

9800 WLC 간 외부 앵커 설정의 트래픽 흐름 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[외래 앵커 시나리오 개요](#)

[토폴로지](#)

[레이어 2 인증을 사용하는 WLAN](#)

[구성 요구 사항](#)

[레이어 2 외부 앵커 기반 SSID의 흐름](#)

[로그를 통한 외부 앵커 설정의 레이어 2 SSID 흐름 분석](#)

[외부 컨트롤러의 로그](#)

[Anchor 9800 컨트롤러의 로그](#)

[외부 및 앵커 컨트롤러 모두의 클라이언트 상태](#)

[레이어 3 인증을 사용하는 WLAN](#)

[로컬 웹 인증](#)

[외부 앵커 설정의 로컬 Webauth SSID에 대한 흐름](#)

[로그를 통한 외부 앵커 설정에서 로컬 Webauth SSID 흐름 분석](#)

[외부 컨트롤러의 로그](#)

[앵커 컨트롤러에서 로그](#)

[외부 및 앵커 컨트롤러 모두의 클라이언트 상태](#)

[중앙 웹 인증](#)

[외부 앵커 설정의 중앙 Webauth SSID에 대한 흐름](#)

[로그를 통한 외부 앵커 설정의 중앙 Webauth SSID 흐름 분석](#)

[외부 컨트롤러의 로그](#)

[앵커 컨트롤러에서 로그](#)

[외부 및 앵커 컨트롤러 모두의 클라이언트 상태](#)

[외부 웹 인증](#)

[외부 앵커 설정의 외부 Webauth SSID에 대한 흐름](#)

[로그를 통한 외부 앵커 설정의 외부 Webauth SSID 흐름 분석](#)

[외부 컨트롤러의 로그](#)

[앵커 컨트롤러에서 로그](#)

[외부 및 앵커 컨트롤러 모두의 클라이언트 상태](#)

[여러 앵커 컨트롤러 간 로드 밸런싱](#)

[외부 앵커 시나리오에서 클라이언트 연결 문제 해결](#)

[외부 및 앵커 컨트롤러에서 로그 수집](#)

[관련 정보](#)

소개

이 문서에서는 L2/L3 클라이언트 온보딩 및 트러블슈팅에 대한 Cisco 9800 WLC 간 외부 앵커 설정의 트래픽 흐름에 대해 설명합니다.

사전 요구 사항

외부 컨트롤러와 앵커 컨트롤러 간의 모빌리티 터널

UDP 포트 16666 및 16667은 두 WLC 간에 허용됩니다.

중앙 스위칭에 대해 구성된 정책 프로파일

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add × Delete ↺

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

1 - 2 of 2 items ↺

외부 WLC의 모빌리티 터널 상태

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add × Delete ↺

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

1 - 2 of 2 items ↺

앵커 WLC의 모빌리티 터널 상태

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 무선 컨트롤러에 대한 CLI(Command Line Interface) 또는 GUI(Graphic User Interface) 액세스

스

- Cisco WLC(Wireless LAN Controller)의 모빌리티
- 9800 Wireless Controller
- 9800 WLC의 방사성 추적 및 패킷 캡처

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800 모델 WLC
- Cisco IOS XE 17.15.5 버전
- 9100 series AP 모델

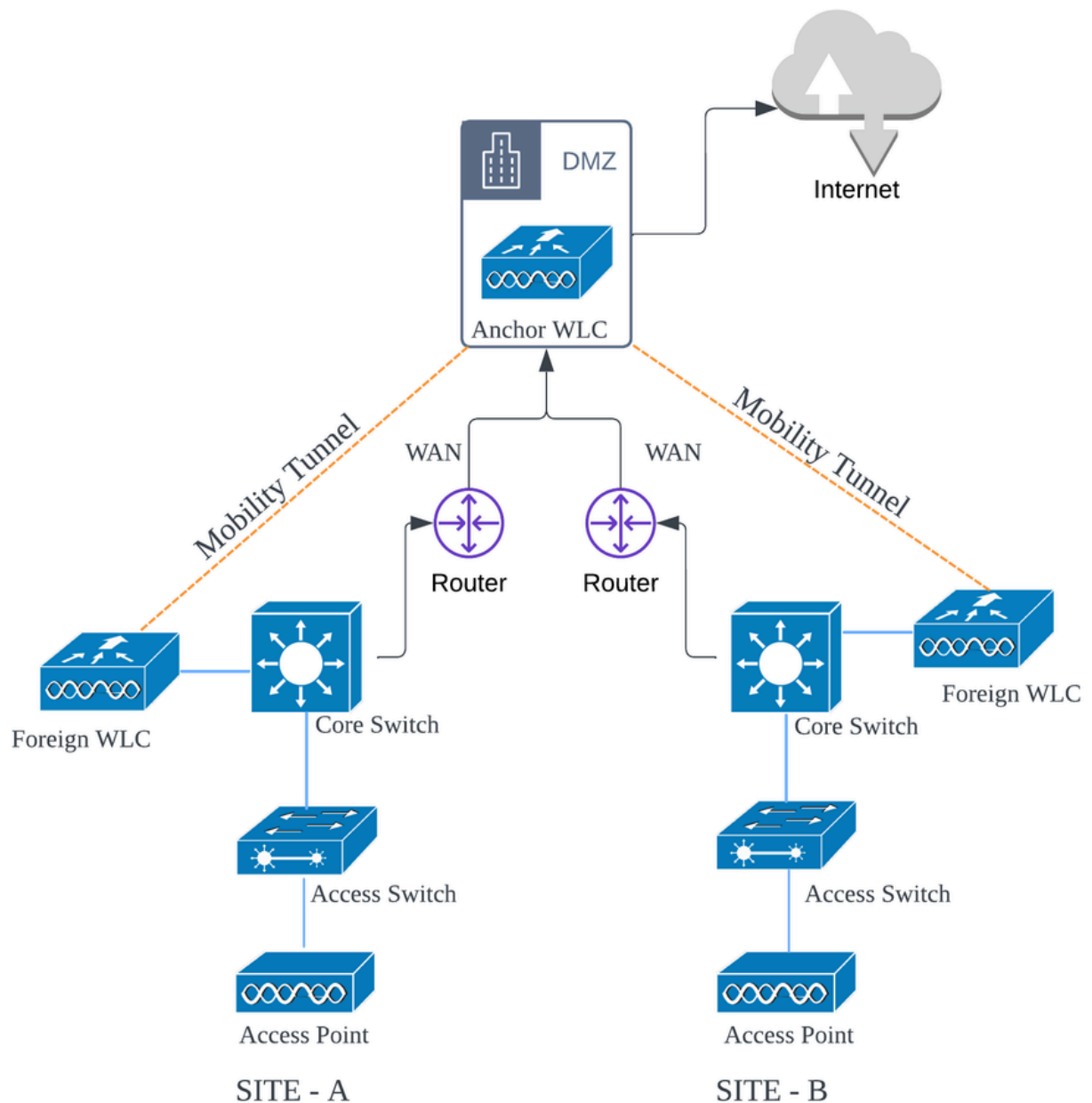
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

외래 앵커 시나리오 개요

- 외부 컨트롤러: 이 WLC는 레이어 2 또는 네트워크의 무선 측면을 관리합니다. 여기에 연결된 액세스 포인트가 있으며, 연결된 WLAN에 대한 모든 클라이언트 트래픽이 모빌리티 터널로 캡슐화되어 앵커 컨트롤러로 전송됩니다. 트래픽은 외부 컨트롤러에서 로컬로 종료되지 않습니다.
- 앵커 컨트롤러: 레이어 3 종료 지점 역할을 합니다. 외부 컨트롤러에서 모빌리티 터널을 통해 클라이언트 트래픽을 수신하고 VLAN(Exit Point)으로 클라이언트 트래픽을 역캡슐화하거나 종료합니다. 네트워크에서 클라이언트가 표시되는 위치입니다.

외부 WLC의 액세스 포인트는 WLAN SSID를 브로드캐스트하고 WLAN 프로파일을 적절한 정책 프로파일과 연결하는 정책 태그가 할당됩니다. 무선 클라이언트가 이 SSID에 연결되면 외부 컨트롤러는 클라이언트 정보의 일부로 SSID 이름 및 정책 프로파일을 모두 앵커 WLC에 전송합니다. 수신 시 앵커 WLC는 SSID 이름 및 정책 프로파일 이름과 일치하도록 자체 컨피그레이션을 확인합니다. 앵커 WLC가 일치 항목을 찾으면 해당 컨피그레이션을 적용하고 무선 클라이언트에 대한 종료 지점을 제공합니다. 따라서 WLAN 및 정책 프로파일 이름 및 컨피그레이션이 외부 및 앵커 9800 WLC 모두에서 일치해야 합니다. 단, 정책 프로파일의 VLAN은 예외입니다.

토폴로지



9800 WLC 간 외부 앵커 설정

레이어 2 인증을 사용하는 WLAN

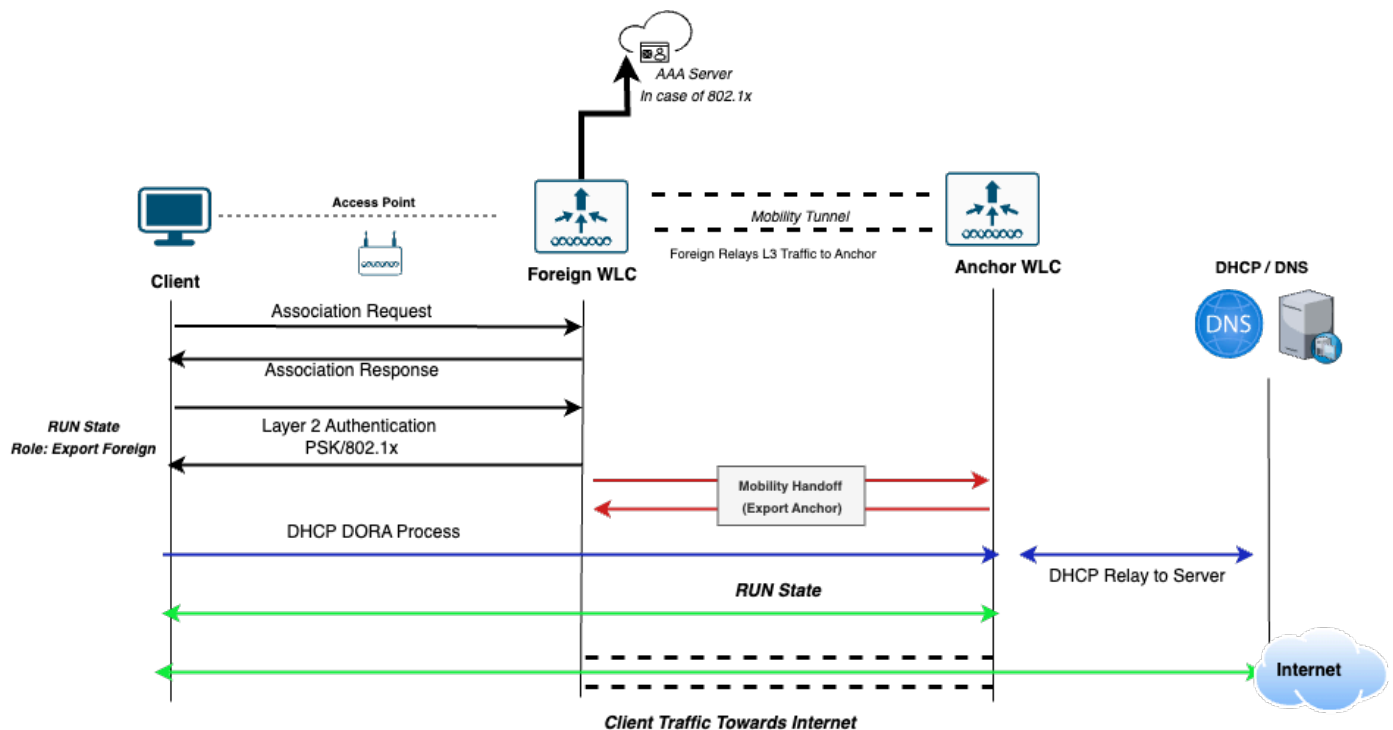
구성 요구 사항

1. WLAN 이름 및 컨피그레이션이 외부 및 앵커 WLC에서 동일하며 레이어 2 인증(PSK 또는 802.1x)을 위해 구성되어 있는지 확인합니다.
2. 컨피그레이션이 동일한 외부 및 앵커 WLC에서 동일한 이름으로 정책 프로필을 생성합니다.
3. 외부 WLC에서 해당 정책 프로필 내에 앵커 WLC 매핑을 구성합니다.

4. Anchor WLC에서 컨트롤러를 Export Anchor로 지정하도록 정책 프로필을 구성합니다.
5. 외부 WLC에서 정책 태그를 사용하여 WLAN을 적절한 정책 프로파일에 매핑합니다.

레이어 2 외부 앵커 기반 SSID의 흐름

1. 클라이언트가 외부 WLC에서 브로드캐스트한 SSID에 대한 연결을 시작합니다. 외부 WLC는 레이어 2 인증을 수행하여 구성된 보안 정책에 따라 로컬에서 또는 외부 AAA 서버를 통해 자격 증명을 검증합니다.
2. 인증에 성공하면 클라이언트 세션이 앵커 WLC에 고정됩니다. 클라이언트에 IP 주소가 할당되고 앵커 WLC에서 RUN 상태로 전환됩니다.
3. 세션이 설정되면 모든 클라이언트 데이터 트래픽이 외부 WLC에서 앵커 WLC로 터널링되고, 여기서 네트워크로 이그레스(egress)됩니다.



레이어 2 외부 앵커 기반 WLAN 흐름도

로그를 통한 외부 앵커 설정의 레이어 2 SSID 흐름 분석

이 섹션에서는 RA 추적(Radioactive Trace), EPC(Embedded Packet Captures), 외래 및 앵커 컨트롤러 모두에서 클라이언트 상태를 사용하여 레이어 2 클라이언트 연결을 구성하는 흐름에 대해 설명합니다.

외부 컨트롤러의 로그

방사선 흔적

!! Client Association started !!

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

!! Layer 2 Authentication started !!

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

!! Mobility Handoff !!

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

```
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
{wncd_x_R0-0}{1} [client-orch-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
```

패킷 캡처

클라이언트는 연결 요청을 전송하고 외부 컨트롤러에서 처리하는 레이어 2 인증을 수행합니다.

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

클라이언트 연결 + 레이어 2 인증 트래픽

모빌리티 전달은 UDP 포트 16667을 통해 외부 컨트롤러와 앵커 컨트롤러 간에 트리거됩니다. 모빌리티 이벤트가 성공하면 클라이언트 상태가 Export Foreign(외부 내보내기) 역할로 RUN(실행)으로 전환됩니다.

외부 컨트롤러는 CAPWAP 터널을 통해 클라이언트 DHCP 트래픽을 수신한 다음 추가 처리를 위해 앵커 컨트롤러에 전달합니다.

	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

외부 컨트롤러에서 수신된 클라이언트 DHCP 트래픽이 모빌리티 터널을 사용하여 앵커 컨트롤러로 전달됨

Anchor 9800 컨트롤러의 로그

앵커의 방사선 흔적

!! Mobility Handoff !!

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

!! Client DHCP Traffic !!

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

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

앵커의 패킷 캡처

모빌리티 핸드오프 후 앵커 컨트롤러는 모빌리티 터널을 통해 외부 컨트롤러로부터 DHCP 트래픽을 수신합니다.

DORA 프로세스가 완료되면 클라이언트는 Export Anchor 역할과 함께 RUN 상태가 됩니다. 이 시점부터 Anchor Controller는 클라이언트 데이터 트래픽의 종료 지점 역할을 합니다.

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

앵커 컨트롤러의 클라이언트 DHCP 트래픽이 외부 컨트롤러에서 수신됨

외부 및 앵커 컨트롤러 모두의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

< Delete ↺

Selected 0 out of 1 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	[REDACTED]	10.105.60.226	fe80::877c:b748:ddc:4fc0	[REDACTED]	1	DMZ_LWA	11	WLAN	Run	11ac		N/A	Export Foreign	No

1 - 1 of 1 clients ↺

외래의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

< Delete ↺

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients ↺

앵커의 클라이언트 상태

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

외래의 클라이언트 속성

Client

[360 View](#)[General](#)[QOS Statistics](#)[ATF Statistics](#)[Mobility History](#)[Call Statistics](#)

Client Properties

[AP Properties](#)[Security Information](#)[Client Statistics](#)[QOS Properties](#)

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

Complete Timestamp

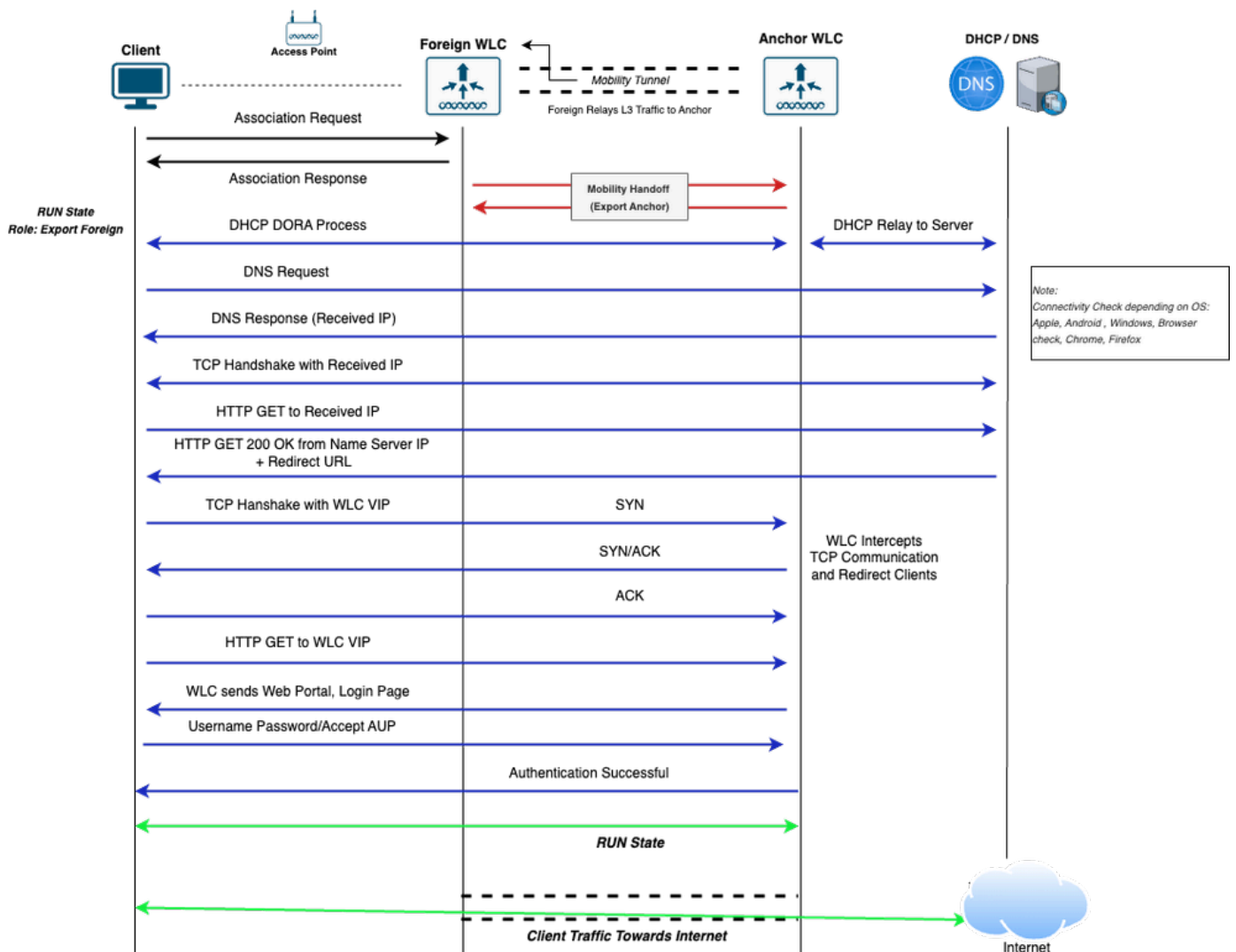
01/03/2025 07:36:27 UTC

레이어 3 인증을 사용하는 WLAN

로컬 웹 인증

외부 앵커 설정의 로컬 Webauth SSID에 대한 흐름

1. 클라이언트가 외부 WLC에서 광고하는 SSID에 대한 연결을 시작합니다.
2. 레이어 2 인증이 수행되지 않으므로 클라이언트가 바로 앵커 WLC에 고정됩니다. 클라이언트는 외부 WLC에서 RUN 상태가 되며 모빌리티 역할이 Export Foreign(외부 내보내기)으로 지정됩니다.
3. 클라이언트가 IP 주소를 얻고 웹 페이지로 리디렉션됩니다. 이 트래픽은 앵커 컨트롤러에 의해 처리됩니다.
4. 포털에서 인증에 성공하면 클라이언트는 Export Anchor 역할과 함께 Anchor WLC에서 RUN 상태로 전환됩니다.



로그를 통한 외부 앵커 설정에서 로컬 Webauth SSID 흐름 분석

이 섹션에서는 RA 추적(Radioactive Trace), EPC(Embedded Packet Captures), 외부 및 앵커 컨트롤러 모두에서 클라이언트 상태를 사용하여 로컬 웹 인증 SSID에 대한 클라이언트 연결의 흐름을 설명합니다.

외부 컨트롤러의 로그

방사선 흔적

!! Client Association Phase !!

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

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

{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC dot11 send association response. Sending asso

!! L2 Auth : None !!

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

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

{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_L2

!! Mobility Handoff Phase !!

□{mobilityd_R0-0}{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gr

{mobilityd_R0-0}{1} [mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP □{mobilityd_R0-0}{1} [mm-client] [1

{mobilityd_R0-0}{1} [mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P

□{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o

□{wncd_x_R0-0}{1} [mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_ANN

{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Sending export_Anchor_req of XID (XID) to (

{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o

{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE

{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce

{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282

{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o

{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS

{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc

□{wncd_x_R0-0}{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed□[mm-client] [17047] (info) MAC

[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF

{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_C

{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE

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

!! Client AAA Traffic handling !!

{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M

{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o

{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (10452) 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_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-pmtu] [18401]: (debug): Peer IP: Anchor-WLC-IP PMTU size is 1006 and calculate
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC Sending aaa_handoff_ack of XID (1045
{wncd_x_R0-0}{1}: [auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] auth mgr attr add/change not
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [17047]: (info): [Client_MAC:capwap_90000003] SM Notified attrib
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa handoff ack successfully forward

패킷 캡처

클라이언트는 외부 컨트롤러에서 처리하는 연결 요청을 보냅니다.

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=.....

외부 컨트롤러와의 클라이언트 연결 단계

모빌리티 전달은 포트 UDP 16667을 통해 외부 컨트롤러와 앵커 컨트롤러 간에 트리거됩니다. 모빌리티 이벤트가 성공하면 클라이언트 상태가 Export Foreign(외부 내보내기) 역할로 RUN(실행)으로 전환됩니다.
외부 컨트롤러는 CAPWAP 터널을 통해 클라이언트 DHCP 트래픽을 수신한 다음 추가 처리를 위해 앵커 컨트롤러에 전달합니다.

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

외부 컨트롤러에서 수신된 클라이언트 DHCP 트래픽이 모빌리티 터널을 사용하여 앵커 컨트롤러로 전달됨

마찬가지로 클라이언트는 CAPWAP 터널을 통해 외부 WLC에 네트워크 연결 상태 및 웹 페이지 액세스 확인 트래픽을 전송합니다. 외부 WLC는 모빌리티 터널을 사용하여 이를 앵커 WLC에 전달합니다. 앵커 컨트롤러는 이 터널을 사용하여 트래픽을 가로채거나 처리합니다.

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

외부 컨트롤러에 대한 네트워크 연결 상태 확인

> Frame 2176: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits)
> Ethernet II, Src: Cisco_63:8b:8b (08:00:0c:2c:63:8b), Dst: (08:00:0c:2c:63:8b)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: F.
> Logical-Link Control
> Internet Protocol Version 4, Src: , Dst: 10.105.60.226
> Transmission Control Protocol, Src Port: 80, Dst Port: 52887, Seq: 1, Ack: 112, Len: 633
✓ Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Location: https://192.0.2.1/login.html?redirect=https://192.0.2.1/login.html\r\n
Content-Type: text/html\r\n
> Content-Length: 472\r\n
\r\n
[Request in frame: 2169]
[Time since request: 0.001007000 seconds]
[Request URI: /connecttest.txt]
[Full request URI: https://192.0.2.1/login.html?redirect=https://192.0.2.1/login.html]
File Data: 472 bytes
> Line-based text data: text/html (9 lines)

클라이언트로 전송된 URL 리디렉션

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

인증 세부 정보를 제공하는 로컬 Webauth 페이지에 대한 클라이언트 액세스

앵커 컨트롤러에서 로그

방사선 흔적

!! Mobility Handoff !!

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

!! Session Created for Client !!

```
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][ 0.0.0.0]Applying IPv4 i
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_CR
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_INIT -> S_MA
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.
[wncd_x_R0-0]{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.>> Client is successf
```

!! Client DHCP Traffic !!

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

!! Local Web Authentication !!

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

{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State G
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52910/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52910/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52919/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52919/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52923/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52924/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]52924/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State G
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse 1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53007/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53008/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse G
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [webauth-error] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Parse 1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53009/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53011/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53011/1
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53020/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53022/235
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]POST rc
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]get ur
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Read co
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -1526718499,s
{wncd_x_R0-0}{1}: [caaa-authen] [24229]: (info): [CAAA:AUTHEN:4000544] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list 1761615853,sm
{wncd_x_R0-0}{1}: [caaa-author] [24229]: (info): [CAAA:AUTHOR:4000544] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]State A
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Unapply I
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template D
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.226]Unapply I
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template D
{wncd_x_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client_MAC Link-local bridging not enabled for
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Authc success from WebAuth
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event APPLY_USER_PR
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event RX_METHOD_AUT

```

{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : username 0 Guest1
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-type 0 1 (0x1)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-service 0 16 (0x10)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : addr 0 0xa693ce2
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : method 0 1 [webauth]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : intf-id 0 2684354561 (0xa0000001)
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [24229]: (info): [Client_MAC:mobility_a0000001] SM Notified attr
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Received User-Name Guest1
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Method webauth changing st
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event AUTHZ_SUCCESS
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Applying
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Applying Svc Templ IP-Adm-V4-LOGOUT-ACL (ML:NONE)
{wncd_x_R0-0}{1}: [epm] [24229]: (info): [Client_MAC:mobility_a0000001] Feature (EPM URL PLUG-IN) has b
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Response of epm is SYNC with return code Success
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template A
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [24229]: (ERR): authc policy update from SANet v1an 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 Tem
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [rog-proxy-capwap] [24229]: (debug): Managed client RUN state notification: Client_MA
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Client has Anchor role
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Guest client detected. S
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

```

패킷 캡처

모빌리티 핸드오프 후 앵커 컨트롤러는 모빌리티 터널을 통해 외부 컨트롤러로부터 DHCP 트래픽을 수신합니다.

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

앵커 컨트롤러의 클라이언트 DHCP 트래픽이 외부 컨트롤러에서 수신됨

앵커 컨트롤러는 추가 처리를 위해 연결 확인, 웹 페이지 액세스 요청 및 인증 세부 정보를 수신합니다.

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...	10.107.79.30	10.105.60.114	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

앵커 컨트롤러에 대한 네트워크 연결 상태 확인

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

클라이언트로 전송된 URL 리디렉션

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...	10.105.60.114	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

인증 세부 정보를 제공하는 로컬 Webauth 페이지에 대한 클라이언트 액세스

로컬 웹 인증에 성공하면 클라이언트는 Export Anchor 역할의 RUN 상태가 됩니다. 이 시점부터 Anchor Controller는 클라이언트 데이터 트래픽의 종료 지점 역할을 합니다.

외부 및 앵커 컨트롤러 모두의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

✕ Delete ↺

XLS

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients ↻

외래의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

✕ Delete ↺

XLS

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients ↻

앵커의 클라이언트 상태

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability

802.11ac Wave 2

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Anchor IP Address

10.105.60.114

Point of Presence

0xA0000003

AuthC Status

True

Move Count

0

Role

Export Foreign

Roam Type

L3 Requested

외래의 클라이언트 속성

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

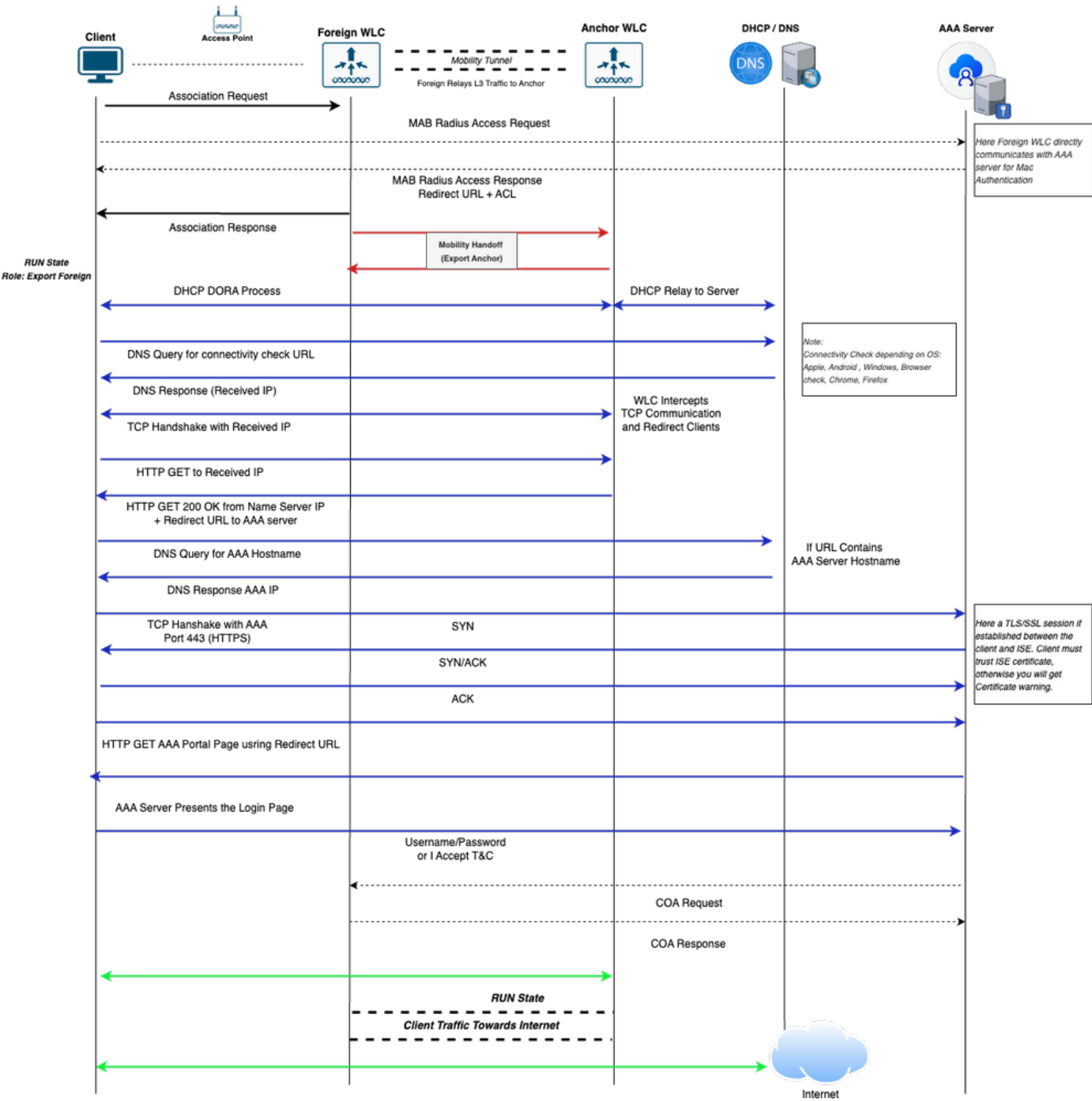
앵커의 클라이언트 속성

중앙 웹 인증

외부 앵커 설정의 중앙 Webauth SSID에 대한 흐름

1. 클라이언트가 WLC(Foreign Wireless LAN Controller)에서 브로드캐스트하는 SSID에 대한 연결 요청을 보냅니다.
2. 외부 WLC는 RADIUS 서버에 액세스 요청을 보내 MAC 필터링을 수행합니다. RADIUS 서버는 필요한 리디렉션 URL 및 ACL(Access Control List)을 포함하는 Access-Accept로 응답합니다.
3. 외부 WLC가 클라이언트에 연결 응답을 보냅니다.
4. 클라이언트가 앵커 WLC에 고정됩니다. 클라이언트는 외부 WLC에서 RUN 상태가 되며, 모빌리티 역할이 Export Foreign(외부 내보내기)으로 설정됩니다.
5. 클라이언트가 IP 주소를 얻습니다. 이 단계에서 앵커 WLC는 리디렉션 트래픽을 처리하여 클라이언트를 인증 포털로 디렉션합니다.
6. 리디렉션되면 클라이언트는 RADIUS 서버와 직접 통신합니다. 이 트래픽은 앵커 WLC를 통해 RADIUS 서버로 터널링됩니다.
7. 클라이언트가 RADIUS 서버에 인증 자격 증명을 입력합니다. 인증에 성공하면 RADIUS 서버는

- 외부 WLC에 CoA(Change of Authorization) 요청을 보냅니다.
8. 외부 WLC가 RADIUS 서버에 CoA 응답을 보냅니다. 클라이언트는 Anchor WLC에서 RUN 상태로 전환되며, 역할은 Export Anchor로 설정됩니다.
9. 모든 후속 클라이언트 트래픽은 외부 WLC에서 앵커 WLC로 터널링되며, 여기서 네트워크를 빠져나갑니다.



외부 앵커 설정의 중앙 Webauth SSID에 대한 클라이언트 연결 흐름도

로그를 통한 외부 앵커 설정의 중앙 Webauth SSID 흐름 분석

이 섹션에서는 RA 추적(Radioactive Trace), EPC(Embedded Packet Captures), 외부 및 앵커 컨트

롤러 모두에서 클라이언트 상태를 사용하여 중앙 웹 인증 SSID에 대한 클라이언트 연결의 흐름을 설명합니다.

외부 컨트롤러의 로그

방사선 흔적

!! Client Association Phase !!

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

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

!! MAC Authentication !!

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

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

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

{wncd_x_R0-0}{1}: [auth-mgr-feat-wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authc_list: l

{wncd_x_R0-0}{1}: [auth-mgr-feat-wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authz_list: l

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Airespace-WLAN-ID [1] 6 12

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Nas-Identifier [32] 16 ForeignSiteWLC

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Started 5 sec timeout

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Received from id 1812/245 10.106.32.130:0, Access-A

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

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 19 Client_MAC

```

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 37
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 31 url-redirect-ac1=REDIRECT_ACL
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 191
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 185 url-redirect=https://10.106.32
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat

{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB received an Access-Accept for
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC Processing MAB authentication resu
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_MA
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC dot11 send association response. Sending ass
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_MAB_PENDING
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC L2 Authentication of station issu
{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_ANN
{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Sending export_Anchor_req of XID (XID) to (
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
□{wncd_x_R0-0}{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed□[mm-client] [17047] (info) MAC
[mm-client] Mobility Successful. Roam Type L3 Requested, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IF
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_C
{wncd_x_R0-0}{1} [client-orch-state] Client state transition S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LE
□{wncd_x_R0-0}{1} [client-orch-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 Successful 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
```

패킷 캡처

클라이언트는 연결 요청을 전송하고 MAC 인증을 수행하며, 이 트래픽은 외부 컨트롤러에서 처리됩니다.

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=.....

무선 MAB를 사용하는 외부 컨트롤러의 클라이언트 연결 단계

모빌리티 전달은 포트 UDP 16667을 통해 외부 컨트롤러와 앵커 컨트롤러 간에 트리거됩니다. 모빌리티 이벤트가 성공하면 클라이언트 상태가 Export Foreign(외부 내보내기) 역할로 RUN(실행)으로 전환됩니다.

외부 컨트롤러는 CAPWAP 터널을 통해 클라이언트 DHCP 트래픽을 수신한 다음 추가 처리를 위해 앵커 컨트롤러에 전달합니다.

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

외부 컨트롤러에서 수신된 클라이언트 DHCP 트래픽이 모빌리티 터널을 사용하여 앵커 컨트롤러로 전달됨

마찬가지로 클라이언트는 CAPWAP 터널을 통해 외부 WLC에 네트워크 연결 상태 및 웹 페이지 액세스 확인 트래픽을 전송합니다. 외부 WLC는 모빌리티 터널을 사용하여 이를 앵커 WLC에 전달합니다. 앵커 컨트롤러는 이 터널을 사용하여 트래픽을 가로채거나 처리합니다.

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

외부 컨트롤러에 대한 네트워크 연결 상태 확인

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

클라이언트로 전송된 URL 리디렉션

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

인증 세부 정보를 제공하는 중앙 Webauth 페이지에 대한 클라이언트 액세스

외부 컨트롤러는 중앙 웹 인증에 성공한 후 CoA 요청을 처리합니다.

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

외부 컨트롤러와의 COA(Change of Authorization)

앵커 컨트롤러에서 로그

방사선 흔적

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

!! 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}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [24229]: (debug): MAC: Client_MAC L2 Authentication of station is su
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_CR
{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MACMMIF FSM transition: S_MA_INIT -> S_M
{wncd_x_R0-0}{1}: [mm-client] [24229]: (info): MAC: Client_MACRoam type changed - None -> L3 Requested
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully proc
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.
{□wncd_x_R0-0}{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export A
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is AnchorED.>> Client is successf

!! Central Web Authentication Applied !!

{wncd_x_R0-0}{1}: [webauth-dev] [24229]: (info): Central Webauth URL Redirect, Received a request to cr
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]State Invalid State -> INIT
{wncd_x_R0-0}{1}: [epm-redirect] [24229]: (info): [0000.0000.0000:unknown] URL-Redirect = https://10.10
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: method 0 2 [mab]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: intf-id 0 2415919107 (0x90000000
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: username 0 D0-37-45-88-25-52
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: class 0 43 41 43 53 3a 31 45 34
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: url-redirect-ac1 0 REDIRECT_ACL
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applied User Profile: url-redirect 0 https://10.106.3

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

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

!! Central Web Authentication !!

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

패킷 캡처

모빌리티 핸드오프 후 앵커 컨트롤러는 모빌리티 터널을 통해 외부 컨트롤러로부터 DHCP 트래픽을 수신합니다.

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

앵커 컨트롤러의 클라이언트 DHCP 트래픽이 외부 컨트롤러에서 수신됨

앵커 컨트롤러는 추가 처리를 위해 연결 확인, 웹 페이지 액세스 요청 및 인증 세부 정보를 수신합니다.

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

앵커 컨트롤러에 대한 네트워크 연결 상태 확인

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

클라이언트로 전송된 URL 리디렉션

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

인증 세부 정보를 제공하는 로컬 Webauth 페이지에 대한 클라이언트 액세스

중앙 웹 인증이 성공하면 CoA(Change of Authorization)가 트리거됩니다. CoA가 성공하면 클라이언트는 Export Anchor 역할의 RUN 상태로 전환됩니다.

외부 및 앵커 컨트롤러 모두의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

× Delete ↺

1 - 1 of 1 clients ↻

Selected 0 out of 1 Clients

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

1 10

외래의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

× Delete ↺

1 - 1 of 1 clients ↻

Selected 0 out of 1 Clients

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

1 10

앵커의 클라이언트 상태

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability

802.11ac Wave 2

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Anchor IP Address

10.105.60.114

Point of Presence

0xA0000003

AuthC Status

True

Move Count

0

Role

Export Foreign

Roam Type

L3 Requested

외래의 클라이언트 속성

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

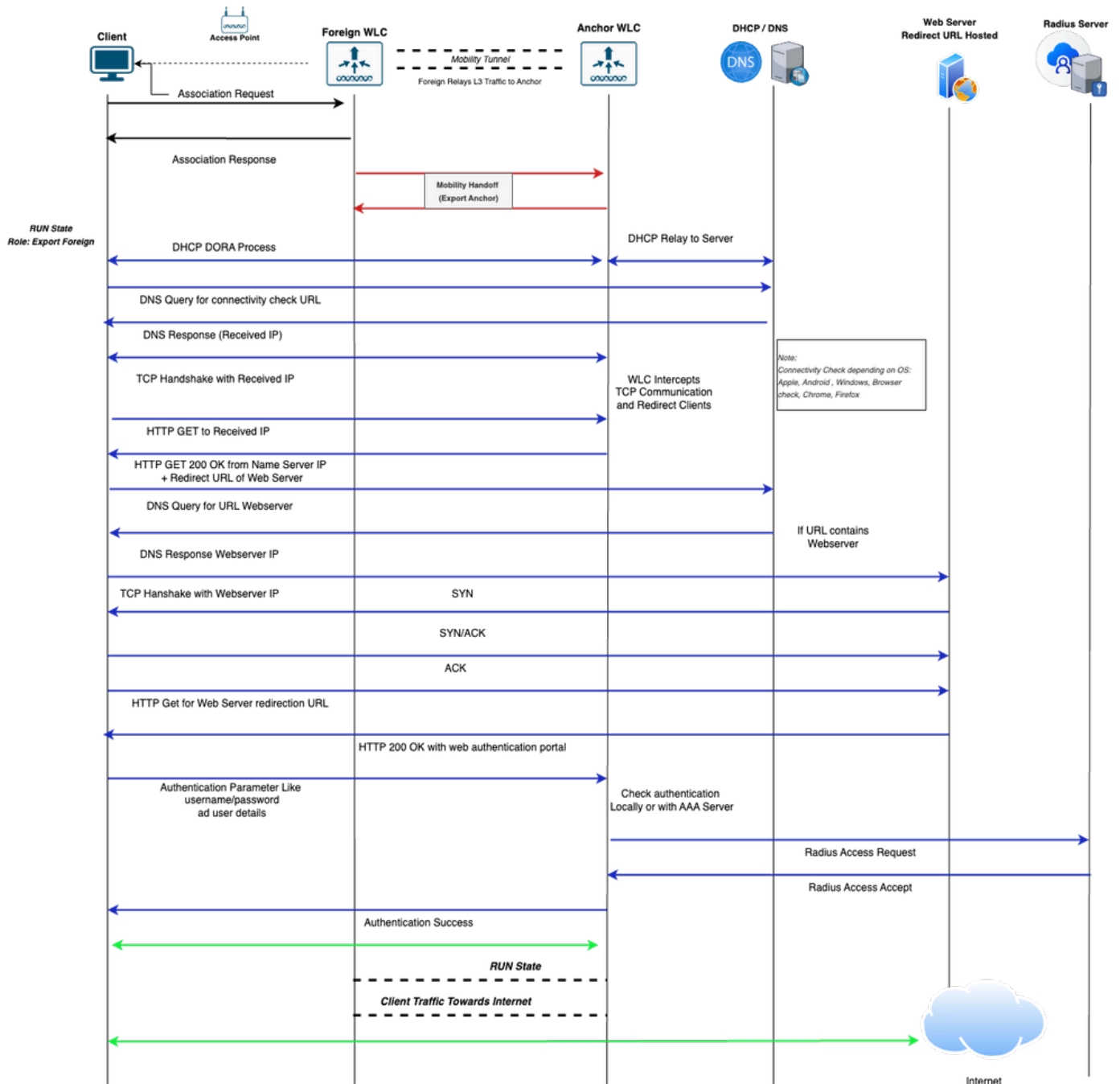
L3 Requested

앵커의 클라이언트 속성

외부 웹 인증

외부 앵커 설정의 외부 Webauth SSID에 대한 흐름

1. 클라이언트가 외부 WLC에서 브로드캐스트하는 SSID에 대한 연결을 시작합니다.
2. 레이어 2 인증이 필요하지 않으므로 클라이언트가 앵커 WLC에 고정됩니다. 클라이언트는 외부 WLC에서 RUN 상태로 전환되며, 모빌리티 역할이 Export Foreign(외부 내보내기)으로 지정됩니다.
3. 클라이언트가 IP 주소를 취득합니다. 앵커 WLC는 트래픽을 인터셉트하고 웹 인증 매개변수에 정의된 대로 클라이언트를 외부 웹 서버 포털로 리디렉션합니다.
4. 클라이언트가 포털을 통해 인증 자격 증명을 제출합니다. 이러한 자격 증명은 구성된 보안 정책에 따라 WLC에서 로컬로 또는 외부 인증 서버를 통해 검증됩니다.
5. 인증에 성공하면 클라이언트는 Export Anchor 역할을 가정하여 Anchor WLC에서 RUN 상태로 전환됩니다.
6. 인증에 성공하면 모든 후속 클라이언트 트래픽이 외부 WLC에서 앵커 WLC로 터널링되고 여기서 네트워크가 이그레스(egress)됩니다.



외부 앵커 설정의 외부 Webauth SSID에 대한 클라이언트 연결 흐름도

로그를 통한 외부 앵커 설정의 외부 Webauth SSID 흐름 분석

이 섹션에서는 RA 추적(Radioactive Trace), EPC(Embedded Packet Captures), 외부 및 앵커 컨트롤러 모두에서 클라이언트 상태를 사용하여 외부 웹 인증 SSID에 대한 클라이언트 연결의 흐름을 설명합니다.

외부 컨트롤러의 로그

방사선 흔적

!! Client Association Phase !!

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

!! Layer 2 Authentication None !!

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

!! Mobility Handoff !!

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

!! Client AAAA Traffic !!

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

패킷 캡처

클라이언트는 외부 컨트롤러에서 처리하는 연결 요청을 보냅니다.

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=.....

외부 컨트롤러와의 클라이언트 연결 단계

모빌리티 전달은 포트 UDP 16667을 통해 외부 컨트롤러와 앵커 컨트롤러 간에 트리거됩니다. 모빌리티 이벤트가 성공하면 클라이언트 상태가 Export Foreign(외부 내보내기) 역할로 RUN(실행)으로 전환됩니다. 외부 컨트롤러는 CAPWAP 터널을 통해 클라이언트 DHCP 트래픽을 수신한 다음 추가 처리를 위해 앵커 컨트롤러에 전달합니다.

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

외부 컨트롤러에서 수신된 클라이언트 DHCP 트래픽이 모빌리티 터널을 사용하여 앵커 컨트롤러로 전달됨

마찬가지로 클라이언트는 CAPWAP 터널을 통해 외부 WLC에 네트워크 연결 상태 및 웹 페이지 액세스 확인 트래픽을 전송합니다. 외부 WLC는 모빌리티 터널을 사용하여 이를 앵커 WLC에 전달합니다. 앵커 컨트롤러는 이 터널을 사용하여 트래픽을 가로채거나 처리합니다.

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

외부 컨트롤러에 대한 네트워크 연결 상태 확인

```

> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco (00:0c:29:00:00:00), Dst: Cisco (00:0c:29:00:00:00)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1415
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.107.79.129
> User Datagram Protocol, Src Port: 5247, Dst Port: 5264
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.107.79.30, Dst: 10.105.60.254
> Transmission Control Protocol, Src Port: 80, Dst Port: 62437, Seq: 1, Ack: 112, Len: 849
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Location: https://10.106.32.130:8443/portal/PortalSetup.action?portal=d06bc251-f644-4fc3-b09f-dae9bd8a86
    Content-Type: text/html\r\n
  > Content-Length: 580\r\n
    \r\n
    [Request in frame: 788]
    [Time since request: 0.000991000 seconds]
    [Request URI: /connecttest.txt]
    [Full request URI: ]
    File Data: 580 bytes
  > Line-based text data: text/html (9 lines)

```

클라이언트로 전송된 URL 리디렉션

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.	10.107.79.30	10.105.60.114	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

인증 세부 정보를 제공하는 외부 Webauth 페이지에 대한 클라이언트 액세스

앵커 컨트롤러에서 로그

방사선 흔적

!! Mobility Handoff !!

```

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

```

!! Session Created for Client !!

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

!! Client DHCP Traffic !!

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

!! External Web Authentication !!

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

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

{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition

{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3

{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_ANCHOR -> S_MA_ANCHOR_WAIT

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff base check is VALID

{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_MC_ANCHOR_WAIT

{mobilityd_R0-0}{1}: [mm-client] [26021]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 of

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) to

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type: 0 of

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID

{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID

{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_ANCHOR_WAIT -> S_MC_RUN

패킷 캡처

모빌리티 핸드오프 후 앵커 컨트롤러는 모빌리티 터널을 통해 외부 컨트롤러로부터 DHCP 트래픽을 수신합니다.

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

앵커 컨트롤러의 클라이언트 DHCP 트래픽이 외부 컨트롤러에서 수신됨

앵커 컨트롤러는 추가 처리를 위해 연결 확인, 웹 페이지 액세스 요청 및 인증 세부 정보를 수신합니다.

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

앵커 컨트롤러에 대한 네트워크 연결 상태 확인

```

> 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)

```

클라이언트로 전송된 URL 리디렉션

클라이언트는 포털을 통해 인증 자격 증명을 제출합니다. 이러한 자격 증명은 구성된 보안 정책에 따라 WLC에서 로컬로 또는 외부 인증 서버를 통해 검증됩니다.

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...	10.105.60.114	10.106.32.130	1119	UDP	16667	→ 16667 Len=1073
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1061	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1015	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	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

인증 세부 정보를 제공하는 외부 Webauth 페이지에 대한 클라이언트 액세스

외부 및 앵커 컨트롤러 모두의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete



Selected 0 out of 1 Clients

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

1 - 1 of 1 clients

외래의 클라이언트 상태

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients

앵커의 클라이언트 상태

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability	802.11ac Wave 2
Wi-Fi to Cellular Steering	Not implemented
Cellular Capability	N/A
Regular ASR support	DISABLED

Mobility

Anchor IP Address	10.105.60.114
Point of Presence	0xA0000003
AuthC Status	True
Move Count	0
Role	Export Foreign
Roam Type	L3 Requested

외래의 클라이언트 속성

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

FlexConnect Authentication

N/A

Number of Tx Total Dropped Packets

0

Client Scan Report Time

Timer not running

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Foreign IP Address

10.107.79.30

Point of Presence

0

Move Count

1

Role

Export Anchor

Roam Type

L3 Requested

앵커의 클라이언트 속성

여러 앵커 컨트롤러 간 로드 밸런싱

둘 이상의 앵커 컨트롤러가 단일 WLAN에 매핑되는 경우 트래픽 분배는 우선 순위에 따라 달라집니다. 세 가지 우선순위 레벨을 구성할 수 있습니다. Primary, Secondary 및 Tertiary입니다. 게스트 앵커 우선 순위 기능은 앵커 컨트롤러 간의 활성/대기 로드 분배 메커니즘을 제공합니다. 이는 각 앵커 컨트롤러에 고정 우선 순위를 할당함으로써 달성할 수 있습니다. 로드는 우선순위가 가장 높은 컨트롤러로 분산되며, 동일한 우선순위 값을 공유하는 컨트롤러 간에 라운드 로빈 방식으로 분산됩니다.

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

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

Mobility Anchors

Export Anchor

☐

Static IP Mobility

☐ DISABLED

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

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

Available (0)

Anchor IP

No anchors available

Selected (1)

Anchor IP

Anchor Priority



10.105.60.114

Tertiary (3)



매핑 앵커 우선 순위



참고: 기본적으로 우선 순위 3차는 외부 컨트롤러에서 앵커 컨트롤러 매핑 중에 구성됩니다

외부 앵커 시나리오에서 클라이언트 연결 문제 해결

1. 클라이언트 온보딩 문제

- i. 터널 상태: 외부 컨트롤러와 앵커 컨트롤러 간의 모빌리티 터널이 활성화 상태인지 확인합니다.
- ii. 구성 불일치: 두 컨트롤러 간의 컨피그레이션 패리티를 확인합니다. WLAN 이름, 정책 프로파일 이름 또는 고급 설정(예: AAA 재정의, IPv4 DHCP 요구 사항, NAC)의 불일치로 인해 프로파일 불일치 또는 앵커 거부 오류가 발생합니다.
- iii. 기타: 컨피그레이션 문제 없이 터널이 가동되는 경우, 트러블슈팅 접근 방식은 일반적인 클라이언트 연결 문제와 유사하므로 영향을 받는 트래픽을 처리하는 각 컨트롤러를 확인합니다.

2. 간헐적 연결

- i. 터널 폴랩: 두 컨트롤러 간의 keepalive 패킷이 도착하지 못하면 터널이 폴랩되어 클라이언트가 SSID에 대한 연결을 유지할 수 없습니다.
- ii. 낮은 대역폭: 모빌리티 피어 간의 경로 MTU(PMTU)가 더 낮은 값(576)으로 떨어지면 클라이언트의 성능이 저하됩니다. 이 문제는 대개 두 모빌리티 피어 간에 경로 mtu 킥얼라이브 메시지가 누락된 경우에 발생합니다



참고: 모빌리티 MAC 주소가 더 낮은 컨트롤러는 표준 keepalive 메시지와 경로 MTU keepalive 메시지를 모두 시작합니다.

3. 특정 웹 사이트 액세스 문제

- i. 모빌리티 트래픽 헤더에는 모빌리티 그룹 식별자, MAC 주소, IP 주소 및 UDP 포트 16666 및 16667을 통해 교환되는 암호화된 CAPWAP DTLS 패킷이 포함됩니다. 이 오버헤드는 기존 CAPWAP 헤더에 추가됩니다. TCP 트래픽의 경우, AP에 대해 구성된 TCP MSS를 사후 조정하는 경우, 패킷 크기가 이 추가 오버헤드로 인해 모빌리티 PMTU(최대 1385바이트)를 초과할 경우 프래그먼트화가 발생합니다. 일반적으로 프래그먼트화는 네트워크에서 처리되지만, 패킷이 순서를 벗어났거나 늦게 도착할 경우 문제가 발생합니다. 이러한 조건은 패킷 재결합에 영향을 미치며 특정 웹 사이트의 데이터 액세스 실패로 이어집니다.

외부 및 앵커 컨트롤러에서 로그 수집

1. 모든 명령에 대한 시간 참조를 포함하도록 term exec 프롬프트 타임스탬프를 활성화합니다.
2. 컨피그레이션을 검토하려면 show tech-support wireless!!을(를) 사용하십시오.
3. 모빌리티 터널 상태 show wireless mobility summary(무선 모빌리티 요약 정보 표시)를 확인할 수 !!
4. 링크 상태, 클라이언트 데이터 및 이벤트를 포함하는 모빌리티 피어에 대한 통계, 연결 유지 통계는 무선 모빌리티 피어 IP <IP>를 표시합니다.
5. 모빌리티 피어 IP/MAC 주소 및 클라이언트 MAC 주소에 대한 방사성 추적을 활성화합니다.

CLI를 통해:

무선 {MAC 디버그 | ip} {aaaa.bbb.cccc | x.x.x.x } {monitor-time} {N초} !! 시간을 설정하면 최대 24일 동안 추적을 활성화할 수 있습니다.

디버그 무선 없음 {MAC | ip} {aaaa.bbb.cccc | x.x.x.x !! 디버깅을 비활성화하려면

WLC는 Client_info 명령을 사용하여 디버그 추적 파일을 생성하며, 디버그 추적 파일이 생성된 dir bootflash를 확인합니다. | 디버그 !!



경고: 조건부 디버깅은 디버그 레벨 로깅을 활성화하므로 생성된 로그의 볼륨이 증가합니다. 이 작업을 계속 실행하면 로그를 볼 수 있는 시간이 줄어듭니다. 따라서 트러

불슈팅 세션이 끝날 때 항상 디버깅을 비활성화하는 것이 좋습니다.

6. 모든 디버깅을 비활성화하려면 다음 명령을 실행합니다.

모든 !! 플랫폼 상태 지우기

모든 디버그 !!

GUI를 통해:

1단계. Troubleshooting(문제 해결) > Radioactive Trace(방사능 추적)로 이동합니다.

2단계. Add(추가)를 클릭하고 트러블슈팅할 Mobility Peer MAC/IP 주소 또는 클라이언트 MAC 주소를 입력합니다.

3단계. 방사능 추적을 시작할 준비가 되면 Start(시작)를 클릭합니다. 일단 시작되면, 추적된 MAC 주소와 관련된 제어 평면 처리에 대한 디버깅 로깅은 디스크에 기록됩니다.

4단계. 트러블슈팅할 문제를 재현하면 Stop(중지)을 클릭합니다.

5단계. 디버깅된 각 MAC 주소에 대해 Generate(생성)를 클릭하여 해당 MAC 주소와 관련된 모든 로그를 취합하는 로그 파일을 생성할 수 있습니다.

6단계. 취합된 로그 파일을 사용할 기간을 선택하고 Apply to Device(디바이스에 적용)를 클릭합니다.

7단계. 이제 파일 이름 옆에 있는 작은 아이콘을 클릭하여 파일을 다운로드할 수 있습니다. 이 파일은 컨트롤러의 부트 플래시 드라이브에 있으며 CLI를 통해 즉시 복사할 수도 있습니다.

7. 임베디드 캡처

CLI를 통해:

모니터링 캡처 MYCAP 지우기 !!

모니터링 캡처 MYCAP 인터페이스 Po1 둘 다 !!

모니터 캡처 MYCAP 버퍼 크기 100!!

monitor capture MYCAP match access-list name !!(WLC 간 모빌리티 터널 트래픽을 추적하는 경우)

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

모니터링 캡처 MYCAP 시작 !!

!!복제

모니터 캡처 MYCAP 중지

모니터 캡처 MYCAP 내보내기 플래시:|tftp:|http:../filename.pcap

GUI를 통해:

1단계. Troubleshooting(문제 해결) > Packet Capture(패킷 캡처) > +Add(추가)로 이동합니다.

2단계. 패킷 캡처의 이름을 정의합니다. 최대 8자까지 허용됩니다.

3단계. 필터(있는 경우)를 정의합니다.

4단계. 시스템 CPU로 유입되어 데이터 플레인으로 다시 유입되는 트래픽을 보려면 Monitor Control

Traffic(제어 트래픽 모니터링) 상자를 선택합니다.

5단계. 버퍼 크기를 정의합니다. 최대 100MB가 허용됩니다.

6단계. 원하는 대로 1~1000000초 범위를 허용하는 기간 또는 1~100000 패킷 범위를 허용하는 패킷 수로 제한을 정의합니다.

7단계. 왼쪽 열의 인터페이스 목록에서 인터페이스를 선택하고 화살표를 선택하여 오른쪽 열로 이동합니다.

8단계. Save and Apply to Device(저장 및 디바이스에 적용)를 클릭합니다.

9단계. 캡처를 시작하려면 시작을 선택합니다.

10단계. 정의된 한도까지 캡처를 실행할 수 있습니다. 캡처를 수동으로 중지하려면 중지를 선택합니다.

11단계. 일단 중지되면 HTTP 또는 TFTP 서버나 FTP 서버 또는 로컬 시스템 하드 디스크나 플래시를 통해 로컬 데스크톱에 캡처 파일(.pcap)을 다운로드하는 옵션과 함께 내보내기 버튼을 클릭할 수 있습니다.

관련 정보

[Catalyst 9800 WLC에서 모빌리티 토폴로지 구성](#)

[Catalyst 9800에서 WLAN Anchor Mobility 기능 구성](#)

[기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.