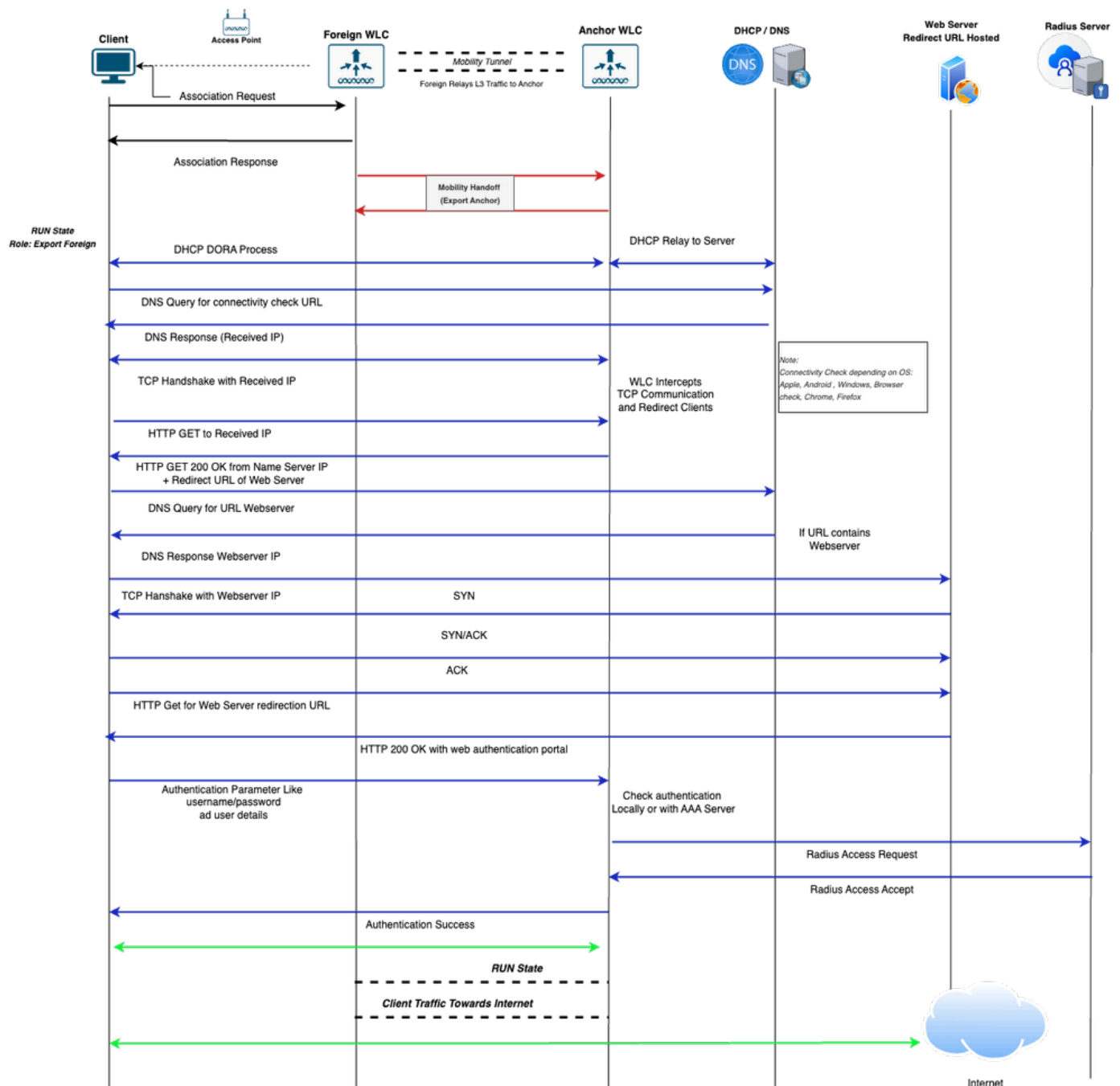


Diagramma di flusso della connettività client per SSID Webauth esterno in configurazione ancoraggio esterno

Analisi del flusso SSID Webauth esterno nell'impostazione dell'ancoraggio esterno tramite i log

In questa sezione viene illustrato il flusso della connettività client per SSID di autenticazione Web esterna tramite la traccia radioattiva (RA Trace), l'EPC (Embedded Packet Capture) e lo stato del client sui controller esterno e di ancoraggio.

## Registri da controller esterno

### Tracce radioattive

!! 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:

## Acquisizione pacchetti

Il client invia una richiesta di associazione, che viene gestita dal controller esterno.

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

Fase di associazione client con controller esterno

Viene attivato un handoff di mobilità tra i controller esteri e ancorati tramite la porta UDP 16667.

Se un evento di mobilità ha esito positivo, lo stato del client passa a ESEGUI con un ruolo Esporta esterno.

Il controller esterno riceve il traffico DHCP del client tramite il tunnel CAPWAP e lo inoltra al controller di ancoraggio per un'ulteriore elaborazione.

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

Il traffico DHCP client ricevuto sul controller esterno viene inoltrato al controller di ancoraggio tramite il tunnel della mobilità

Analogamente, il client invia lo stato della connettività di rete e il traffico di controllo dell'accesso alla pagina Web al WLC esterno tramite il tunnel CAPWAP; il WLC esterno lo inoltra al WLC di ancoraggio utilizzando il tunnel per la mobilità, dove il controller di ancoraggio intercetta o elabora il traffico.

| 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                                                        |

Controllo stato connettività di rete su controller esterno

```

> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco (08:00:0c:2c:3e:00), Dst: Cisco (08:00:0c:2c:3e:00)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.105.60.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 62437, Seq: 1, Ack: 112, Len: 849
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://10.106.32.130:8443/portal/PortalSetup.action?portal=d06bc251-f644-4fc3-b09f-dae9bd8a86
    Content-Type: text/html\r\n
  > Content-Length: 580\r\n
\r\n
[Request in frame: 788]
[Time since request: 0.000991000 seconds]
[Request URI: /connecttest.txt]
[Full request URI: ]
File Data: 580 bytes
> Line-based text data: text/html (9 lines)

```

Reindirizza URL inviato al 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                                                                |

Accesso client alla pagina WebAuth esterna per fornire i dettagli di autenticazione

Registri da controller di ancoraggio

Tracce radioattive

!! 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  
{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

Acquisizione pacchetti

Dopo il passaggio della mobilità, il controller di ancoraggio riceve il traffico DHCP dal controller esterno tramite il tunnel della mobilità.

| 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                     |

Traffico DHCP client su controller di ancoraggio ricevuto da controller esterno

Il controller di ancoraggio riceve i controlli di connettività, le richieste di accesso alle pagine Web e i dettagli di autenticazione per continuare l'elaborazione.

| 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... | 10.105.60.254  | Resolved IP         | 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                           |

Controllo dello stato della connettività di rete sul controller di ancoraggio

```

> 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)

```

Reindirizza URL inviato al client

Il client invia le credenziali di autenticazione tramite il portale. Queste credenziali vengono convalidate localmente sul WLC o tramite un server di autenticazione esterno, a seconda dei criteri di sicurezza configurati.

| UTC Arrival Time         | Source Address | Destination Address | Length | Protocol | TID | Info                                                                              |
|--------------------------|----------------|---------------------|--------|----------|-----|-----------------------------------------------------------------------------------|
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 124    | UDP      |     | 16667 → 16667 Len=78                                                              |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 66     | TCP      |     | 62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM                |
| Jan 14, 2025 16:19:12... | 10.106.32.130  | 10.105.60.254       | 70     | TCP      |     | 8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128     |
| Jan 14, 2025 16:19:12... | 10.105.60.114  | 10.107.79.30        | 120    | UDP      |     | 16667 → 16667 Len=78                                                              |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 54     | TCP      |     | 62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0                                   |
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 112    | UDP      |     | 16667 → 16667 Len=66                                                              |
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 659    | UDP      |     | 16667 → 16667 Len=613                                                             |
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 1342   | UDP      |     | 16667 → 16667 Len=1296                                                            |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 1304   | TCP      |     | 62449 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 717]   |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 537    | TLSv1..  |     | Client Hello                                                                      |
| Jan 14, 2025 16:19:12... | 10.106.32.130  | 10.105.60.254       | 1308   | TCP      |     | 8443 → 62449 [ACK] Seq=1 Ack=1734 Win=34688 Len=1250 [TCP PDU reassembled in 724] |
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 446    | UDP      |     | 16667 → 16667 Len=404                                                             |
| Jan 14, 2025 16:19:12... | 10.106.32.130  | 10.105.60.254       | 863    | TLSv1..  |     | Server Hello, Certificate, Server Key Exchange, Server Hello Done                 |
| Jan 14, 2025 16:19:12... | 10.105.60.114  | 10.107.79.30        | 913    | UDP      |     | 16667 → 16667 Len=871                                                             |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 54     | TCP      |     | 62449 → 8443 [ACK] Seq=1734 Ack=2056 Win=131072 Len=0                             |
| Jan 14, 2025 16:19:12... | 10.107.79.30   | 10.105.60.114       | 112    | UDP      |     | 16667 → 16667 Len=66                                                              |
| Jan 14, 2025 16:19:12... | 10.105.60.254  | 10.106.32.130       | 180    | TLSv1..  |     | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message              |
| Jan 14, 2025 16:19:12... | 10.106.32.130  | 10.105.60.254       | 64     | TLSv1..  |     | Change Cipher Spec                                                                |
| Jan 14, 2025 16:19:12... | 10.105.60.114  | 10.107.79.30        | 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... | 10.105.60.114  | 10.106.32.130       | 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                                            |

Accesso client alla pagina WebAuth esterna per fornire i dettagli di autenticazione

Stato client su controller esterno e ancoraggio

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

> Delete



Selected 0 out of 1 Clients

| <input type="checkbox"/> | 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 |
|--------------------------|--------------------|---------------|--------------------------|------------|---------|---------|---------|-------------|-------|----------|-----------|-------------|----------------|------------|
| <input type="checkbox"/> | [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

Stato client all'esterno

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

Stato client su ancoraggio

| Client                         |                                                     |
|--------------------------------|-----------------------------------------------------|
| 360 View                       | GeneralQOS StatisticsATF StatisticsMobility History |
| Client Properties              | AP PropertiesSecurity InformationClient Statistics  |
| Max Client Protocol Capability | 802.11ac Wave 2                                     |
| Wi-Fi to Cellular Steering     | Not implemented                                     |
| Cellular Capability            | N/A                                                 |
| Regular ASR support            | DISABLED                                            |
| Mobility                       |                                                     |
| Anchor IP Address              | 10.105.60.114                                       |
| Point of Presence              | 0xA0000003                                          |
| AuthC Status                   | True                                                |
| Move Count                     | 0                                                   |
| Role                           | Export Foreign                                      |
| Roam Type                      | L3 Requested                                        |

Proprietà client su esterno

## 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

Proprietà client su ancoraggio

## Bilanciamento del carico tra più controller di ancoraggio

Quando si esegue il mapping di più controller di ancoraggio a una singola WLAN, la distribuzione del traffico dipende dalla priorità. È possibile configurare tre livelli di priorità: Principale, Secondario e Terziario. La funzione di priorità di ancoraggio guest fornisce un meccanismo per la distribuzione del carico attivo/standby tra i controller di ancoraggio. Ciò si ottiene assegnando una priorità fissa a ciascun controller di ancoraggio: il carico viene distribuito al controller con la priorità più alta e in modo round robin tra i controller che condividono lo stesso valore di priorità.

⚠ 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)



Mappatura della priorità di ancoraggio



Nota: Per impostazione predefinita, il terziario di priorità viene configurato durante il mapping del controller di ancoraggio sul controller esterno.

## Risoluzione dei problemi di connettività dei client nello scenario di ancoraggio esterno

### 1. Problemi di caricamento client

- Stato tunnel: Verificare che il tunnel di mobilità tra i controller esterni e di ancoraggio rimanga attivo.
- Configurazione non corrispondente: Verificare la parità di configurazione tra entrambi i controller. Le discrepanze nei nomi delle WLAN, nei nomi dei profili delle policy o nelle impostazioni avanzate, ad esempio l'override AAA, i requisiti DHCP IPv4 e il NAC, possono causare errori di mancata corrispondenza dei profili o di rifiuto di ancoraggio.
- Altro: Se il tunnel è attivo senza problemi di configurazione, l'approccio per la risoluzione dei problemi è simile al normale problema di connettività dei client e consente di controllare il rispettivo controller che gestisce il traffico interessato.

## 2. Connettività intermittente

- i. Tunnel Flap: Se i pacchetti keepalive tra i due controller non arrivano, il tunnel si blocca, impedendo al client di mantenere una connessione con l'SSID.
- ii. Larghezza di banda bassa: Se la PMTU (Path MTU) tra peer mobili scende a un valore inferiore (576), le prestazioni dei client diminuiscono. Questo si verifica in genere quando i messaggi keepalive mtu del percorso non vengono visualizzati tra entrambi i peer mobilità



Nota: Il controller con l'indirizzo MAC con mobilità inferiore avvia sia i messaggi keepalive standard che i messaggi keepalive MTU percorso.

---

## 3. Problemi specifici di accesso al sito Web

- i. Le intestazioni del traffico di mobilità includono gli identificatori dei gruppi di mobilità, gli indirizzi MAC, gli indirizzi IP e i pacchetti DTLS CAPWAP crittografati scambiati sulle porte UDP 1666 e 1667. Questo sovraccarico si aggiunge all'intestazione CAPWAP esistente. Nel caso del traffico TCP, dopo la regolazione del valore TCP MSS configurato per il punto di accesso, se le dimensioni del pacchetto superano la PMTU di mobilità (massimo 1385 byte) a causa di questo sovraccarico aggiuntivo, si verifica la frammentazione. Mentre la frammentazione è in genere gestita dalla rete, si verificano problemi se i pacchetti arrivano fuori servizio o in ritardo. Queste condizioni influiscono sul riassemblaggio dei pacchetti e determinano errori di accessibilità dei dati per siti Web specifici.

## Raccolta registri da controller esterno e ancoraggio

1. Abilitare il timestamp del prompt di esecuzione dei termini per avere un riferimento temporale per tutti i comandi.
2. Utilizzare `show tech-support wireless !!` per rivedere la configurazione.
3. È possibile controllare lo stato del tunnel per la mobilità e visualizzare il riepilogo della mobilità wireless.
4. Le statistiche per Mobility Peer che includono lo stato del collegamento, i dati e gli eventi del client, le statistiche keep-alive mostrano l'ip peer mobilità wireless <IP>
5. Abilitare la traccia radioattiva per l'indirizzo IP/MAC del peer mobilità e l'indirizzo MAC del client.

Via CLI:

```
debug {MAC wireless | ip} {aaaa.bbbb.ccc | x.x.x.x } {tempo-monitor} {N secondi} !!
```

L'impostazione della durata consente di attivare le tracce per un massimo di 24 giorni.

```
nessun {MAC} wireless di debug | ip} {aaaa.bbbb.ccc | x.x.x!! Per disattivare il debug
```

WLC genera un file di traccia di debug con Client\_info, comando per controllare se il file di traccia di debug è stato generato con dir bootflash: | esegui il debug!!

---



Avviso: Il debug condizionale abilita la registrazione a livello di debug che a sua volta aumenta il volume dei log generati. Se si lascia attiva questa opzione, si riduce il tempo di visualizzazione dei log. Si consiglia pertanto di disattivare sempre il debug al termine della sessione di risoluzione dei problemi.

---

6. Per disabilitare tutte le operazioni di debug, eseguire i seguenti comandi:

# cancellazione di tutte le condizioni della piattaforma !!

# undebbug all !!

Tramite GUI:

Passaggio 1. Passare a Risoluzione dei problemi > Traccia radioattiva.

Passaggio 2. Fare clic su Add (Aggiungi) e immettere un indirizzo MAC/IP Mobility Peer o un indirizzo MAC client che si desidera risolvere.

Passaggio 3. Quando si è pronti per avviare il rilevamento radioattivo, fare clic su Start (Avvia). Una volta avviato, il log di debug viene scritto su disco in relazione a qualsiasi elaborazione del control plane correlata agli indirizzi MAC tracciati.

Passaggio 4. Quando si riproduce il problema che si desidera risolvere, fare clic su Stop.

Passaggio 5. Per ogni indirizzo MAC sottoposto a debug, è possibile generare un file di log che fascicola tutti i log relativi a tale indirizzo MAC facendo clic su Genera.

Passaggio 6. Scegliere il periodo di tempo che deve trascorrere prima che il file di log fascicolato venga completato e fare clic su Applica al dispositivo.

Passaggio 7. È ora possibile scaricare il file facendo clic sull'icona piccola accanto al nome del file. Questo file è presente nell'unità flash di avvio del controller e può anche essere copiato dalla CLI.

7. Acquisizioni incorporate

Via CLI:

cattura monitor MYCAP cancellata!!

il monitor acquisisce l'interfaccia MYCAP Po1!!

monitoraggio acquisizione buffer MYCAP dimensione 100 !!

monitor capture MYCAP match access-list name !! (se si tiene traccia del traffico del tunnel di mobilità tra WLC)

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

avvio cattura MYCAP!!

!!Riproduci

cattura monitor MYCAP stop

acquisizione del monitor flash di esportazione MYCAP:|tftp:|http:.../filename.pcap

Tramite GUI:

Passaggio 1. Passare a Risoluzione dei problemi > Acquisizione pacchetti > +Aggiungi.

Passaggio 2. Definire il nome dell'acquisizione del pacchetto. È consentito un massimo di 8 caratteri.

Passaggio 3. Definire gli eventuali filtri.

Passaggio 4. Selezionare la casella per monitorare il traffico di controllo se si desidera visualizzare il traffico puntato alla CPU del sistema e inserito nuovamente nel piano dati.

Passaggio 5. Definire le dimensioni del buffer. È consentito un massimo di 100 MB.

Passaggio 6. Definire il limite, in base alla durata, per un intervallo da 1 a 1000000 secondi, o in base al numero di pacchetti, per un intervallo da 1 a 100000 pacchetti, in base alle esigenze.

Passaggio 7. Scegliere l'interfaccia dall'elenco di interfacce nella colonna sinistra e selezionare la freccia per spostarla nella colonna destra.

Passaggio 8. Fare clic su Save and Apply to Device (Salva e applica al dispositivo).

Passaggio 9. Per avviare l'acquisizione, selezionare Start.

Passaggio 10. È possibile eseguire l'acquisizione fino al limite definito. Per interrompere manualmente la cattura, selezionare Interrompi.

Passaggio 11. Una volta arrestato, diventa disponibile un pulsante Esporta con l'opzione di scaricare il file di acquisizione (.pcap) sul desktop locale tramite server HTTP o TFTP o server FTP o disco rigido o flash del sistema locale.

## Informazioni correlate

[Configurazione delle topologie di mobilità sui WLC di Catalyst 9800](#)

[Configurazione della funzione WLAN Anchor Mobility su Catalyst 9800](#)

[Documentazione e supporto tecnico – Cisco Systems](#)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).