了解9800 WLC之间的外部锚点设置中的流量

目录

简介

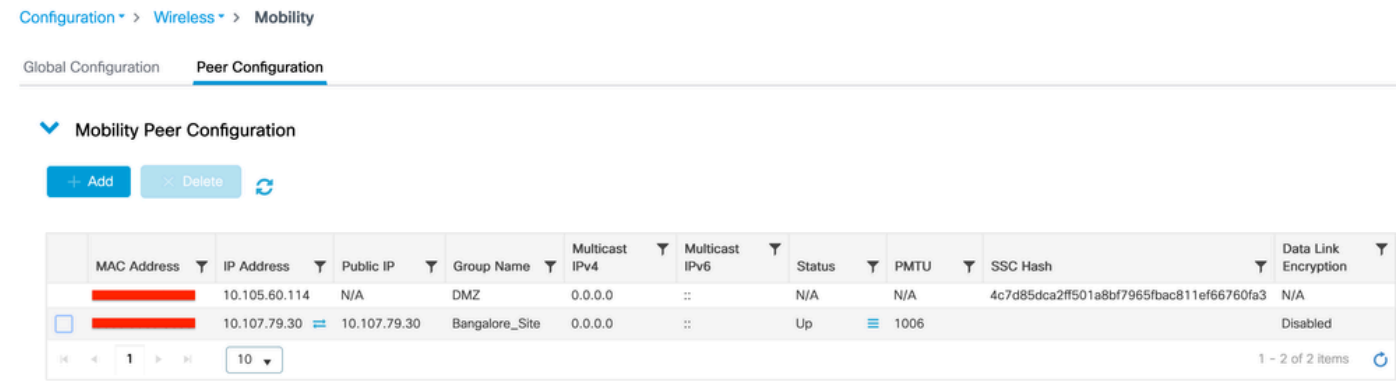
本文档介绍Cisco 9800 WLC之间的外部锚点设置中的流量，包括L2/L3客户端自注册和故障排除。

先决条件

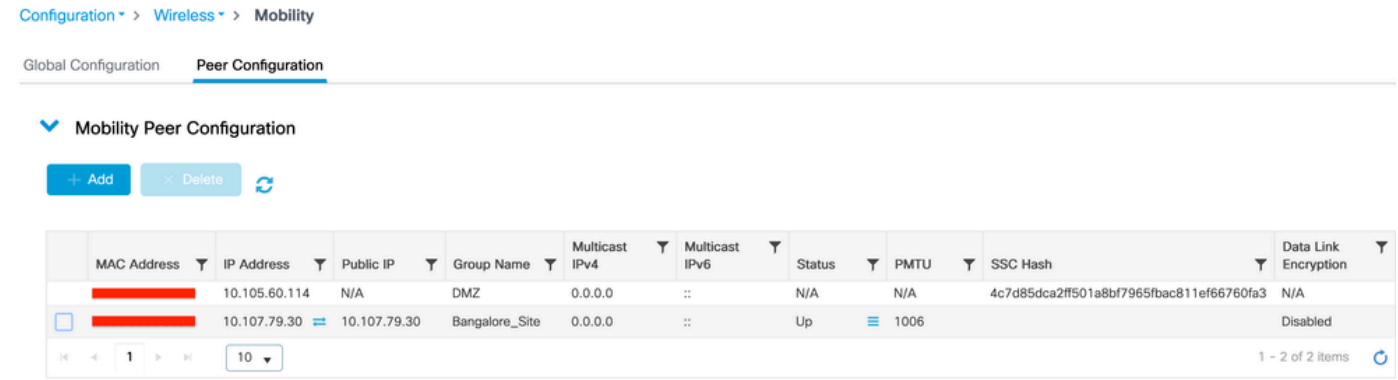
外部和锚点控制器之间的移动隧道。

两个WLC之间允许UDP端口16666和16667。

为中央交换配置的策略配置文件。



外部WLC上的移动隧道状态



锚点WLC上的移动隧道状态

要求

思科建议您了解以下主题：

- 对无线控制器的命令行界面(CLI)或图形用户界面(GUI)访问
- 思科无线局域网控制器(WLC)上的移动性

- 9800无线控制器
- 9800 WLC上的放射性痕迹和数据包捕获

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800型WLC
- Cisco IOS XE 17.15.5版本
- 9100系列无线接入点型号

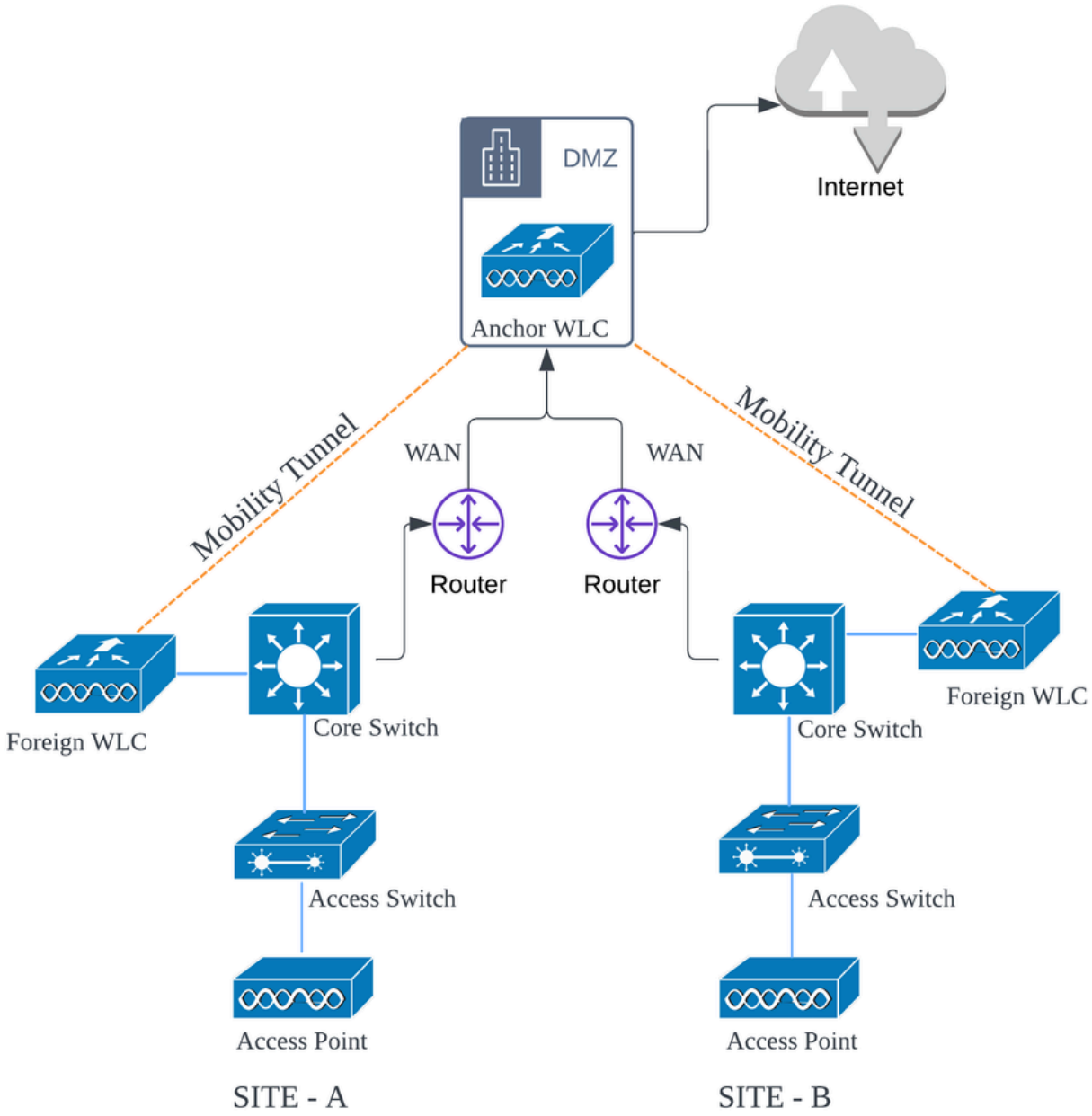
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

外部锚点方案概述

- 外部控制器：此WLC管理网络的第2层或无线端。它连接了接入点，并且锚定WLAN的所有客户端流量都封装到移动隧道中并发送到锚点控制器。流量不会在外部控制器上本地退出。
- 锚控制器:这用作第3层出口点。它通过移动隧道从外部控制器接收客户端流量，并将客户端流量解封或终止到出口点(VLAN)。 这是网络中客户端所在的位置。

外部WLC上的接入点广播WLAN SSID，并分配了一个策略标记，用于将WLAN配置文件与相应的策略配置文件链接。当无线客户端连接到此SSID时，外部控制器将SSID名称和策略配置文件作为客户端信息的一部分发送到锚点WLC。接收时，锚点WLC检查自己的配置以匹配SSID名称以及策略配置文件名称。锚点WLC找到匹配项后，它会应用相应的配置并为无线客户端提供出口点。因此，除了策略配置文件下的VLAN外，必须匹配外部和锚点9800 WLC上的WLAN和策略配置文件名称和配置。

拓扑



9800 WLC之间的外部锚点设置

采用第2层身份验证的WLAN

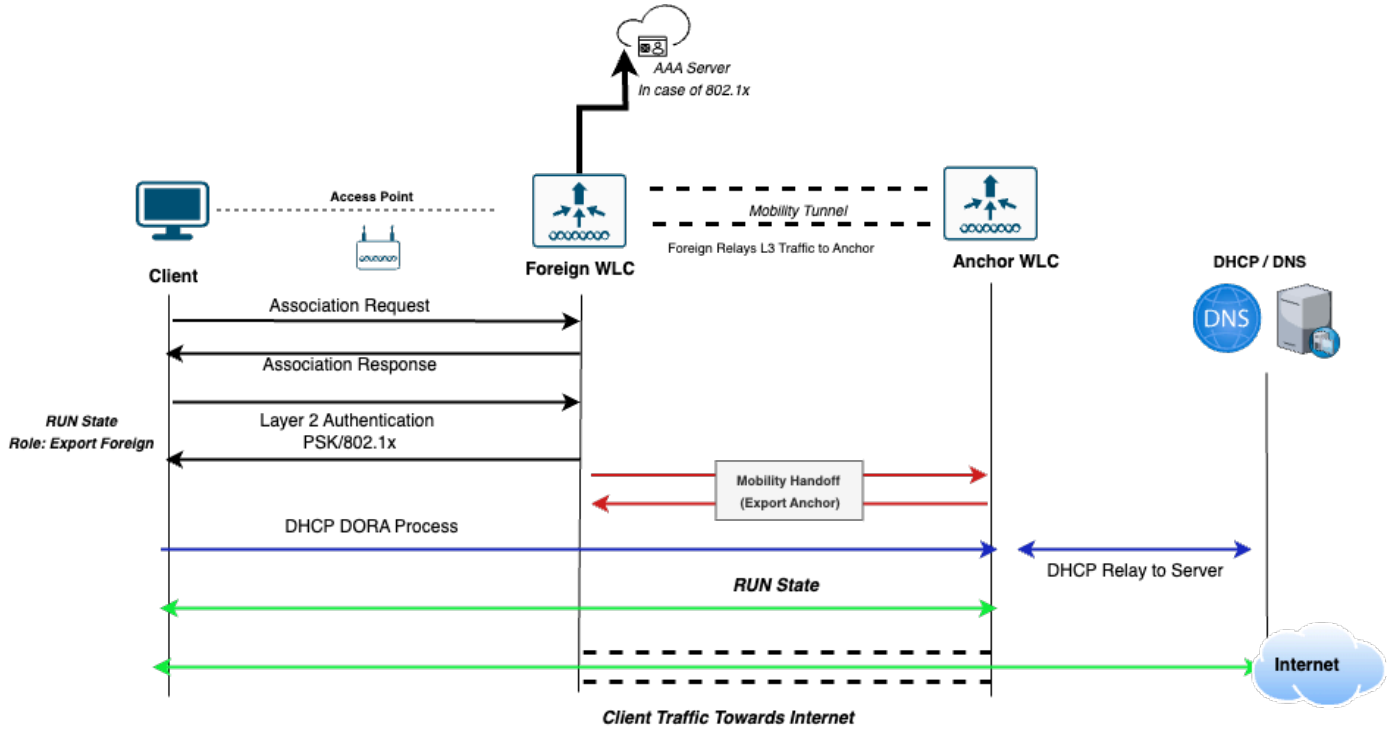
配置要求

1.确保外部WLC和锚点WLC上的WLAN名称和配置相同，并且配置为第2层身份验证（PSK或802.1x）。
2.在具有相同配置的外部WLC和锚点WLC上创建具有相同名称的策略配置文件。
3.在外部WLC上，在各自的策略配置文件中配置锚点WLC映射。

4.在锚点WLC上，配置策略配置文件以将控制器指定为导出锚点。
5.在外部WLC上，使用策略标记将WLAN映射到相应的策略配置文件。

第2层基于外部锚点的SSID的流

1.客户端发起到外部WLC广播的SSID的连接。外部WLC执行第2层身份验证，根据配置的安全策略在本地或通过外部AAA服务器验证凭证。
2.身份验证成功后，客户端会话将锚定到锚点WLC。为客户端分配IP地址，并在锚点WLC上转换为RUN状态。
3.建立会话后，所有客户端数据流量通过隧道从外部WLC传输到锚点WLC，从锚点WLC进入网络。



基于第2层外部锚点的WLAN流程图

通过日志分析外部锚点设置中的第2层SSID流

本部分介绍通过使用外部和锚点控制器上的放射性跟踪（RA跟踪）、嵌入式数据包捕获(EPC)和客户端状态的第2层客户端连接的流程。

来自外部控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

客户端发送关联请求并执行第2层身份验证，由外部控制器处理。

	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)

客户端关联+第2层身份验证流量

移动切换通过UDP端口16667在外部控制器和锚点控制器之间触发。移动事件成功后，客户端状态将转换为RUN并具有“导出外部”角色。
外部控制器通过CAPWAP隧道接收客户端DHCP流量并将其转发到锚点控制器进行进一步处理。

	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

在外部控制器上接收的客户端DHCP流量使用移动隧道转发到锚点控制器

来自Anchor 9800控制器的日志

锚上的放射性痕迹

```
!! 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
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.
{□wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.>> Client is successf

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

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

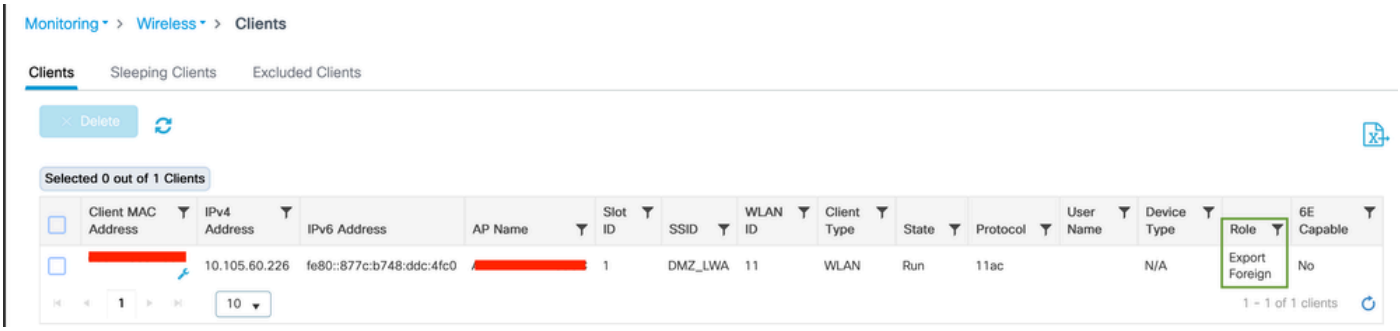
锚点上的数据包捕获

在移动切换后，锚点控制器通过移动隧道接收来自外部控制器的DHCP流量。
完成DORA进程后，客户端将进入具有导出锚点角色的RUN状态。从此以后，锚点控制器将作为客户端数据流量的出口点。

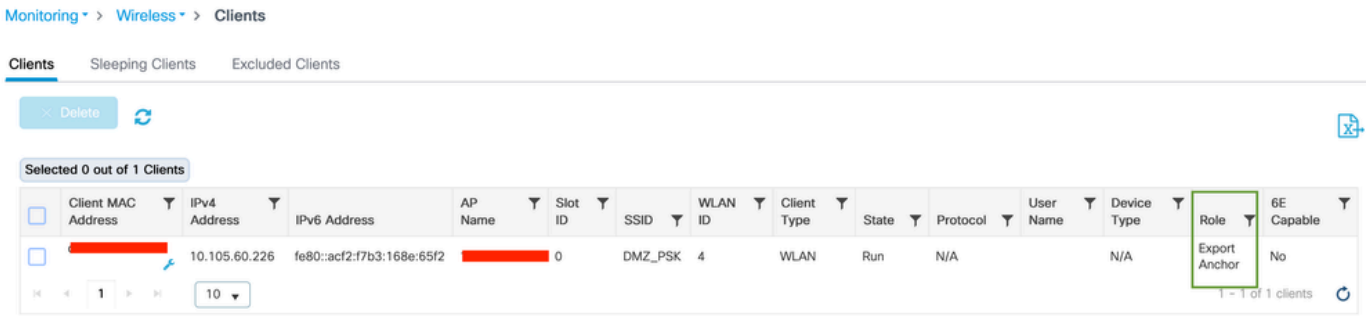
UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 3, 2025 07:36:39…	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 3, 2025 07:36:39…	0.0.0.0	255.255.255.255	346	DHCP		DHCP Discover - Transaction ID 0x9f36b979
Jan 3, 2025 07:36:41…	10.105.60.69	10.105.60.226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

从外部控制器接收的锚点控制器上的客户端DHCP流量

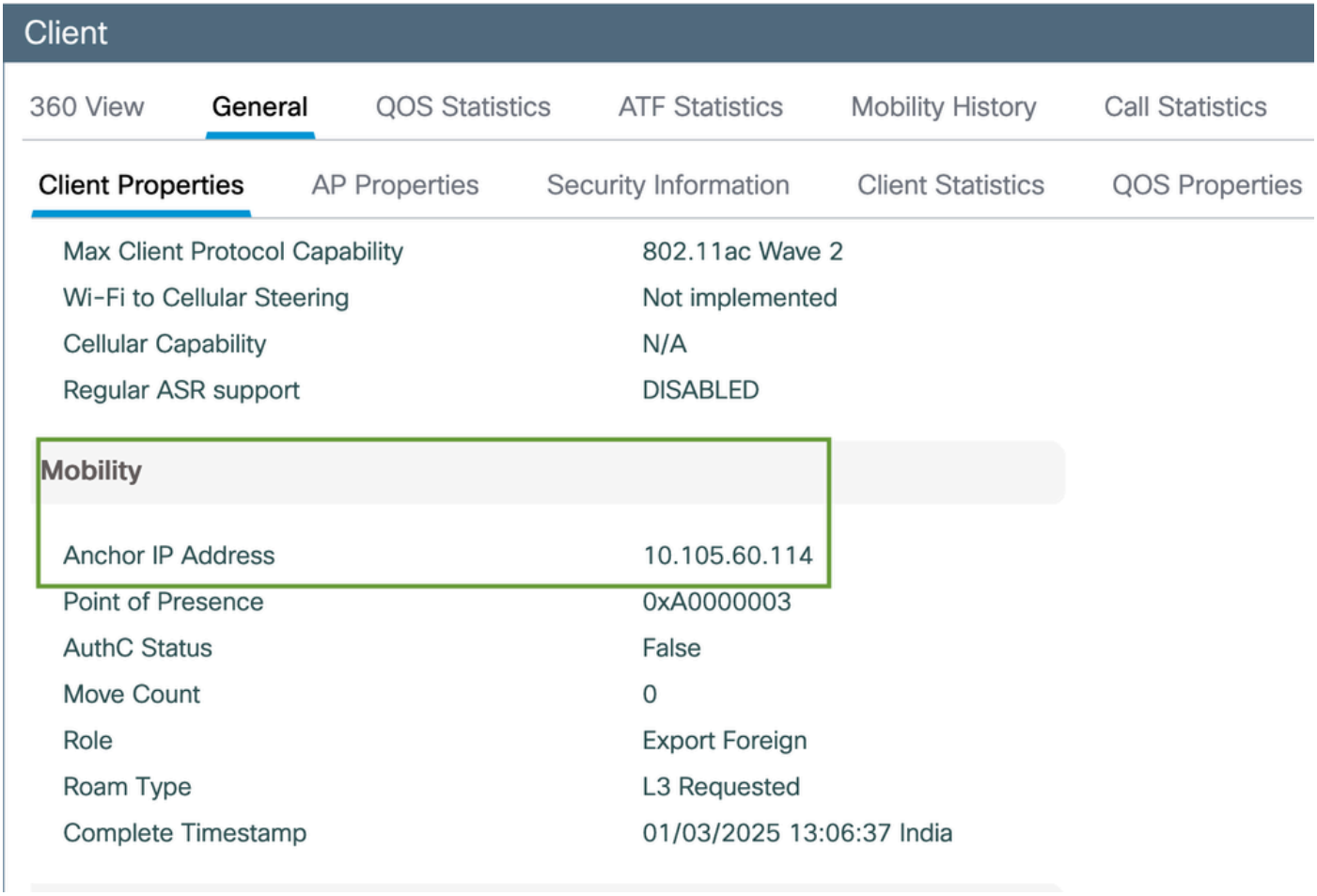
外部和锚点控制器上的客户端状态



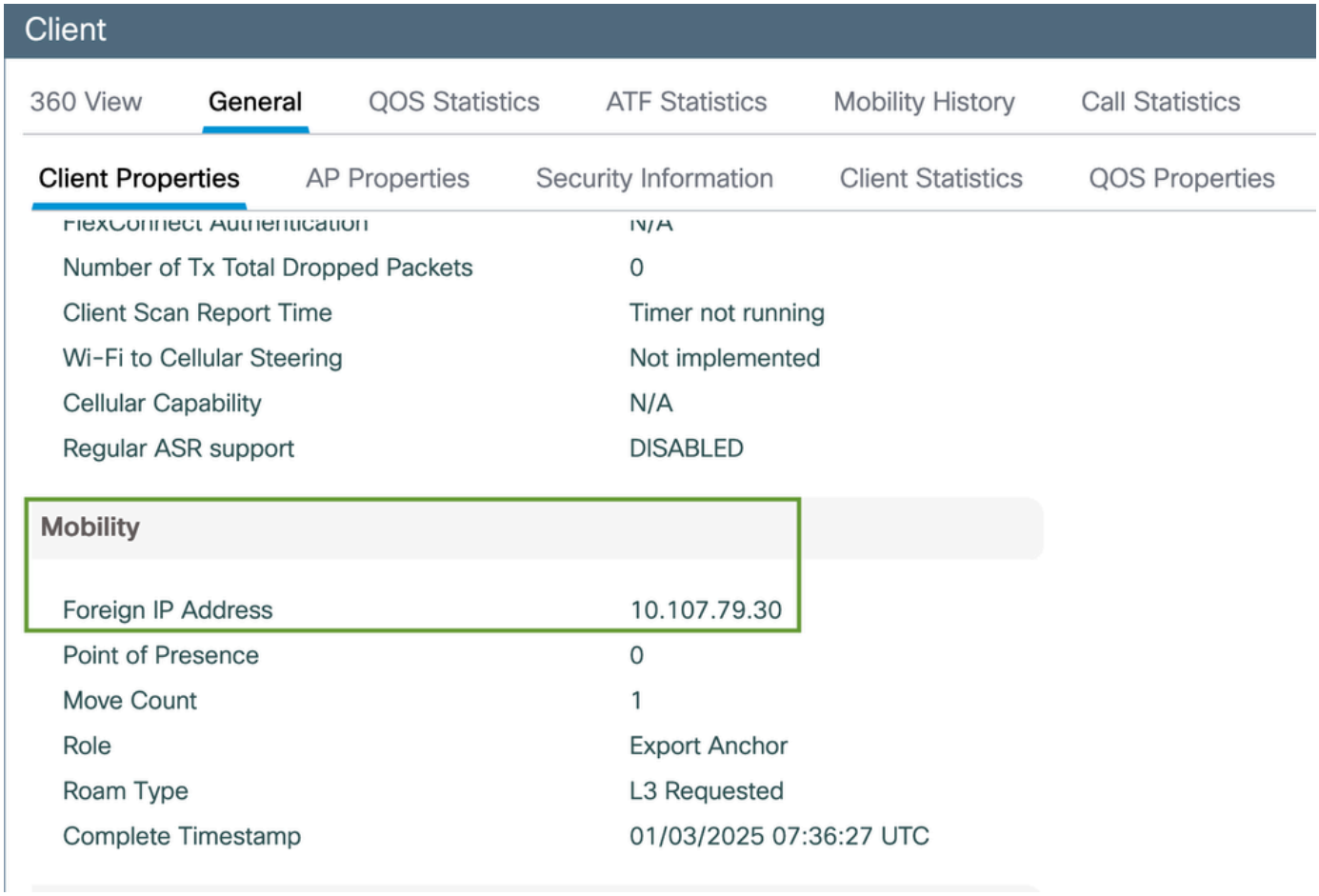
外部客户端状态



锚点上的客户端状态


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

外部客户端属性

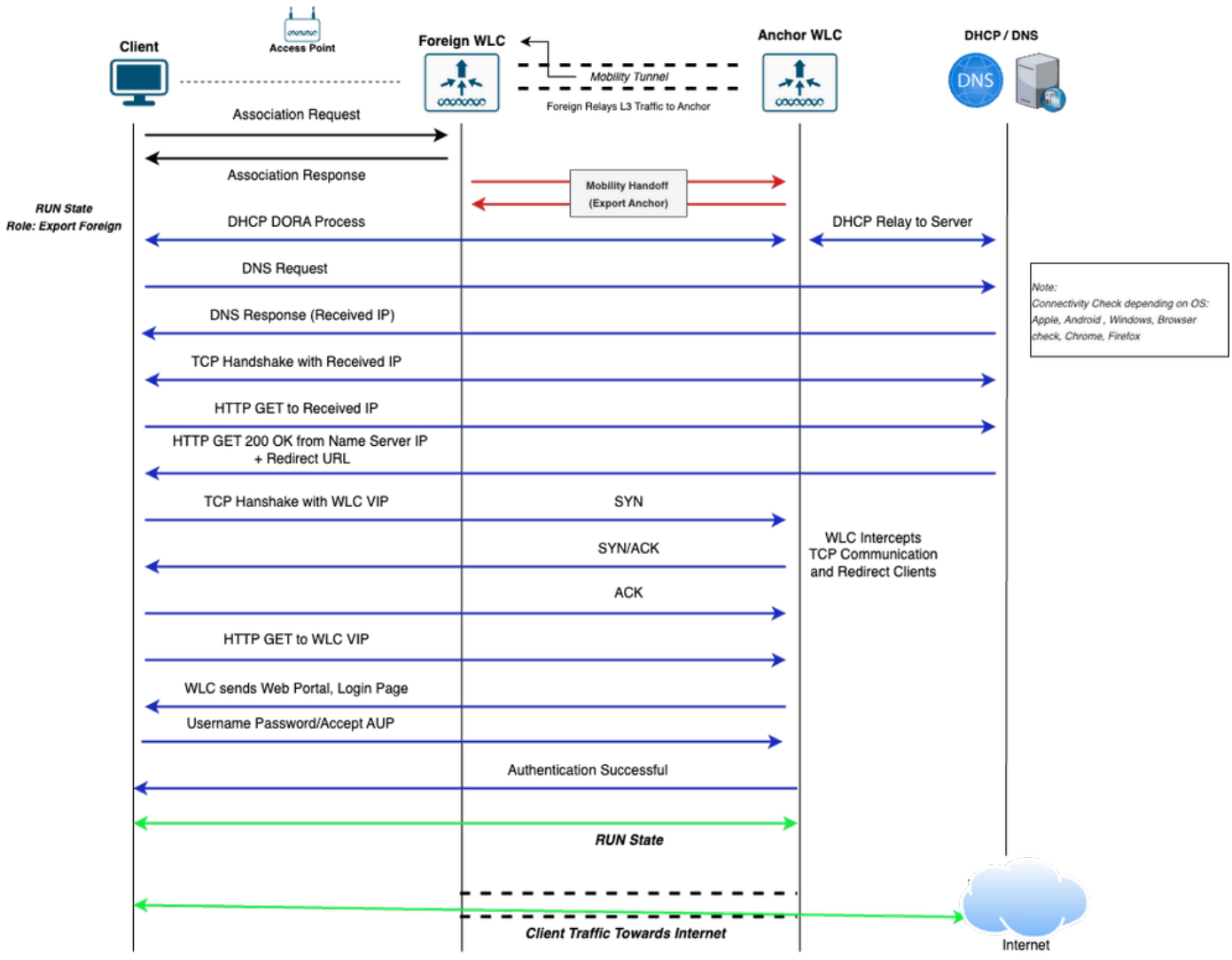

Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
Number of Tx Total Dropped Packets
0
Client Scan Report Time
Timer not running
Wi-Fi to Cellular Steering
Not implemented
Cellular 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

采用第3层身份验证的WLAN

本地Web身份验证

外部锚点设置中本地Webauth SSID的流

1.客户端发起到外部WLC通告的SSID的连接。
2.由于未执行第2层身份验证，因此客户端会立即锚定到锚点WLC。客户端在外部WLC上进入RUN状态，其移动角色指定为Export Foreign。
3.客户端获取IP地址并重定向到网页。此流量由锚点控制器处理。
4.成功在门户进行身份验证后，客户端将在锚点WLC上转换为RUN状态，并具有“导出锚点”角色。



外部锚点设置中本地Webauth SSID的客户端连接流程图

通过日志分析外部锚点设置中的本地Webauth SSID流

本部分介绍通过使用外部控制器和锚点控制器上的放射性跟踪（RA跟踪）、嵌入式数据包捕获(EPC)和客户端状态进行本地Web身份验证SSID的客户端连接流程。

来自外部控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

客户端发送关联请求，由外部控制器处理。

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=........

客户端与外部控制器的关联阶段

移动切换通过端口UDP 16667在外部控制器和锚点控制器之间触发。移动事件成功后，客户端状态将转换为RUN并具有“导出外部”角色。
外部控制器通过CAPWAP隧道接收客户端DHCP流量并将其转发到锚点控制器进行进一步处理。

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

在外部控制器上接收的客户端DHCP流量使用移动隧道转发到锚点控制器

同样，客户端通过CAPWAP隧道将网络连接状态和网页访问检查流量发送到外部WLC;外部WLC使用移动隧道将此流量转发到锚点WLC，锚点控制器在该隧道中拦截或处理流量。

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 raff
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

外部控制器的网络连接状态检查

```
> 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)
```

重定向发送到客户端的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

客户端访问本地Webauth页面以提供身份验证详细信息

来自锚点控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

在移动切换后，锚点控制器通过移动隧道接收来自外部控制器的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

从外部控制器接收的锚点控制器上的客户端DHCP流量

锚点控制器接收连接检查、网页访问请求和身份验证详细信息以进行进一步处理。

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

锚点控制器上的网络连接状态检查

```
> 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)
```

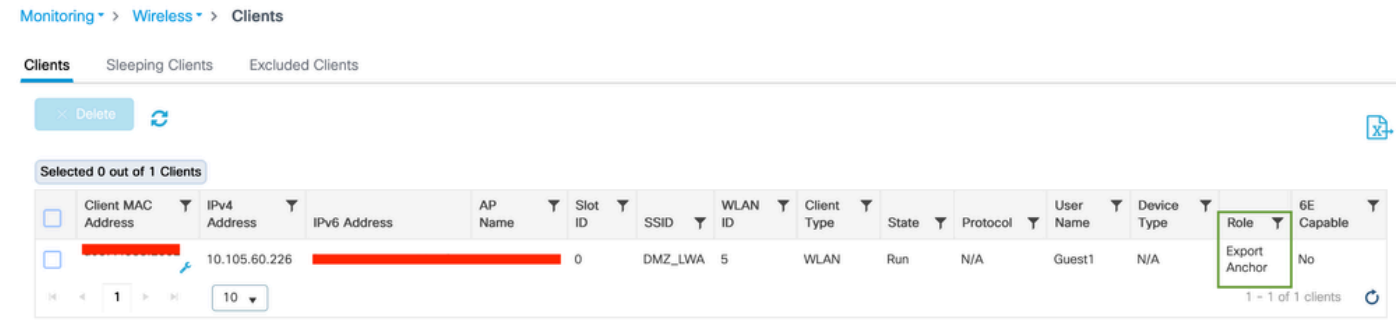
重定向发送到客户端的URL

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

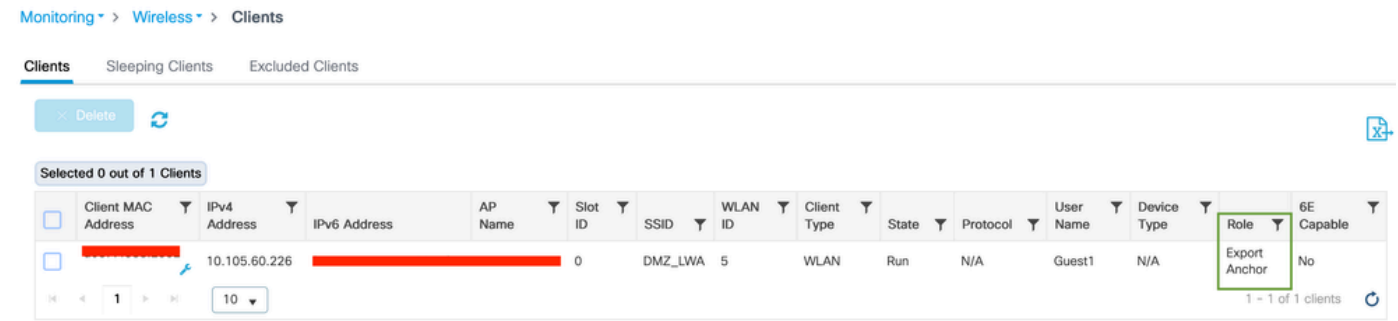
客户端访问本地Webauth页面以提供身份验证详细信息

成功进行本地Web身份验证后，客户端将进入具有导出锚点角色的RUN状态。从此以后，锚点控制器将作为客户端数据流量的出口点。

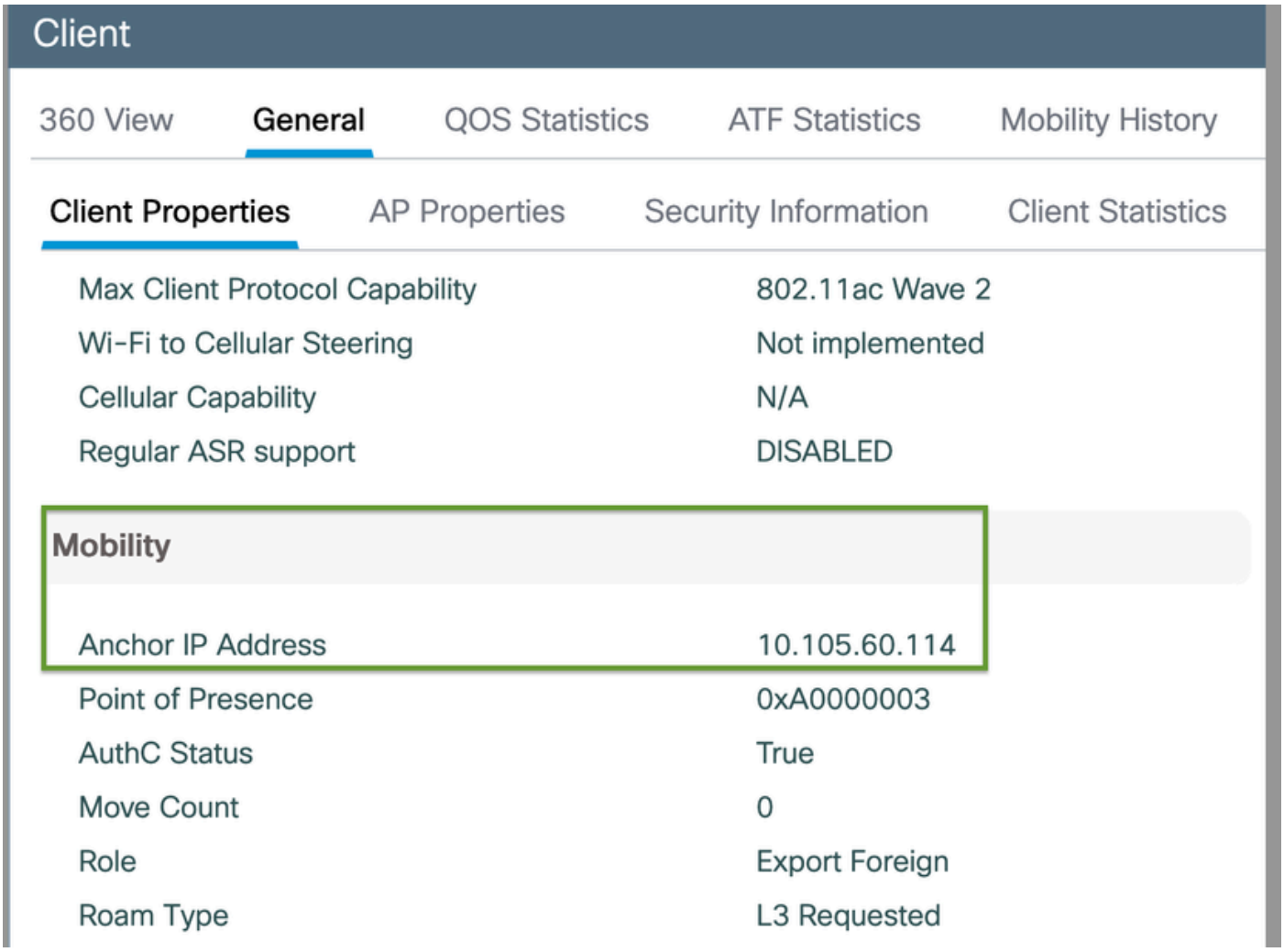
外部和锚点控制器上的客户端状态



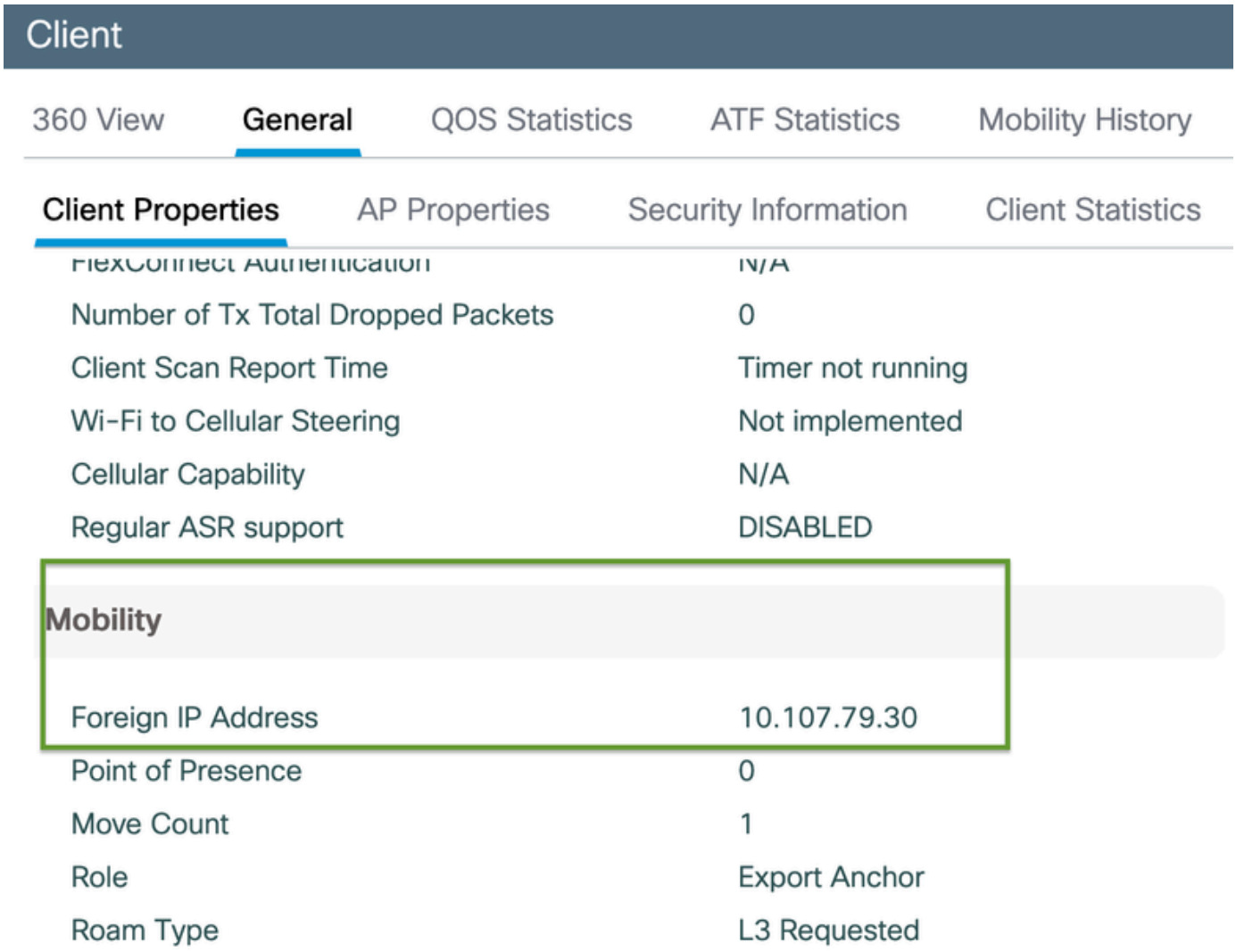
外部客户端状态



锚点上的客户端状态



外部客户端属性



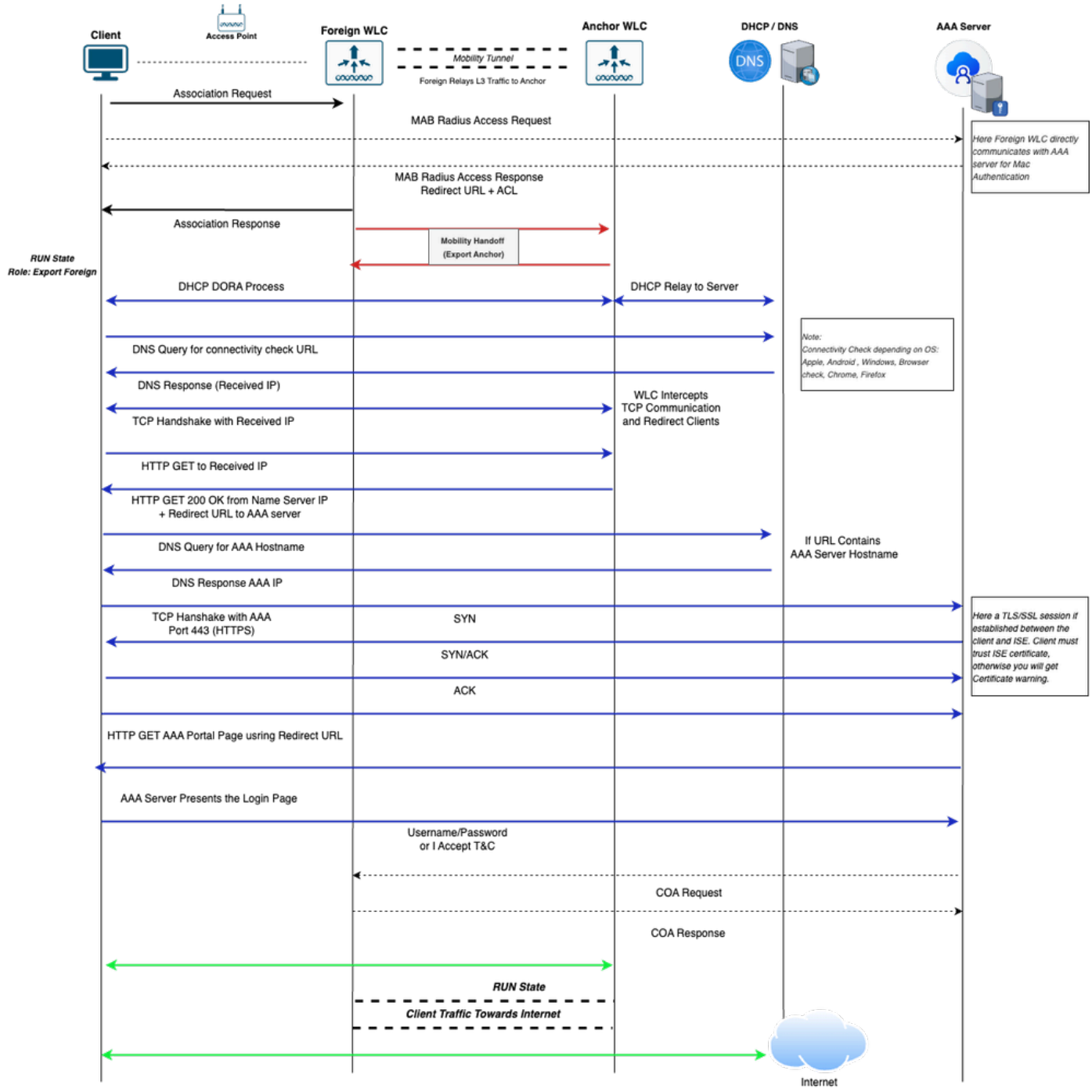
锚点上的客户端属性

集中Web身份验证

外部锚点设置中集中式Webauth SSID的流程

1.客户端向外部无线局域网控制器(WLC)广播的SSID发送关联请求。
2.外部WLC通过向RADIUS服务器发送访问请求来执行MAC过滤。RADIUS服务器以访问接受响应，包括必要的重定向URL和访问控制列表(ACL)。
3.外部WLC将关联响应发送到客户端。
4.客户端锚定到锚点WLC。客户端在外部WLC上进入RUN状态，移动角色设置为Export Foreign。
5.客户端获取IP地址。在此阶段，锚点WLC处理重定向流量，将客户端定向到身份验证门户。
6.重定向后，客户端将直接与RADIUS服务器通信。此流量通过锚点WLC隧道传输到RADIUS服务器。
7.客户端向RADIUS服务器输入身份验证凭证。身份验证成功后，RADIUS服务器向外部WLC发送授权更改(CoA)请求。
8.外部WLC向RADIUS服务器发送CoA响应。客户端在锚点WLC上转换为RUN状态，角色设置为Export Anchor。

9.所有后续客户端流量通过隧道从外部WLC传输到锚点WLC，从锚点WLC退出网络。



外部锚点设置中中心Webauth SSID的客户端连接流程图

通过日志分析外部锚点设置中的中心Webauth SSID流

本部分介绍通过使用外部控制器和锚点控制器上的放射性跟踪（RA跟踪）、嵌入式数据包捕获(EPC)和客户端状态，实现中心Web身份验证SSID的客户端连接流程。

来自外部控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

客户端发送关联请求并执行MAC身份验证，此流量由外部控制器处理。

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=........

外部控制器上与无线MAB的客户端关联阶段

移动切换通过端口UDP 16667在外部控制器和锚点控制器之间触发。移动事件成功后，客户端状态将转换为RUN并具有“导出外部”角色。

外部控制器通过CAPWAP隧道接收客户端DHCP流量并将其转发到锚点控制器进行进一步处理。

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

在外部控制器上接收的客户端DHCP流量使用移动隧道转发到锚点控制器

同样，客户端通过CAPWAP隧道将网络连接状态和网页访问检查流量发送到外部WLC;外部WLC使用移动隧道将此流量转发到锚点WLC，锚点控制器在该隧道中拦截或处理流量。

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, Resolved IP	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,	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

外部控制器的网络连接状态检查

```
> 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)
```

重定向发送到客户端的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

客户端访问中心Webauth页面以提供身份验证详细信息

外部控制器在中心Web身份验证成功后处理CoA请求。

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权更改(COA)

来自锚点控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

在移动切换后，锚点控制器通过移动隧道接收来自外部控制器的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

从外部控制器接收的锚点控制器上的客户端DHCP流量

锚点控制器接收连接检查、网页访问请求和身份验证详细信息以进行进一步处理。

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 … Connectivity Check URL
Jan 8, 2025 13:09:44…	DNS IP	10.105.60.249	237	DNS		Standard query response 0xd4c8 A Connectivity Check URL rafficma
Jan 8, 2025 13:09:44…	10.105.60.114	10.107.79.30	287	UDP		16667 → 16667 Len=245
Jan 8, 2025 13:09:44…	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:44…	10.105.60.249	Resolved IP	70	TCP		59484 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 8, 2025 13:09:44…	Resolved IP	10.105.60.249	66	TCP		80 → 59484 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 8, 2025 13:09:44…	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 8, 2025 13:09:44…	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 8, 2025 13:09:44…	10.107.79.30	10.105.60.114	223	UDP		16667 → 16667 Len=177
Jan 8, 2025 13:09:44…	10.105.60.249	Resolved IP	58	TCP		59484 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 8, 2025 13:09:44…	10.105.60.249	…	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

锚点控制器上的网络连接状态检查

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

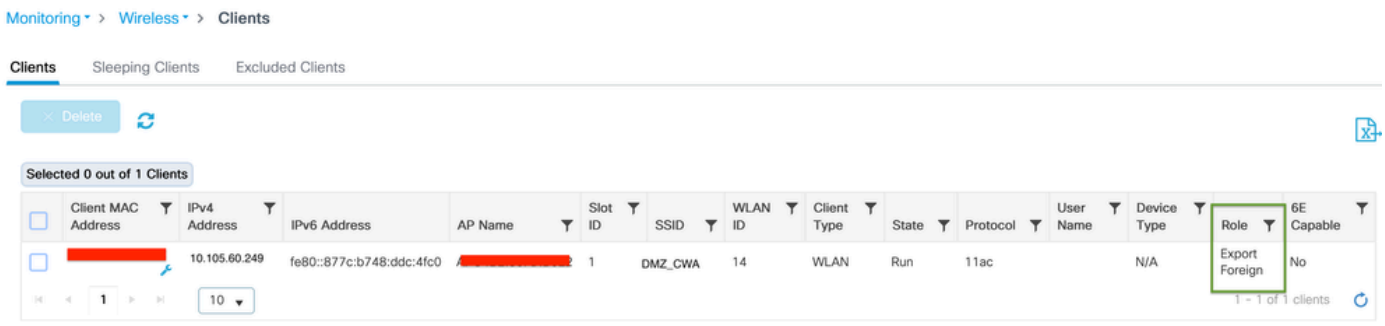
重定向发送到客户端的URL

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

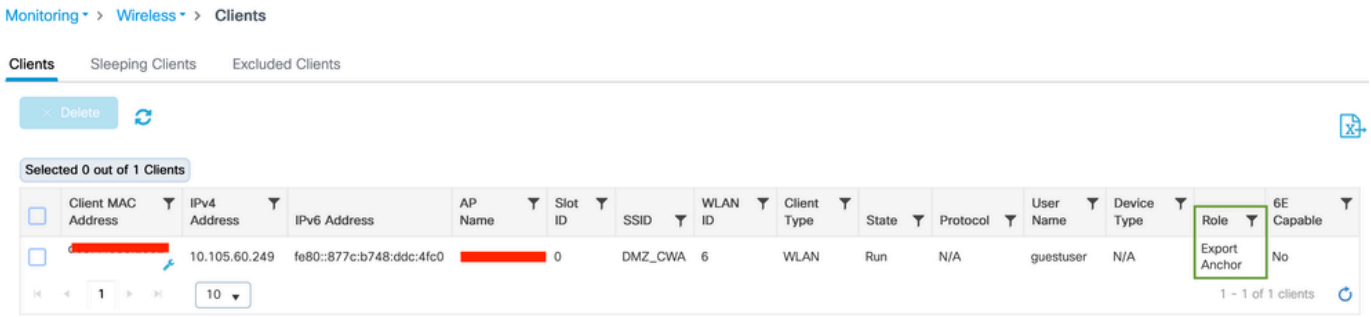
客户端访问本地Webauth页面以提供身份验证详细信息

当中心Web身份验证成功时，将触发授权更改(CoA)。CoA成功后，客户端将转换为具有导出锚点角色的RUN状态。

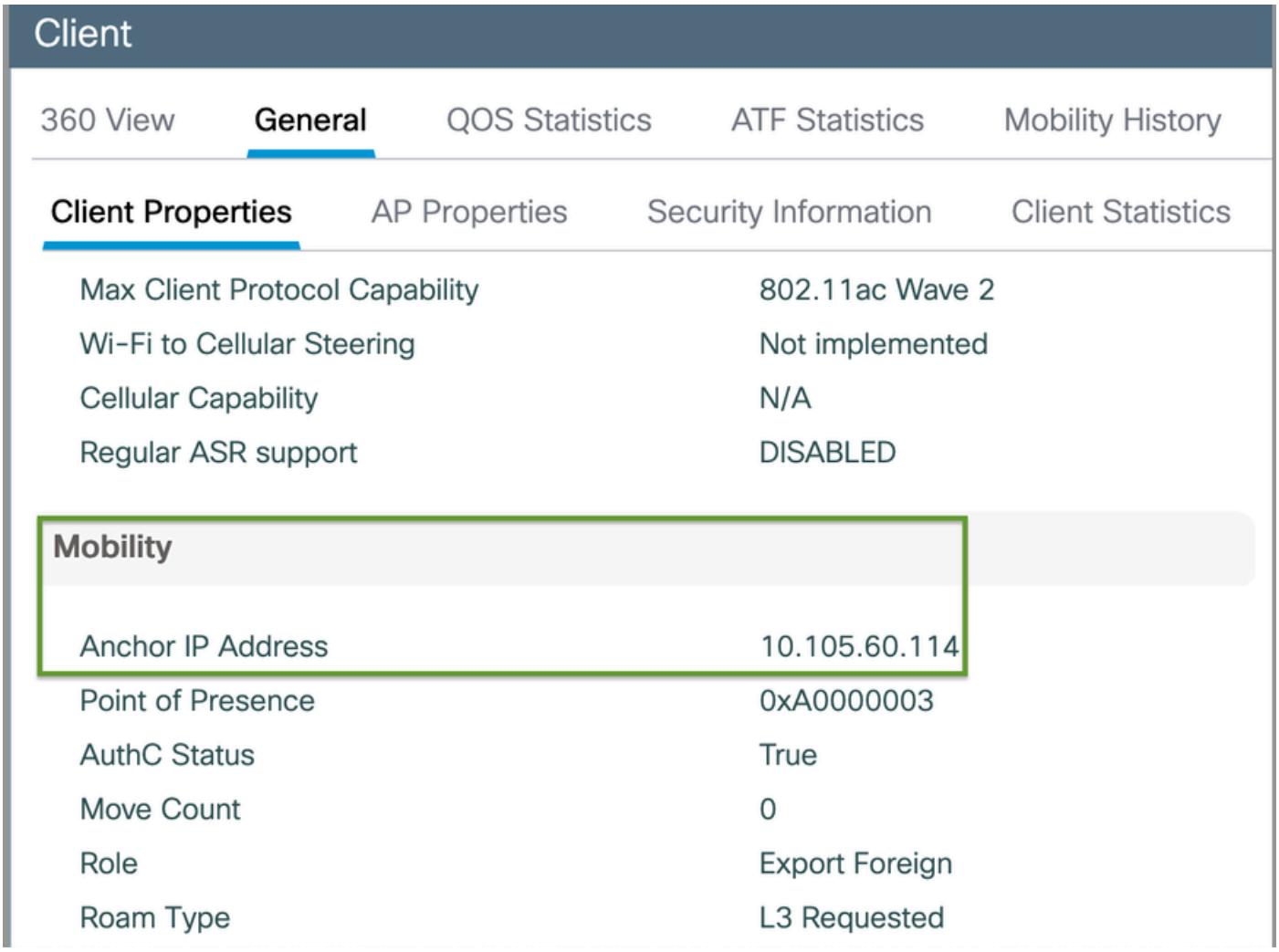
外部和锚点控制器上的客户端状态



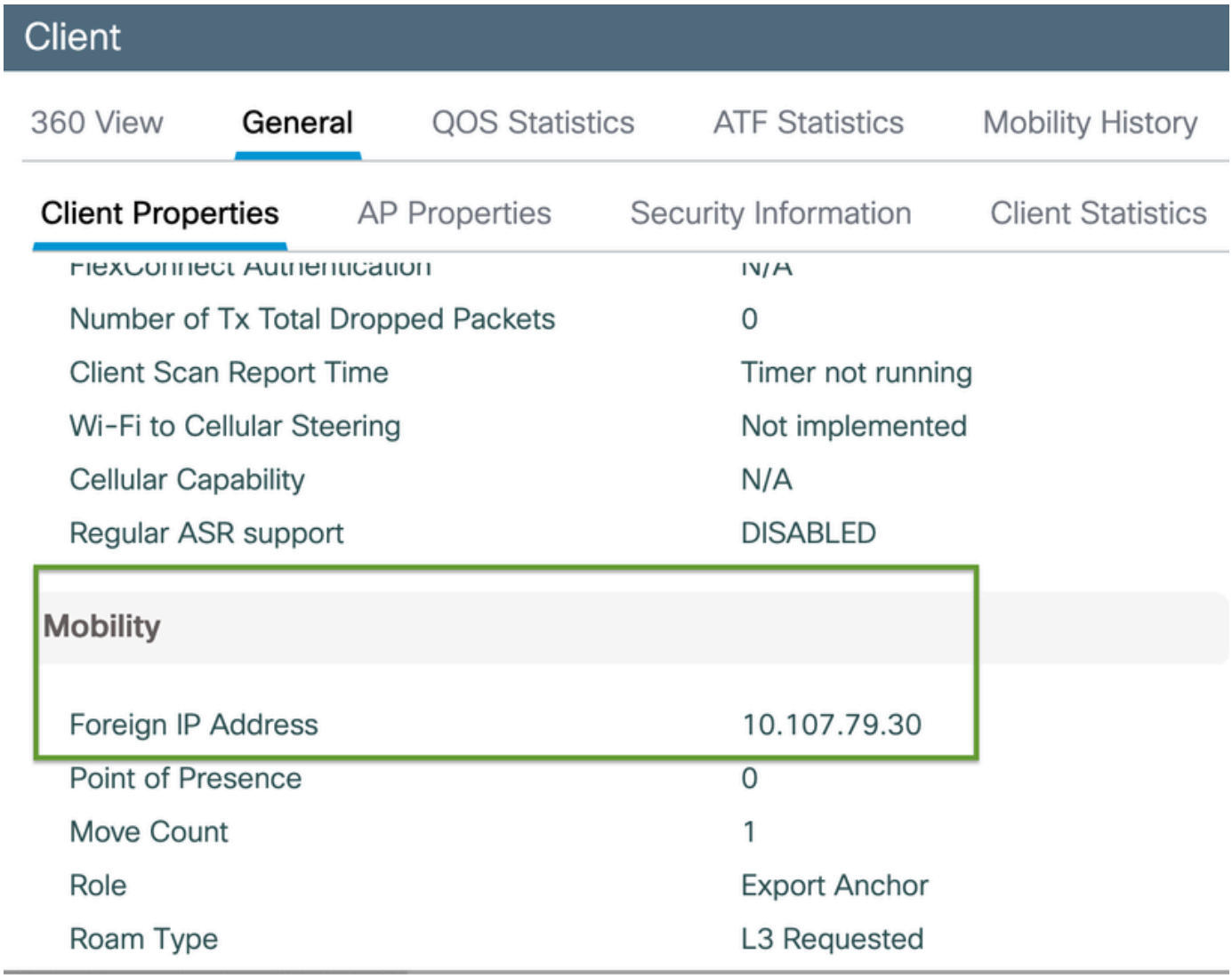
外部客户端状态



锚点上的客户端状态



外部客户端属性

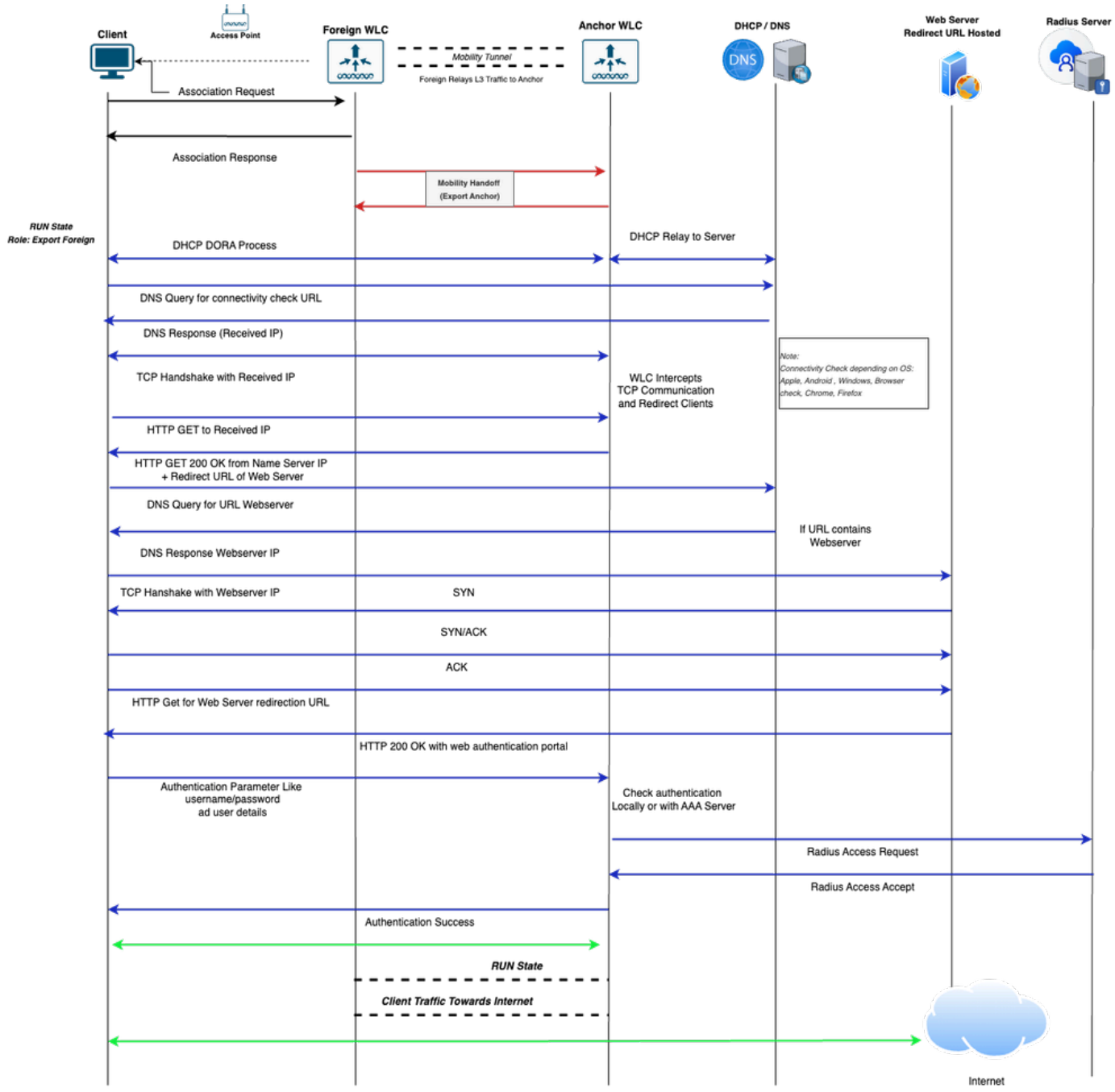


锚点上的客户端属性

外部Web身份验证

外部锚点设置中的外部Webauth SSID流

1.客户端发起到外部WLC广播的SSID的连接。
2.由于不需要第2层身份验证，因此客户端将锚定到锚点WLC。客户端在外部WLC上转换为RUN状态，移动角色指定为Export Foreign。
3.客户端获取IP地址。锚点WLC会拦截流量并将客户端重定向到Web身份验证参数中定义的外部Web服务器门户。
4.客户端通过门户提交身份验证凭证。这些凭证在WLC上进行本地验证，或通过外部身份验证服务器进行验证，具体取决于配置的安全策略。
5.身份验证成功后，客户端将在锚点WLC上转换到RUN状态，并承担导出锚点角色。
6.身份验证成功后，所有后续客户端流量通过隧道从外部WLC传输到锚点WLC，从锚点WLC流出网络。



外部锚点设置中外部Webauth SSID的客户端连接流程图

通过日志分析外部锚点设置中的外部Webauth SSID流

本部分介绍通过使用外部和锚点控制器上的放射性跟踪（RA跟踪）、嵌入式数据包捕获(EPC)和客户端状态的外部Web身份验证SSID的客户端连接流程。

来自外部控制器的日志

无线电主动跟踪

```
!! 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:
```

数据包捕获

客户端发送关联请求，由外部控制器处理。

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=........

客户端与外部控制器的关联阶段

移动切换通过端口UDP 16667在外部控制器和锚点控制器之间触发。移动事件成功后，客户端状态将转换为RUN并具有“导出外部”角色。
外部控制器通过CAPWAP隧道接收客户端DHCP流量并将其转发到锚点控制器进行进一步处理。

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

在外部控制器上接收的客户端DHCP流量使用移动隧道转发到锚点控制器

同样，客户端通过CAPWAP隧道将网络连接状态和网页访问检查流量发送到外部WLC;外部WLC使用移动隧道将此流量转发到锚点WLC，锚点控制器在该隧道中拦截或处理流量。

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

外部控制器的网络连接状态检查

```
> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco_[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], Dst: 10.105.60.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 62437, Seq: 1, Ack: 112, Len: 849
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://10.106.32.130:8443/portal/PortalSetup.action?portal=d06bc251-f644-4fc3-b09f-dae9bd8a86
    Content-Type: text/html\r\n
  > Content-Length: 580\r\n
    \r\n
    [Request in frame: 788]
    [Time since request: 0.000991000 seconds]
    [Request URI: /connecttest.txt]
    [Full request URI: [redacted]
    File Data: 580 bytes
> Line-based text data: text/html (9 lines)
```

重定向发送到客户端的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

客户端访问外部Webauth页面以提供身份验证详细信息

来自锚点控制器的日志

无线电主动跟踪

```
!! 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
```

数据包捕获

在移动切换后，锚点控制器通过移动隧道接收来自外部控制器的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

从外部控制器接收的锚点控制器上的客户端DHCP流量

锚点控制器接收连接检查、网页访问请求和身份验证详细信息以进行进一步处理。

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

锚点控制器上的网络连接状态检查

```
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)
```

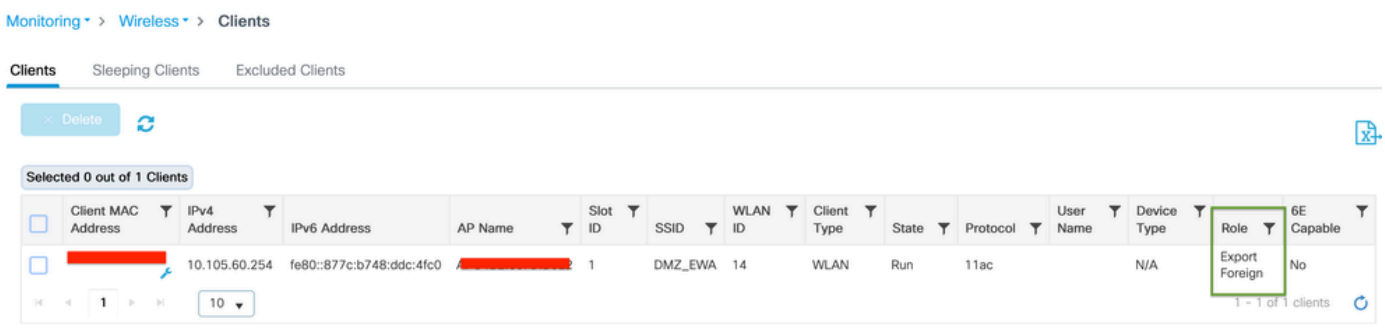
重定向发送到客户端的URL

客户端通过门户提交身份验证凭证。这些凭证在WLC上进行本地验证，或通过外部身份验证服务器进行验证，具体取决于配置的安全策略。

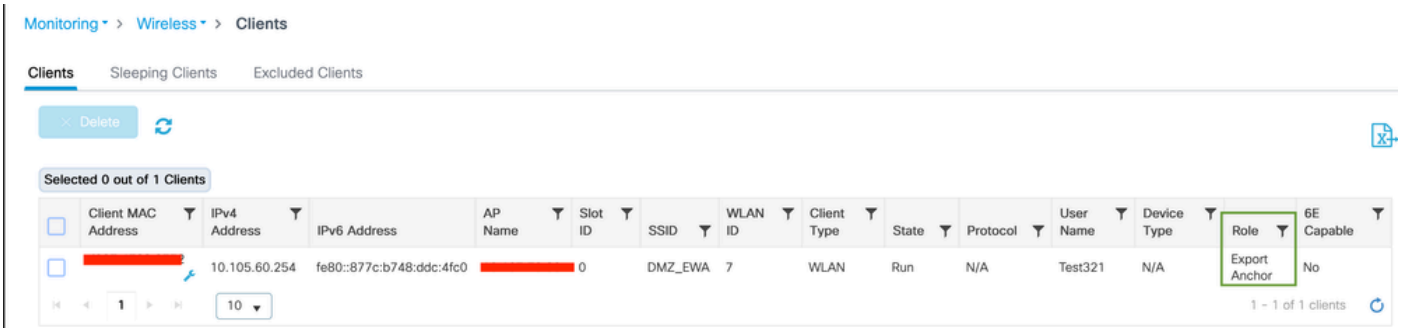
UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:12.…	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12.…	10.105.60.254	10.106.32.130	66	TCP		62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:12.…	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

客户端访问外部Webauth页面以提供身份验证详细信息

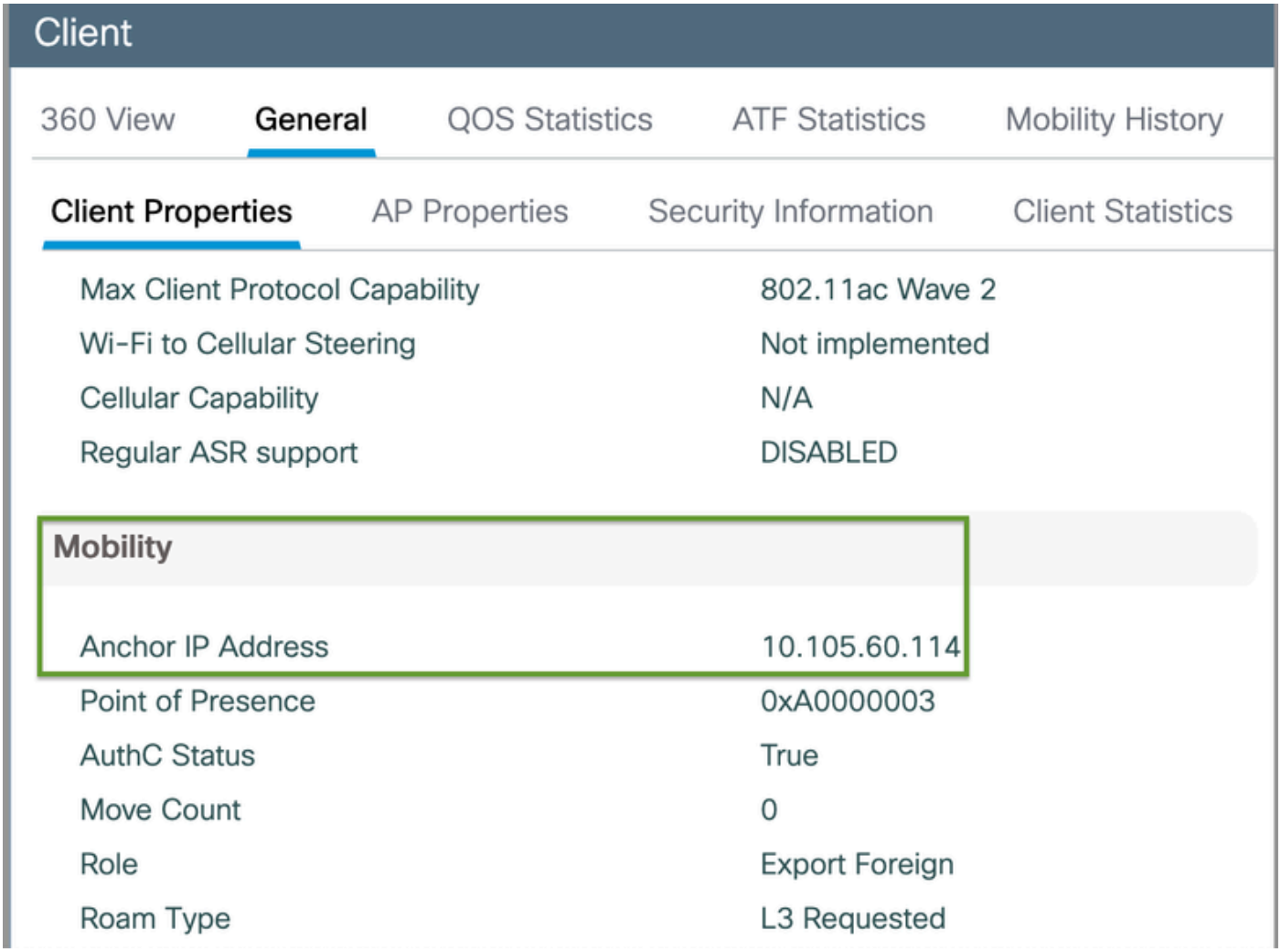
外部和锚点控制器上的客户端状态



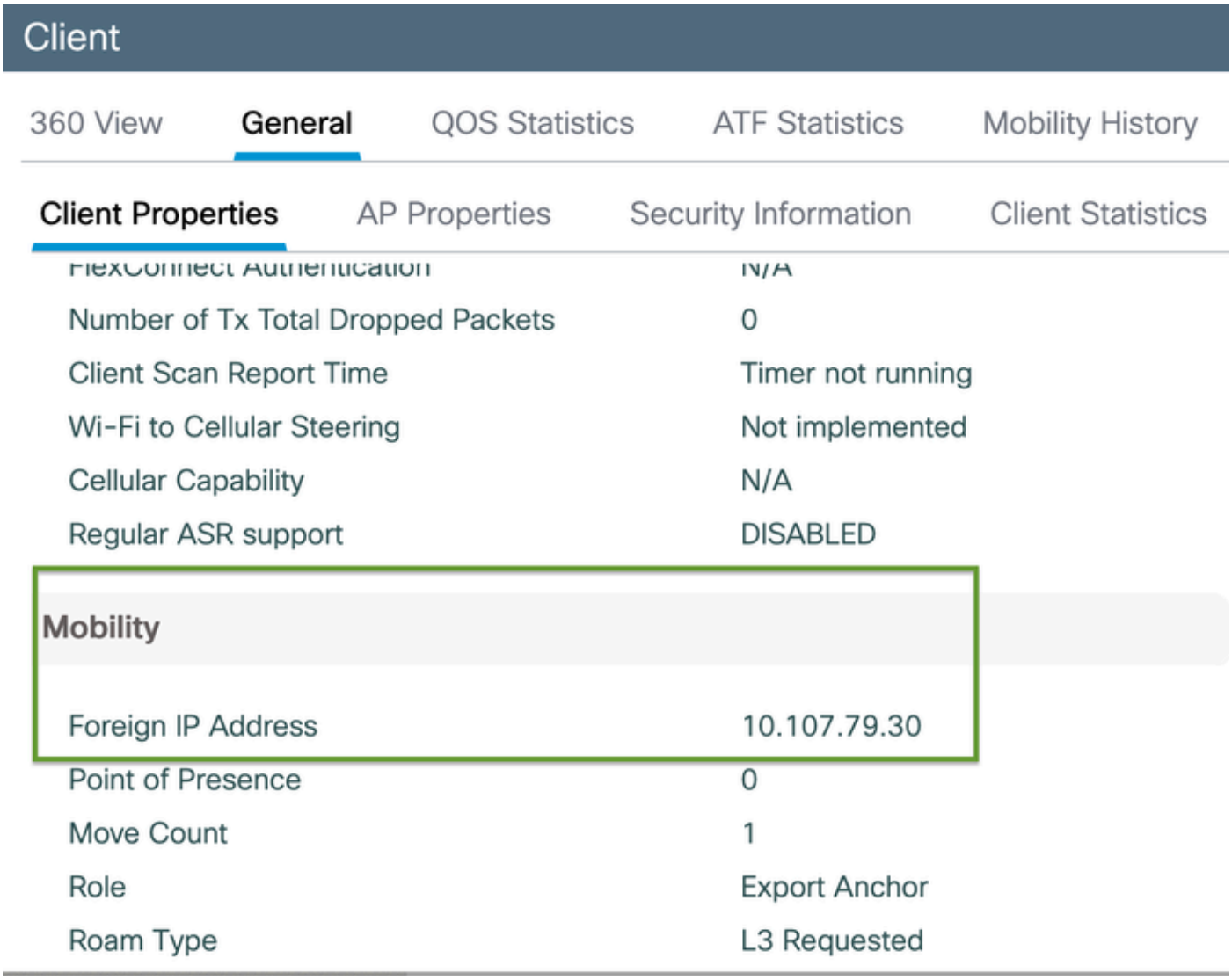
外部客户端状态



锚点上的客户端状态



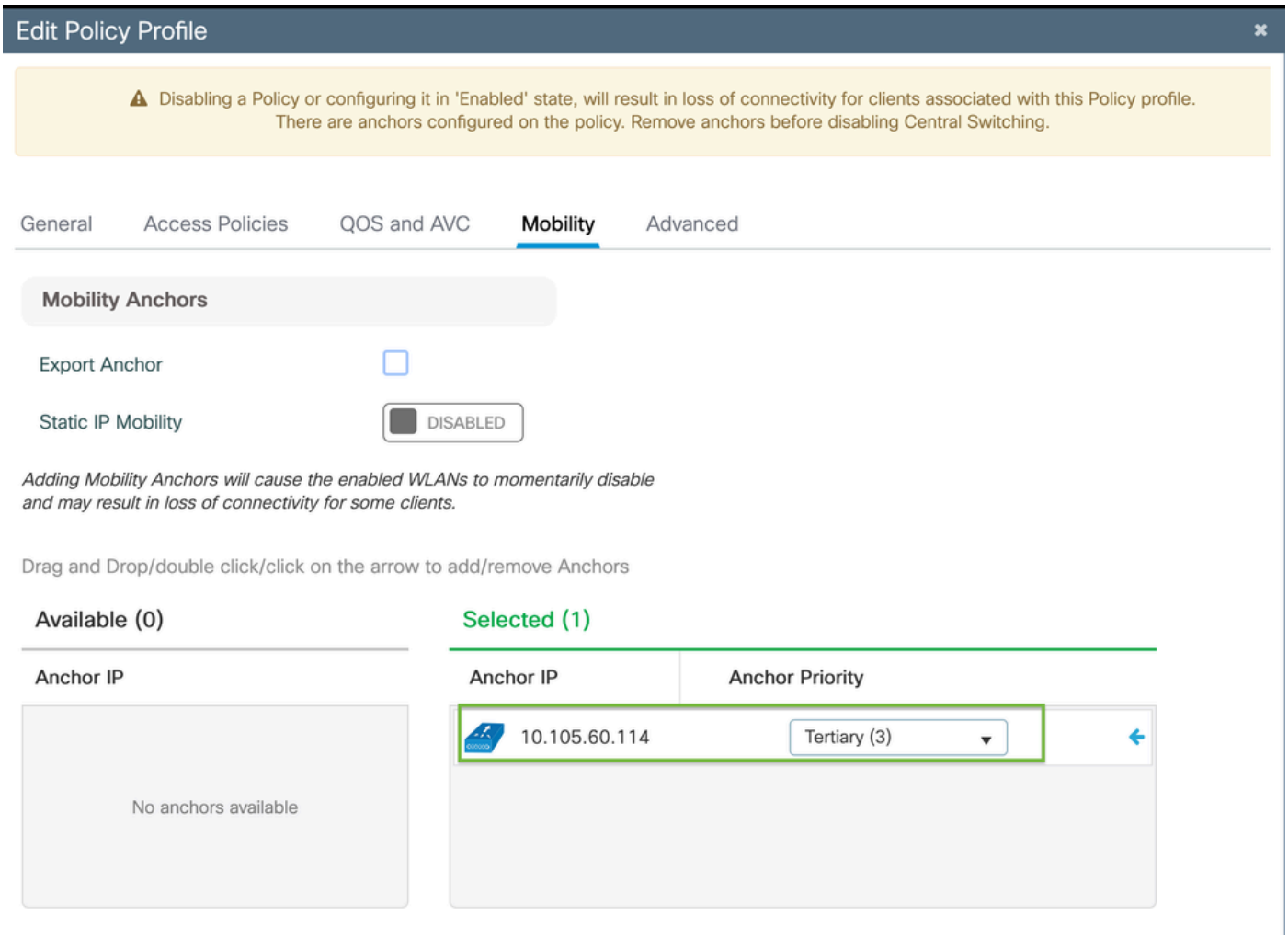
外部客户端属性



锚点上的客户端属性

多个锚点控制器之间的负载均衡

当多个锚点控制器映射到单个WLAN时，流量分配取决于优先级。可以配置三个优先级：小学、中学和高等教育。访客锚点优先级功能提供了在锚点控制器之间分配主用/备用负载的机制。这通过为每个锚点控制器分配固定优先级来实现：负载以轮询方式分配到共享相同优先级值的控制器中的最高优先级控制器。



映射锚点优先级

注意：默认情况下，优先级三级是在外部控制器上的锚点控制器映射期间配置的。

排除外部锚点方案中的客户端连接故障

1. 客户端自注册问题
   i. 通道状态:验证外部控制器和锚点控制器之间的移动隧道保持活动状态。
   ii. 配置不匹配：确保两个控制器之间的配置奇偶校验。WLAN名称、策略配置文件名称或高级设置（例如AAA覆盖、IPv4 DHCP要求和NAC）之间的差异会导致配置文件不匹配或锚点拒绝错误。
   iii. 其他：如果Tunnel is up without any configuration issue，则故障排除方法类似于正常的客户端连接问题，确保检查处理受影响流量的相应控制器。

2. 间歇性连接
   i. 隧道抖动：如果两个控制器之间的keepalive数据包无法到达，隧道将会摆动，使客户端无法保持与SSID的连接。
   ii. 低带宽:如果移动对等体之间的路径MTU(PMTU)降至较低的值(576)，客户端会经历性能

下降。当两个移动对等体之间的路径mtu keepalive消息丢失时，通常会发生这种情况

注意：具有较低移动MAC地址的控制器会启动标准keepalive消息和路径MTU keepalive消息。

3. 特定网站访问问题
   i. 移动流量报头包括通过UDP端口16666和16667交换的移动组标识符、MAC地址、IP地址和加密CAPWAP DTLS数据包。此开销会添加到现有的CAPWAP报头。对于TCP流量，如果数据包大小因这种额外开销而超过移动PMTU（最大1385字节），则调整后为AP配置的TCP MSS，则会发生分段。虽然分段通常由网络处理，但如果数据包到达顺序混乱或延迟，则会出现问题。这些情况会影响数据包的重组，并导致特定网站的数据访问失败。

从外部和锚点控制器收集日志

1. 启用term exec prompt timestamp，以便为所有命令提供时间参考。
2. 使用show tech-support wireless !!查看配置。
3. 您可以检查移动隧道状态show wireless mobility summary !!
4. 包括链路状态、客户端数据和事件的移动对等体统计信息、保持连接统计信息show wireless mobility peer ip <IP>
5. 启用移动对等IP/MAC地址和客户端MAC地址的放射性跟踪。

   通过CLI:

   debug wireless {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !!设置时间允许我们启用最多24天的跟踪。

   no debug wireless {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x !!禁用调试

   WLC使用Client_info生成调试跟踪文件，命令检查生成的调试跟踪文件dir bootflash: | i debug !!

警告：条件调试启用调试级别日志记录，从而增加生成的日志量。持续运行条件调试会缩短可以回溯查看的日志的时间范围。因此，建议在故障排除会话结束时始终禁用调试。

6. 要禁用所有调试，请运行以下命令：

   # clear platform condition all !!

   # undebug all !!
   通过GUI:

步骤1.导航到故障排除>放射性跟踪。

步骤2.单击Add并输入要排除故障的移动对等MAC/IP地址或客户端MAC地址。
步骤3.准备好开始放射性示踪后，单击开始。启动后，调试日志记录会写入磁盘，记录与跟踪的MAC地址相关的任何控制平面处理。
步骤4.重现要排除故障的问题时，单击Stop。
步骤5.对于已调试的每个MAC地址，您可以通过点击Generate来生成log file，该文件整理与该MAC地址相关的所有日志。
第6步：选择想要经过整理的日志文件回溯多长时间，然后点击应用到设备。
步骤7.现在可以通过点击文件名旁边的小图标来下载文件。此文件存在于控制器的引导闪存驱动器中，也可以通过CLI从盒中复制。

7. 嵌入式捕获

通过CLI:
monitor capture MYCAP clear !!
监控器捕获MYCAP接口Po1和!!
monitor capture MYCAP buffer size 100 !!
monitor capture MYCAP match access-list name !!（如果跟踪WLC之间的移动隧道流量）
monitor capture MYCAP match any/ipv4/ipv6.MAC !!
monitor capture MYCAP start !!
!! 重现
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap

通过GUI:

步骤1.导航到故障排除>数据包捕获> +添加。
步骤2.定义数据包捕获的名称。最多允许 8 个字符。
步骤3.定义过滤器（如果有）。
步骤4.如果要查看传送到系统CPU并注入回数据平面的流量，请选中Monitor Control Traffic复选框。
第 5 步： 定义缓冲区大小，最多允许100 MB。
步骤6.根据需要定义限制(按允许范围1 - 1000000秒的持续时间或按允许范围1 - 100000个数据包的数据包数量)。
步骤7.从左列中的接口列表中选择interface，然后选择箭头将其移动到右列。
步骤8.单击保存并应用到设备。
步骤9.要开始捕获，请选择开始。
第 10 步： 可以运行捕获，直至达到所定义的限制。要手动停止捕获，请选择停止。
步骤11.停止后，可使用Export按钮点击选项，通过HTTP或TFTP服务器、FTP服务器、本地系统硬盘或闪存将捕获文件(.pcap)下载到本地桌面。

相关信息

在Catalyst 9800 WLC上配置移动拓扑

在Catalyst 9800上配置WLAN锚点移动功能

技术支持和文档 - Cisco Systems

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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