瞭解9800 WLC之間的外部錨點設定中的流量傳輸

目錄

簡介

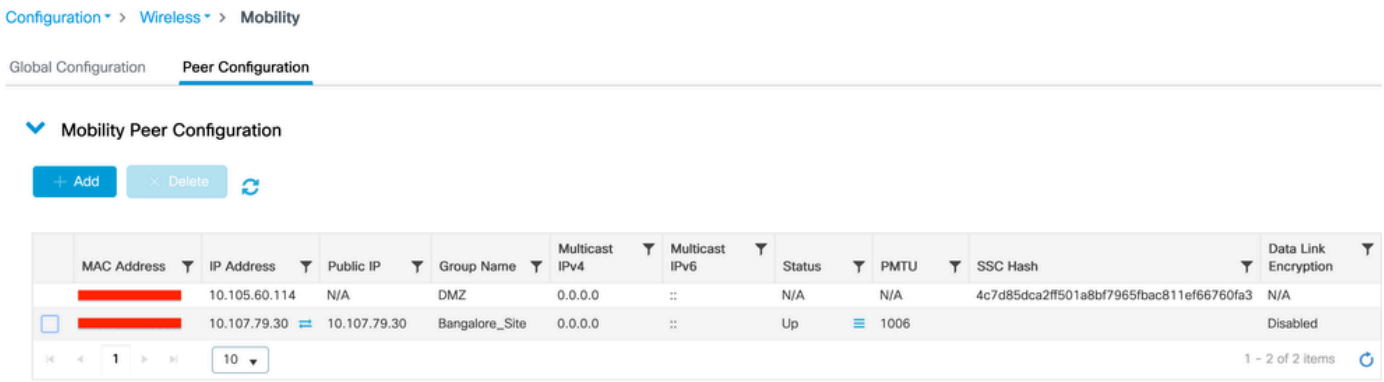
本檔案介紹Cisco 9800 WLC之間的外部錨點設定中的流量流，範圍涵蓋L2/L3使用者端載入和疑難排解。

必要條件

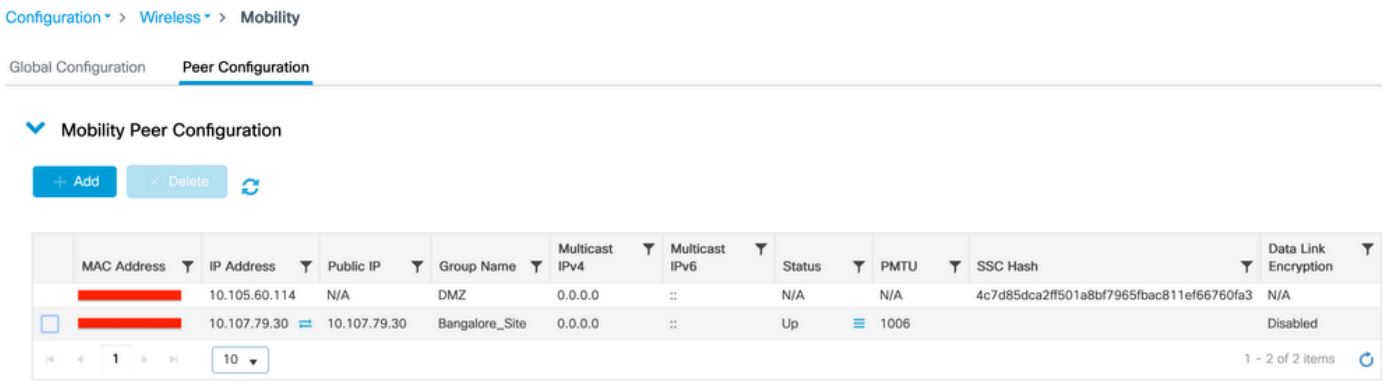
外部和錨點控制器之間的移動隧道。

兩台WLC之間允許UDP連線埠16666和16667。

為中央交換配置的策略配置檔案。



外部WLC上的行動通道狀態



錨點WLC上的行動通道狀態

需求

思科建議您瞭解以下主題：

- 對無線控制器的命令列介面(CLI)或圖形使用者介面(GUI)訪問

- 思科無線LAN控制器(WLC)上的行動化
- 9800無線控制器
- 9800 WLC上的放射性痕跡和封包擷取

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800型號WLC
- Cisco IOS XE 17.15.5版本
- 9100系列AP型號

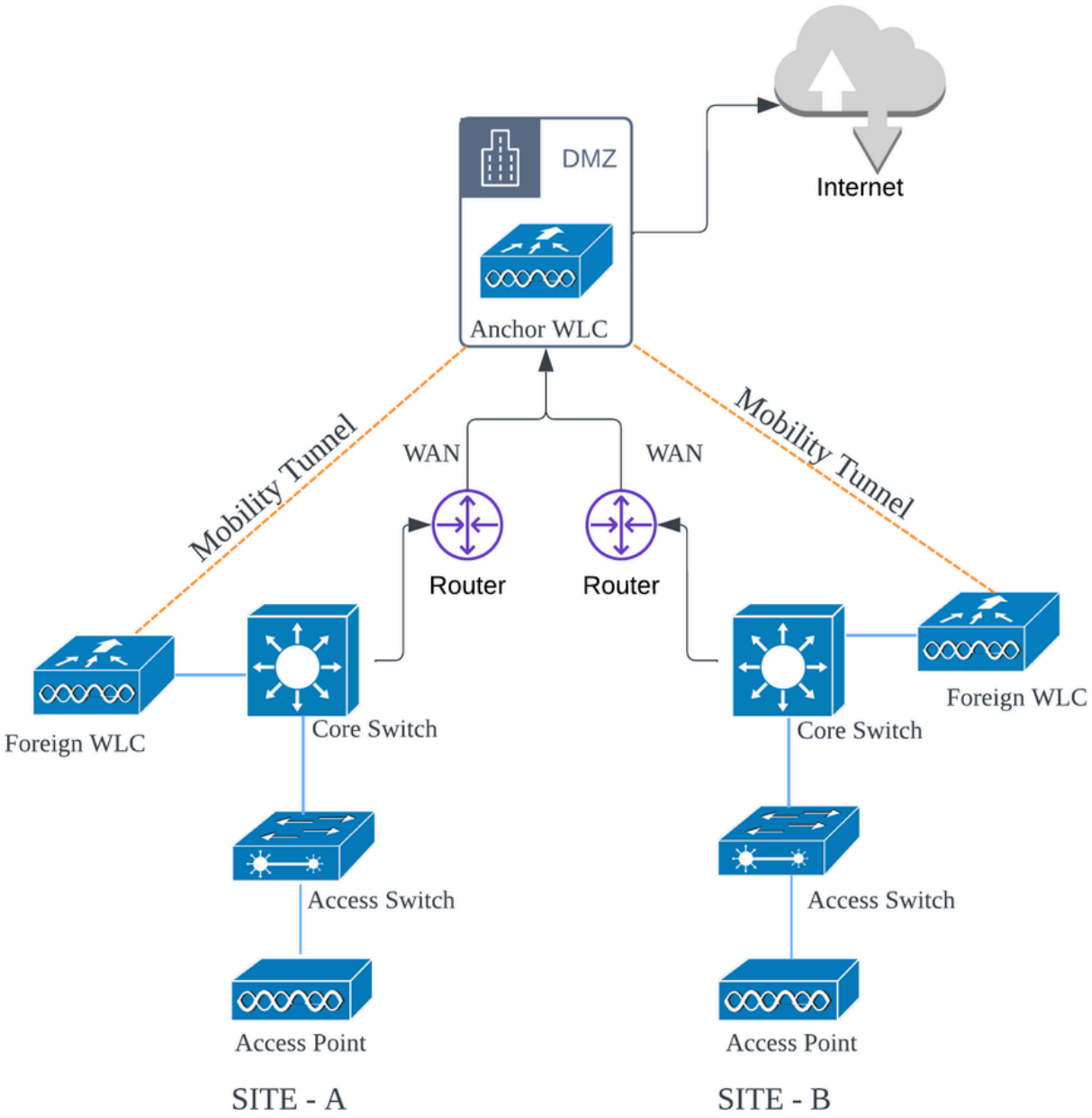
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Foreign-Anchor方案概述

- 外部控制器：此WLC管理網路的第2層或無線端。它有連線到它的存取點，並且錨點WLAN的所有使用者端流量都會封裝到行動通道中並傳送到錨點控制器。流量不會從外部控制器本地退出。
- 錨點控制器：這用作第3層出口點。它透過行動通道從外部控制器接收使用者端流量，並將使用者端流量解除封裝或終止到出口點(VLAN)。 這是網路中客戶端可見的地方。

外部WLC上的接入點廣播WLAN SSID，並分配了將WLAN配置檔案與相應策略配置檔案連結起來的策略標籤。當無線客戶端連線到此SSID時，外部控制器將SSID名稱和策略配置檔案作為客戶端資訊的一部分傳送到錨點WLC。收到資料包後，錨點WLC會檢查自己的配置，以匹配SSID名稱以及策略配置檔名稱。錨點WLC找到相符專案後，會套用對應的組態，並為無線使用者端提供退出點。因此，除了策略配置檔案下的VLAN外，外地和錨點9800 WLC上的WLAN和策略配置檔名稱和配置必須匹配。

拓撲



9800 WLC之間的外部錨點設定

採用第2層驗證的WLAN

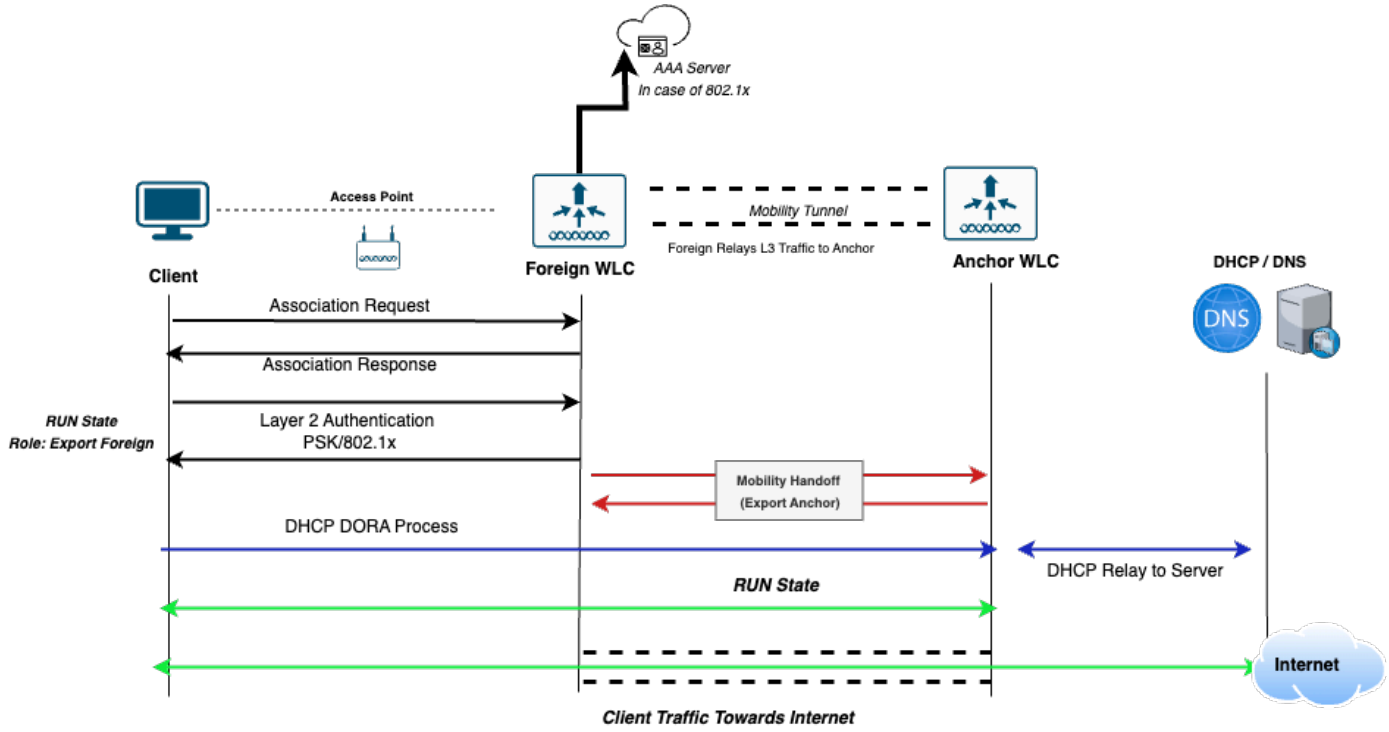
配置要求

1.確保外地和錨點WLC上的WLAN名稱和配置相同，並且配置為第2層身份驗證（PSK或802.1x）。
2.在具有相同組態的外部WLC和錨點WLC上建立同名原則設定檔。
3.在外部WLC上，在各自的原則設定檔中設定錨點WLC對應。
4.在錨點WLC上，設定原則設定檔以將控制器指定為匯出錨點。

5.在外部WLC上，使用策略標籤將WLAN對映到相應的策略配置檔案。

基於第2層外部錨點的SSID的流程

1.客戶端發起到外部WLC廣播的SSID的連線。外部WLC執行第2層身份驗證，根據配置的安全策略在本地或通過外部AAA伺服器驗證憑證。
2.成功驗證後，使用者端作業階段會錨定到錨點WLC。為客戶端分配IP地址，並在錨點WLC上轉換為RUN狀態。
3.建立作業階段後，所有使用者端資料流量都會從外部WLC通道傳送到錨點WLC，並在錨點WLC進入網路。



基於第2層外部錨點的WLAN流程圖

通過日誌分析外部錨點設定中的第2層SSID流

本節介紹通過使用外部和錨點控制器上的放射性跟蹤（RA跟蹤）、嵌入式資料包捕獲(EPC)和客戶端狀態的第2層客戶端連線的流程。

來自外部控制器的日誌

放射性痕跡

```
!! 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. AKMPSK CipherCCMP WPA Version WPA2 >> !! client succesf

!! 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_ANNO
{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-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
```

資料包捕獲

客戶端傳送關聯請求並執行第2層身份驗證，由外部控制器處理。

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

客戶端關聯+第2層身份驗證流量

通過UDP埠16667觸發外部控制器和錨點控制器之間的移動切換。移動事件成功後，客戶端狀態將轉換為RUN並具有「匯出外部」角色。
外部控制器通過CAPWAP隧道接收客戶端DHCP流量，並將其轉發到錨點控制器進行進一步處理。

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

使用移動隧道將外部控制器上接收的客戶端DHCP流量轉發到錨點控制器

來自錨點9800控制器的日誌

錨中的放射性痕跡

```
!! Mobility Handoff !!
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of X
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of X
{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 successfu

!! Client DHCP Traffic !!
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILITY
{wncd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_PL
{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
```

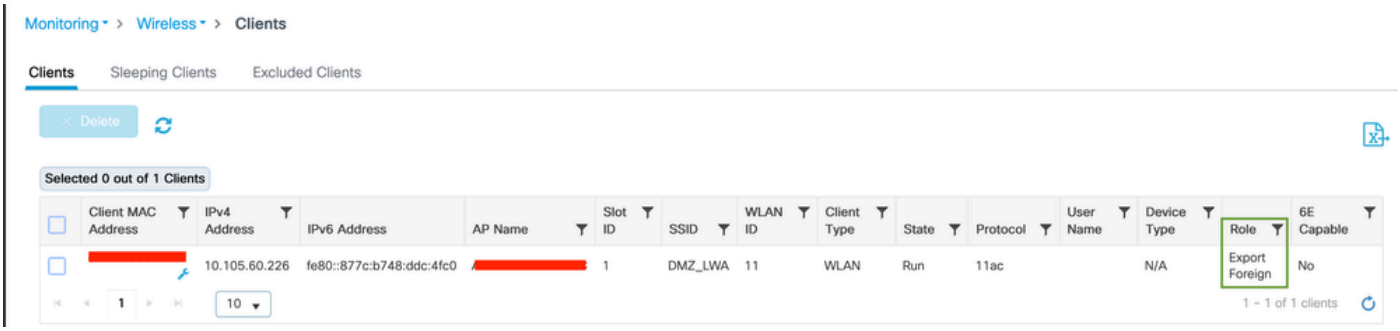
錨點上的資料包捕獲

在移動性切換之後，錨點控制器通過移動隧道接收來自外部控制器的DHCP流量。
完成DORA進程後，客戶端將進入RUN狀態並具有Export Anchor角色。從此以後，錨點控制器將作為客戶端資料流量的出口點。

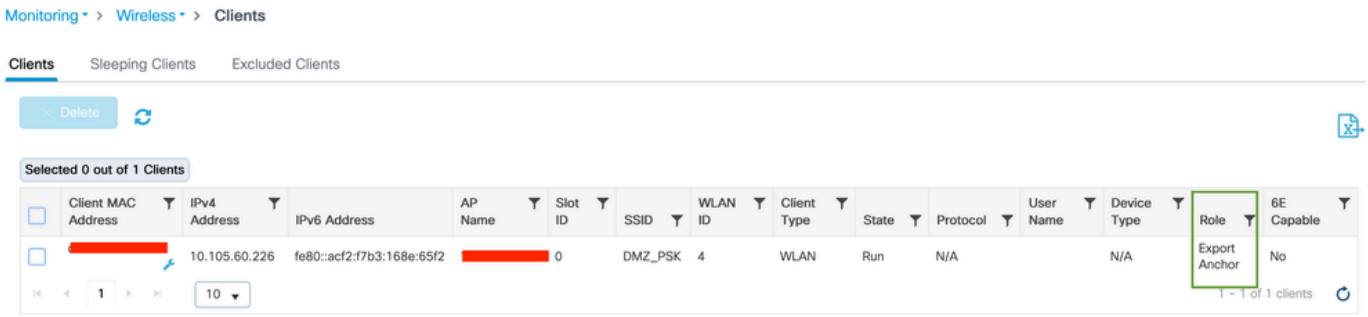
UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 3, 2025 07:36:39…	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 3, 2025 07:36:39…	0.0.0.0	255.255.255.255	346	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41…	10.105.60.69	10.105.60.226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

從外部控制器接收的錨點控制器上的客戶端DHCP流量

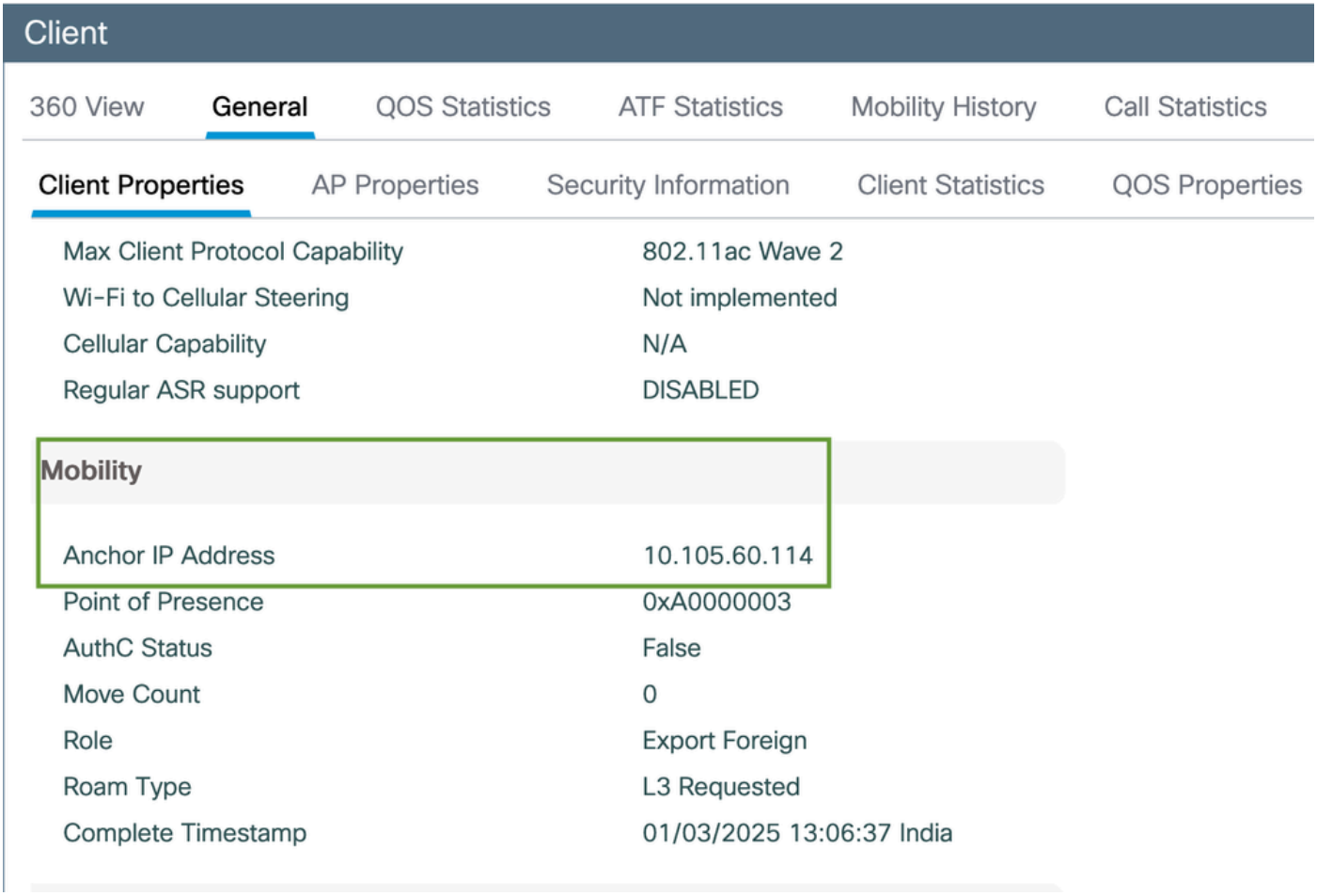
外部和錨點控制器上的客戶端狀態



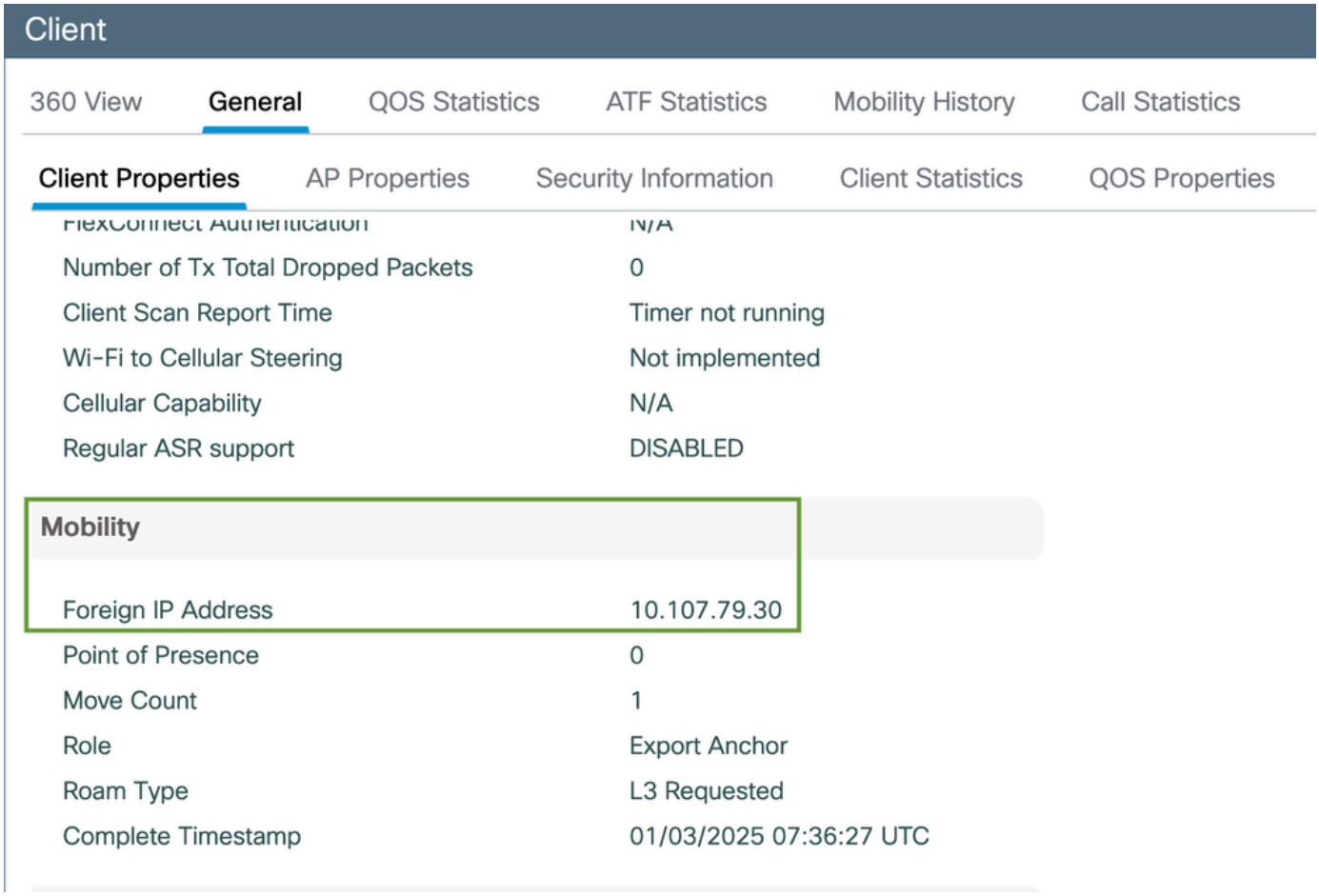
外部客戶端狀態



錨點上的客戶端狀態


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
802.11ac 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
False
Move Count
0
Role
Export Foreign
Roam Type
L3 Requested
Complete Timestamp
01/03/2025 13:06:37 India

外部客戶端屬性

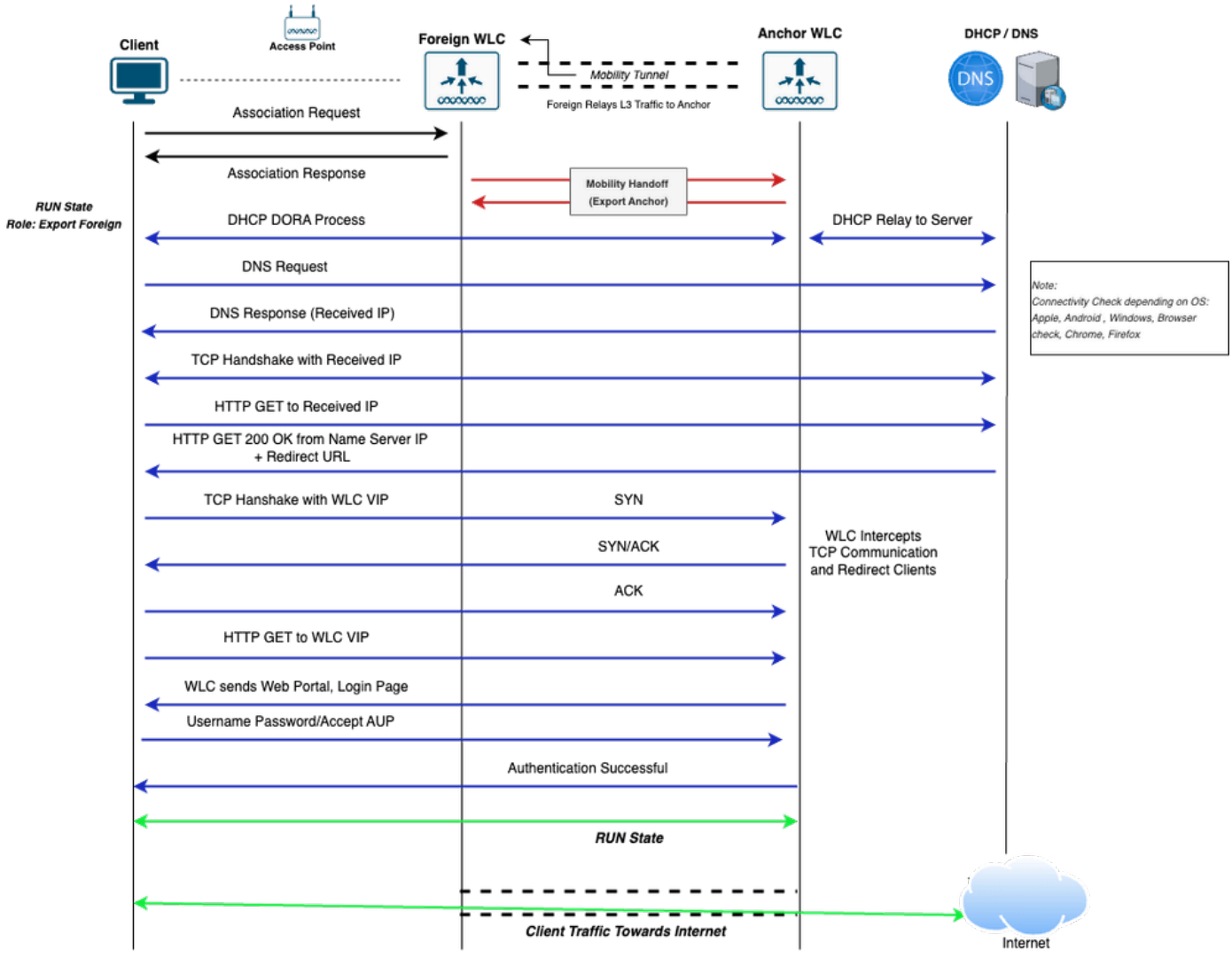

Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
Number of Tx Total Dropped Packets
0
Client Scan Report Time
Timer not running
Wi-Fi to Cellular Steering
Not implemented
Cellular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

採用第3層驗證的WLAN

本地Web驗證

外部錨點設定中本地Webauth SSID的流程

1.客戶端發起到外部WLC通告的SSID的連線。
2.由於未執行第2層驗證，因此使用者端會立即錨定到錨點WLC。使用者端在外部WLC上進入RUN狀態，其行動角色指定為Export Foreign。
3.客戶端獲取IP地址並將其重定向到網頁。此流量由錨點控制器處理。
4.成功在入口進行身份驗證後，客戶端將在具有匯出錨點角色的錨點WLC上轉換為RUN狀態。



外部錨點設定中本地Webauth SSID的客戶端連線流程圖

通過日誌分析外部錨點設定中的本地Webauth SSID流

本節介紹通過在外部和錨點控制器上使用放射性追蹤（RA追蹤）、嵌入式封包擷取(EPC)和使用者端狀態來建立本地Web驗證SSID的使用者端連線流程。

來自外部控制器的日誌

放射性痕跡

```
!! Client Association Phase !!
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Association received. BSSID BSSID_MA
{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_ANNO
{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) 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=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_RO-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_RO-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
{mobilityd_RO-0}{1}: [mm-pmtu] [18401]: (debug): Peer IP: Anchor-WLC-IP PMTU size is 1006 and calculate
{mobilityd_RO-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (1045
{wncd_x_RO-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] auth mgr attr add/change not
{wncd_x_RO-0}{1}: [auth-mgr-feat_acct] [17047]: (info): [Client_MAC:capwap_90000003] SM Notified attrib
{mobilityd_RO-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa handoff ack successfully forward
```

封包捕獲

客戶端傳送外部控制器處理的關聯請求。

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=........

與外部控制器的客戶端關聯階段

通過埠UDP 16667觸發外部控制器和錨點控制器之間的移動切換。移動事件成功後，客戶端狀態將轉換為RUN並具有「匯出外部」角色。
外部控制器通過CAPWAP隧道接收客戶端DHCP流量，並將其轉發到錨點控制器進行進一步處理。

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

使用移動隧道將外部控制器上接收的客戶端DHCP流量轉發到錨點控制器

同樣地，使用者端會透過CAPWAP通道將網路連線狀態和網頁存取檢查流量傳送到外部WLC;外部WLC使用行動通道將此轉送到錨點WLC，錨點控制器會在此攔截或處理流量。

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
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,	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,	10.107.79.129,10.105.…	128	TCP	0	80 → 52887 [FIN, ACK] Seq=634 Ack=112 Win=64256 Len=0

外部控制器上的網路連線狀態檢查

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

重定向傳送到客戶端的URL

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…	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…	128	TCP	0	443 → 53024 [ACK] Seq=1 Ack=1251 Win=64128 Len=0
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,192.0.2.1	747	TLSv1…	0	Client Hello
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,142.250…	148	TCP	0	53025 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25…	10.107.79.30,192.0.2.1	10.107.79.129,10.105…	128	TCP	0	443 → 53024 [ACK] Seq=1 Ack=1862 Win=64128 Len=0
Jan 5, 2025 12:22:25…	10.105.60.114	10.107.79.30	277	UDP		16667 → 16667 Len=231
Jan 5, 2025 12:22:25…	10.107.79.30,192.0.2.1	10.107.79.129,10.105…	293	TLSv1…	0	Server Hello, Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,192.0.2.1	143	TLSv1…	0	Alert (Level: Fatal, Description: Certificate Unknown)
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,192.0.2.1	148	TCP	0	53027 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,192.0.2.1	211	TLSv1…	0	Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25…	10.107.79.30	10.105.60.114	187	UDP		16667 → 16667 Len=141
Jan 5, 2025 12:22:25…	10.107.79.129,10.105.60.226	10.107.79.30,192.0.2.1	781	TLSv1…	0	Application Data
Jan 5, 2025 12:22:25…	10.107.79.30	10.105.60.114	757	UDP		16667 → 16667 Len=711
Jan 5, 2025 12:22:25…	10.105.60.114	10.107.79.30	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25…	10.107.79.30,192.0.2.1	10.107.79.129,10.105…	181	TLSv1…	0	Encrypted Alert

Certificate Verification for HTTPS Connection

Post HTTPS session details(client authentication)will be encrypted

使用者端存取本地Webauth頁面以提供驗證詳細資訊

來自錨點控制器的日誌

放射性痕跡

```
!! 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 o
{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

!! 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-acl] [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 Athentication !!
{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-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State GE
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Sending W
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53007/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53007/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53007/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]GET rcvd
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]HTTP GET
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Read com
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse le
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53007/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53007/19
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53008/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53009/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53009/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]GET rcvd
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]HTTP GET
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Read com
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Parse le
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53009/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53009/19
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53011/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53011/19
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53020/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53022/235 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/195 I
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/195 I
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]POST rcv
{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 com
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -1526718499,sm
{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-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State LO
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/195 I
{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-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State AU
{wncd_x_R0-0}{1}: [webauth-acl] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Unapply IP
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template De
{wncd_x_R0-0}{1}: [webauth-acl] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Unapply IP
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template De
{wncd_x_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client_MAC Link-local bridging not enabled for
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Authc success from WebAuth
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event APPLY_USER_PRO
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event RX_METHOD_AUTH

{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 no
{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-acl] [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
{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 Temp
{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
```

封包捕獲

在移動性切換之後，錨點控制器通過移動隧道接收來自外部控制器的DHCP流量。

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

從外部控制器接收的錨點控制器上的客戶端DHCP流量

錨點控制器接收連通性檢查、網頁訪問請求和驗證詳細資訊以進行進一步處理。

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

錨點控制器上的網路連線狀態檢查

```
> 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
v 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: [redacted]]
    File Data: 472 bytes
> Line-based text data: text/html (9 lines)
```

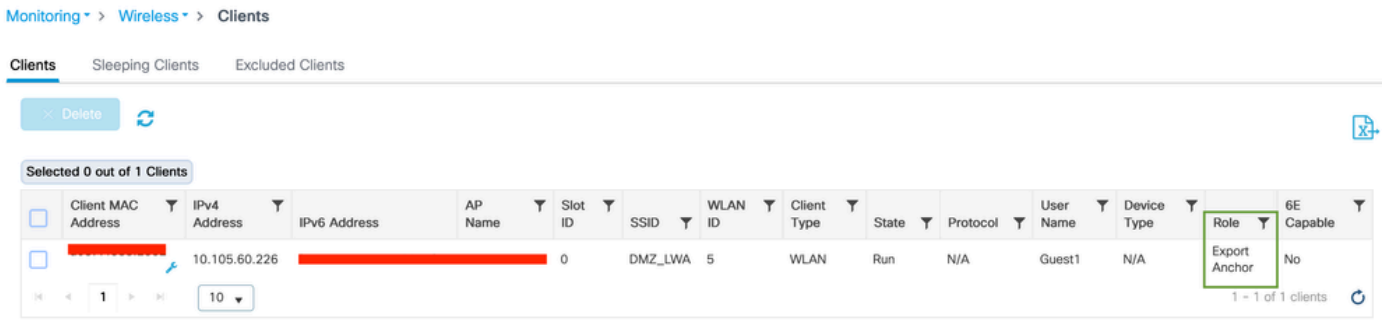
重定向傳送到客戶端的URL

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

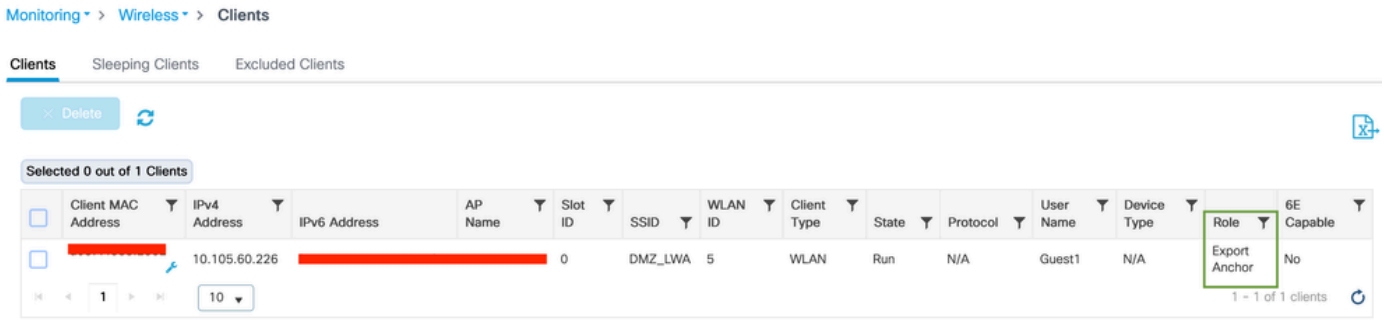
使用者端存取本地Webauth頁面以提供驗證詳細資訊

成功進行本地Web身份驗證後，客戶端將進入RUN狀態並具有Export Anchor角色。從此以後，錨點控制器將作為客戶端資料流量的出口點。

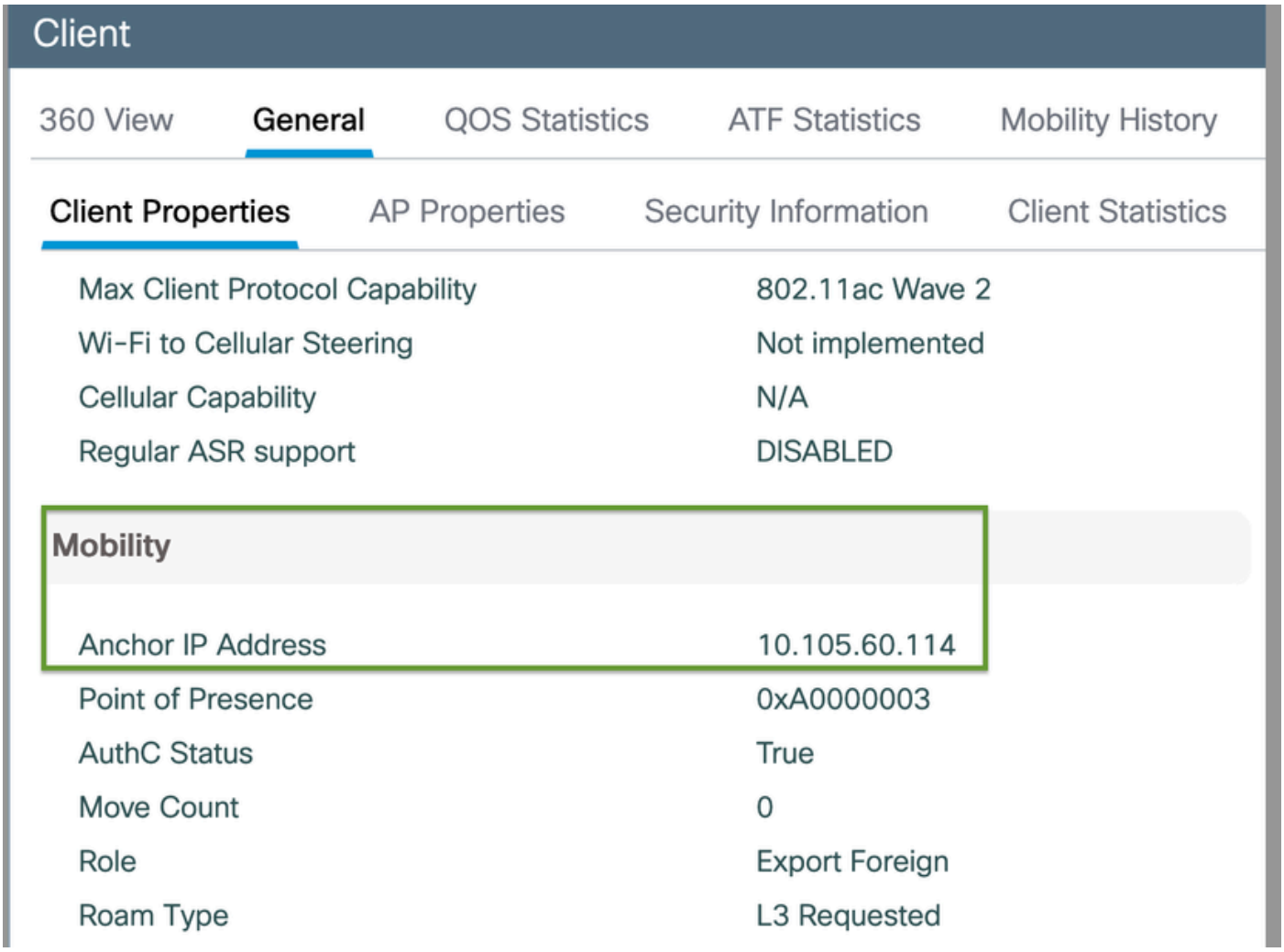
外部和錨點控制器上的客戶端狀態



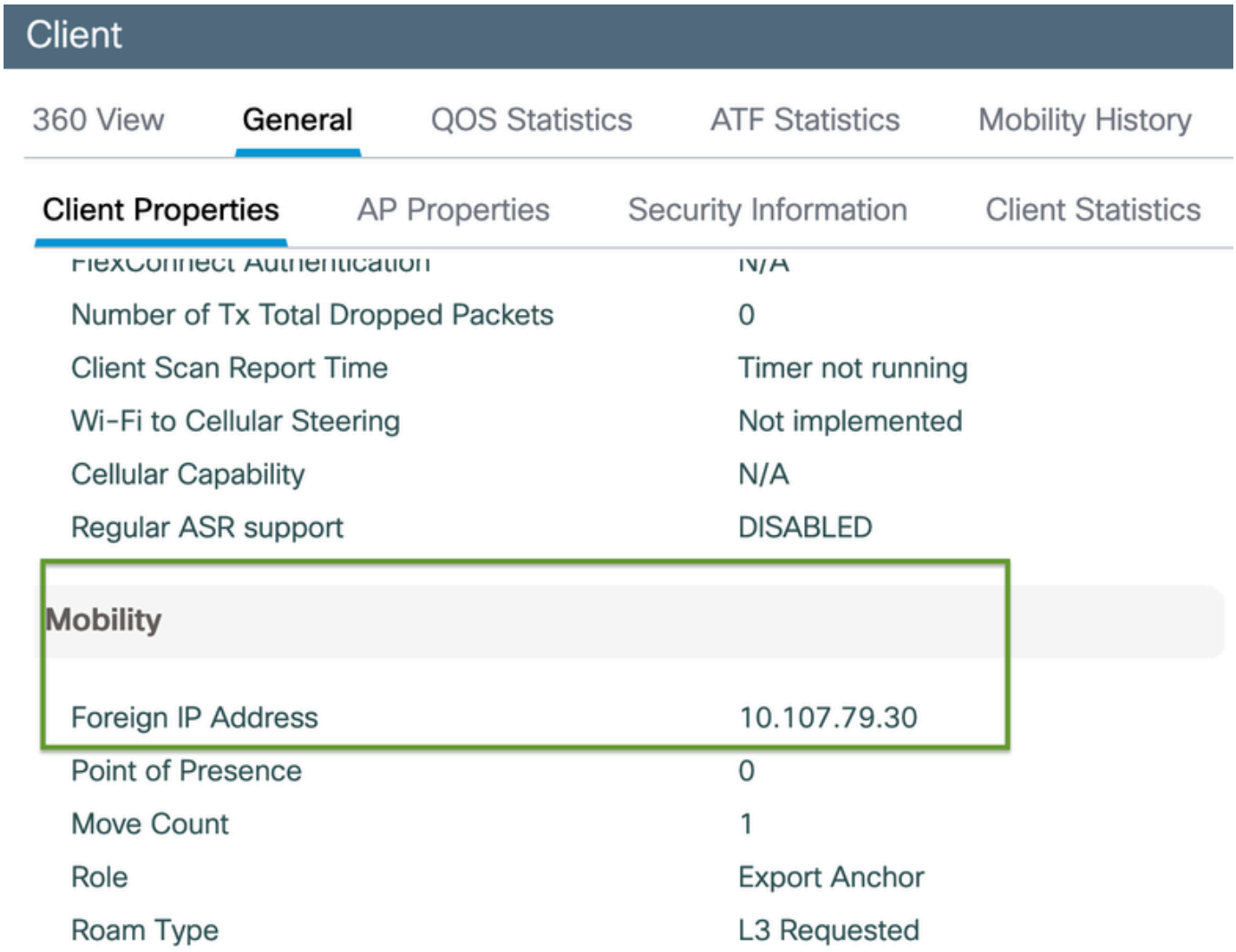
外部客戶端狀態



錨點上的客戶端狀態



外部客戶端屬性



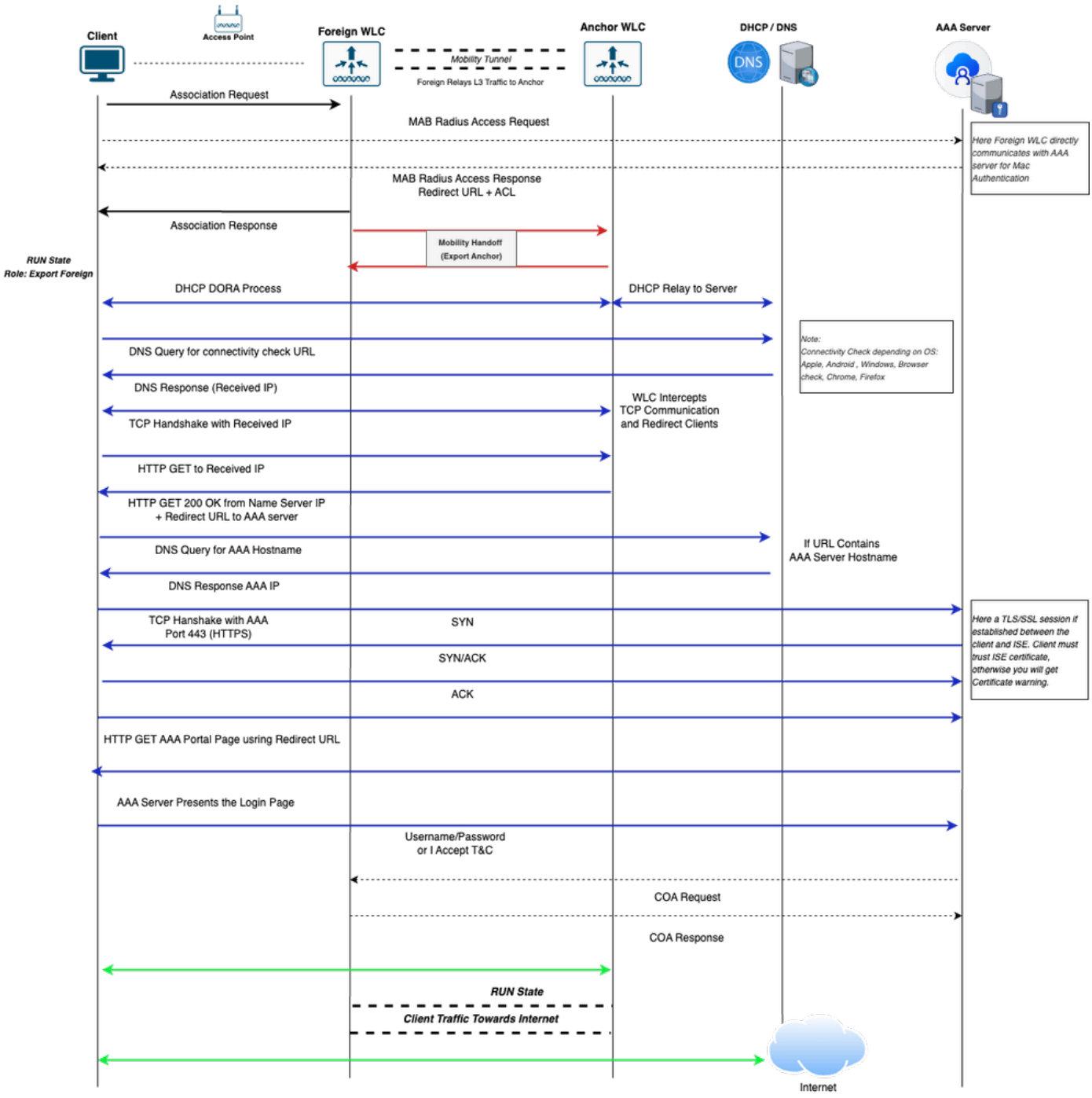
錨點上的客戶端屬性

中央 Web 驗證

外錨設定中中央Webauth SSID的流量

1.客戶端傳送由外部無線LAN控制器(WLC)廣播的SSID關聯請求。
2.外部WLC透過向RADIUS伺服器傳送存取要求來執行MAC過濾。RADIUS伺服器使用Access-Accept進行回應，包括必需的重新導向URL和存取控制清單(ACL)。
3.外部WLC將關聯響應傳送到使用者端。
4.使用者端錨定到錨點WLC。使用者端在外部WLC上進入RUN狀態，行動角色設定為Export Foreign。
5.客戶端獲取IP地址。在這個階段，錨點WLC會處理重新導向流量，將使用者端導向驗證入口網站。
6.重定向後，客戶端將直接與RADIUS伺服器通訊。此流量通過錨點WLC通道連線到RADIUS伺服器。
7.客戶端向RADIUS伺服器輸入身份驗證憑證。成功驗證後，RADIUS伺服器會將授權變更(CoA)要求傳送到外部WLC。

8.外部WLC將CoA回應傳送到RADIUS伺服器。客戶端在錨點WLC上轉換為RUN狀態，角色設定為Export Anchor。
9.所有後續的客戶端流量都從外部WLC通過隧道傳輸到錨點WLC，在此它退出網路。



外部錨點設定中中央Webauth SSID的客戶端連線流程圖

通過日誌分析外部錨點設定中的中央Webauth SSID流

本節介紹通過使用外部和錨點控制器上的放射性追蹤（RA追蹤）、嵌入式封包擷取(EPC)和使用者端狀態，中央Web驗證SSID的使用者端連線流程。

來自外部控制器的日誌

放射性痕跡

```
!! Client Association Phase !!
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Association received. BSSID BSSID_MA
{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:
{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authz_list:
{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-acl=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 !!
□{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_ANNO
{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-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 >> !

!! Post Succesful Web authentication, Change of Authorization !!
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Processing CoA request und
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Reauthenticate request (0x
{wncd_x_R0-0}{1}: [sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list -50323943,sm_
{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB re-authentication started for
{wncd_x_R0-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Context changing state from
{wncd_x_R0-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Method mab changing state fr
{wncd_x_R0-0}{1}: [aaa-coa] [17047]: (info): radius coa proxy relay coa resp(wncd)
{wncd_x_R0-0}{1}: [aaa-coa] [17047]: (info): CoA Response Details
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17047]: (info): << ssg-command-code 0 32 >>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17047]: (info): << formatted-clid 0 Client_MAC>>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [17047]: (info): << error-cause 0 1 [Success]>>
{wncd_x_R0-0}{1}: [aaa-coa] [17047]: (info): server:10.107.79.30 cfg_saddr:10.107.79.30 udpport:51304 s
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER] CoA response sent
{wncd_x_R0-0}{1}: [caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Identity preserved: MAC (C
{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] Received event 'MAB_REAUTHENTICAT
{smd_R0-0}{1}: [aaa-coa] [18867]: (info): ++++++ Received CoA response Attribute List ++++++
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS(00000000): Send CoA Ack Response to 10.106.32.130:51304
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: authenticator
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Vendor, Cisco [26] 9
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: ssg-command-code [252] 3 ...
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Calling-Station-Id [31] 16 Client_MAC
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Dynamic-Author-Error-Cause[101] 6 Success [200]
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Message-Authenticator[80] 18 ...
{smd_R0-0}{1}: [aaa-pod] [18867]: (info): CoA response source port = 0, udpport = 51304,
```

```
{wncd_x_R0-0}{1}: [sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list 1627397682,sm
```

資料包捕獲

客戶端傳送關聯請求並執行MAC身份驗證，此流量由外部控制器處理。

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=........

基於無線MAB的外部控制器上的客戶端關聯階段

通過埠UDP 16667觸發外部控制器和錨點控制器之間的移動切換。移動事件成功後，客戶端狀態將轉換為RUN並具有「匯出外部」角色。

外部控制器通過CAPWAP隧道接收客戶端DHCP流量，並將其轉發到錨點控制器進行進一步處理。

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.…	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.…	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.…	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.…	416	DHCP	0	DHCP ACK - Transaction ID 0x9f36b979

使用移動隧道將外部控制器上接收的客戶端DHCP流量轉發到錨點控制器

同樣地，使用者端會透過CAPWAP通道將網路連線狀態和網頁存取檢查流量傳送到外部WLC;外部WLC使用行動通道將此轉送到錨點WLC，錨點控制器會在此攔截或處理流量。

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 A 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 A 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, Resolved IP	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,	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

外部控制器上的網路連線狀態檢查

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

重定向傳送到客戶端的URL

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

使用者端存取中央Webauth頁面以提供驗證詳細資訊

中央Web驗證成功後，外部控制器會處理CoA請求。

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

使用外部控制器的授權更改(COA)

來自錨點控制器的日誌

放射性痕跡

```
!! Mobility Handoff !!
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of X
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of X
{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

!! Session Created for Client !!
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_ASS
{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_CRI
{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 successfu

!! Central Web Authentication Applied !!

{wncd_x_R0-0}{1}: [webauth-dev] [24229]: (info): Central Webauth URL Redirect, Received a request to cre
{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 (0x9000000
{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-acl 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
```

資料包捕獲

在移動性切換之後，錨點控制器通過移動隧道接收來自外部控制器的DHCP流量。

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

從外部控制器接收的錨點控制器上的客戶端DHCP流量

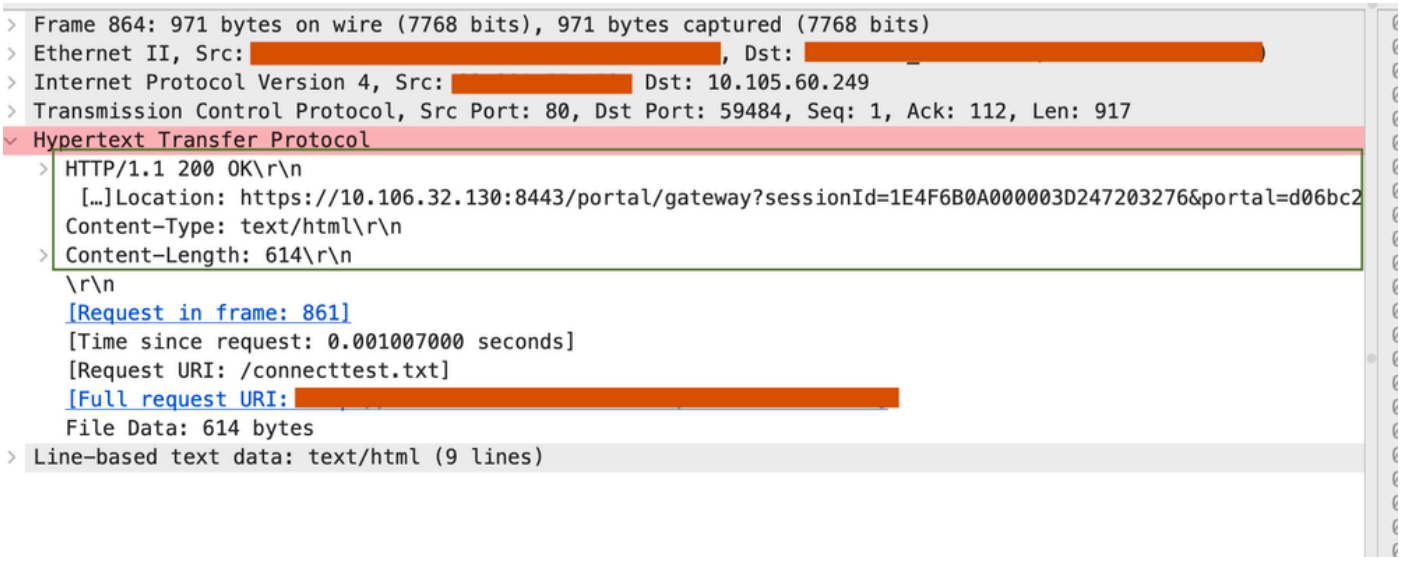
錨點控制器接收連通性檢查、網頁訪問請求和驗證詳細資訊以進行進一步處理。

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
Jan 8, 2025 13:09:44…	DNS IP	10.105.60.249	237	DNS		Standard query response 0xd4c8 A
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		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	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		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

Connectivity Check URL

Connectivity Check URL

錨點控制器上的網路連線狀態檢查



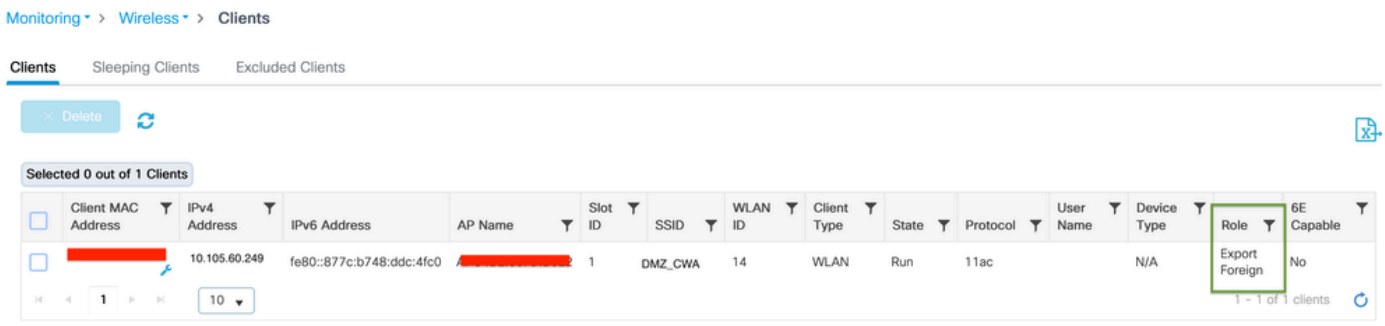
重定向傳送到客戶端的URL

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

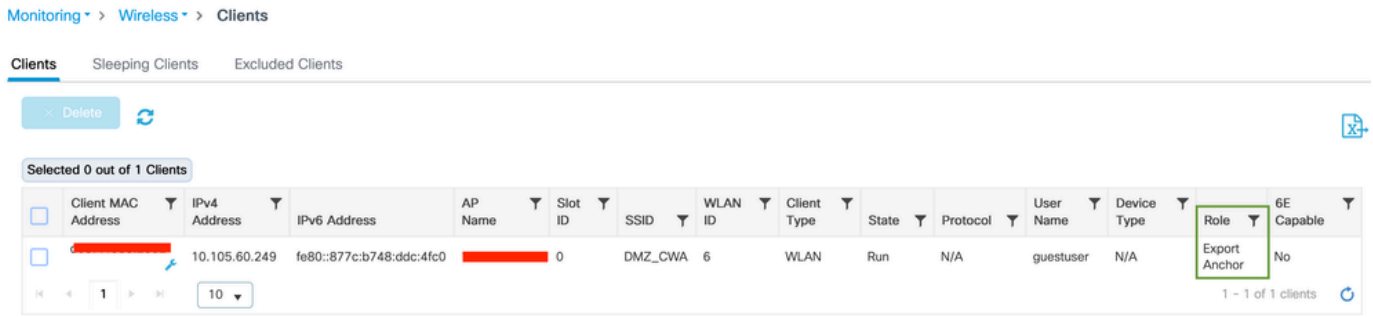
客戶端訪問本地Webauth頁面以提供身份驗證詳細資訊

當中央Web驗證成功時，會觸發授權變更(CoA)。成功執行CoA後，客戶端將轉換為具有匯出錨點角色的RUN狀態。

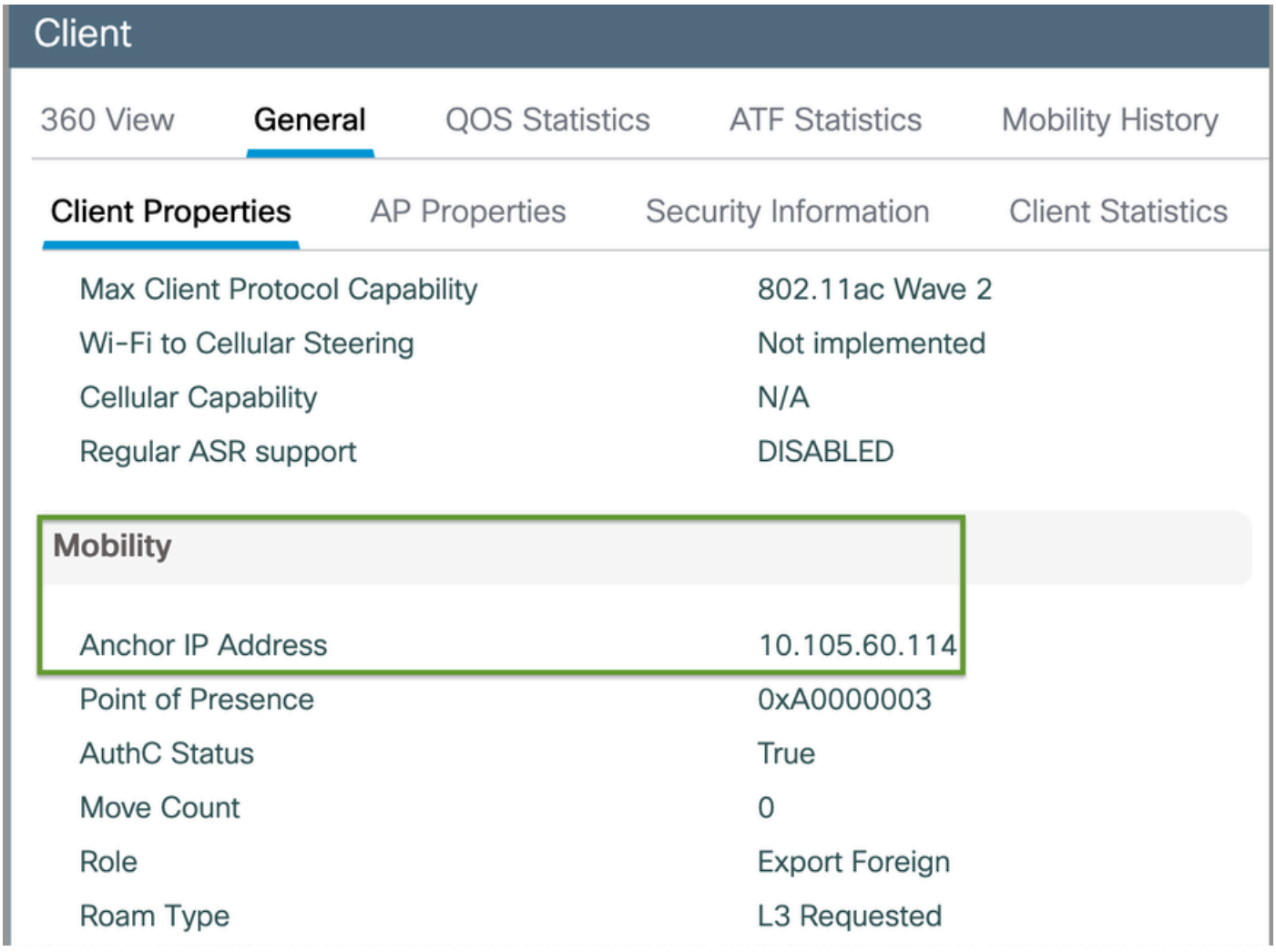
外部和錨點控制器上的客戶端狀態



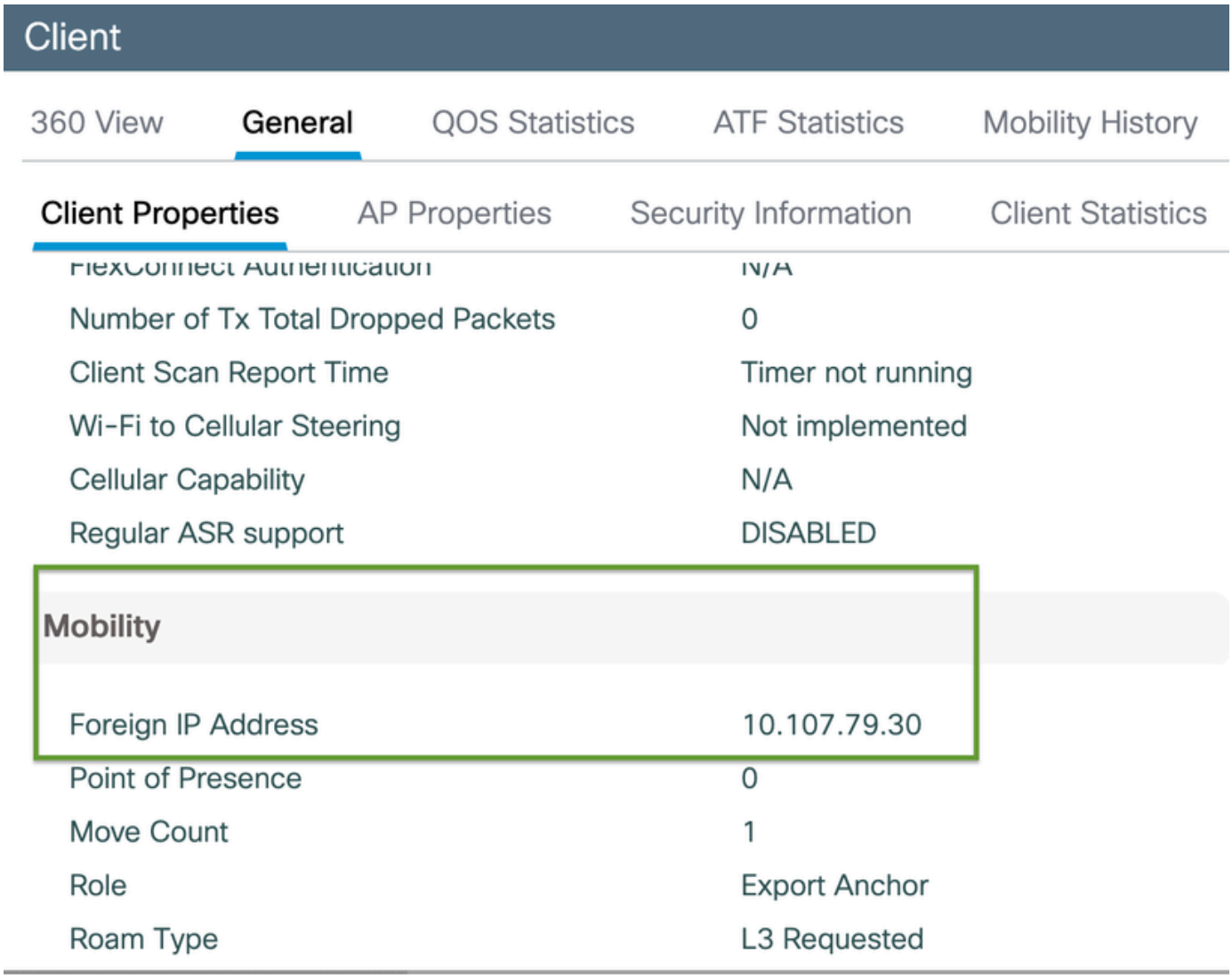
外部客戶端狀態



錨點上的客戶端狀態



外部客戶端屬性

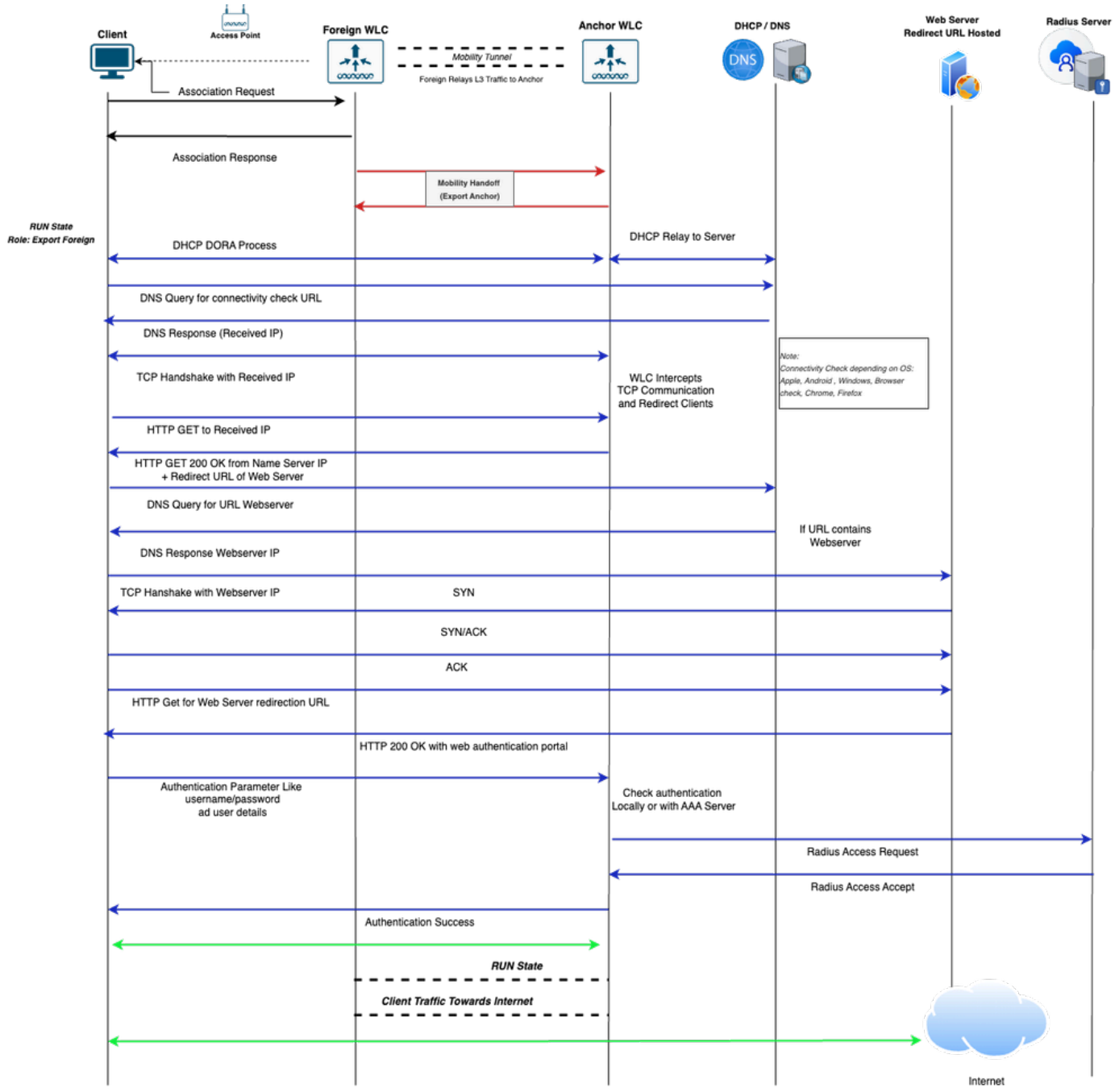


錨點上的客戶端屬性

外部Web驗證

外部錨點設定中外部Webauth SSID的流程

1.客戶端發起到外部WLC廣播的SSID的連線。
2.由於不需要第2層驗證，因此使用者端錨定到錨點WLC。使用者端在外部WLC上轉換為RUN狀態，行動角色指定為Export Foreign。
3.客戶端獲取IP地址。錨點WLC會攔截流量，並將使用者端重新導向到外部Web伺服器入口網站（如Web驗證引數中所定義）。
4.客戶端通過門戶提交身份驗證憑證。這些憑證在WLC本機上或透過外部驗證伺服器進行驗證，這取決於已設定的安全原則。
5.身份驗證成功後，客戶端將在錨點WLC上轉換到RUN狀態（假設具有「匯出錨點」角色）。
6.成功驗證後，所有後續使用者端流量都會從外部WLC通道傳送到錨點WLC，後者會在錨點中流出網路。



外部錨點設定中外部Webauth SSID的客戶端連線流程圖

通過日誌分析外部錨點設定中的外部Webauth SSID流

本節介紹通過在外部和錨點控制器上使用放射性追蹤（RA追蹤）、嵌入式封包擷取(EPC)和使用者端狀態來建立外部Web驗證SSID的使用者端連線流程。

來自外部控制器的日誌

放射性痕跡

```
!! Client Association Phase !!
{wncd_x_R0-1}{1}: [client-orch-sm] [17162]: (note): MAC: Client_MAC Association received. BSSID BSSID_MA
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_INI
{wncd_x_R0-1}{1}: [dot11] [17162]: (info): MAC: Client_MAC dot11 send association response. Sending asso
{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_DOT

!! Layer 2 Authentication None !!
{wncd_x_R0-1}{1}: [client-orch-state] [17162]: (note): MAC: Client_MAC Client state transition: S_CO_ASS
{wncd_x_R0-1}{1}: [client-auth] [17162]: (note): MAC: Client_MAC L2 Authentication initiated. method WEB
{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_MOB

!! Mobility Handoff !!
{mobilityd_R0-0}{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to grou
{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_PE
□{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_ANNO
{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_REQ
{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_RSP
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
□{wncd_x_R0-0}{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed□[mm-client] [17047] (info) MAC
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEA
{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_MC
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 of
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) 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 XID
{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_MC
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
```

資料包捕獲

客戶端傳送外部控制器處理的關聯請求。

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=........

與外部控制器的客戶端關聯階段

通過埠UDP 16667觸發外部控制器和錨點控制器之間的移動切換。移動事件成功後，客戶端狀態將轉換為RUN並具有「匯出外部」角色。
外部控制器通過CAPWAP隧道接收客戶端DHCP流量，並將其轉發到錨點控制器進行進一步處理。

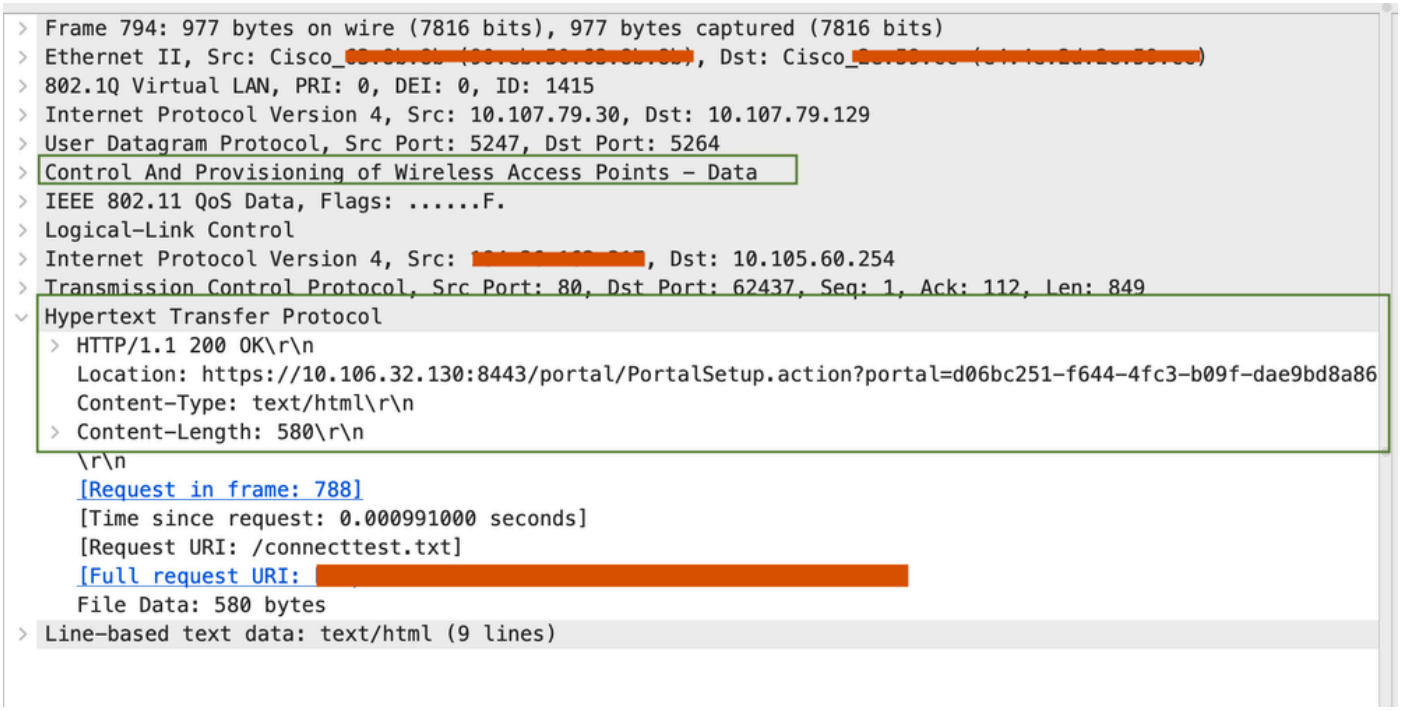
UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:01…	10.107.79.129,0.0.0.0	10.107.79.30,255.255.…	424	DHCP	0	DHCP Discover - Transaction ID 0x9f36b979
Jan 14, 2025 16:19:01…	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 14, 2025 16:19:03…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

使用移動隧道將外部控制器上接收的客戶端DHCP流量轉發到錨點控制器

同樣地，使用者端會透過CAPWAP通道將網路連線狀態和網頁存取檢查流量傳送到外部WLC;外部WLC使用行動通道將此轉送到錨點WLC，錨點控制器會在此攔截或處理流量。

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,	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

外部控制器上的網路連線狀態檢查



重定向傳送到客戶端的URL

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

使用者端存取外部Webauth頁面，以提供驗證詳細資訊

來自錨點控制器的日誌

放射性痕跡

```
!! Mobility Handoff !!
{mobilityd_RO-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of
{mobilityd_RO-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received mobile_announce, sub type 0 of
{mobilityd_RO-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
{mobilityd_RO-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Number of client is BELOW wlan limit
{mobilityd_RO-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-acl] [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, l
{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-acl] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Unapply I
{wncd_x_R0-0}{1}: [webauth-acl] [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
{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 ->
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of
{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_M
{mobilityd_R0-0}{1}: [mm-client] [26021]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) t
{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:
{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_WAI
```

資料包捕獲

在移動性切換之後，錨點控制器通過移動隧道接收來自外部控制器的DHCP流量。

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

從外部控制器接收的錨點控制器上的客戶端DHCP流量

錨點控制器接收連通性檢查、網頁訪問請求和驗證詳細資訊以進行進一步處理。

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		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

錨點控制器上的網路連線狀態檢查

```
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)
```

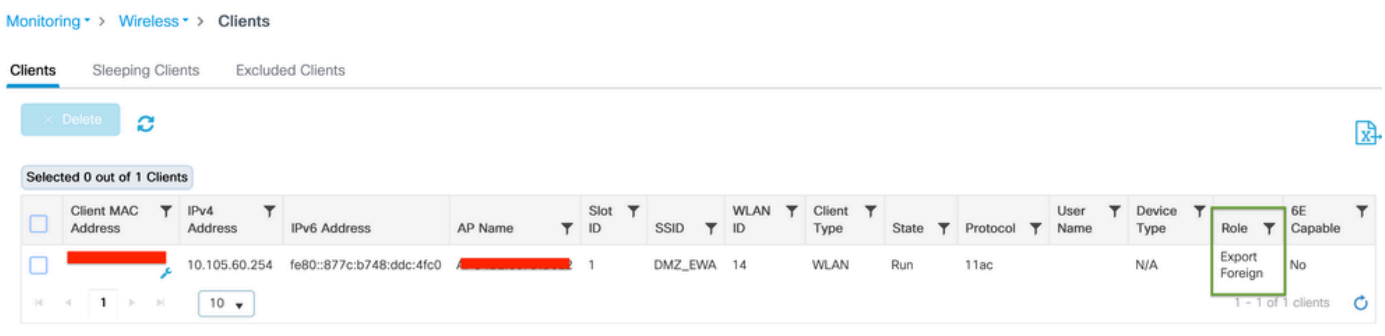
重定向傳送到客戶端的URL

客戶端通過門戶提交身份驗證憑證。這些憑證在WLC本機上或透過外部驗證伺服器進行驗證，這取決於已設定的安全原則。

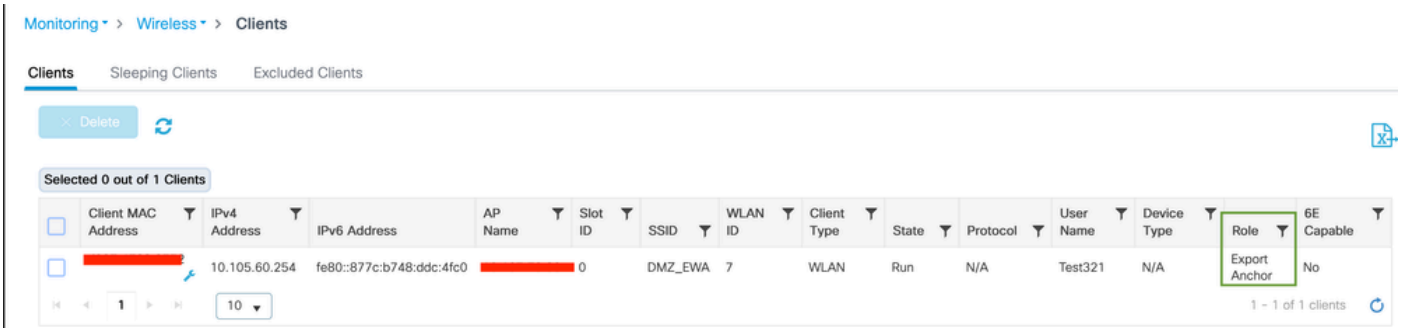
UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:12.…	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12.…	10.105.60.254	10.106.32.130	66	TCP		62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:12.…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

使用者端存取外部Webauth頁面，以提供驗證詳細資訊

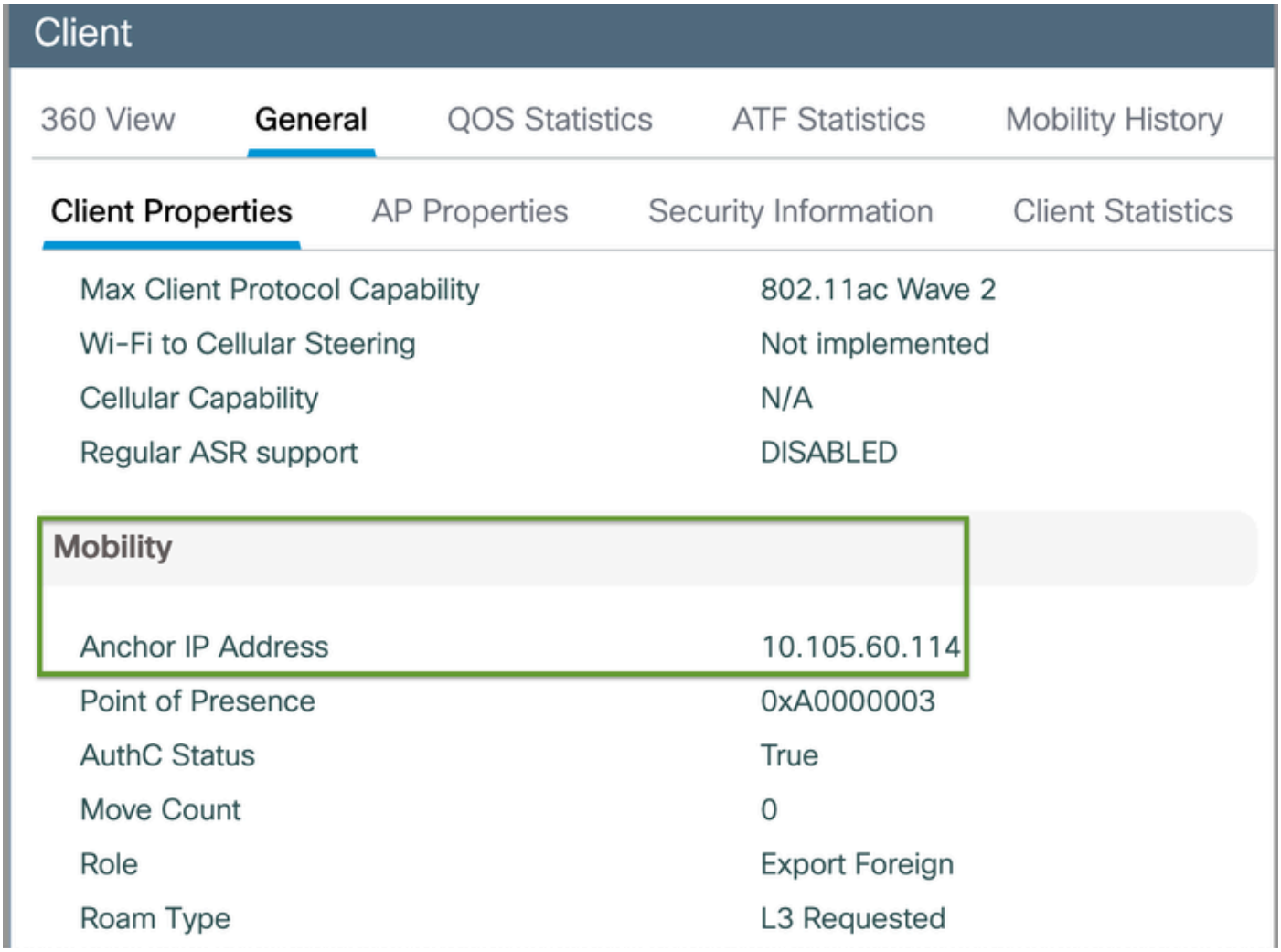
外部和錨點控制器上的客戶端狀態



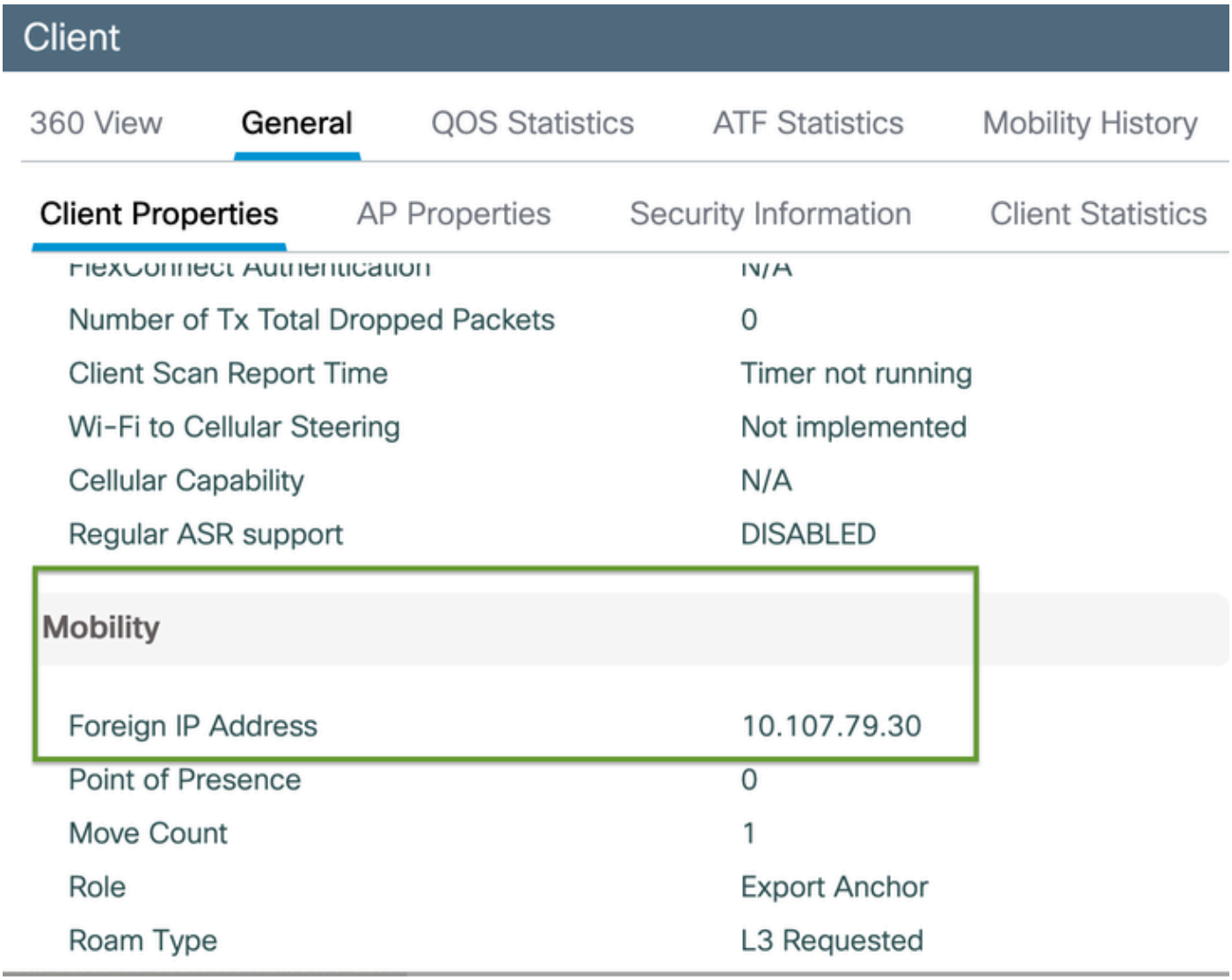
外部客戶端狀態



錨點上的客戶端狀態



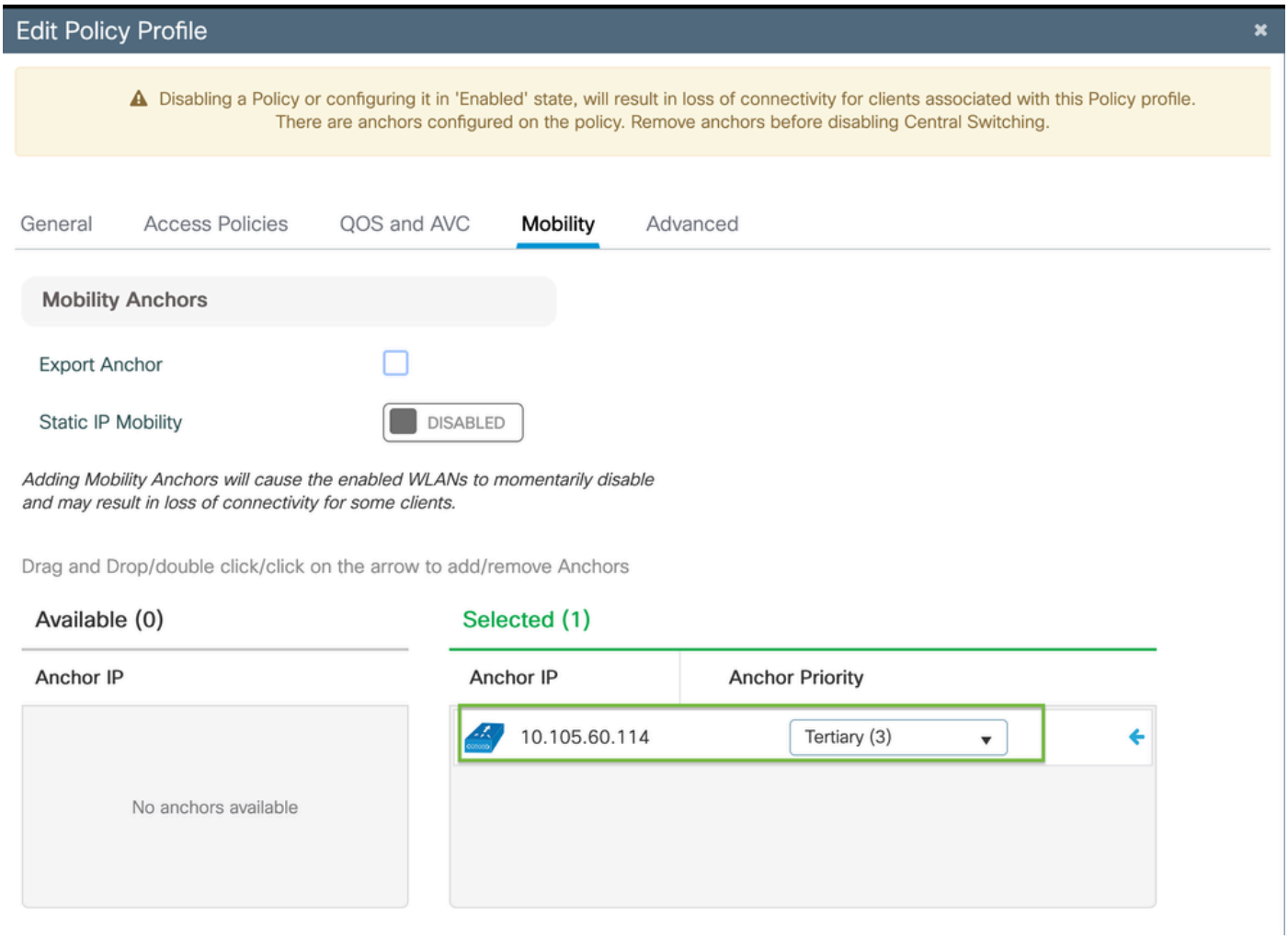
外部客戶端屬性



錨點上的客戶端屬性

多個錨點控制器之間的負載平衡

當多個錨點控制器對映到單個WLAN時，流量分配取決於優先順序。可以配置三個優先順序級別：主要、次要和第三級。訪客錨點優先順序功能提供錨點控制器之間主用/備用負載分配的機制。這是通過向每個錨點控制器分配固定優先順序來實現的：負載會分散到最高優先順序的控制器，並在共用相同優先順序值的控制器之間以循環方式分配。



對映錨點優先順序

附註：預設情況下，優先順序三級是在外部控制器上的錨點控制器對映期間配置的。

Foreign-Anchor方案中的客戶端連線故障排除

1. 客戶端加入問題
   i. 通道狀態：驗證外部控制器和錨點控制器之間的移動隧道是否保持活動狀態。
   ii. 配置不匹配：確保兩個控制器之間的配置奇偶校驗。WLAN名稱、策略配置檔名稱或高級設定（例如AAA覆蓋、IPv4 DHCP要求和NAC）中的差異會導致配置檔案不匹配或錨點拒絕錯誤。
   iii. 其他:如果通道處於開啟狀態且沒有任何組態問題，疑難排解方法與正常使用者端連線問題類似，可確保檢查處理受影響流量的對應控制器。

2. 間歇性連線
   i. 通道擺動：如果兩個控制器之間的keepalive資料包未能到達，則通道會抖動，使客戶端無法保持與SSID的連線。
   ii. 低頻寬：如果行動對等點之間的路徑MTU(PMTU)下降到較小的值(576)，使用者端會遇

到效能下降的情況。當兩個行動對等點之間的路徑mtu keepalive訊息都遺失時，通常會發生這種情況

附註：行動性MAC位址較低的控制器會啟動標準keepalive和路徑MTU keepalive訊息。

3. 特定網站訪問問題
   i. 移動流量報頭包括通過UDP埠16666和16667交換的移動組識別符號、MAC地址、IP地址和加密的CAPWAP DTLS資料包。此開銷會新增到現有的CAPWAP報頭。對於TCP流量，如果由於此額外開銷導致資料包大小超過移動PMTU（最大1385位元組），則調整後為AP配置的TCP MSS，則會進行分段。雖然分段通常由網路處理，但如果資料包到達順序混亂或延遲，則會出現問題。這些情況會影響資料包的重組，並導致特定網站的資料可訪問性失敗。

從外部和錨點控制器收集日誌

1. 啟用term exec prompt timestamp，以便對所有命令進行時間引用。
2. 使用show tech-support wireless !!檢視配置。
3. 您可以檢查行動通道狀態show wireless mobility summary !!
4. 包括鏈路狀態、客戶端資料和事件的移動對等體統計資訊、保持活動統計資訊show wireless mobility peer ip <IP>
5. 為移動對等IP/MAC地址和客戶端MAC地址啟用放射性跟蹤。

   通過CLI:

   debug wireless {MAC | ip} {aaaa.bbb.cccc | x.x.x.x } {monitor-time} {N seconds} !!設定時間允許我們啟用最多24天的跟蹤。

   no debug wireless {MAC | ip} {aaaa.bbb.cccc | x.x.x.x !!禁用調試

   WLC使用Client_info生成調試跟蹤檔案，並命令檢查生成的調試跟蹤檔案dir bootflash: | i debug !!

警告：條件調試啟用調試級別日誌記錄，從而增加生成的日誌量。保持此運行可減少檢視日誌的時間間隔。因此，建議在故障排除會話結束時始終禁用調試。

6. 要禁用所有調試，請運行以下命令：

   # clear platform condition all !!

   # undebug all !!
   通過GUI:

步驟1.導覽至Troubleshooting > Radiative Trace。

步驟2.按一下Add，然後輸入您要疑難排解的行動化對等MAC/IP位址或使用者端MAC位址。
步驟3.準備好開始放射性示蹤後，按一下開始。啟動後，調試日誌記錄會寫入磁碟，記錄與跟蹤的MAC地址相關的任何控制平面處理。
步驟4.重現要診斷的問題時，按一下Stop。
步驟5.對於已調試的每個MAC地址，您可以通過按一下Generate生成一個日誌檔案，該檔案整理與該MAC地址相關的所有日誌。
步驟6.選擇想要整理日誌檔案的回溯時間，然後按一下Apply to Device。
步驟7.現在，您可以按一下檔案名稱旁邊的小圖示來下載檔案。此檔案存在於控制器的啟動快閃記憶體驅動器中，也可以通過CLI從盒中複製出來。

7. 嵌入式捕獲

通過CLI:
monitor capture MYCAP clear !!
監控擷取MYCAP介面Po1 both !!
monitor capture MYCAP buffer size 100 !!
monitor capture MYCAP match access-list name !!（如果跟蹤WLC之間的行動通道流量）
monitor capture MYCAP match any/ipv4/ipv6.MAC !!
monitor capture MYCAP start !!
!!複製
監視器捕獲MYCAP停止
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap

通過GUI:

步驟1.導覽至Troubleshooting > Packet Capture > +Add。
步驟2.定義資料包捕獲的名稱。最多允許8個字元。
步驟3.定義過濾器（如果有）。
步驟4.如果要檢視發往系統CPU並注入回資料平面的流量，請選中以監視控制流量框。
步驟5.定義緩衝區大小。最多允許100 MB。
步驟6.根據需要定義限制(按允許範圍1 - 1000000秒的持續時間或按允許範圍1 - 100000個資料包的資料包數量)。
步驟7.從左欄中的介面清單中選擇interface，然後選擇箭頭將其移至右欄。
步驟8.按一下「Save and Apply to Device」。
步驟9.要開始捕獲，請選擇開始。
步驟10.您可以讓捕獲運行到定義的限制。要手動停止捕獲，請選擇停止。
步驟11.停止後，可以使用Export按鈕按一下此選項以通過HTTP或TFTP伺服器、FTP伺服器、本地系統硬碟或快閃記憶體將捕獲檔案(.pcap)下載到本地案頭。

相關資訊

在Catalyst 9800 WLC上配置移動拓撲

在Catalyst 9800上設定WLAN錨點行動功能

技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。