

Verkeersstroom in buitenlandse ankeropstelling tussen 9800 WLC begrijpen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht van Foreign-Anchor Scenario](#)

[Topologie](#)

[WLAN met Layer 2-verificatie](#)

[Configuratievereiste](#)

[Flow voor Layer 2 SSID op basis van externe ankers](#)

[Layer 2 SSID-stroom analyseren in configuratie met vreemde ankers via logs](#)

[Logboeken van buitenlandse controller](#)

[Logs van de 9800-controller voor anker](#)

[Cliëntstatus op zowel buitenlandse als ankercontroller](#)

[WLAN met Layer 3-verificatie](#)

[Lokale webverificatie](#)

[Flow voor lokale website-SSID in buitenlandse ankerinstellingen](#)

[Analyseren van lokale webgebaseerde SSID-stroom in buitenlandse ankerinstellingen via logboeken](#)

[Logboeken van buitenlandse controller](#)

[Logboeken van de ankercontroller](#)

[Cliëntstatus op zowel buitenlandse als ankercontroller](#)

[Centrale webverificatie](#)

[Flow voor centrale webgebaseerde SSID in buitenlandse ankerinstellingen](#)

[Centrale webgebaseerde SSID-stroom analyseren in configuratie met buitenlandse ankers via logboeken](#)

[Logboeken van buitenlandse controller](#)

[Logboeken van de ankercontroller](#)

[Cliëntstatus op zowel buitenlandse als ankercontroller](#)

[Externe webverificatie](#)

[Flow voor externe website-SSID in buitenlandse ankerinstellingen](#)

[Externe webgebaseerde SSID-stroom analyseren in configuratie met buitenlandse ankers via logboeken](#)

[Logboeken van buitenlandse controller](#)

[Logboeken van de ankercontroller](#)

[Cliëntstatus op zowel buitenlandse als ankercontroller](#)

[taakverdeling tussen meerdere ankercontrollers](#)

[Problemen oplossen met clientconnectiviteit in scenario met buitenlandse ankers](#)

[Logboekverzameling van buitenlandse en ankercontroller](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de verkeersstroom beschreven in de configuratie van Foreign-Anchor tussen Cisco 9800 WLC's, waarbij de onboarding en probleemoplossing van de L2/L3-client wordt behandeld.

Voorwaarden

Mobiliteitstunnel tussen buitenlandse en ankercontroller.

UDP-poort 16666 en 16667 toegestaan tussen beide WLC.

Beleidsprofiel geconfigureerd voor centrale switching.

Configuration > Wireless > Mobility

Global ConfigurationPeer Configuration

Mobility Peer Configuration

AddDeleteRefresh

	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

110

1 - 2 of 2 items

Mobiliteitstunnelstatus op buitenlandse WLC

Configuration > Wireless > Mobility

Global ConfigurationPeer Configuration

Mobility Peer Configuration

AddDeleteRefresh

	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

110

1 - 2 of 2 items

Status van mobiliteitstunnel op WLC-anker

Vereisten

Cisco raadt u aan om kennis te hebben van deze onderwerpen:

- Toegang tot de draadloze controllers via de Command Line Interface (CLI) of de grafische gebruikersinterface (GUI)
- Mobiliteit op draadloze LAN-controllers (WLC's) van Cisco
- 9800 draadloze controllers
- Radioactieve sporen en pakketopname op 9800 WLC

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 9800 Model WLC
- Cisco IOS XE 17.15.5-versie
- 9100 reeks AP Model

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

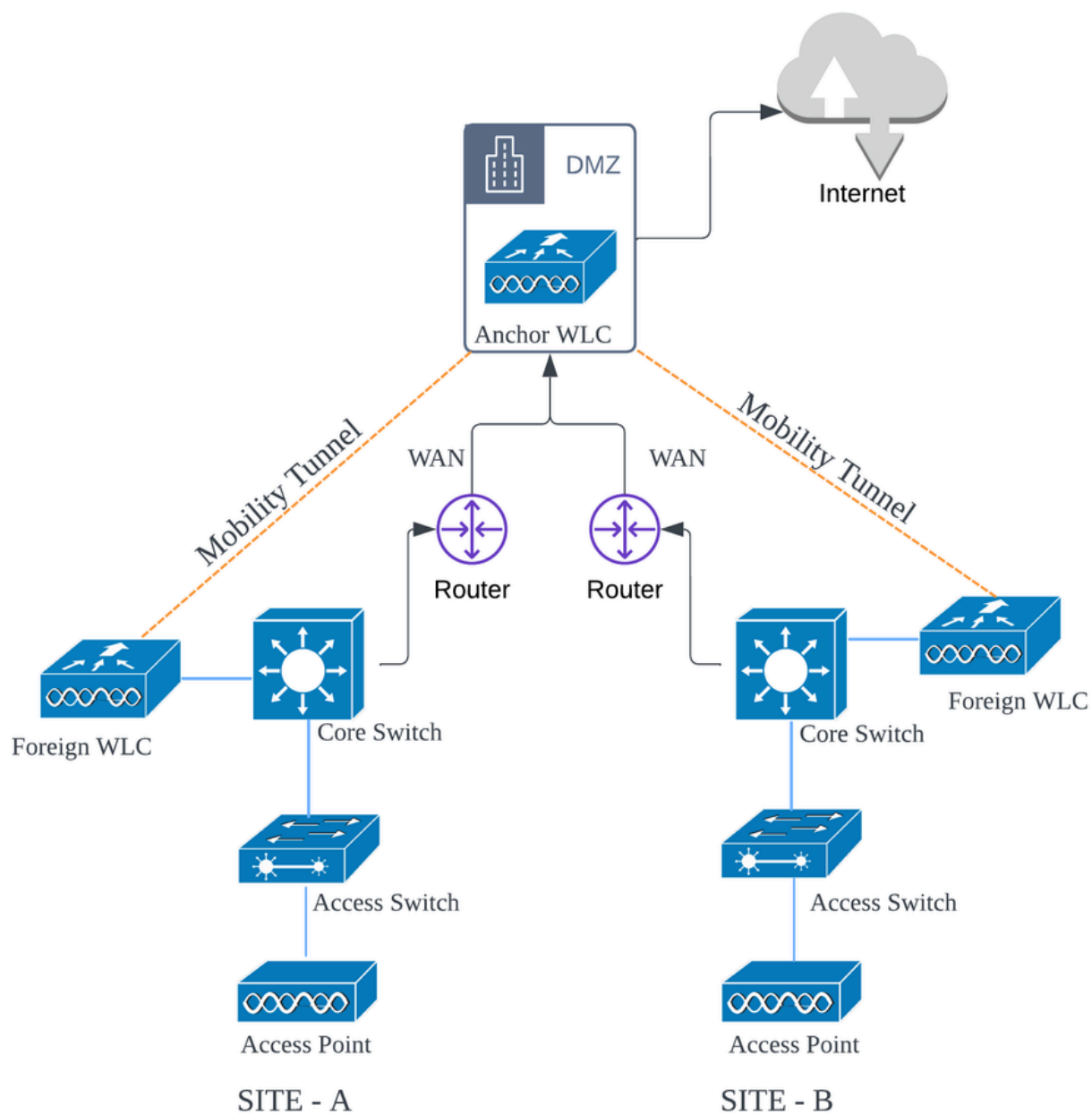
Overzicht van Foreign-Anchor Scenario

- Foreign Controller: Deze WLC beheert Layer 2 of de draadloze kant van het netwerk. Er zijn toegangspunten op aangesloten en al het clientverkeer voor de verankerde WLAN's wordt ingekapseld in de mobiliteitstunnel en naar de ankercontroller verzonden. Het verkeer wordt niet lokaal afgesloten op de Foreign Controller.
- Anchor Controller: Dit dient als het Layer 3-afsluitpunt. Het ontvangt clientverkeer via de mobiliteitstunnel van de Foreign Controllers en decapsuleert of beëindigt het clientverkeer naar het uitgangspunt (VLAN). Dit is waar klanten worden gezien in het netwerk.

Toegangspunten op de Foreign WLC zenden de WLAN-SSID's uit en hebben een beleidstag toegewezen die het WLAN-profiel koppelt aan het juiste beleidsprofiel. Wanneer een draadloze client verbinding maakt met deze SSID, verzendt de Foreign Controller zowel de SSID-naam als het beleidsprofiel als onderdeel van de clientgegevens naar de WLC-verankering. Na ontvangst controleert de WLC Anchor zijn eigen configuratie om te voldoen aan de SSID-naam en de naam van het beleidsprofiel. Zodra het WLC-ankerpunt een overeenkomst heeft gevonden, past het de bijbehorende configuratie toe en biedt het een afsluitpunt voor de draadloze client. Daarom is het

verplicht dat de namen en configuraties van de WLAN- en beleidsprofielen overeenkomen op de WLC's Foreign en Anchor 9800, met uitzondering van het VLAN onder het beleidsprofiel.

Topologie



Opstelling voor buitenlands anker tussen 9800 WLC

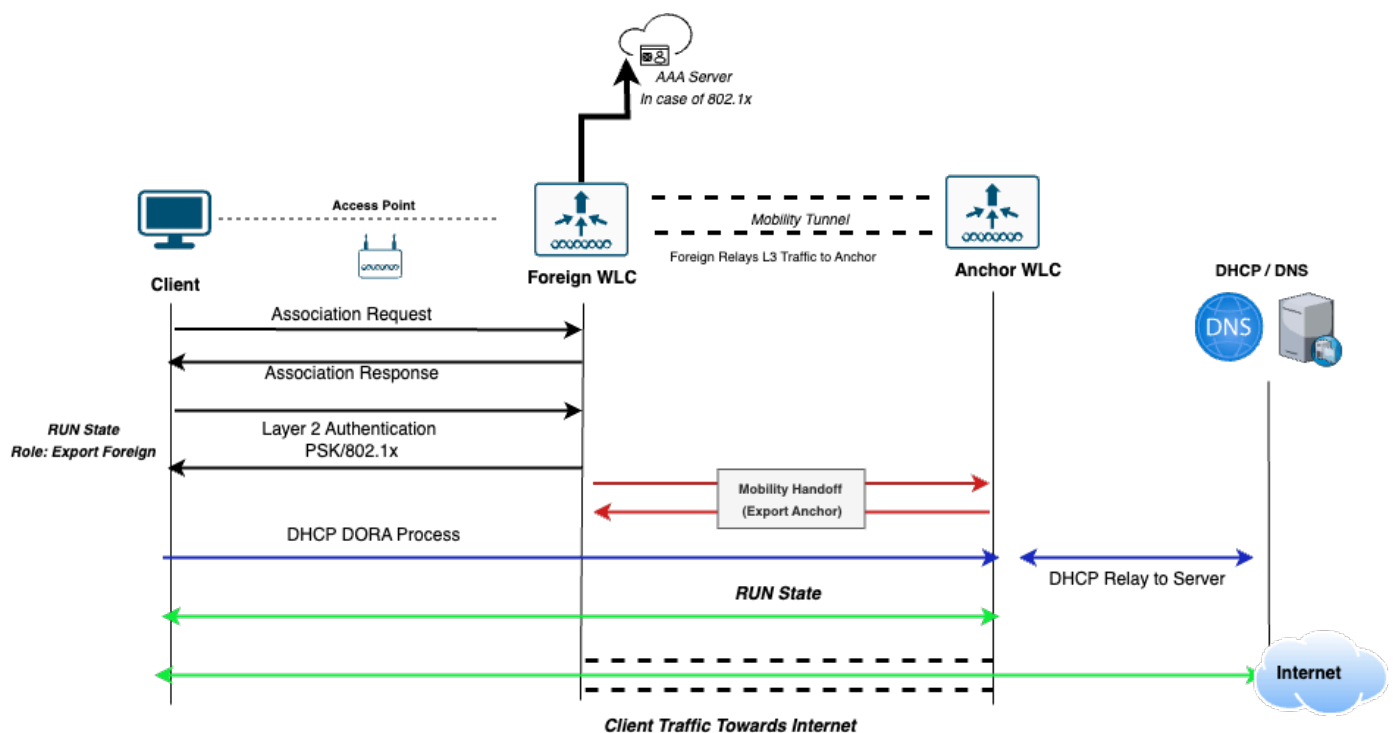
WLAN met Layer 2-verificatie

Configuratievereiste

1. Zorg ervoor dat de WLAN-naam en -configuratie identiek zijn op zowel de Foreign als Anchor WLC's en dat deze zijn geconfigureerd voor Layer 2-verificatie (PSK of 802.1x).
2. Maak een beleidsprofiel met dezelfde naam op de WLC's voor Buitenlandse en Anker met dezelfde configuratie.
3. Configureer op de Foreign WLC de WLC-toewijzing voor ankers in het respectieve beleidsprofiel.
4. Configureer op de WLC Anker het beleidsprofiel om de controller aan te wijzen als een exportanker.
5. Koppel het WLAN op de Foreign WLC aan het juiste beleidsprofiel met behulp van een beleidstag.

Flow voor Layer 2 SSID op basis van externe ankers

1. De client initieert een verbinding met de SSID die wordt uitgezonden door de Foreign WLC. De Foreign WLC voert Layer 2-verificatie uit en valideert referenties lokaal of via een externe AAA-server, afhankelijk van het geconfigureerde beveiligingsbeleid.
2. Na succesvolle verificatie is de cliensessie verankerd in de WLC voor anker. De client krijgt een IP-adres toegewezen en gaat over naar de status RUN op de WLC voor anker.
3. Zodra de sessie is ingesteld, wordt al het clientgegevensverkeer van de Foreign WLC naar de Anchor WLC geleid, waar het naar het netwerk wordt geleid.



Layer 2 Foreign Anchor Based WLAN Flow Diagram

In dit gedeelte wordt de stroom van Layer 2-clientconnectiviteit uitgelegd met behulp van Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) en de status van de client op zowel de buitenlandse als de ankercontrollers.

radioactieve sporen

Packet capture

De client stuurt een associatieverzoek en voert Layer 2-verificatie uit, die wordt afgehandeld door de Foreign Controller.

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

Clientkoppeling + Layer 2-verificatieverkeer

Een mobiliteitsafgifte tussen de Foreign en Anchor Controllers via UDP-poort 16667. Na een succesvol mobiliteitsevenement gaat de cliëntstatus over naar RUN met een rol in Export Foreign. De Foreign Controller ontvangt het DHCP-verkeer van de klant via de CAPWAP-tunnel en stuurt het door naar de Anchor Controller voor verdere verwerking.

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

DHCP-clientverkeer ontvangen op buitenlandse controller wordt doorgestuurd naar ankercontroller met behulp van mobiliteitstunnel

Logs van de 9800-controller voor anker

Radioactieve sporen van anker

!! 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
[wnacd_x_R0-0]{1} [mm-client] [24229] (info) MAC Client-MAC Roam type changed - None -> L3 Requested
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Export Anchor Response successfully processed
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Forwarding Anchor Response to Foreign.
{mobilityd_R0-0}{1} [mm-client] [26021] (info) MAC Client-MAC Forwarding export_Anchor_rsp, sub type 0 of 1
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.
[wnacd_x_R0-0]{1} [mm-client] [24229] (info) MAC Client-MAC Mobility role changed - Unassoc -> Export Anchor
{mobilityd_R0-0}{1} [mm-client] [26021] (debug) MAC Client-MAC Client is Anchored.>> Client is successfully
```

!! Client DHCP Traffic !!

```
{wnacd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_MOBILITY
{wnacd_x_R0-0}{1} [client-orch-state] [24229] (note) MAC Client-MAC Client state transition S_CO_DPATH_P
{wnacd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wnacd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MAC
{wnacd_x_R0-0}{1} [sisf-packet] TX DHCPv4 from interface Tw0/0/1 on vlan 31 Src MAC DHCP-Reply-Source-MAC
{wnacd_x_R0-0}{1} [sisf-packet] RX DHCPv4 from interface mobility_a0000001 on vlan 31 Src MAC Client-MAC
{wnacd_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
```

Pakketvastlegging op anker

Na de mobiliteitsoverdracht ontvangt de Anchor Controller DHCP-verkeer van de Foreign Controller via de mobiliteitstunnel.

Na voltooiing van het DORA-proces komt de client in de STATUS RUN met een rol voor Exportanker. Vanaf dit punt dient de ankercontroller als het afsluitpunt voor clientgegevensverkeer.

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

DHCP-clientverkeer op ankercontroller ontvangen van buitenlandse controller

Clientstatus op zowel buitenlandse als ankercontroller

Monitoring > Wireless > Clients

Clients

Sleeping Clients

Excluded Clients

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐		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

Clientstaat op buitenlands

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1

10

1 - 1 of 1 clients

Clientstatus voor 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

802.11 ac Wave 2

Wi-Fi to Cellular Steering

Not implemented

Cellular Capability

N/A

Regular ASR support

DISABLED

Mobility

Anchor IP Address

10.105.60.114

Point of Presence

0xA0000003

AuthC Status

False

Move Count

0

Role

Export Foreign

Roam Type

L3 Requested

Complete Timestamp

01/03/2025 13:06:37 India

Klanteigenschappen op buitenlands

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

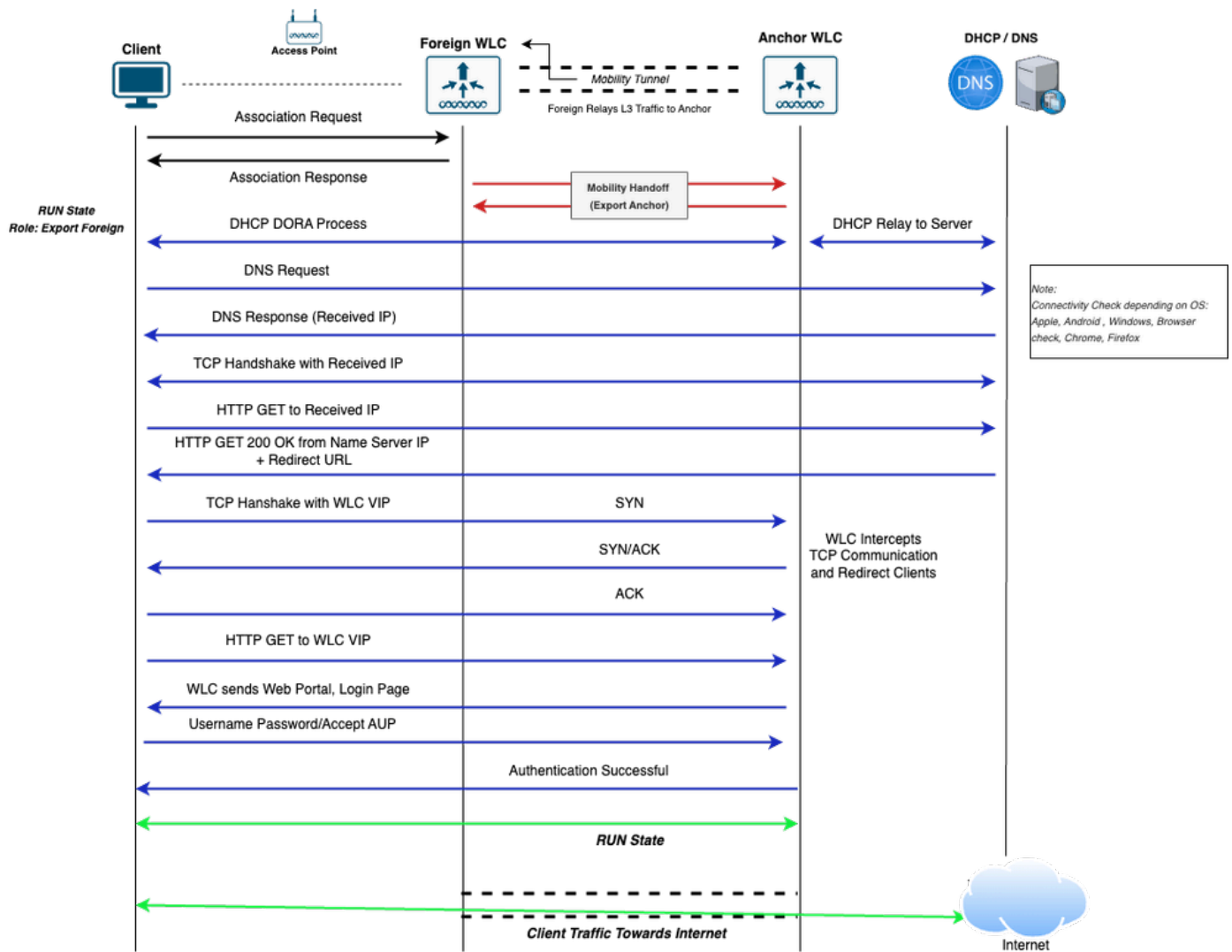
Clienteigenschappen voor anker

WLAN met Layer 3-verificatie

Lokale webverificatie

Flow voor lokale website-SSID in buitenlandse ankerinstellingen

1. De client initieert een verbinding met de SSID die wordt geadverteerd door de Foreign WLC.
2. Aangezien er geen Layer 2-verificatie wordt uitgevoerd, wordt de client onmiddellijk verankerd aan de WLC voor anker. De klant betreedt de RUN-status op de Foreign WLC, met zijn mobiliteitsrol aangeduid als Export Foreign.
3. De client krijgt een IP-adres en wordt doorgestuurd naar een webpagina. Dit verkeer wordt afgehandeld door Anchor Controller.
4. Na succesvolle verificatie op het portaal gaat de client over naar de status RUN op de WLC Anker, met de rol Exportanker.



Clientconnectiviteitsstroomdiagram voor lokale website-SSID in installatie voor buitenlandse ankers

Analysen van lokale webgebaseerde SSID-stroom in buitenlandse ankerinstellingen via logboeken

In dit gedeelte wordt de stroom van clientconnectiviteit voor lokale webverificatie-SSID uitgelegd met behulp van Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) en clientstatus op zowel de buitenlandse als de ankercontrollers.

Logboeken van buitenlandse controller

radioactieve sporen

!! Client Association Phase !!

```

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

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

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

pakketopname

De opdrachtgever stuurt een associatieverzoek, dat door de Foreign Controller wordt afgehandeld.

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=.....

Een mobiliteitsafgifte tussen de Foreign en Anchor Controllers via poort UDP 16667. Na een succesvol mobiliteitsevenement gaat de cliëntstatus over naar RUN met een rol in Export Foreign. De Foreign Controller ontvangt het DHCP-verkeer van de klant via de CAPWAP-tunnel en stuurt het door naar de Anchor Controller voor verdere verwerking.

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

DHCP-clientverkeer ontvangen op buitenlandse controller wordt doorgestuurd naar ankercontroller met behulp van mobiliteitstunnel

Op dezelfde manier stuurt de client netwerkconnectiviteitsstatus en webpaginatoegangsverkeer naar de Foreign WLC via de CAPWAP-tunnel; de Foreign WLC stuurt dit door naar de Anchor WLC met behulp van de mobiliteitstunnel, waar de Anchor Controller het verkeer onderschept of verwerkt.

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

Controle van netwerkconnectiviteitsstatus op buitenlandse 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)

```

URL voor doorsturen naar klant verzonden

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

Clienttoegang tot de lokale webpagina om verificatiegegevens op te geven

Logboeken van de ankercontroller

radioactieve sporen

!! Mobility Handoff !!

```

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

```

!! Session Created for Client !!

```

{wncd_x_R0-0}{1}: [client-orch-state] [24229]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [24229]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [webauth-state] [24229]: (info): [Client_MAC][ 0.0.0.0]Param-map used: global

```

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

!! Client DHCP Traffic !!

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

!! Local Web Authentication !!

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

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

pakketopname

Na de mobiliteitsoverdracht ontvangt de Anchor Controller DHCP-verkeer van de Foreign Controller via de mobiliteitstunnel.

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

DHCP-clientverkeer op ankercontroller ontvangen van buitenlandse controller

De ankercontroller ontvangt connectiviteitscontroles, verzoeken om toegang tot webpagina's en verificatiegegevens om deze verder te verwerken.

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

Controle van de netwerkverbindingstatus op de ankercontroller

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

URL voor doorsturen naar klant verzonden

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

Clienttoegang tot de lokale webpagina om verificatiegegevens op te geven

Nadat de lokale webverificatie is voltooid, voert de client de status RUN in met de rol Exportanker. Vanaf dit punt dient de ankercontroller als het afsluitpunt voor clientgegevensverkeer.

Cliëntstatus op zowel buitenlandse als 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

Clïëntstaat op buitenlands

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

Clientstatus voor anker

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Client Properties

AP Properties

Security Information

Client Statistics

Max Client Protocol Capability

Wi-Fi to Cellular Steering

Cellular Capability

Regular ASR support

802.11ac Wave 2

Not implemented

N/A

DISABLED

Mobility

Anchor IP Address

Point of Presence

AuthC Status

Move Count

Role

Roam Type

10.105.60.114

0xA0000003

True

0

Export Foreign

L3 Requested

Klanteigenschappen op buitenlands

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

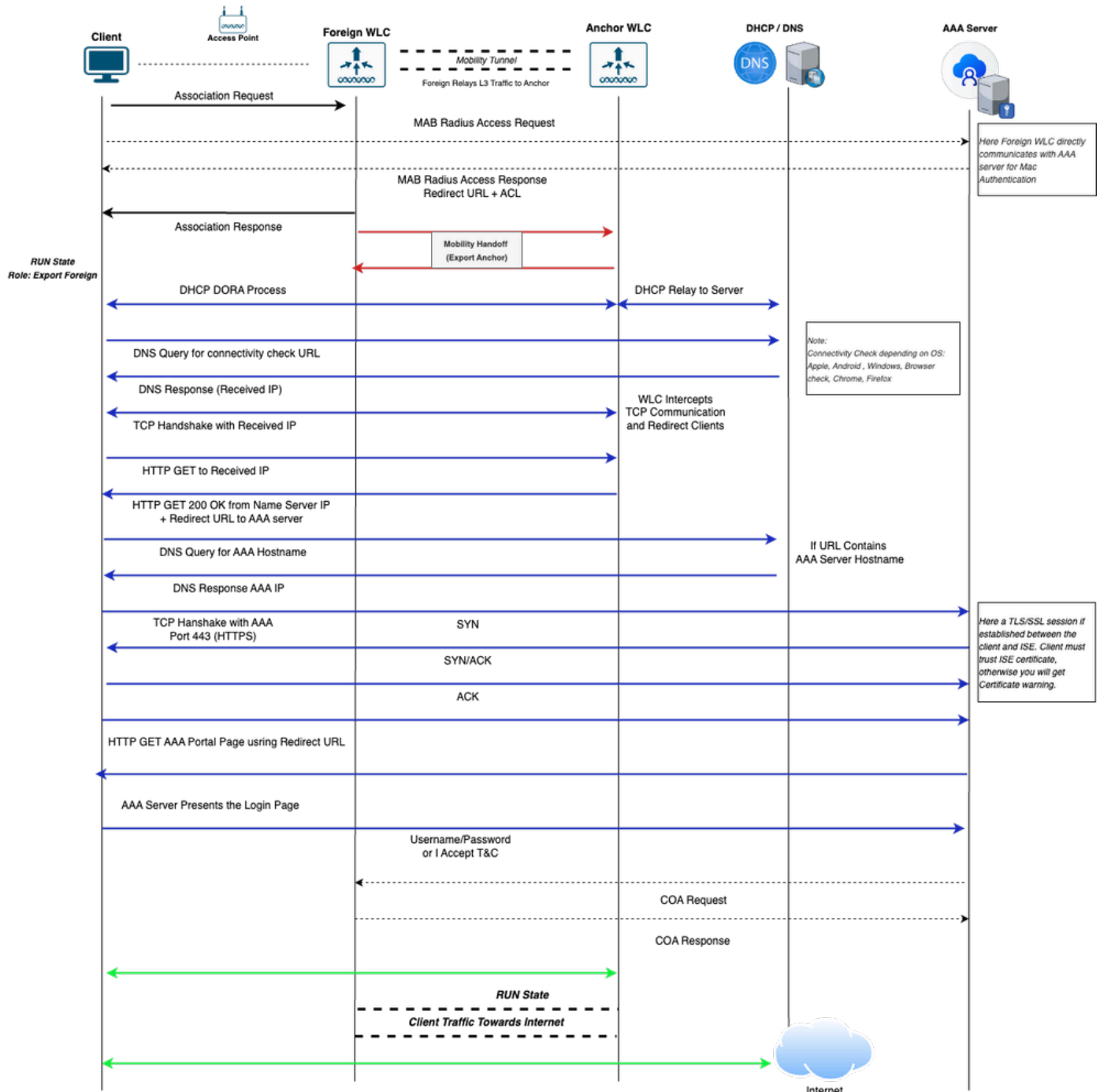
Clienteigenschappen voor anker

Centrale webverificatie

Flow voor centrale webgebaseerde SSID in buitenlandse ankerinstellingen

1. De client verzendt een associatieverzoek voor de SSID die wordt uitgezonden door de WLC (Foreign Wireless LAN Controller).
2. De Foreign WLC voert MAC-filtering uit door een Access-Request naar de RADIUS-server te sturen. De RADIUS-server reageert met een Access-Accept, die de nodige Redirect URL en Access Control List (ACL) bevat.
3. De Foreign WLC stuurt het verenigingsantwoord naar de opdrachtgever.
4. De client is verankerd in het WLC-anker. De client gaat de RUN-status in op de Foreign WLC, waarbij de mobiliteitsrol is ingesteld op Export Foreign.
5. De klant krijgt een IP-adres. In dit stadium verwerkt de WLC Anchor het omleidingsverkeer en wordt de client naar het verificatieportaal geleid.
6. Na omleiding communiceert de client rechtstreeks met de RADIUS-server. Dit verkeer wordt via de Anchor WLC naar de RADIUS-server geleid.

7. De client voert de verificatiereferenties in op de RADIUS-server. Na succesvolle authenticatie stuurt de RADIUS-server een verzoek tot wijziging van de autorisatie (CoA) naar de Foreign WLC.
8. De Foreign WLC stuurt een CoA-antwoord naar de RADIUS-server. De client gaat over naar de status RUN op de WLC Anker, waarbij de rol is ingesteld op Anker exporteren.
9. Al het daaropvolgende clientverkeer wordt van de Foreign WLC naar de Anchor WLC geleid, waar het het netwerk verlaat.



Clientconnectiviteitsstroomdiagram voor centrale webgebaseerde SSID in installatie voor buitenlandse ankers

Centrale webgebaseerde SSID-stroom analyseren in configuratie met buitenlandse ankers via logboeken

In dit gedeelte wordt de stroom van clientconnectiviteit voor de SSID voor centrale webverificatie uitgelegd met behulp van Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) en de clientstatus op zowel de buitenlandse als de ankercontrollers.

Logboeken van buitenlandse controller

radioactieve sporen

!! Client Association Phase !!

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

!! MAC Authentication !!

```
{wncd_x_R0-0}{1}: [dot11] [17047]: (info): MAC: Client_MAC DOT11 state transition: S_DOT11_INIT -> S_DO
{wncd_x_R0-0}{1}: [client-orch-state] [17047]: (note): MAC: Client_MAC Client state transition: S_CO_AS
{wncd_x_R0-0}{1}: [client-auth] [17047]: (note): MAC: Client_MAC MAB Authentication initiated. Policy V
{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authc_list: M
{wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [17047]: (info): [Client_MAC:capwap_90000003] - authz_list: M
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
{wncd_x_R0-0}{1}: [mab] [17047]: (info): [Client_MAC:capwap_90000003] Received event 'MAB_CONTINUE' on
{wncd_x_R0-0}{1}: [caaa-author] [17047]: (info): [CAAA:AUTHOR:a30003a6] NULL ATTR LIST
```

```
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Send Access-Request to 10.106.32.130:1812 id 0/245,
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 14 user-MAC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Password [2] 18 *
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Service-Type [6] 6 Call Check [10]
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 31
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 25 service-type=Call Check
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Framed-MTU [12] 6 1485
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: EAP-Key-Name [102] 2 *
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 49
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 43 audit-session-id=1E4F6B0A000003
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 18
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 12 method=mab
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 32
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 26 client-iif-id=3556776730
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-IP-Address [4] 6 10.107.79.30
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19]
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: NAS-Port [5] 6 141522
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 31
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 25 cisco-wlan-ssid=DMZ_CWA
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 33
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 27 wlan-profile-name=DMZ_CWA
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Called-Station-Id [30] 27 called-station-id
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Calling-Station-Id [31] 19 client-MAC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Airespace [26] 12
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Airespace-WLAN-ID [1] 6 12
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Nas-Identifier [32] 16 ForeignSiteWLC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Started 5 sec timeout
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Received from id 1812/245 10.106.32.130:0, Access-A
```

```

{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: authenticator
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: User-Name [1] 19 Client_MAC
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Class [25] 56 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Message-Authenticator[80] 18 ...
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 37
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 31 url-redirect-ac1=REDIRECT_ACL
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 191
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 185 url-redirect=https://10.106.32
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Vendor, Cisco [26] 42
{wncd_x_R0-0}{1}: [radius] [17047]: (info): RADIUS: Cisco AVpair [1] 36 profile-name=Windows10-Workstat

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

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

!! Post Successful Web authentication, Change of Authorization !!
[client-auth] [17047]: (info): MAC: Client_MAC Client auth-interface state transition
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Processing CoA request und
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Reauthenticate request (0x
[sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list -50323943,sm
[mab] [17047]: (info): [Client_MAC:capwap_90000003] MAB re-authentication started for
[auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Context changing state from
[auth-mgr] [17047]: (info): [Client_MAC:capwap_90000003] Method mab changing state fr
[aaa-coa] [17047]: (info): radius coa proxy relay coa resp(wncd)
[aaa-coa] [17047]: (info): CoA Response Details
[aaa-attr-inf] [17047]: (info): << ssg-command-code 0 32 >>
[aaa-attr-inf] [17047]: (info): << formatted-clid 0 Client_MAC>>
[aaa-attr-inf] [17047]: (info): << error-cause 0 1 [Success]>>
[aaa-coa] [17047]: (info): server:10.107.79.30 cfg_saddr:10.107.79.30 udpport:51304 s
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER] CoA response sent
[caaa-ch] [17047]: (info): [CAAA:COMMAND HANDLER:a30003a6] Identity preserved: MAC (C
[mab] [17047]: (info): [Client_MAC:capwap_90000003] Received event 'MAB_REAUTHENTICAT
[smd_R0-0]{1}: [aaa-coa] [18867]: (info): ++++++ Received CoA response Attribute List ++++++

```

```
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS(00000000): Send CoA Ack Response to 10.106.32.130:51304
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: authenticator
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Vendor, Cisco [26] 9
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: ssg-command-code [252] 3 ...
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Calling-Station-Id [31] 16 Client_MAC
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Dynamic-Author-Error-Cause[101] 6 Success [200]
{smd_R0-0}{1}: [radius] [18867]: (info): RADIUS: Message-Authenticator[80] 18 ...
{smd_R0-0}{1}: [aaa-pod] [18867]: (info): CoA response source port = 0, udpport = 51304,
{wncd_x_R0-0}{1}: [sadb-attr] [17047]: (info): Removing ipv6 addresses from the attr list 1627397682,sm
```

Packet capture

De client verzendt een associatieverzoek en voert MAC-verificatie uit, dit verkeer wordt afgehandeld door de Foreign Controller.

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 Association Phase on Foreign Controller with Wireless MAB

Een mobiliteitsafgifte tussen de Foreign en Anchor Controllers via poort UDP 16667. Na een succesvol mobiliteitsevenement gaat de cliëntstatus over naar RUN met een rol in Export Foreign.

De Foreign Controller ontvangt het DHCP-verkeer van de klant via de CAPWAP-tunnel en stuurt het door naar de Anchor Controller voor verdere verwerking.

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

DHCP-clientverkeer ontvangen op buitenlandse controller wordt doorgestuurd naar ankercontroller met behulp van mobiliteitstunnel

Op dezelfde manier stuurt de client netwerkconnectiviteitsstatus en webpaginatoegangsverkeer naar de Foreign WLC via de CAPWAP-tunnel; de Foreign WLC stuurt dit door naar de Anchor WLC met behulp van de mobiliteitstunnel, waar de Anchor Controller het verkeer onderschept of verwerkt.

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

Controle van netwerkconnectiviteitsstatus op buitenlandse 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: ..., 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://www.msftconnecttest.com/connecttest.aspx
    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)
```

URL voor doorsturen naar klant verzonden

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

Clienttoegang tot centrale webpagina om verificatiegegevens op te geven

De Foreign Controller verwerkt het CoA-verzoek na succesvolle Central Web Authentication.

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

Wijziging van autorisatie (COA) met buitenlandse controller

Logboeken van de ankercontroller

radioactieve sporen

!! Mobility Handoff !!

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

!! Session Created for Client !!

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

!! Central Web Authentication Applied !!

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

!! Client DHCP Traffic !!

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

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

!! Central Web Authentication !!

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

Packet capture

Na de mobiliteitsoverdracht ontvangt de Anchor Controller DHCP-verkeer van de Foreign Controller via de mobiliteitstunnel.

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

DHCP-clientverkeer op ankercontroller ontvangen van buitenlandse controller

De ankercontroller ontvangt connectiviteitscontroles, verzoeken om toegang tot webpagina's en verificatiegegevens om deze verder te verwerken.

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

Controle van de netwerkverbindingstatus op de ankercontroller

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

URL voor doorsturen naar klant verzonden

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

Clienttoegang tot de lokale webpagina om verificatiegegevens op te geven

Wanneer centrale webverificatie succesvol is, wordt een wijziging van de autorisatie (CoA) geactiveerd. Na een succesvolle CoA gaat de client over naar de status RUN met een rol voor Exportanker.

Cliëntstatus op zowel buitenlandse als 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 - 1 of 1 clients

Cliëntstaat op buitenlands

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 - 1 of 1 clients

Clientstatus voor 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

Klanteigenschappen op buitenlands

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

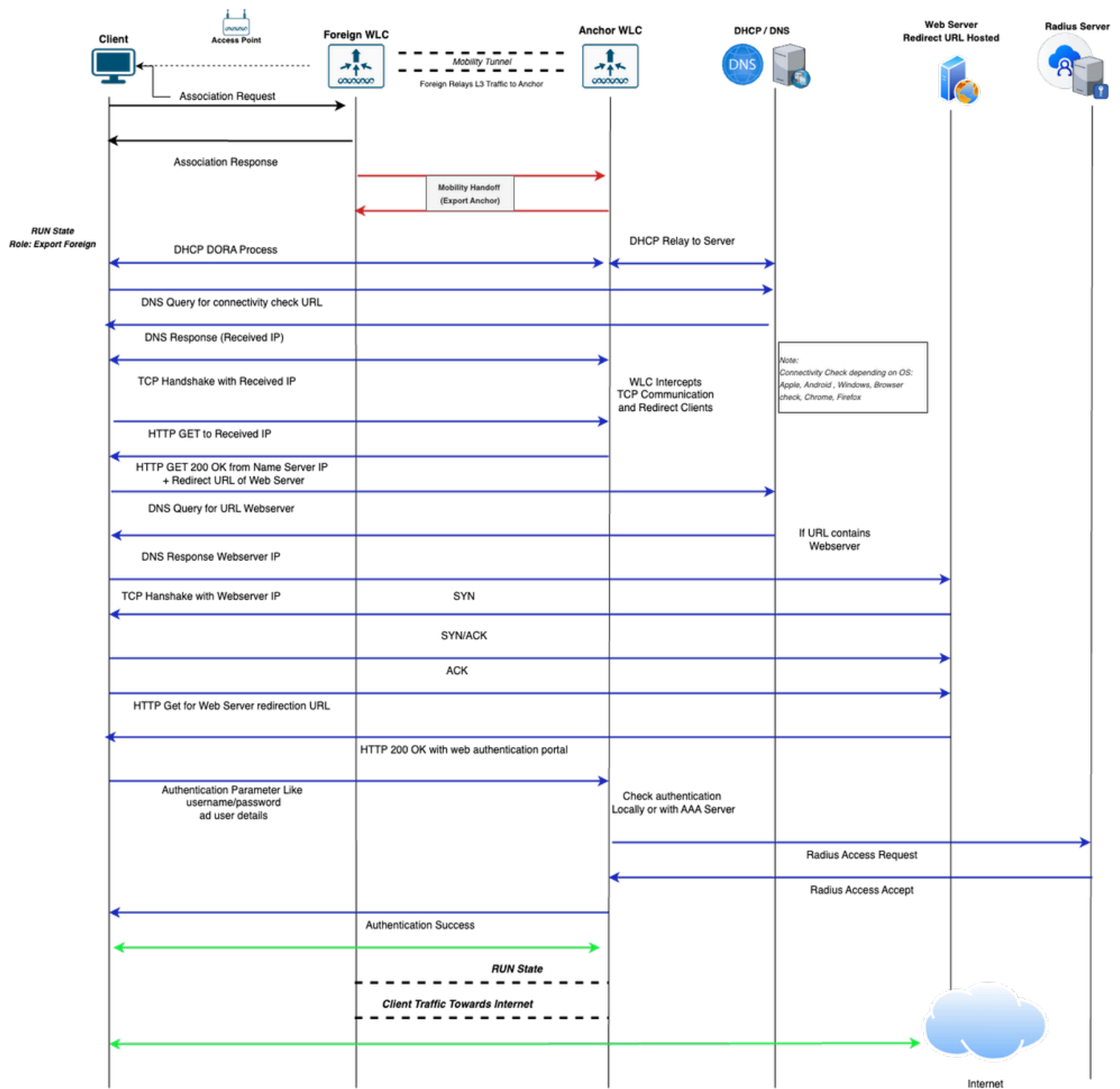
Clienteigenschappen voor anker

Externe webverificatie

Flow voor externe website-SSID in buitenlandse ankerinstellingen

1. De client initieert een verbinding met de SSID die wordt uitgezonden door de Foreign WLC.
2. Aangezien er geen Layer 2-verificatie vereist is, is de client verankerd aan de WLC voor anker. De klant gaat over naar de RUN-status op de Foreign WLC, met de mobiliteitsrol aangeduid als Export Foreign.
3. De klant krijgt een IP-adres. De WLC Anchor onderschept het verkeer en leidt de client door naar het externe webserverportaal zoals gedefinieerd in de webverificatieparameters.
4. De client dient de verificatiegegevens in via het portaal. Deze referenties worden lokaal op de WLC of via een externe verificatieserver gevalideerd, afhankelijk van het geconfigureerde beveiligingsbeleid.
5. Na succesvolle verificatie gaat de client over naar de status RUN op de WLC Anker, waarbij de rol Exportanker wordt aangenomen.

6. Na succesvolle verificatie wordt al het daaropvolgende clientverkeer van de Foreign WLC naar de Anchor WLC geleid, waar het het netwerk verlaat.



Clientconnectiviteitsstroomdiagram voor externe webgebaseerde SSID in installatie voor buitenlandse ankers

Externe webgebaseerde SSID-stroom analyseren in configuratie met buitenlandse ankers via logboeken

In dit gedeelte wordt de stroom van clientconnectiviteit voor de SSID voor externe webverificatie uitgelegd met behulp van Radioactive Trace (RA Trace), Embedded Packet Captures (EPC) en de clientstatus op zowel de buitenlandse als de ankercontrollers.

Logboeken van buitenlandse controller

radioactieve sporen

!! Client Association Phase !!

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

!! Layer 2 Authentication None !!

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

!! Mobility Handoff !!

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

!! Client AAAA Traffic !!

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

```
{mobilityd_R0-0}{1}: [mm-client] [18401]: (debug): MAC: Client_MAC aaa_handoff_ack is VALID
{mobilityd_R0-0}{1}: [mm-transition] [18401]: (info): MAC: Client_MAC MMFSM transition: S_MC_RUN -> S_M
{mobilityd_R0-0}{1}: [mm-client] [18401]: (info): MAC: Client_MAC Forwarding aaa_handoff_ack, sub type:
```

Packet capture

De opdrachtgever stuurt een associatieverzoek, dat door de Foreign Controller wordt afgehandeld.

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=.....

Clientassociatiefase met buitenlandse controller

Een mobiliteitsafgifte tussen de Foreign en Anchor Controllers via poort UDP 16667. Na een succesvol mobiliteitsevenement gaat de cliëntstatus over naar RUN met een rol in Export Foreign. De Foreign Controller ontvangt het DHCP-verkeer van de klant via de CAPWAP-tunnel en stuurt het door naar de Anchor Controller voor verdere verwerking.

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

DHCP-clientverkeer ontvangen op buitenlandse controller wordt doorgestuurd naar ankercontroller met behulp van mobiliteitstunnel

Op dezelfde manier stuurt de client netwerkconnectiviteitsstatus en webpaginatoegangsverkeer naar de Foreign WLC via de CAPWAP-tunnel; de Foreign WLC stuurt dit door naar de Anchor WLC met behulp van de mobiliteitstunnel, waar de Anchor Controller het verkeer onderschepst of verwerkt.

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

Controle van netwerkconnectiviteitsstatus op buitenlandse controller

```

> Frame 794: 977 bytes on wire (7816 bits), 977 bytes captured (7816 bits)
> Ethernet II, Src: Cisco (08:00:0c:2d:3d:3d), Dst: Cisco (08:00:0c:2d:3d:3d)
> 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)

```

URL voor doorsturen naar klant verzonden

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	148	TCP	0	62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	124	UDP	16667	→ 16667 Len=78
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	124	UDP	16667	→ 16667 Len=78
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	140	TCP	1	8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	1386	TCP	0	62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 1180]
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	683	TLSv1..	0	Client Hello
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	659	UDP	16667	→ 16667 Len=613
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	1342	UDP	16667	→ 16667 Len=1296
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	450	UDP	16667	→ 16667 Len=404
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	917	UDP	16667	→ 16667 Len=871
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	1378	TCP	0	8443 → 62448 [ACK] Seq=1 Ack=1798 Win=33280 Len=1250 [TCP PDU reassembled in 1192]
Jan 14, 2025 16:19:11..	10.107.79.30,10.106.32.130	10.107.79.129,10.105.60.254	933	TLSv1..	0	Server Hello, Certificate, Server Key Exchange, Server Hello Done
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [ACK] Seq=1798 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	143	TLSv1..	0	Alert (Level: Fatal, Description: Certificate Unknown)
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62448 → 8443 [FIN, ACK] Seq=1805 Ack=2056 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	262	TLSv1..	0	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	118	UDP	16667	→ 16667 Len=72
Jan 14, 2025 16:19:11..	10.105.60.114	10.107.79.30	157	UDP	16667	→ 16667 Len=111
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	136	TCP	0	62449 → 8443 [ACK] Seq=1860 Ack=2107 Win=131072 Len=0
Jan 14, 2025 16:19:11..	10.107.79.129,10.105.60.254	10.107.79.30,10.106.32.130	1143	TLSv1..	0	Application Data
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	112	UDP	16667	→ 16667 Len=66
Jan 14, 2025 16:19:11..	10.107.79.30	10.105.60.114	1119	UDP	16667	→ 16667 Len=1073
Jan 14, 2025 16:19:11..	10.107.79.129,10.106.32.130	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

Clienttoegang tot externe webpagina om verificatiegegevens op te geven

Logboeken van de ankercontroller

radioactieve sporen

!! Mobility Handoff !!

```

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

```

!! Session Created for Client !!

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

!! Client DHCP Traffic !!

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

!! External Web Authentication !!

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Packet capture

Na de mobiliteitsoverdracht ontvangt de Anchor Controller DHCP-verkeer van de Foreign Controller via de mobiliteitstunnel.

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

DHCP-clientverkeer op ankercontroller ontvangen van buitenlandse controller

De ankercontroller ontvangt connectiviteitscontroles, verzoeken om toegang tot webpagina's en verificatiegegevens om deze verder te verwerken.

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

Controle van de netwerkverbindingstatus op de ankercontroller

```

> 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)

```

URL voor doorsturen naar klant verzonden

De client dient de verificatiegegevens in via het portaal. Deze referenties worden lokaal op de WLC of via een externe verificatieserver gevalideerd, afhankelijk van het geconfigureerde beveiligingsbeleid.

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	124	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	66	TCP		62448 → 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1250 WS=256 SACK_PERM
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	70	TCP		8443 → 62448 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1254 SACK_PERM WS=128
Jan 14, 2025 16:19:12...	10.105.60.114	10.107.79.30	120	UDP		16667 → 16667 Len=78
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	54	TCP		62448 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	112	UDP		16667 → 16667 Len=66
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	659	UDP		16667 → 16667 Len=613
Jan 14, 2025 16:19:12...	10.107.79.30	10.105.60.114	1342	UDP		16667 → 16667 Len=1296
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	1304	TCP		62449 → 8443 [ACK] Seq=1 Ack=1 Win=131072 Len=1250 [TCP PDU reassembled in 717]
Jan 14, 2025 16:19:12...	10.105.60.254	10.106.32.130	537	TLSv1..		Client Hello
Jan 14, 2025 16:19:12...	10.106.32.130	10.105.60.254	1308	TCP		8443 → 62449 [ACK] Seq=1 Ack=1734 Win=34688 Len=1250 [TCP PDU reassembled in 724]
Jan 14, 2025 16:19:12...	10.107.79.30	10.107.79.30	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...	10.106.32.130	10.105.60.254	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

Clienttoegang tot externe webpagina om verificatiegegevens op te geven

Clientstatus op zowel buitenlandse als 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

Clïëntstaat op buitenlands

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

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

1 - 1 of 1 clients

Clientstatus voor 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

Klanteigenschappen op buitenlands

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

Clienteigenschappen voor anker

taakverdeling tussen meerdere ankercontrollers

Wanneer meer dan één ankercontroller is toegewezen aan één WLAN, hangt de verkeersverdeling af van de prioriteit. Er kunnen drie prioriteitsniveaus worden geconfigureerd: Primair, Secundair en Tertiair. De functie Guest Anchor Priority biedt een mechanisme voor actieve/standby-lastverdeling tussen de ankercontrollers. Dit wordt bereikt door een vaste prioriteit toe te kennen aan elke ankercontroller: de belasting wordt verdeeld over de controller met de hoogste prioriteit en op round-robin-wijze onder controllers die dezelfde prioriteitswaarde delen.

⚠ 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)



Prioriteit anker in kaart brengen



Opmerking: Standaard wordt de tertiaire prioriteit geconfigureerd tijdens de toewijzing van de ankercontroller op de buitenlandse controller.

Problemen oplossen met clientconnectiviteit in scenario met buitenlandse ankers

1. Problemen met onboarding van clients

- Tunnel Status: Controleer of de mobiliteitstunnel tussen de Foreign en Anchor Controllers actief blijft.
- Mismatch in configuratie: zorg voor configuratiepariteit tussen beide controllers. Discrepancies in WLAN-namen, namen van beleidsprofielen of geavanceerde instellingen, zoals AAA-overschrijving, IPv4-DHCP-vereisten en NAC, leiden tot fouten in de profielovereenkomst of ankerweigering.
- Anders: als Tunnel is ingeschakeld zonder configuratieproblemen, is de aanpak voor probleemoplossing vergelijkbaar met een normaal probleem met de clientconnectiviteit, waarbij wordt gecontroleerd op de respectieve controller die het getroffen verkeer verwerkt.

2. Intermitterende connectiviteit

- i. Tunnel Flaps: Als pakketjes tussen de twee controllers niet aankomen, kleppen de tunnelkleppen, waardoor de client geen verbinding met de SSID kan onderhouden.
- ii. Lage bandbreedte: als de Path MTU (PMTU) tussen mobiliteitspeers daalt naar een lagere waarde (576), ervaren klanten een verslechtering van de prestaties. Dit gebeurt meestal wanneer path mtu keepalive-berichten worden gemist tussen beide mobiliteitsgenoten



Opmerking: De controller met het MAC-adres met lagere mobiliteit initieert zowel de standaard keepalive als de Path MTU keepalive-berichten.

3. Specifieke problemen met toegang tot de website

- i. Mobiliteitsverkeer headers omvatten mobiliteit groep identifiers, MAC-adressen, IP-adressen, en gecodeerde CAPWAP DTLS pakketten uitgewisseld over UDP poorten 16666 en 16667. Deze overhead wordt toegevoegd aan de bestaande CAPWAP-header. Voor TCP-verkeer, na het aanpassen van TCP MSS geconfigureerd voor AP, als de pakketgrootte groter is dan de Mobility PMTU (maximaal 1385 bytes) als gevolg van deze extra overhead, treedt fragmentatie op. Hoewel fragmentatie over het algemeen wordt afgehandeld door het netwerk, ontstaan er problemen als pakketten buiten bedrijf of te laat komen. Deze voorwaarden hebben invloed op het opnieuw samenstellen van pakketten en leiden tot fouten in de toegankelijkheid van gegevens voor specifieke websites.

Logboekverzameling van buitenlandse en ankercontroller

1. Schakel de term exec prompt timestamp in om een tijdreferentie te hebben voor alle opdrachten.
2. Gebruik show tech-support wireless!! om de configuratie te bekijken.
3. U kunt de status van de mobiliteitstunnel controleren en een overzicht van de draadloze mobiliteit weergeven!
4. Statistieken voor Peer Mobility die linkstatus, clientgegevens en gebeurtenissen, keep-alive-statistieken bevatten, tonen peer-ip voor draadloze mobiliteit <IP>
5. Radioactief traceren inschakelen voor IP/MAC-adres van mobiliteitspeer en MAC-adres van client.

Via CLI:

foutopsporing draadloos {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconden}!
Met het instellen van de tijd kunnen we traces tot 24 dagen inschakelen.

geen foutopsporing draadloos {MAC | ip} {aaaa.bbbb.cccc | x.x.x.x} De foutopsporing uitschakelen

WLC genereert een debug trace bestand met Client_info, opdracht om te controleren op debug trace bestand gegenereerd dir bootflash: | i debug!



Waarschuwing: Het voorwaardelijk debuggen maakt het mogelijk om op debug-niveau te loggen, wat op zijn beurt het volume van de gegenereerde logs verhoogt. Als u dit actief laat, neemt de afstand terug in de tijd af waarvandaan u logs kunt bekijken. Het wordt dus aanbevolen om foutopsporing altijd uit te schakelen aan het einde van de sessie voor probleemoplossing.

6. Voer de volgende opdrachten uit om alle foutopsporing uit te schakelen:

Duidelijke platformconditie allemaal!

#undebug alles!

Via GUI:

Stap 1. Ga naar Problemen oplossen > Radioactief spoor.

Stap 2. Klik op Toevoegen en voer een Mobility Peer MAC/IP-adres of client MAC-adres in dat u wilt oplossen.

Stap 3. Wanneer u klaar bent om het radioactieve traceren te starten, klikt u op Start. Eenmaal gestart, wordt debug logging geschreven naar schijf over elke control plane verwerking met betrekking tot de bijgehouden MAC-adressen.

Stap 4. Klik op Stoppen wanneer u het probleem dat u wilt oplossen, reproduceert.

Stap 5. Voor elk MAC-adres waarvoor een foutopsporing is opgetreden, kunt u een logbestand genereren waarin alle logs met betrekking tot dat MAC-adres zijn verzameld door op Genereren te klikken.

Stap 6. Kies hoe lang terug u wilt dat het samengevoegde logbestand gaat en klik op Toepassen op apparaat.

Stap 7. U kunt het bestand nu downloaden door op het kleine pictogram naast de bestandsnaam te klikken. Dit bestand is aanwezig in de opstartflashdrive van de controller en kan ook uit de doos worden gekopieerd via CLI.

7. Ingebouwde opnamen

Via CLI:

monitor capture MYCAP clear!

monitor capture MYCAP interface Po1 beide!

monitor capture MYCAP buffer size 100!

monitor capture MYCAP match access-list naam! (indien het traceren van mobiliteitstunnelverkeer tussen WLC)

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

monitor capture MYCAP start!

! Voortplanten

monitor capture MYCAP stop

monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap

Via GUI:

Stap 1. Navigeer naar Problemen oplossen > Pakketvastlegging > +Toevoegen.

Stap 2. Definieer de naam van de pakketopname. Er zijn maximaal 8 tekens toegestaan.

Stap 3. Definieer eventuele filters.

Stap 4. Schakel het selectievakje in om het verkeer te controleren als u wilt zien dat het verkeer op de CPU van het systeem wordt weergegeven en opnieuw in het gegevensvlak wordt geïnjecteerd.

Stap 5. Definieer de buffergrootte. Maximaal 100 MB is toegestaan.

Stap 6. Definieer de limiet, hetzij door de duur die een bereik van 1 - 1000000 seconden mogelijk maakt, hetzij door het aantal pakketten dat een bereik van 1 - 100000 pakketten mogelijk maakt, zoals gewenst.

Stap 7. Kies de interface uit de lijst met interfaces in de linkerkolom en selecteer de pijl om deze naar de rechterkolom te verplaatsen.

Stap 8. Klik op Opslaan en Toepassen op apparaat.

Stap 9. Selecteer Start om het vastleggen te starten.

Stap 10. U kunt de opname tot de gedefinieerde limiet laten lopen. Selecteer Stoppen als u het vastleggen handmatig wilt stoppen.

Stap 11. Zodra deze is gestopt, wordt een knop Exporteren beschikbaar om te klikken met de optie om het opnamebestand (.pcap) op het lokale bureaublad te downloaden via HTTP- of TFTP-server of FTP-server of lokale systeemharde schijf of flash.

Gerelateerde informatie

[Mobiliteitstopologieën configureren op Catalyst 9800 WLC's](#)

[WLAN Anchor Mobility Feature configureren op Catalyst 9800](#)

[Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.