

Analyse des Datenverkehrsflusses beim Einrichten von Foreign-Anchor zwischen 9800 WLC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick über das Szenario für Auslandsanker](#)

[Topologie](#)

[WLAN mit Layer-2-Authentifizierung](#)

[Konfigurationsanforderung](#)

[Fluss für Layer 2 Foreign-Anchor-basierte SSID](#)

[Analyse des Layer-2-SSID-Datenflusses im Foreign-Anchor-Setup über Protokolle](#)

[Protokolle von Foreign Controller](#)

[Protokolle vom Anchor 9800-Controller](#)

[Client-Status auf Fremd- und Ankercontroller](#)

[WLAN mit Layer-3-Authentifizierung](#)

[Lokale Webauthentifizierung](#)

[Fluss für lokale Webauthentifizierungs-SSID im Foreign-Anchor-Setup](#)

[Analyse des lokalen Webauthentifizierungs-SSID-Datenflusses im Foreign-Anchor-Setup mithilfe von Protokollen](#)

[Protokolle von Foreign Controller](#)

[Protokolle vom Anker-Controller](#)

[Client-Status auf Fremd- und Ankercontroller](#)

[Zentrale Webauthentifizierung](#)

[Fluss für zentrale Webauthentifizierungs-SSID im Foreign-Anchor-Setup](#)

[Analyse des zentralen WebAuth SSID-Datenflusses im Foreign-Anchor-Setup mithilfe von Protokollen](#)

[Protokolle von Foreign Controller](#)

[Protokolle vom Anker-Controller](#)

[Client-Status auf Fremd- und Ankercontroller](#)

[Externe Webauthentifizierung](#)

[Fluss für externe Webauthentifizierungs-SSID im Foreign-Anchor-Setup](#)

[Analyse des externen Webauthentifizierungs-SSID-Datenflusses im Foreign-Anchor-Setup über Protokolle](#)

[Protokolle von Foreign Controller](#)

[Protokolle vom Anker-Controller](#)

[Client-Status auf Fremd- und Ankercontroller](#)

[Lastenausgleich zwischen mehreren Anker-Controllern](#)

[Fehlerbehebung bei Client-Verbindungen im Foreign-Anchor-Szenario](#)

[Protokollerfassung vom Fremd- und Ankercontroller](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt den Datenverkehrsfluss zwischen den Cisco 9800 WLCs in der Foreign-Anchor-Konfiguration und behandelt die Integration und Fehlerbehebung von L2-/L3-Clients.

Voraussetzungen

Mobility-Tunnel zwischen Foreign und Anchor Controller

UDP-Port 16666 und 16667 zwischen beiden WLCs zulässig.

Für das zentrale Switching konfiguriertes Richtlinienprofil.

[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

Mobility Tunnel-Status auf fremdem WLC

[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

Mobility-Tunnelstatus auf Anker-WLC

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Zugriff auf die Wireless Controller über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Mobilität mit Cisco Wireless LAN Controllern (WLCs)
- Wireless Controller 9800
- Radioaktive Spuren und Paketerfassung auf 9800 WLC

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Modell WLC 9800
- Cisco IOS XE 17.15.5
- AP-Modell der Serie 9100

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

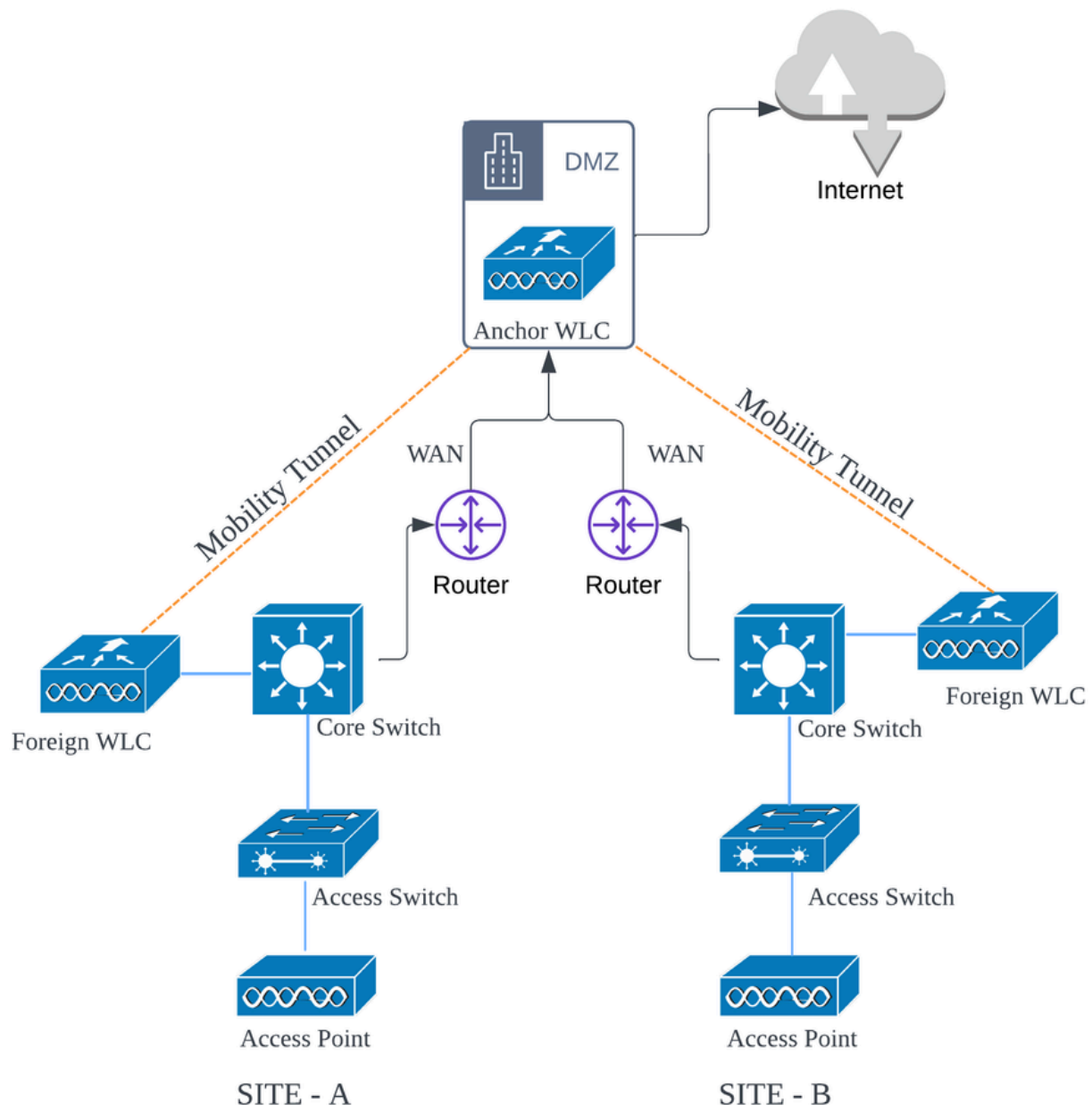
Überblick über das Szenario für Auslandsanker

- Ausländischer Controller: Dieser WLC verwaltet Layer 2 oder die Wireless-Seite des Netzwerks. Es ist mit Access Points verbunden, und der gesamte Client-Datenverkehr für die verankerten WLANs wird in den Mobility-Tunnel gekapselt und an den Anchor Controller gesendet. Der Datenverkehr wird auf dem Foreign Controller nicht lokal beendet.
- Anker-Controller: Dieser dient als Ausgangspunkt für Layer 3. Er empfängt Client-Datenverkehr über einen Mobility Tunnel von den Foreign Controllern und entkapselt oder terminiert den Client-Datenverkehr an den Ausgangspunkt (VLAN). An dieser Stelle werden Clients im Netzwerk angezeigt.

Access Points auf dem ausländischen WLC senden die WLAN-SSIDs und verfügen über ein zugewiesenes Richtlinien-Tag, das das WLAN-Profil mit dem entsprechenden Richtlinien-Profil verknüpft. Wenn ein Wireless-Client eine Verbindung mit dieser SSID herstellt, sendet der Foreign Controller sowohl den SSID-Namen als auch das Richtlinienprofil als Teil der Client-Informationen an den Anker-WLC. Beim Empfang überprüft der Anker-WLC seine eigene Konfiguration auf

Übereinstimmung mit dem SSID-Namen und dem Richtlinienprofilnamen. Sobald der Anker-WLC eine Übereinstimmung findet, wird die entsprechende Konfiguration angewendet und ein Ausgangspunkt für den Wireless-Client bereitgestellt. Aus diesem Grund ist es erforderlich, dass die Namen und Konfigurationen der WLAN- und Richtlinienprofile auf den Foreign Controllern und den Anchor 9800 WLCs übereinstimmen, mit Ausnahme des VLANs unter dem Richtlinienprofil.

Topologie



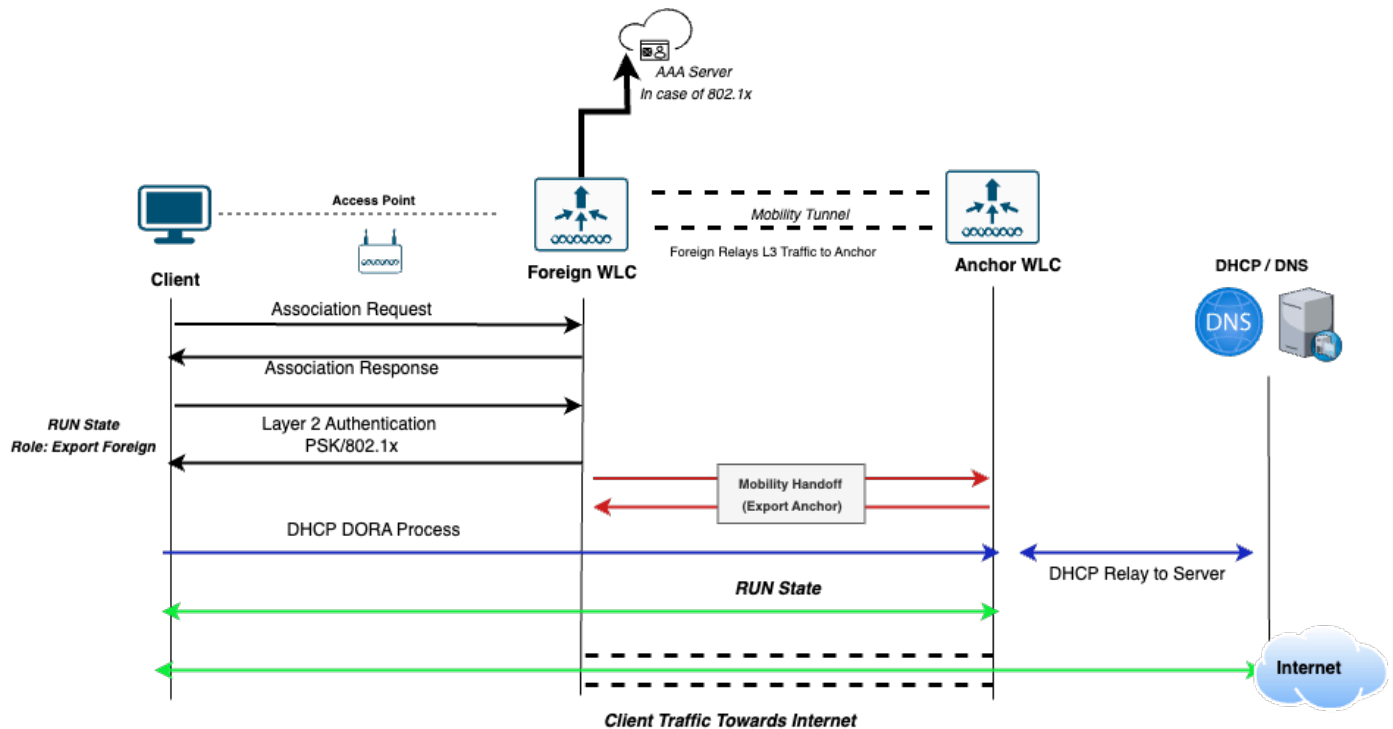
WLAN mit Layer-2-Authentifizierung

Konfigurationsanforderung

1. Stellen Sie sicher, dass der WLAN-Name und die Konfiguration auf den Fremd- und Anker-WLCs identisch sind und für die Layer-2-Authentifizierung (PSK oder 802.1x) konfiguriert sind.
2. Erstellen Sie ein Richtlinienprofil mit dem gleichen Namen auf den externen und externen WLCs mit der gleichen Konfiguration.
3. Konfigurieren Sie auf dem ausländischen WLC die Anker-WLC-Zuordnung im entsprechenden Richtlinienprofil.
4. Konfigurieren Sie auf dem Anker-WLC das Richtlinienprofil so, dass der Controller als Export-Anker festgelegt wird.
5. Ordnen Sie auf dem ausländischen WLC das WLAN mithilfe eines Policy Tags dem entsprechenden Richtlinienprofil zu.

Fluss für Layer 2 Foreign-Anchor-basierte SSID

1. Der Client stellt eine Verbindung mit dem vom ausländischen WLC per Broadcast gesendeten SSID her. Der ausländische WLC führt eine Layer-2-Authentifizierung durch und validiert die Anmeldeinformationen entweder lokal oder über einen externen AAA-Server, je nach konfigurierter Sicherheitsrichtlinie.
2. Nach erfolgreicher Authentifizierung wird die Client-Sitzung am Anchor-WLC verankert. Dem Client wird eine IP-Adresse zugewiesen, und er wechselt in den RUN-Status des Anchor WLC.
3. Sobald die Sitzung hergestellt ist, wird der gesamte Client-Datenverkehr vom ausländischen WLC zum Anker-WLC getunnelt, wo er in das Netzwerk eintritt.



Layer 2 Foreign Anchor-basiertes WLAN-Flussdiagramm

Analyse des Layer-2-SSID-Datenflusses im Foreign-Anchor-Setup über Protokolle

In diesem Abschnitt wird der Verbindungsfluss des Layer-2-Clients mithilfe von Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) und dem Client-Status auf dem Fremd- und dem Anker-Controller erläutert.

Protokolle von Foreign Controller

Radioaktive Spuren

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

!! Mobility Handoff !!

```

{mobilityd_R0-0}{1} [mm-dgram-io] [18401] (debug) MAC Client-MAC Sending message mobile_announce to gr
{mobilityd_R0-0}{1} [mm-pmtu] [18401] (debug) Peer IP Anchor-WLC-IP {mobilityd_R0-0}{1} [mm-client] [1
{mobilityd_R0-0}{1} [mm-transition] MMFSM transition S_MC_WAIT_ANNOUNCE_RSP -> S_MC_ANNOUNCE_TIMEDOUT_P
{wncd_x_R0-0}{1} [mm-client] [17047] (debug) MAC Client-MAC Received mobile_announce_nak, sub type 2 o
{wncd_x_R0-0}{1} [mm-transition] [17047] (info) MAC Client-MAC MMIF FSM transition S_MA_INIT_WAIT_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_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

```

Paketerfassung

Der Client sendet eine Zuordnungsanforderung und führt eine Layer-2-Authentifizierung durch, die vom Foreign Controller behandelt wird.

Time	Source Address	Destination Address	Length	Protocol	TID	Info
417 07:36:34.347973	10.107.79.129	10.107.79.30	272	802.11		Association Request, SN=1600, FN=0, Flags=....R..., SSID="DMZ_PSK"
418 07:36:34.347973	10.107.79.129	10.107.79.30	268	802.11		Association Request, SN=1600, FN=0, Flags=....R..., SSID="DMZ_PSK"
419 07:36:34.348980	10.107.79.30	10.107.79.129	211	802.11		Association Response, SN=0, FN=0, Flags=.....
420 07:36:34.348980	10.107.79.30	10.107.79.129	215	802.11		Association Response, SN=0, FN=0, Flags=.....
421 07:36:34.350979	10.107.79.129	10.107.79.30	110	LLC	0	U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more commo
426 07:36:34.354977	10.107.79.30	10.107.79.129	203	EAPOL		Key (Message 1 of 4)
427 07:36:34.354977	10.107.79.30	10.107.79.129	207	EAPOL		Key (Message 1 of 4)
428 07:36:34.360973	10.107.79.129	10.107.79.30	217	EAPOL	0	Key (Message 2 of 4)
429 07:36:34.361980	10.107.79.129	10.107.79.30	213	EAPOL	0	Key (Message 2 of 4)
430 07:36:34.361980	10.107.79.30	10.107.79.129	237	EAPOL	0	Key (Message 3 of 4)
431 07:36:34.361980	10.107.79.30	10.107.79.129	241	EAPOL	0	Key (Message 3 of 4)
432 07:36:34.368968	10.107.79.129	10.107.79.30	195	EAPOL	0	Key (Message 4 of 4)
433 07:36:34.368968	10.107.79.129	10.107.79.30	191	EAPOL	0	Key (Message 4 of 4)

Client-Zuordnung + Layer-2-Authentifizierungsverkehr

Ein Mobility Handoff löst über den UDP-Port 16667 eine Mobility Handoff zwischen dem Foreign- und dem Anchor-Controller aus. Bei einem erfolgreichen Mobility-Ereignis wechselt der Client-Status zu RUN mit einer Export Foreign-Rolle.

Der Foreign Controller empfängt den DHCP-Datenverkehr des Clients über den CAPWAP-Tunnel und leitet ihn zur weiteren Verarbeitung an den Anchor Controller weiter.

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

Client-DHCP-Datenverkehr, der auf einem ausländischen Controller empfangen wurde, wird über Mobility Tunnel an den Anker-Controller weitergeleitet

Protokolle vom Anchor 9800-Controller

Radioaktive Spuren aus dem Anker

!! Mobility Handoff !!

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

!! Client DHCP Traffic !!

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

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

Paketerfassung auf Anker

Nach der Mobility-Übergabe empfängt der Anchor Controller DHCP-Datenverkehr vom Foreign Controller über den Mobility-Tunnel.

Nach Abschluss des DORA-Prozesses wechselt der Client in den RUN-Status mit einer Export Anchor-Rolle. Von diesem Punkt an dient der Anchor Controller als Ausgangspunkt für den Client-Datenverkehr.

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

Client-DHCP-Datenverkehr auf Anker-Controller von ausländischem Controller empfangen

Client-Status auf Fremd- und Ankercontroller

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients

Kundenstatus im Ausland

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients

Client-Status auf Anker

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

Clienteigenschaften in Fremdsprachen

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

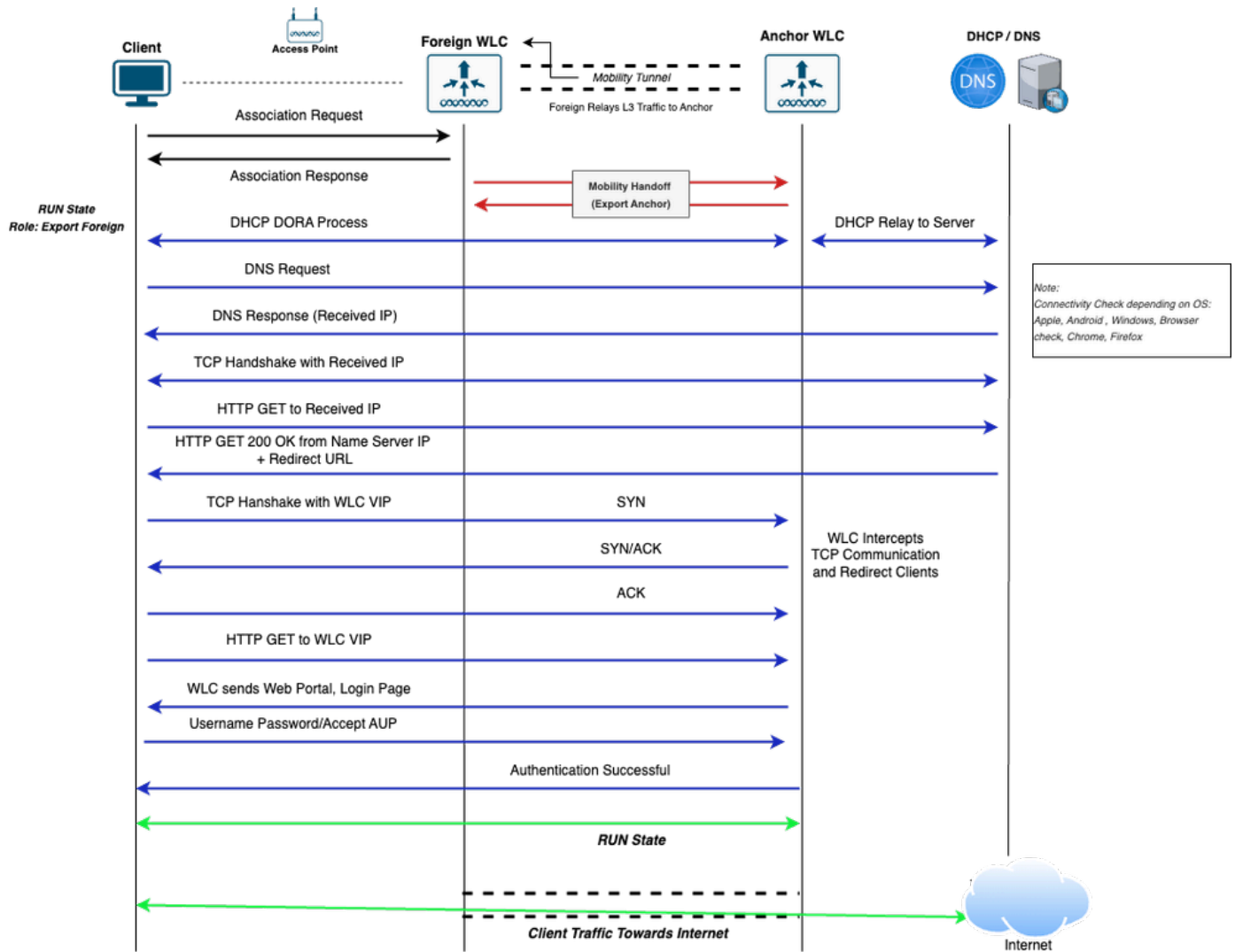
01/03/2025 07:36:27 UTC

WLAN mit Layer-3-Authentifizierung

Lokale Webauthentifizierung

Fluss für lokale Webauthentifizierungs-SSID im Foreign-Anchor-Setup

1. Der Client stellt eine Verbindung mit der vom ausländischen WLC angekündigten SSID her.
2. Da keine Layer-2-Authentifizierung durchgeführt wird, ist der Client sofort am Anchor-WLC verankert. Der Client wechselt auf dem ausländischen WLC in den Status "RUN", und seine Mobilitätsrolle wird als "Export Foreign" bezeichnet.
3. Der Client erhält eine IP-Adresse und wird auf eine Webseite umgeleitet. Dieser Datenverkehr wird vom Anchor Controller verarbeitet.
4. Nach erfolgreicher Authentifizierung im Portal wechselt der Client auf dem Anchor WLC in den RUN-Status mit der Rolle "Export Anchor".



Client-Konnektivitäts-Flussdiagramm für die lokale Webauth-SSID im Foreign-Anchor-Setup

Analyse des lokalen Webauthentifizierungs-SSID-Datenflusses im Foreign-Anchor-Setup mithilfe von Protokollen

In diesem Abschnitt wird der Verbindungsverlauf für die lokale Web-Authentifizierungs-SSID durch die Verwendung von Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) und des Client-Status sowohl auf dem Fremd- als auch auf dem Anker-Controller erläutert.

Protokolle von Foreign Controller

Radioaktive Spuren

!! Client Association Phase !!

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

```

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

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

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

```

Paketerfassung

Der Client sendet eine Zuordnungsanforderung, die vom Foreign Controller verarbeitet wird.

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=.....

Ein Mobility Handoff löst über Port UDP 16667 eine Mobility Handoff zwischen dem Foreign und dem Anchor Controller aus. Bei einem erfolgreichen Mobility Event wechselt der Client-Status zu RUN mit einer Export Foreign-Rolle.

Der Foreign Controller empfängt den DHCP-Datenverkehr des Clients über den CAPWAP-Tunnel und leitet ihn zur weiteren Verarbeitung an den Anchor Controller weiter.

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

Client-DHCP-Datenverkehr, der auf einem ausländischen Controller empfangen wurde, wird über Mobility Tunnel an den Anker-Controller weitergeleitet

Ebenso sendet der Client über den CAPWAP-Tunnel den Status der Netzwerkverbindung und den Datenverkehr für die Überprüfung des Webseitenzugriffs an den ausländischen WLC. Der Foreign WLC leitet diese Nachricht über den Mobility Tunnel an den Anchor WLC weiter, wo der Anchor Controller den Datenverkehr abfängt oder verarbeitet.

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

Überprüfung des Netzwerkverbindungsstatus auf einem externen Controller

```

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

```

An Client gesendete URL umleiten

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

Clientzugriff auf die lokale Webauthentifizierungsseite zur Bereitstellung von Authentifizierungsdetails

Protokolle vom Anker-Controller

Radioaktive Spuren

!! 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_Auth
□{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_AUTH
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global

```

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

!! Client DHCP Traffic !!

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

!! Local Web Authentication !!

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

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

{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute: username 0 Guest1
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-type 0 1 (0x1)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : aaa-author-service 0 16 (0x10)
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : addr 0 0xa693ce2
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : method 0 1 [webauth]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 Client_MAC
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : intf-id 0 2684354561 (0xa0000001)
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [24229]: (info): [Client_MAC:mobility_a0000001] SM Notified attr
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Received User-Name Guest1

```
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Method webauth changing st
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event AUTHZ_SUCCESS
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Applying
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Applying Svc Templ IP-Adm-V4-LOGOUT-ACL (ML:NONE)
{wncd_x_R0-0}{1}: [epm] [24229]: (info): [Client_MAC:mobility_a0000001] Feature (EPM URL PLUG-IN) has b
{wncd_x_R0-0}{1}: [svm] [24229]: (info): SVM_INFO: Response of epm is SYNC with return code Success
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raising ext evt Template A
{wncd_x_R0-0}{1}: [sanet-shim-miscellaneous] [24229]: (ERR): authc policy update from SANet vlan 31
{wncd_x_R0-0}{1}: [llbridge-main] [24229]: (debug): MAC: Client_MAC Link-local bridging not enabled for
{wncd_x_R0-0}{1}: [webauth-sess] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Param-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]State A
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/195
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.226]53023/1
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] SM will not send event Tem
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [rog-proxy-capwap] [24229]: (debug): Managed client RUN state notification: Client_MA
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Client has Anchor role
{wncd_x_R0-0}{1}: [avc-afc] [24229]: (info): ReAnchor [client MAC: Client_MAC] Guest client detected. S
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3.
```

Paketerfassung

Nach der Mobility-Übergabe empfängt der Anchor Controller DHCP-Datenverkehr vom Foreign Controller über den Mobility-Tunnel.

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

Client-DHCP-Datenverkehr auf Anker-Controller von ausländischem Controller empfangen

Der Anchor Controller empfängt Verbindungsprüfungen, Webseitenzugriffsanforderungen und Authentifizierungsdetails, um die Verarbeitung fortzusetzen.

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

Überprüfung des Netzwerkverbindungsstatus auf dem Anker-Controller

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

An Client gesendete URL umleiten

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	70	TCP		53024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	66	TCP		443 → 53024 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	58	TCP		53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	450	UDP		16667 → 16667 Len=404
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	1308	TCP		53024 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 3273]
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53024 [ACK] Seq=1 Ack=1251 Win=64128 Len=0
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	723	UDP		16667 → 16667 Len=677
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	669	TLSv1..		Client Hello
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53024 [ACK] Seq=1 Ack=1862 Win=64128 Len=0
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	108	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	219	TLSv1..		Server Hello, Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	273	UDP		16667 → 16667 Len=231
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	65	TLSv1..		Alert (Level: Fatal, Description: Certificate Unknown)
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	58	TCP		53024 → 443 [FIN, ACK] Seq=1869 Ack=166 Win=131072 Len=0
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	187	UDP		16667 → 16667 Len=141
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	133	TLSv1..		Change Cipher Spec, Encrypted Handshake Message
Jan 5, 2025 12:22:25...	10.107.79.30	10.105.60.114	757	UDP		16667 → 16667 Len=711
Jan 5, 2025 12:22:25...	10.105.60.226	192.0.2.1	703	TLSv1..		Application Data
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	107	TLSv1..		Encrypted Alert
Jan 5, 2025 12:22:25...	10.105.60.114	10.107.79.30	161	UDP		16667 → 16667 Len=119
Jan 5, 2025 12:22:25...	192.0.2.1	10.105.60.226	54	TCP		443 → 53027 [FIN, ACK] Seq=219 Ack=2678 Win=64128 Len=0

Clientzugriff auf die lokale Webauthentifizierungsseite zur Bereitstellung von Authentifizierungsdetails

Nach erfolgreicher lokaler Webauthentifizierung wechselt der Client in den RUN-Status mit einer Export Anchor-Rolle. Von diesem Punkt an dient der Anchor Controller als Ausgangspunkt für den Client-Datenverkehr.

Client-Status auf Fremd- und Ankercontroller

Delete

Selected 0 out of 1 Clients

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

1

10

1 - 1 of 1 clients

Kundenstatus im Ausland

Delete

Selected 0 out of 1 Clients

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

1

10

1 - 1 of 1 clients

Client-Status auf Anker

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

Clienteigenschaften in Fremdsprachen

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

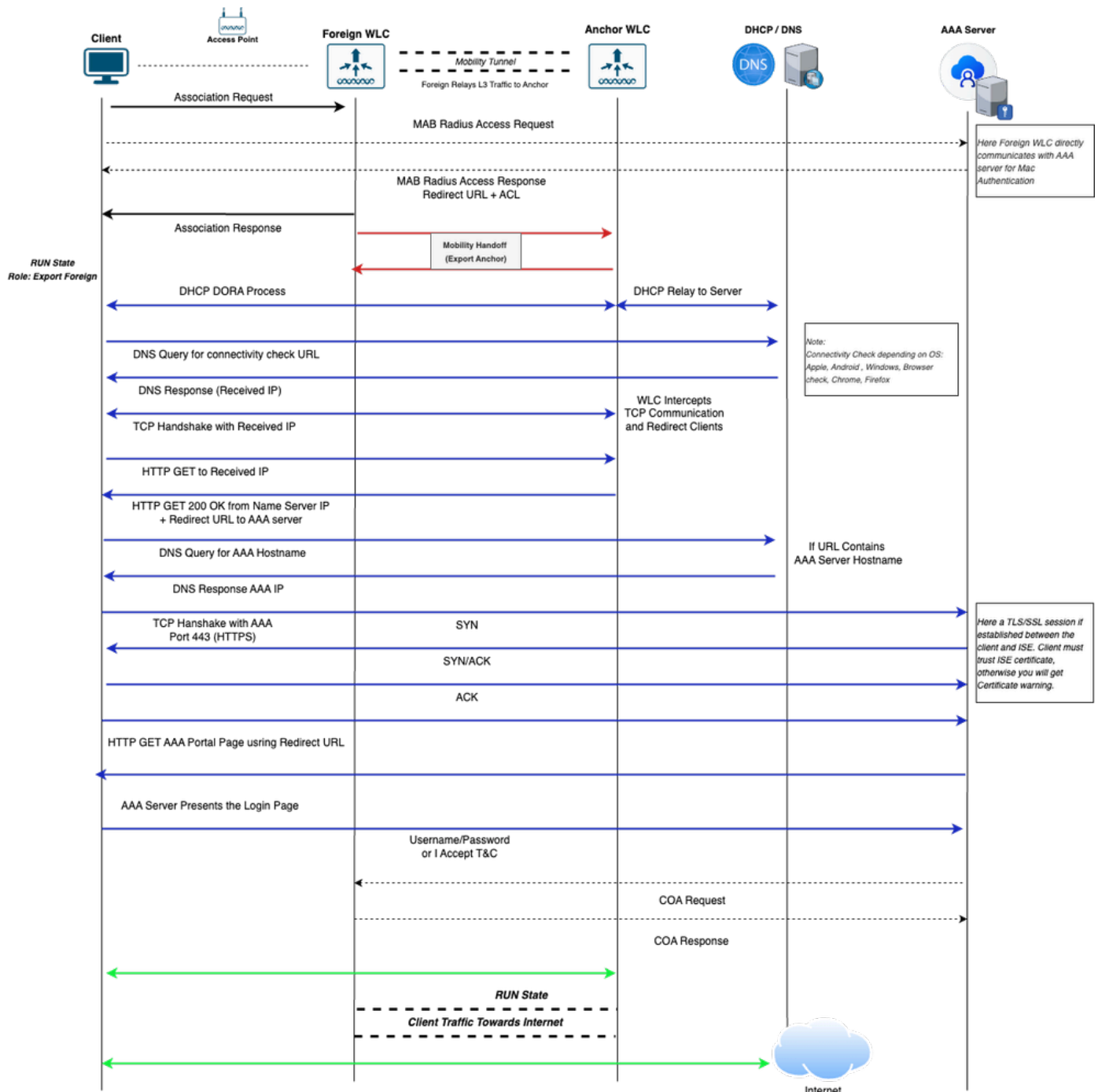
Client-Eigenschaften auf Anker

Zentrale Webauthentifizierung

Fluss für zentrale Webauthentifizierungs-SSID im Foreign-Anchor-Setup

1. Der Client sendet eine Zuordnungsanforderung für den SSID-Broadcast vom Foreign Wireless LAN Controller (WLC).
2. Der ausländische WLC führt eine MAC-Filterung durch, indem er eine Access-Request an den RADIUS-Server sendet. Der RADIUS-Server antwortet mit einem Access-Accept, das die erforderliche Redirect URL (URL) und Access Control List (ACL) enthält.
3. Der ausländische WLC sendet die Assoziationsantwort an den Client.
4. Der Client ist am Anchor WLC verankert. Der Client wechselt auf dem ausländischen WLC in den Status "RUN", und die Mobilitätsrolle wird auf "Export Foreign" festgelegt.
5. Der Client erhält eine IP-Adresse. Zu diesem Zeitpunkt verarbeitet der Anchor WLC den Umleitungsverkehr und leitet den Client an das Authentifizierungsportal weiter.
6. Nach der Umleitung kommuniziert der Client direkt mit dem RADIUS-Server. Dieser Datenverkehr wird über den Anker-WLC zum RADIUS-Server geleitet.

7. Der Client gibt Authentifizierungsdaten für den RADIUS-Server ein. Nach erfolgreicher Authentifizierung sendet der RADIUS-Server eine Change of Authorization (CoA)-Anfrage an den Foreign WLC.
8. Der ausländische WLC sendet eine CoA-Antwort an den RADIUS-Server. Der Client wechselt auf dem Anker-WLC in den RUN-Status, und die Rolle wird auf "Anker exportieren" festgelegt.
9. Der gesamte nachfolgende Client-Datenverkehr wird vom ausländischen WLC zum Anchor-WLC getunnelt, wo er das Netzwerk verlässt.



Client-Verbindungsverlauf für zentrale Webauth-SSID im Foreign-Anchor-Setup

Analyse des zentralen WebEth SSID-Datenflusses im Foreign-Anchor-Setup mithilfe von

Protokollen

In diesem Abschnitt wird der Verbindungsfluss der Client-Verbindung für die zentrale Web-Authentifizierungs-SSID unter Verwendung von Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) und des Client-Status auf dem Fremd- und dem Anker-Controller erläutert.

Protokolle von Foreign Controller

Radioaktive Spuren

!! Client Association Phase !!

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

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

!! MAC Authentication !!

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

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

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

{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authc_list: M

{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authz_list: M

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Airespace-WLAN-ID [1] 6 12
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Nas-Identifier [32] 16 ForeignSiteWLC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Started 5 sec timeout
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Received from id 1812/245 10.106.32.130:0, Access-A
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 19 Client_MAC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 37
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 31 url-redirect-ac1=REDIRECT_ACL
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 191
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 185 url-redirect=https://10.106.32
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat

{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB received an Access-Accept for
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC Processing MAB authentication resu
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_MA
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC dot11 send association response. Sending ass
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_MAB_PENDING
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (debug): MAC: Client_MAC L2 Authentication of station is su
{wncd_x_R0-0}{1}: [client-orch-sm] [17047]: (note): MAC: Client_MAC Mobility discovery triggered. Clie
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_L2.

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

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

```

```
{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
```

Paketerfassung

Der Client sendet eine Zuordnungsanforderung und führt eine MAC-Authentifizierung durch. Dieser Datenverkehr wird vom Foreign Controller verarbeitet.

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=.....

Client-Zuordnungsphase auf fremdem Controller mit drahtlosem MAB

Ein Mobility Handoff löst über Port UDP 16667 eine Mobility Handoff zwischen dem Foreign und dem Anchor Controller aus. Bei einem erfolgreichen Mobility Event wechselt der Client-Status zu RUN mit einer Export Foreign-Rolle.

Der Foreign Controller empfängt den DHCP-Datenverkehr des Clients über den CAPWAP-Tunnel und leitet ihn zur weiteren Verarbeitung an den Anchor Controller weiter.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 8, 2025 13:09:12...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	424	DHCP	0	DHCP Discover - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:12...	10.107.79.30	10.105.60.114	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0	DHCP Offer - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:14...	10.107.79.129,0.0.0.0	10.107.79.30,255.255...	452	DHCP	0	DHCP Request - Transaction ID 0x9f36b979
Jan 8, 2025 13:09:14...	10.107.79.30	10.105.60.114	428	UDP		16667 → 16667 Len=382
Jan 8, 2025 13:09:14...	10.105.60.114	10.107.79.30	400	UDP		16667 → 16667 Len=354
Jan 8, 2025 13:09:14...	10.107.79.30,10.105.60.69	10.107.79.129,10.105...	416	DHCP	0	DHCP ACK - Transaction ID 0x9f36b979

Client-DHCP-Datenverkehr, der auf einem ausländischen Controller empfangen wurde, wird über Mobility Tunnel an den Anker-Controller weitergeleitet

Ebenso sendet der Client über den CAPWAP-Tunnel den Status der Netzwerkverbindung und den Datenverkehr für die Überprüfung des Webseitenzugriffs an den ausländischen WLC. Der Foreign WLC leitet diese Nachricht über den Mobility Tunnel an den Anchor WLC weiter, wo der Anchor Controller den Datenverkehr abfängt oder verarbeitet.

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

Überprüfung des Netzwerkverbindungsstatus auf einem externen Controller

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

An Client gesendete URL umleiten

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

Clientzugriff auf die zentrale Webauthentifizierungsseite zur Bereitstellung von Authentifizierungsdetails

Der Foreign Controller verarbeitet die CoA-Anfrage nach erfolgreicher zentraler Web-Authentifizierung.

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

Autorisierungsänderung (COA) bei ausländischem Controller

Protokolle vom Anker-Controller

Radioaktive Spuren

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

!! Central Web Authentication Applied !!

```
{wncd_x_R0-0}{1}: [webauth-dev] [24229]: (info): Central Webauth URL Redirect, Received a request to cr
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]State Invalid State -> INIT
{wncd_x_R0-0}{1}: [epm-redirect] [24229]: (info): [0000.0000.0000:unknown] URL-Redirect = https://10.106.3
{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-act 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-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_
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
```

Paketerfassung

Nach der Mobility-Übergabe empfängt der Anchor Controller DHCP-Datenverkehr vom Foreign Controller über den Mobility-Tunnel.

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

Client-DHCP-Datenverkehr auf Anker-Controller vom ausländischen Controller empfangen

Der Anchor Controller empfängt Verbindungsprüfungen, Webseitenzugriffsanforderungen und Authentifizierungsdetails, um die Verarbeitung fortzusetzen.

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

Überprüfung des Netzwerkverbindungsstatus auf dem Anker-Controller

```
> 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)
```

An Client gesendete URL umleiten

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

Clientzugriff auf die Seite "Lokale Webauthentifizierung", um Authentifizierungsdetails bereitzustellen

Wenn die zentrale Webauthentifizierung erfolgreich war, wird eine Autorisierungsänderung (Change of Authorization, CoA) ausgelöst. Nach erfolgreicher CoA wechselt der Client in den Status "RUN" mit einer Export Anchor-Rolle.

Client-Status auf Fremd- und Ankercontroller

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1

10

1 - 1 of 1 clients

Kundenstatus im Ausland

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1

10

1 - 1 of 1 clients

Client-Status auf Anker

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

Clienteigenschaften in Fremdsprachen

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

Client-Eigenschaften auf Anker

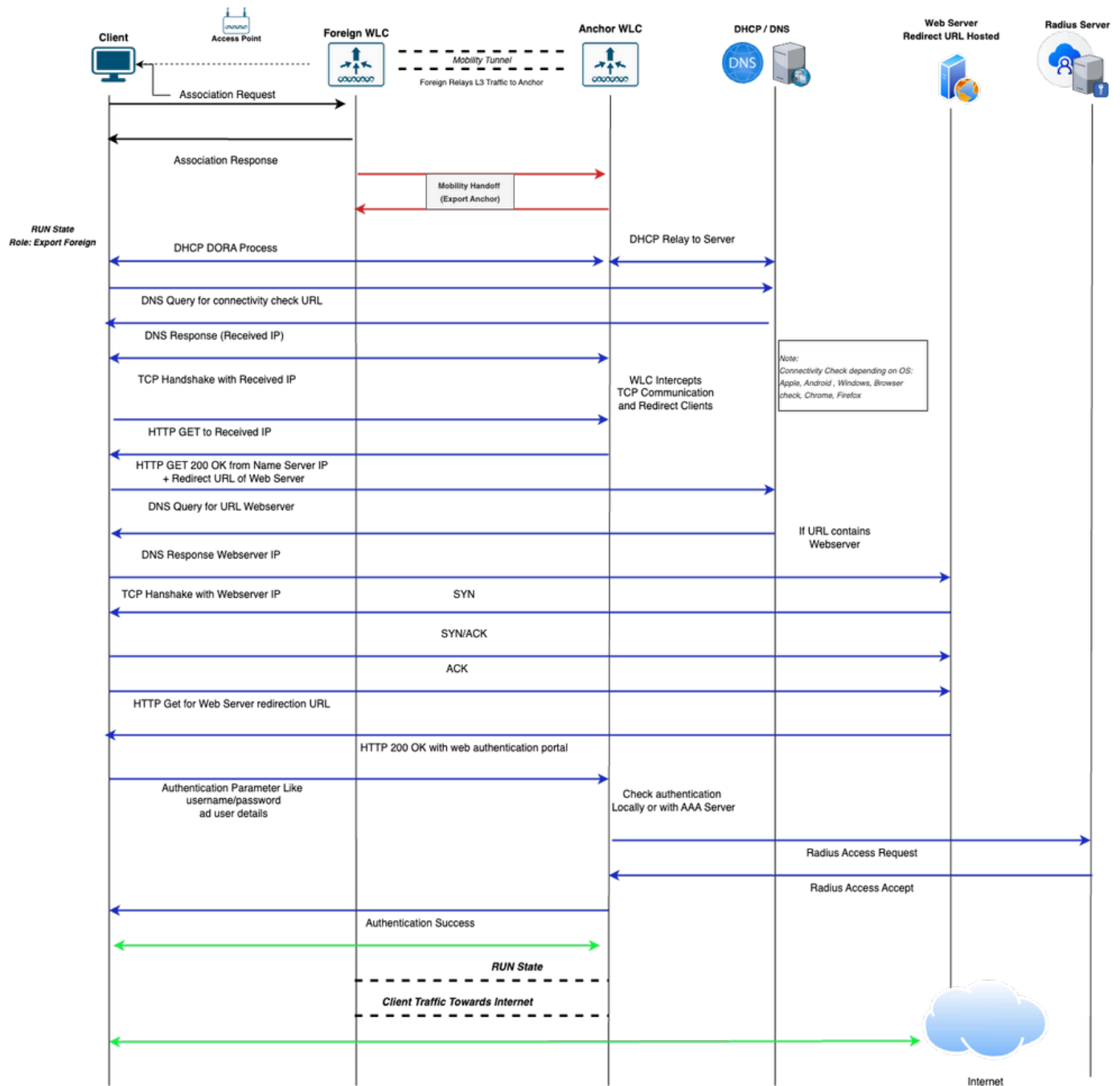
Externe Webauthentifizierung

Fluss für externe Webauthentifizierungs-SSID im Foreign-Anchor-Setup

1. Der Client stellt eine Verbindung mit dem vom ausländischen WLC ausgestrahlten SSID her.
2. Da keine Layer-2-Authentifizierung erforderlich ist, ist der Client am Anchor-WLC verankert. Der Client wechselt auf dem ausländischen WLC in den Status "RUN", wobei die Mobilitätsrolle als "Export Foreign" bezeichnet wird.
3. Der Client erhält eine IP-Adresse. Der Anchor-WLC fängt den Datenverkehr ab und leitet den Client wie in den Web-Authentifizierungsparametern definiert an das externe Webserver-Portal weiter.
4. Der Client sendet Authentifizierungsdaten über das Portal. Diese Anmeldeinformationen werden je nach konfigurierter Sicherheitsrichtlinie entweder lokal auf dem WLC oder über einen externen Authentifizierungsserver validiert.
5. Nach erfolgreicher Authentifizierung wechselt der Client auf dem Anchor-WLC in den RUN-

Status und übernimmt die Rolle "Export Anchor".

6. Nach erfolgreicher Authentifizierung wird der gesamte nachfolgende Client-Datenverkehr vom ausländischen WLC zum Anchor-WLC getunnelt, wo er in das Netzwerk eintritt.



Client-Verbindungsverlauf für externe Webauth-SSID im Foreign-Anchor-Setup

Analyse des externen Webauthentifizierungs-SSID-Datenflusses im Foreign-Anchor-Setup über Protokolle

In diesem Abschnitt wird der Verbindungsfluss der Clients für die externe Web-Authentifizierungs-SSID unter Verwendung von Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) und des Client-Status auf dem Fremd- und dem Anker-Controller erläutert.

Protokolle von Foreign Controller

Radioaktive Spuren

!! 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 Sending export_Anchor_req of XID (XID) to (
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_req, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RE
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Request successfully proce
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Sending export_Anchor_req of XID (176282)
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Received export_Anchor_rsp, sub type 0 o
{mobilityd_R0-0}{1} [mm-transition] [18401] (info) MAC Client-MAC MMFSM transition S_MC_WAIT_EXP_ANC_RS
{mobilityd_R0-0}{1} [mm-client] [18401] (debug) MAC Client-MAC Export Anchor Response successfully proc
[mobilityd_R0-0]{1} [epm-misc] [17047] (info) Anchor Vlan-id 31 processed[mobilityd_R0-0]{1} [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 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
```

```
{wnacd_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:
```

Paketerfassung

Der Client sendet eine Zuordnungsanforderung, die vom Foreign Controller verarbeitet wird.

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=.....

Clientzuordnungsphase mit ausländischem Controller

Ein Mobility Handoff löst über Port UDP 16667 eine Mobility Handoff zwischen dem Foreign und dem Anchor Controller aus. Bei einem erfolgreichen Mobility Event wechselt der Client-Status zu RUN mit einer Export Foreign-Rolle.

Der Foreign Controller empfängt den DHCP-Datenverkehr des Clients über den CAPWAP-Tunnel und leitet ihn zur weiteren Verarbeitung an den Anchor Controller weiter.

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

Client-DHCP-Datenverkehr, der auf einem ausländischen Controller empfangen wurde, wird über Mobility Tunnel an den Anker-Controller weitergeleitet

Ebenso sendet der Client über den CAPWAP-Tunnel den Status der Netzwerkverbindung und den Datenverkehr für die Überprüfung des Webseitenzugriffs an den ausländischen WLC. Der Foreign WLC leitet diese Nachricht über den Mobility Tunnel an den Anchor WLC weiter, wo der Anchor Controller den Datenverkehr abfängt oder verarbeitet.

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

Überprüfung des Netzwerkverbindungsstatus auf einem externen Controller

```
> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco_08:00:06:00:00:00, Dst: Cisco_08:00:06:00:00:00
> 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)
```

An Client gesendete URL umleiten

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	UDP	0	62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 1180]
Jan 14, 2025 16:19:11...	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	683	TLSv1..	0	Client Hello
Jan 14, 2025 16:19:11...	10.107.79.30	10.105.60.114	659	UDP	16667	→ 16667 Len=613
Jan 14, 2025 16:19:11...	10.107.79.30	10.105.60.114	1342	UDP	16667	→ 16667 Len=1296
Jan 14, 2025 16:19:11...	10.105.60.114	10.107.79.30	450	UDP	16667	→ 16667 Len=404
Jan 14, 2025 16:19:11...	10.105.60.114	10.107.79.30	917	UDP	16667	→ 16667 Len=871
Jan 14, 2025 16:19:11...	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	1378	TCP	0	8443 → 62448 [ACK] Seq=1 Ack=1798 Win=33280 Len=1250 [TCP PDU reassembled in 1192]
Jan 14, 2025 16:19:11...	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	933	TLSv1..	0	Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 14, 2025 16:19:11...	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [ACK] Seq=1798 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11...	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	143	TLSv1..	0	Alert (Level: Fatal, Description: Certificate Unknown)
Jan 14, 2025 16:19:11...	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [FIN, ACK] Seq=1805 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11...	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	262	TLSv1..	0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 14, 2025 16:19:11...	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11...	10.105.60.114	10.107.79.30	118	UDP	16667	→ 16667 Len=72
Jan 14, 2025 16:19:11...	10.105.60.114	10.107.79.30	157	UDP	16667	→ 16667 Len=111
Jan 14, 2025 16:19:11...	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	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

Clientzugriff auf externe Webauthentifizierungsseite zur Bereitstellung von Authentifizierungsdetails

Protokolle vom Anker-Controller

Radioaktive Spuren

!! 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
```

!! 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
□{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 31S
{wncd_x_R0-0}{1}: [sisf-packet] [24229]: (info): TX: IPv6 DHCP from intf mobility_a0000001 on vlan 31S
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62480/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62481/239
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]GET rcv
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]HTTP GE
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Parse G
{wncd_x_R0-0}{1}: [sadb-attr] [24229]: (info): Removing ipv6 addresses from the attr list -654303708,sm
{wncd_x_R0-0}{1}: [caaa-authen] [24229]: (info): [CAAA:AUTHEN:910007e3] NULL ATTR LIST
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]State L
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Send Access-Request to 10.106.32.130:1812 id 0/3, 1
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Calling-Station-Id [31] 19 Client_MAC
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: User-Name [1] 9 Test321
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 49
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 43 audit-session-id=723C690A000007
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Framed-IP-Address [8] 6 10.105.60.254
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 12 vlan-id=31
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-IP-Address [4] 6 10.105.60.114
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-Port-Type [61] 6 Virtual [5]
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: NAS-Port [5] 6 0
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 31
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 25 cisco-wlan-ssid=DMZ_EWA
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 33
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 27 wlan-profile-name=DMZ_EWA
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Called-Station-Id [30] 27 Called-Station-ID
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Airespace [26] 12
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Airespace-WLAN-ID [1] 6 7
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Nas-Identifier [32] 12 DMZSiteWLC
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Started 5 sec timeout
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Received from id 1812/3 10.106.32.130:0, Access-Acc
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: User-Name [1] 9 Test321
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [24229]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat
{wncd_x_R0-0}{1}: [radius] [24229]: (info): Valid Response Packet, Free the identifier
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]State A
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Unapply I
{wncd_x_R0-0}{1}: [webauth-ac1] [24229]: (info): mobility_a0000001[Client_MAC][10.105.60.254]Unapply I
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : username 0 Test321
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : class 0 43 41 43 53 3a 37 32 33
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : Message-Authenticator 0 <hidden>
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : method 0 1 [webauth]
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : clid-MAC-addr 0 d0 37 45 88 25 5
{wncd_x_R0-0}{1}: [aaa-attr-inf] [24229]: (info): Applying Attribute : intf-id 0 2684354561 (0xa0000001)
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n

```

{wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [24229]: (info): [Client_MAC:mobility_a0000001] SM Notified attr
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Received User-Name Test321
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Method webauth changing st
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] auth mgr attr add/change n
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Raised event AUTHZ_SUCCESS
{wncd_x_R0-0}{1}: [auth-mgr] [24229]: (info): [Client_MAC:mobility_a0000001] Context changing state fro
{wncd_x_R0-0}{1}: [webauth-sess] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Param-ma
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Param-m
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]State A
{wncd_x_R0-0}{1}: [webauth-page] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]Sending V
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-io] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62482/238
{wncd_x_R0-0}{1}: [webauth-httpd] [24229]: (info): mobility_a0000001[Client_MAC][ 10.105.60.254]62482/2
{wncd_x_R0-0}{1}: [client-auth] [24229]: (note): MAC: Client_MAC L3 Authentication Successful. ACL:[]
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_L3.

{wncd_x_R0-0}{1}: [mm-transition] [24229]: (info): MAC: Client_MAC MMIF FSM transition: S_MA_ANCHOR ->
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff, sub type: 0 of
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff base check is VALID
{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [26021]: (info): MAC: Client_MAC Forwarding aaa_handoff, sub type: 0 o
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Sending aaa_handoff of XID (38840) t
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff successfully forwarded.
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC Received aaa_handoff_ack, sub type:
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC AAA Handoff Ack successfully handled
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack base check is VALID
{mobilityd_R0-0}{1}: [mm-client] [26021]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [26021]: (info): MAC: Client_MAC MMFSM transition: S_MC_ANCHOR_WAI

```

Paketerfassung

Nach der Mobility-Übergabe empfängt der Anchor Controller DHCP-Datenverkehr vom Foreign Controller über den Mobility-Tunnel.

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

Client-DHCP-Datenverkehr auf Anker-Controller von ausländischem Controller empfangen

Der Anchor Controller empfängt Verbindungsprüfungen, Webseitenzugriffsanforderungen und Authentifizierungsdetails, um die Verarbeitung fortzusetzen.

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

Überprüfung des Netzwerkverbindungsstatus auf dem Anker-Controller

```
> 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)
```

An Client gesendete URL umleiten

Der Client sendet Authentifizierungsdaten über das Portal. Diese Anmeldeinformationen werden je nach konfigurierter Sicherheitsrichtlinie entweder lokal auf dem WLC oder über einen externen Authentifizierungsserver validiert.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	66	TCP		62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	70	TCP		8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	659	UDP		16667 → 16667 Len=613
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1342	UDP		16667 → 16667 Len=1296
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1304	TCP		62449 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 717]
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	537	TLSv1..		Client Hello
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1308	TCP		8443 → 62449 [ACK] Seq=1 Ack=1734 Win=34688 Len=1250 [TCP PDU reassembled in 724]
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	446	UDP		16667 → 16667 Len=404
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	863	TLSv1..		Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	913	UDP		16667 → 16667 Len=871
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62449 → 8443 [ACK] Seq=1734 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	180	TLSv1..		Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	64	TLSv1..		Change Cipher Spec
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	103	TLSv1..		Encrypted Handshake Message
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	114	UDP		16667 → 16667 Len=72
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	153	UDP		16667 → 16667 Len=111
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62449 → 8443 [ACK] Seq=1860 Ack=2107 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1119	UDP		16667 → 16667 Len=1073
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1061	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1015	TLSv1..		Application Data
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	962	UDP		16667 → 16667 Len=920
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1144	UDP		16667 → 16667 Len=1098
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1086	TLSv1..		Application Data
Jan 14, 2025 16:19:25...	10.105.60.114	10.106.32.130	460	RADIUS		Access-Request id=3
Jan 14, 2025 16:19:25...	10.105.60.114	10.106.32.130	460	RADIUS		Access-Request id=3, Duplicate Request
Jan 14, 2025 16:19:25...	10.106.32.130	10.105.60.114	191	RADIUS		Access-Accept id=3
Jan 14, 2025 16:19:25...	10.106.32.130	10.105.60.114	187	RADIUS		Access-Accept id=3, Duplicate Response

Clientzugriff auf externe Webauthentifizierungsseite zur Bereitstellung von Authentifizierungsdetails

Client-Status auf Fremd- und Ankercontroller

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

Kundenstatus im Ausland

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]	0	DMZ_EWA	7	WLAN	Run	N/A	Test321	N/A	Export Anchor	No

1 - 1 of 1 clients

Client-Status auf Anker

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

Clienteigenschaften in Fremdsprachen

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

Client-Eigenschaften auf Anker

Lastenausgleich zwischen mehreren Anker-Controllern

Wenn einem WLAN mehrere Anker-Controller zugeordnet sind, hängt die Verteilung des Datenverkehrs von der Priorität ab. Es können drei Prioritätsebenen konfiguriert werden: Primary, Secondary und Tertiary. Die Guest Anchor Priority-Funktion ermöglicht die Verteilung der Last im aktiven/Standby-Modus auf die Anchor-Controller. Dies wird erreicht, indem jedem Anker-Controller eine feste Priorität zugewiesen wird: Die Last wird auf den Controller mit der höchsten Priorität verteilt, und zwar nach dem Round-Robin-Verfahren auf Controller mit demselben Prioritätswert.

⚠ 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) ▼	←
---	----------------	---

Ankerpriorität zuordnen



Anmerkung: Standardmäßig wird die tertiäre Priorität während der Ankercontroller-Zuordnung auf dem Fremdcontroller konfiguriert.

Fehlerbehebung bei Client-Verbindungen im Foreign-Anchor-Szenario

1. Probleme bei der Client-Integration

- i. Tunnelstatus: Überprüfen Sie, ob der Mobilitätstunnel zwischen dem Fremd- und dem Anker-Controller aktiv bleibt.
- ii. Konfigurationskonflikt: Stellen Sie sicher, dass die Konfiguration auf beiden Controllern gleich ist. Abweichungen bei WLAN-Namen, Richtlinienprofilnamen oder erweiterten Einstellungen, wie z. B. AAA-Übersteuerung, IPv4-DHCP-Anforderungen und NAC, führen zu Profilfehlern oder Anker-Ablehnungsfehlern.
- iii. Andere: Wenn der Tunnel ohne Konfigurationsprobleme hochgefahren ist, ähnelt die Fehlerbehebung dem normalen Verbindungsproblem des Clients. Dabei wird sichergestellt, dass der jeweilige Controller überprüft wird, der den betroffenen Datenverkehr verarbeitet.

2. Unterbrechungsfreie Verbindungen

- i. Tunnelklappen: Wenn die Keepalive-Pakete zwischen den beiden Controllern nicht ankommen, flappert der Tunnel, sodass der Client keine Verbindung zum SSID aufrechterhalten kann.
- ii. Geringe Bandbreite: Wenn die Path-MTU (PMTU) zwischen den Mobility-Peers auf einen niedrigeren Wert (576) fällt, wird die Leistung der Clients beeinträchtigt. Dies geschieht in der Regel, wenn die Pfad-MTU-Keepalive-Nachrichten zwischen den beiden Mobility-Peers verpasst werden.



Anmerkung: Der Controller mit der niedrigeren MAC-Adresse für die Mobilität initiiert sowohl die Standard-Keepalive- als auch die Path-MTU-Keepalive-Meldungen.

3. Spezifische Probleme beim Zugriff auf Websites

- i. Zu den Headern für den Mobilitätsdatenverkehr gehören Mobilitätsgruppen-IDs, MAC-Adressen, IP-Adressen und verschlüsselte CAPWAP DTLS-Pakete, die über die UDP-Ports 16666 und 16667 ausgetauscht werden. Dieser Overhead wird dem vorhandenen CAPWAP-Header hinzugefügt. Bei TCP-Datenverkehr erfolgt die Nachanpassung der für den Access Point konfigurierten TCP-MSS, wenn die Paketgröße aufgrund dieses zusätzlichen Overheads die Mobility PMTU (maximal 1385 Byte) überschreitet. Die Fragmentierung wird zwar im Allgemeinen vom Netzwerk behandelt, es treten jedoch Probleme auf, wenn Pakete nicht mehr in der richtigen Reihenfolge oder verspätet eintreffen. Diese Bedingungen wirken sich auf die Zusammenfügung von Paketen aus und führen zu Fehlern bei der Datenzugriffsmöglichkeit für bestimmte Websites.

Protokollerfassung vom Fremd- und Ankercontroller

1. Aktivieren Sie `term exec prompt timestamp`, um einen Zeitverweis für alle Befehle zu erhalten.
2. Verwenden Sie `show tech-support wireless !!`, um die Konfiguration zu überprüfen.
3. Sie können den Status des Mobility-Tunnels überprüfenÜbersicht zur Wireless-Mobilität anzeigen !!
4. Statistiken für Mobility Peer, einschließlich Verbindungsstatus, Client-Daten und Ereignisse, Keep-Alive-Statistiken zeigen Wireless Mobility Peer IP <IP>.
5. Aktivieren Sie die radioaktive Spur für die IP-/MAC-Adresse des Mobility Peers und die MAC-Adresse des Clients.

Über CLI:

```
debugging wireless {MAC | ip} {aaa.bbb.cccc} | x.x.x.x } {Überwachungszeit} {N Sekunden} !!
```

Die Einstellung der Zeit erlaubt es uns, Traces für bis zu 24 Tage zu aktivieren.

Kein Debugging Wireless {MAC | ip} {aaa.bbb.cccc} | x.x.x !! So deaktivieren Sie das Debuggen

WLC generiert eine Debugablaufverfolgungsdatei mit dem Befehl Client_info, um zu überprüfen, ob die Debugablaufverfolgungsdatei generiert wurde dir bootflash: | i debug !!



Warnung: Das bedingte Debugging ermöglicht die Protokollierung auf Debugebene, wodurch sich wiederum die Menge der generierten Protokolle erhöht. Wenn Sie diese Option aktivieren, wird der Zeitaufwand für das Anzeigen von Protokollen reduziert. Daher wird empfohlen, das Debuggen immer am Ende der Fehlerbehebungssitzung zu deaktivieren.

6. Führen Sie die folgenden Befehle aus, um das Debuggen vollständig zu deaktivieren:

klare Plattformbedingung alle !!

underbug all !!

Über GUI:

Schritt 1: Navigieren Sie zu Fehlerbehebung > Radioaktive Verfolgung.

Schritt 2: Klicken Sie auf Hinzufügen und geben Sie eine Mobility Peer-MAC/IP-Adresse oder eine Client-MAC-Adresse ein, die Sie beheben möchten.

Schritt 3. Wenn Sie bereit sind, die radioaktive Verfolgung zu starten, klicken Sie auf Starten. Nach dem Start wird die Debug-Protokollierung für jede Verarbeitung auf der Steuerungsebene in Bezug auf die verfolgten MAC-Adressen auf die Festplatte geschrieben.

Schritt 4: Wenn Sie das Problem reproduzieren, das Sie beheben möchten, klicken Sie auf Beenden.

Schritt 5: Für jede debuggte MAC-Adresse können Sie eine Protokolldatei generieren, in der alle Protokolle für diese MAC-Adresse aufgelistet sind. Klicken Sie dazu auf Generate (Generieren).

Schritt 6. Wählen Sie aus, wie lange die sortierte Protokolldatei zurückgehen soll, und klicken Sie auf Auf Gerät anwenden.

Schritt 7. Sie können die Datei jetzt herunterladen, indem Sie auf das kleine Symbol neben dem Dateinamen klicken. Diese Datei befindet sich im Boot-Flash-Laufwerk des Controllers und kann auch über die CLI kopiert werden.

7. Eingebettete Aufzeichnungen

Über CLI:

MYCAP klar erfassen !!

MYCAP-Schnittstelle Po1 beide überwachen !!

MYCAP-Puffergröße 100 !! überwachen

monitor capture MYCAP match access-list name !! (if tracking mobility tunnel traffic between WLC)

MYCAP-Übereinstimmung überwachen any/ipv4/ipv6.MAC !!
MYCAP Start überwachen !!
!!Vervielfältigen
MYCAP-Stopp überwachen
MYCAP-Exportflash überwachen:|tftp:|http:.../filename.pcap

Über GUI:

Schritt 1: Navigieren Sie zu Fehlerbehebung > Paketerfassung > + Hinzufügen.
Schritt 2: Definieren Sie den Namen der Paketerfassung. Es sind maximal 8 Zeichen zulässig.
Schritt 3: Definieren Sie ggf. Filter.
Schritt 4: Aktivieren Sie das Kontrollkästchen zur Überwachung des Kontrollverkehrs, wenn der Datenverkehr zur System-CPU geleitet und zurück in die Datenebene geleitet werden soll.
Schritt 5: Puffergröße definieren. Es sind maximal 100 MB zulässig.
Schritt 6: Definieren Sie eine Grenze, entweder nach Dauer, die einen Bereich von 1 - 1000000 Sekunden erlaubt, oder nach Anzahl der Pakete, die einen Bereich von 1 - 100000 Paketen erlaubt, wie gewünscht.
Schritt 7: Wählen Sie die Schnittstelle aus der Liste der Schnittstellen in der linken Spalte, und klicken Sie auf den Pfeil, um sie in die rechte Spalte zu verschieben.
Schritt 8: Klicken Sie auf Speichern und auf Gerät anwenden.
Schritt 9: Um die Erfassung zu starten, wählen Sie Starten.
Schritt 10. Sie können die Erfassung bis zum definierten Limit laufen lassen. Um die Erfassung manuell zu stoppen, wählen Sie Stopp.
Schritt 11: Nach dem Beenden steht eine Schaltfläche "Exportieren" zur Verfügung, auf die Sie mit der Option klicken können, die Erfassungsdatei (.pcap) über den HTTP- oder TFTP-Server oder den FTP-Server oder die Festplatte oder den Flash des lokalen Systems auf den lokalen Desktop herunterzuladen.

Zugehörige Informationen

[Konfiguration von Mobilitätstopologien auf Catalyst 9800 WLCs](#)

[Konfigurieren der Mobilitätsfunktion von WLAN Anchor auf dem Catalyst 9800](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.