

# Fehlerbehebung: CW917X Wi-Fi7 AP-Verbindungsproblem mit Catalyst 9800 WLC

## Inhalt

---

[Einleitung](#)

[Verwendete Komponenten](#)

[AP-Startproblem](#)

[AP kann IP-Adresse nicht erfassen](#)

[Konvertierung des AP Catalyst-Modus fehlgeschlagen](#)

[Probleme mit der schnellen Offline-Migration](#)

[Migrationsprobleme mit DHCP-Option 43\(0xF3\)](#)

[DNS-Migrationsprobleme](#)

[Probleme mit der Offline-Migration](#)

[Migrationsprobleme mit DHCP-Option 43](#)

[DNS-Auflösungsfehler](#)

[Fallback zur Layer-2-CAPWAP-Erkennung](#)

[AP schließt Beitrittsphase nicht ab](#)

[Fehler bei der Auflösung der AP-Zulassung](#)

[AP-Support nach Land \(jeweilige Version\)](#)

[Verwenden von Proximity](#)

[RF-basiert](#)

[CDP-/LLDP-basiert](#)

[Verwenden der RAF-Datei](#)

[AP aufgrund von Lizenzproblemen nicht konform](#)

[Protokollsammlung](#)

[Protokolle von WLC](#)

[Protokolle vom Access Point](#)

[AP im Meraki-Modus](#)

[AP im Catalyst-Modus](#)

[Protokolle vom mit dem AP verbundenen Uplink-Switch](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Fehlerbehebung bei einer mehrphasigen WiFi7-AP-Verbindung beschrieben.

## Verwendete Komponenten

- Wireless Controller der Serie 9800
- Cisco IOS XE Version 17.18.03
- CW9172I

## AP-Startproblem

Wenn ein neuer WiFi7-Access Point entkoppelt ist und nicht richtig gestartet werden kann, überprüfen Sie zuerst den LED-Status und die Konsolenstartprotokolle. In der Hardware-Installationsanleitung des jeweiligen Access Point-Modells können Sie den LED-Status für verschiedene AP-Bedingungen überprüfen: [WiFi7 AP Installationsanleitung](#)

- Prüfen Sie anhand des Datenblatts für die APs die Mindestleistungsanforderung (PoE-Klasse/Wattzahl) und die erwarteten LED-Zustände, um ein Energieproblem auszuschließen: [Datenblatt für Cisco Wireless Access Points der Serie 9172](#)
- Wenn die Stromversorgung ausreicht, wird der Access Point erfolgreich gestartet und das Meraki-Betriebssystem als primäres Image bzw. Standard-Image geladen.
- Zum ersten Mal, bis AP eine IP-Adresse empfängt: Im Meraki-Modus ist der AP über CDP nicht sichtbar. verwenden stattdessen LLDP, um es im Netzwerk zu erkennen.

## AP kann IP-Adresse nicht erfassen

Wenn der Access Point keine IP-Adresse erhält, sehen Sie den Access Point auf der Konsole des Access Points im Offline-Migrationsmodus von Tag 0:

Führen Sie `offline-migration-info` an der Eingabeaufforderung der <Meraki> Konsole aus, um die aktuellen Protokolle und den Status des Migrationsversuchs abzurufen.

```
<#root>
```

```
<Meraki>
```

```
offline-migration-info
```

```
| [2000-01-01 00:00:36.528] AP in day0 - offline migration
```

Wenn der Access Point diesen Status beibehält:

- Überprüfen Sie die Switch-Port-Konfiguration des Uplink Switches: Dabei kann es sich

entweder um den Zugriffsmodus oder um den Trunk-Modus handeln, wobei das AP-Management-VLAN als nativ festgelegt ist.

- Sammeln Sie eine Paketerfassung am Uplink-Switch-Port der APs, und überprüfen Sie den DORA-Fluss (Discover, Offer, Request, Ack), um zu bestätigen, ob DHCP-Anfragen den Server erreichen und Angebote zurückgegeben werden. Das folgende Beispiel zeigt eine erfolgreiche DHCP-Transaktion zwischen dem Access Point und dem DHCP-Server:

dhcp.id == 0x5ca99203							
o.	Time	Source	Destination	Protocol	Length	Info	
97564	978.084928500	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x5ca99203	
97598	981.113901400	10.127.197.201	10.127.197.225	DHCP	342	DHCP Offer - Transaction ID 0x5ca99203	
97599	981.114142500	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x5ca99203	
97600	981.117014900	10.127.197.201	10.127.197.225	DHCP	342	DHCP ACK - Transaction ID 0x5ca99203	

AP-Uplink-Erfassung: Erfolgreiche DHCP-Transaktion (DORA) zwischen dem Access Point und dem DHCP-Server

## Konvertierung des AP Catalyst-Modus fehlgeschlagen

Die Access Points (APs) der Serie CW917x verwenden einen anderen Migrationsmechanismus als ältere Access Points der Serie Catalyst 9100. Zur Umwandlung eines CW917x AP in den Catalyst-Modus sind spezifische Netzwerkkonfigurationen erforderlich, darunter DHCP-Optionen, DNS-Einstellungen und die Cloud-Erreichbarkeit.

Der WAP versucht zunächst, die DHCP-Option 43 zu verwenden. Wenn kein Wert konfiguriert ist oder die IP-Adresse nicht erreichbar ist, wird sie auf die DNS-Methode zurückgesetzt. Hier sind einige häufige Probleme, die diesen Konvertierungsprozess stören können.

### Probleme mit der schnellen Offline-Migration

#### Migrationsprobleme mit DHCP-Option 43(0xF3)

- Ungültiger Wert für Option 43: Der Access Point erhält keinen gültigen Hexadezimalwert (z. B. Fehler beim Starten mit dem richtigen Suboptionstyp, z. B. 0xF3).

```
<#root>
```

```
<Meraki>
```

```
offline-migration-info
```

```
| [2000-01-01 00:00:36.528] AP in day0 - offline migration
| [2000-01-01 00:06:54.265] [init] start offline migration detection (v1.1)
| [2000-01-01 00:07:59.65 ] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:08:04.112] [fast-offline-migration][v4]
```

no fast offline migration by DHCP

| [2000-01-01 00:08:04.113] [fast-offline-migration][v6]

no fast offline migration by DHCP

| [2000-01-01 00:08:04.113] [fast-offline-migration] waiting for 420sec before taking any migration dec

- ICMP-Fehler: Der AP versucht zuerst, eine aufgelöste IP zu erreichen, die von der DHCP-Serveroption 43 (0xF3) empfangen wurde. Wenn keine ICMP-Erreichbarkeit mit der aufgelösten IP besteht, kann der AP nicht in den Catalyst-Modus wechseln.

<#root>

<Meraki> offline-migration-info

| [2000-01-01 00:00:48.388] AP in day0 - offline migration

| [2000-01-01 00:02:59.526] [init] start offline migration detection (v1.2)

| [2000-01-01 00:04:00.774] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST

| [2000-01-01 00:04:10.799] [fast-offline-migration]

[v4][icmp] DHCP: WLC 10.127.197.201 is unreachable >>

Here 10.127.197.201 is IP of Switch present in Network

| [2000-01-01 00:04:15.906] [fast-offline-migration]

[v4][capwap] DHCP: WLC 10.127.197.201 is down

| [2000-01-01 00:04:15.906] [fast-offline-migration][v4] no fast offline migration by DHCP

| [2000-01-01 00:04:15.906] [fast-offline-migration][v6] no fast offline migration by DHCP

o.	UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
3242	Jun 23, 2026 15:11:34	10.127.197.238	10.127.197.201	98	ICMP		Echo (ping) request id=0x235b, seq=0/0, ttl=64 (no response found!)
3252	Jun 23, 2026 15:11:35	10.127.197.238	10.127.197.201	98	ICMP		Echo (ping) request id=0x235c, seq=0/0, ttl=64 (no response found!)
3259	Jun 23, 2026 15:11:36	10.127.197.238	10.127.197.201	98	ICMP		Echo (ping) request id=0x235d, seq=0/0, ttl=64 (no response found!)
3266	Jun 23, 2026 15:11:37	10.127.197.238	10.127.197.201	98	ICMP		Echo (ping) request id=0x235e, seq=0/0, ttl=64 (no response found!)
3278	Jun 23, 2026 15:11:38	10.127.197.238	10.127.197.201	98	ICMP		Echo (ping) request id=0x2365, seq=0/0, ttl=64 (no response found!)
3287	Jun 23, 2026 15:11:40	10.127.197.201,10.127.197.238	10.127.197.238,10.127...	70	ICMP		Destination unreachable (Port unreachable)
3298	Jun 23, 2026 15:11:41	10.127.197.201,10.127.197.238	10.127.197.238,10.127...	70	ICMP		Destination unreachable (Port unreachable)
3308	Jun 23, 2026 15:11:42	10.127.197.201,10.127.197.238	10.127.197.238,10.127...	70	ICMP		Destination unreachable (Port unreachable)
3321	Jun 23, 2026 15:11:43	10.127.197.201,10.127.197.238	10.127.197.238,10.127...	70	ICMP		Destination unreachable (Port unreachable)
3327	Jun 23, 2026 15:11:44	10.127.197.201,10.127.197.238	10.127.197.238,10.127...	70	ICMP		Destination unreachable (Port unreachable)

AP-Uplink-Erfassung: Keine ICMP-Erreichbarkeit zum Auflösen von IP



Anmerkung:

AP führt stets den ICMP-Erreichbarkeitstest durch, gefolgt von der CAPWAP-Erreichbarkeit.

Der ICMP-Erreichbarkeitsmechanismus kann verwendet werden, wenn in Ihrem Netzwerk kein WLC vorhanden ist.

Wenn ein Access Point (AP) die IP-Adresse des Wireless LAN Controller (WLC) über die DHCP-Option 43 (0xF3) bezieht und CAPWAP-Datenverkehr vom AP zum WLC-IP nicht erreichbar ist, jedoch ICMP-Erreichbarkeit zum WLC-IP verfügbar ist, kann der AP dennoch in den Catalyst-Modus wechseln.

Wenn ein Access Point (AP) die IP-Adresse des Wireless LAN Controller (WLC) in einer nicht unterstützten Version über die DHCP-Option 43 (0xF3) bezieht, aber die ICMP-Erreichbarkeit der WLC-IP-Adresse verfügbar ist, kann der AP dennoch in den Catalyst-Modus wechseln. Es kann jedoch nicht dem WLC beitreten.

Dies ist eine erfolgreiche Migration mit ICMP-Erreichbarkeit:

```
<#root>
```

```
<Meraki> offline-migration-info
| [2000-01-01 00:00:49.2 ] AP in day0 - offline migration
| [2000-01-01 00:03:00.367] [init] start offline migration detection (v1.2)
| [2000-01-01 00:04:03.34 ] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:04:08.56 ]
```

```
[fast-offline-migration][v4][icmp] DHCP: WLC 10.127.197.201 is reachable
```

```
| [2000-01-01 00:04:08.56 ]
```

```
[fast-offline-migration][DHCP][IPv4] migrate to Catalyst
```

s.	UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
3429	Jun 23, 2026 15:18:38	10.127.197.239	10.127.197.201	98	ICMP		Echo (ping) request id=0x25dd, seq=0/0, ttl=64 (reply in 3431)
3431	Jun 23, 2026 15:18:38	10.127.197.201	10.127.197.239	98	ICMP		Echo (ping) reply id=0x25dd, seq=0/0, ttl=255 (request in 3429)

AP-Uplink-Erfassung: Erfolgreiche schnelle Migration von AP in den Catalyst-Modus über ICMP-Erreichbarkeit

- Nicht unterstützte WLC-Softwareversion: Auf dem antwortenden WLC wird eine ältere Softwareversion als Cisco IOS XE 17.15.1 (oder die mindestens unterstützte Version für den AP) ausgeführt, wodurch der Catalyst-Modus-Switch ausfällt.

```
<#root>
```

```
<Meraki> offline-migration-info
| [2000-01-01 00:00:36.600] AP in day0 - offline migration
| [2000-01-01 00:02:49.984] [init] start offline migration detection (v1.1)
| [2000-01-01 00:03:53.950] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:04:03.966] [fast-offline-migration][v4][icmp] DHCP: WLC 10.127.197.196 is unreach
| [2000-01-01 00:04:04.42 ]
```

```
[fast-offline-migration][v4][capwap] DHCP: WLC 10.127.197.196 is unsupported - version 17.12.4.22
```

```
| [2000-01-01 00:04:04.42 ] [fast-offline-migration][v4] no fast offline migration by DHCP  
| [2000-01-01 00:04:04.43 ] [fast-offline-migration][v6] no fast offline migration by DHCP  
| [2000-01-01 00:04:04.43 ] [fast-offline-migration][v4] missing DNS config (server and/or domain)  
| [2000-01-01 00:04:04.43 ] [fast-offline-migration][v6] missing DNS config (server and/or domain)  
| [2000-01-01 00:04:04.43 ] [fast-offline-migration] waiting for 420sec before taking any migratio
```

## DNS-Migrationsprobleme

Wenn der Access Point (AP) die schnelle Offline-Migration mithilfe von DHCP nicht abschließen kann, versucht er die DNS-Methode. Zunächst überprüft der WAP, ob er vom DHCP-Server einen gültigen Domännennamen (Option 15) und eine gültige IP-Adresse des DNS-Servers (Option 6) erhalten hat. Anhand dieser Informationen versucht der Access Point, den Hostnamen cisco-automigrate.<Domäne> aufzulösen. Wenn diese Auflösung erfolgreich ist, fährt der Access Point mit der Migration in den Catalyst-Modus fort.

- Fehlende DHCP-Optionen: Der WAP empfängt vom DHCP-Server keinen gültigen Domännennamen (DHCP-Option 15) oder keine DNS-Server-IP (DHCP-Option 6).

<#root>

```
<Meraki> offline-migration-info  
| [2000-01-01 00:00:48.565] AP in day0 - offline migration  
| [2000-01-01 00:02:59.840] [init] start offline migration detection (v1.2)  
| [2026-06-24 11:11:58.392] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST  
| [2026-06-24 11:12:03.438] [fast-offline-migration][v4] no fast offline migration by DHCP  
| [2026-06-24 11:12:03.438] [fast-offline-migration][v6] no fast offline migration by DHCP  
| [2026-06-24 11:12:03.529]
```

```
[fast-offline-migration][v4] missing DNS config (server and/or domain)
```

```
>> DNS Option Missing in DHCP Response  
| [2026-06-24 11:12:03.529]
```

```
[fast-offline-migration][v6] missing DNS config (server and/or domain)
```

#### Dynamic Host Configuration Protocol (Offer)

```
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x5ed813bc
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.127.197.238
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: CiscoMeraki_
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
```

```
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier (10.127.197.201)
> Option: (51) IP Address Lease Time
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value          DHCP Option 15 and 6 Missing
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (43) Vendor-Specific Information
> Option: (255) End
Padding: 000000000000000000000000
```

AP-Uplink-Erfassung: DNS-Server und Domänenname fehlen bei DHCP-Antwort

- Behebungsfehler: Der DNS-Server kann den FQDN cisco-automigrate.<Ihre-Domäne> nicht auflösen.

<#root>

<Meraki> offline-migration-info

```
| [2000-01-01 00:00:48.565] AP in day0 - offline migration
| [2000-01-01 00:02:59.840] [init] start offline migration detection (v1.2)
| [2026-06-24 11:11:58.392] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2026-06-24 11:12:03.438] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2026-06-24 11:12:03.438] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2026-06-24 11:12:03.529]
```

[fast-offline-migration][v4] no fast offline migration by DNS

>> It received a DNS server and domain but unable to resolve the hostname

```
| [2026-06-24 11:12:03.529] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2026-06-24 11:12:03.529] [fast-offline-migration] waiting for 420sec before taking any migration dec
```

```

Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x3d491a56
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.127.197.217
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: CiscoMeraki_da:00:00:00:00:00:00
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (10.127.197.201)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (15) Domain Name
    Length: 12
    Domain Name:
  > Option: (6) Domain Name Server
    Length: 4
    Domain Name Server:
  > Option: (255) End

```

AP-Uplink-Erfassung: Gültiger DNS-Server und Domänenname in DHCP-Antwort vorhanden

UTC Arrival Time	Source Address	Destination Address	Length	Protocol	TID	Info
Jun 24, 2026 09:44:20...	10.127.197.217	DNS Server	90	DNS		Standard query 0x6120 A cisco-automigrate. domain-name
Jun 24, 2026 09:44:20...	DNS Server	10.127.197.217	163	DNS		Standard query response 0x6120 No such name A cisco-automigrate. domain-name

AP-Uplink-Erfassung: Behebungsfehler für Hostname

- Nicht erreichbare aufgelöste IP: Der Access Point löst cisco-automigrate.<Ihre-Domäne> erfolgreich auf, verfügt jedoch über keine ICMP-Erreichbarkeit zu der resultierenden IP-Adresse.

```
<#root>
```

```
<Meraki>
```

```
offline-migration-info
```

```

| [2000-01-01 00:01:58.622] [init] start offline migration detection
| [2000-01-01 00:03:05.252] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:04:05.156] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:04:15.290] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:04:20.271]

```

```
[fast-offline-migration][v4][icmp] DNS automigrate: WLC 10.27.XX.XX is not alive
```

```
>> No ICMP reachability to hostname resolved IP
```

## Probleme mit der Offline-Migration

Wenn ein WAP die schnelle Offline-Migration nicht erfolgreich abschließt, versucht er, eine Verbindung zur Meraki Cloud herzustellen, um zu überprüfen, ob er für ca. 7 Minuten zu einem Meraki-Netzwerk hinzugefügt wurde. Wenn der Access Point in diesem Zeitraum die Kommunikation mit der Meraki Cloud aufrechterhält und zu einem Netzwerk hinzugefügt wird, kann er in den Meraki-Modus wechseln.

Wenn der Access Point die Meraki Cloud jedoch nach 7 Minuten immer noch nicht erreichen kann oder einem Netzwerk nicht hinzugefügt wurde und er nicht mit einer statischen IP-Adresse konfiguriert ist, erneuert er seine IP-Adresse über DHCP. Zu diesem Zeitpunkt tritt der Access Point in die Offline-Migrationsphase ein. Bei der Offline-Migration verwendet der Access Point DHCP, DNS und Layer-2-Erkennungsmethoden, um die Details des Wireless LAN Controller (WLC) im Netzwerk zu ermitteln, und wechselt dann in den Catalyst-Modus. Während der Offline-Migration können verschiedene Probleme auftreten.

### Migrationsprobleme mit DHCP-Option 43

- Nach der IP-Aktualisierung prüft der WAP, ob er eine DHCP-opt-43 mit 0xF1 erhalten hat, eine gültige WLC-IP erhalten hat, ob CAPWAP erreichbar ist und die Antwort von der unterstützten Version vorliegt. Folgende Fehler sind möglich:

```
<#root>
```

```
!! No valid WLC IP recieved on DHCP Option 43 0xF1 !!
```

```
| [2000-01-01 00:14:19.658][fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:15:07.101] [offline-migration] forcing DHCP renew
| [2000-01-01 00:15:07.102] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:15:12.150] [offline-migration] migration decision
| [2000-01-01 00:15:12.150]
```

```
[offline-migration][v4] no WLC IP in DHCP option 43 >> No valid WLC IPv4 received
```

```
| [2000-01-01 00:15:12.150] [offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:15:12.151]
```

```
[offline-migration][v6] no WLC IP in DHCP option 52 >> No valid WLC IPv4 received
```

```
| [2000-01-01 00:15:12.151] [offline-migration][v6] missing DNS config (server and/or domain)
```

```
!! No CAPWAP reachability to recieved IP !!
```

```
| [2000-01-01 00:10:50.713] [offline-migration] migration decision
| [2000-01-01 00:10:50.713] [offline-migration][v4] WLC IP present in DHCP option 43
| [2000-01-01 00:10:55.759]
```

```
[offline-migration][v4][capwap] DHCP: WLC 10.127.197.196 is down
```

```
!! WLC IP received on DHCP option is running on unsupported release !!
```

```
| [2000-01-01 00:39:44.529] [fast-offline-migration] waiting for 48sec before taking any migration deci  
| [2000-01-01 00:40:35.585] [offline-migration] forcing DHCP renew  
| [2000-01-01 00:40:35.586] [offline-migration] forcing DHCPv6 INFORMATION REQUEST  
| [2000-01-01 00:40:41.592] [offline-migration] migration decision  
| [2000-01-01 00:40:41.593] [offline-migration][v4] WLC IP present in DHCP option 43  
| [2000-01-01 00:40:41.675]
```

```
[offline-migration][v4][capwap] DHCP: WLC 10.127.197.196 is unsupported - version 17.12.4.22
```

```
| [2000-01-01 00:40:41.675] [offline-migration][v4] missing DNS config (server and/or domain)  
| [2000-01-01 00:40:41.675] [offline-migration][v6] no WLC IP in DHCP option 52  
| [2000-01-01 00:40:41.675] [offline-migration][v6] missing DNS config (server and/or domain)
```

Wenn die Offline-Migration mit der DHCP-Option fehlschlägt, versucht der Access Point (AP), die DNS-Option zu aktivieren, indem er den Domännennamen und die DNS-Serverinformationen aus der DHCP-Antwort extrahiert. Dieser Vorgang kann mit folgendem Fehler enden:

## DNS-Auflösungsfehler

```
<#root>
```

```
!! No valid DNS server or domain name received in DHCP reply !!
```

```
| [2000-01-01 00:14:19.658] [fast-offline-migration] waiting for 0min before taking any migration decisio  
| [2000-01-01 00:15:07.101] [offline-migration] forcing DHCP renew  
| [2000-01-01 00:15:07.102] [offline-migration] forcing DHCPv6 INFORMATION REQUEST  
| [2000-01-01 00:15:12.150] [offline-migration] migration decision  
| [2000-01-01 00:15:12.150] [offline-migration][v4] no WLC IP in DHCP option 43  
| [2000-01-01 00:15:12.150]
```

```
[offline-migration][v4] missing DNS config (server and/or domain)
```

```
| [2000-01-01 00:15:12.151] [offline-migration][v6] no WLC IP in DHCP option 52  
| [2000-01-01 00:15:12.151]
```

```
[offline-migration][v6] missing DNS config (server and/or domain)
```

```
!! Unable to resolve the hostname
```

```
cisco-capwap-controller.
```

```
!!
| [2026-06-24 11:19:12.395] [offline-migration] migration decision
| [2026-06-24 11:19:12.395] [offline-migration][v4] no WLC IP in DHCP option 43
| [2026-06-24 11:19:12.479]

[offline-migration][v4] no WLC IP resolved by DNS

| [2026-06-24 11:19:12.527] [offline-migration][v4] no PnP IP resolved by DNS

!! No CAPWAP reachability or unsupported version !!

| [2000-01-01 00:15:07.102] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:15:12.150] [offline-migration] migration decision
| [2000-01-01 00:15:12.150] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:15:12.150] [offline-migration][v4]
```

WLC IP resolved by DNS: 10.127.197.233

```
| [2000-01-01 00:15:12.151] [offline-migration][v4][capwap]
```

DNS: WLC 172.16.30.10 is not valid/ unsupported version 17.12.4.22

## Fallback zur Layer-2-CAPWAP-Erkennung

Wenn sowohl die DHCP- als auch die DNS-Methode fehlschlagen, sendet der Access Point eine CAPWAP-Erkennungsanforderung für Layer 2. Zu den häufigen Fehlern gehören:

- Keine Antwort auf CAPWAP-Erkennung

```
<#root>
```

```
| [2000-01-01 00:23:37.901] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:23:42.949] [offline-migration] migration decision
| [2000-01-01 00:23:42.949] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:23:42.949] [offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:23:42.950] [offline-migration][v6] no WLC IP in DHCP option 52
| [2000-01-01 00:23:42.950] [offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:23:48.22 ]
```

```
[offline-migration][v4][capwap-12] 0 WLC(s) detected (unsupported)
```

```
| [2000-01-01 00:23:53.66 ]
```

```
[offline-migration][v6][capwap-12] 0 WLC(s) detected (unsupported)
```

```
| [2000-01-01 00:23:53.66 ] [offline-migration] no migration & not claimed => restart detection
```

Zu diesem Zweck muss auf dem Wireless Controller (WLC) die automatische CAPWAP-Integration aktiviert sein, damit sowohl Unicast- als auch Broadcast-Erkennungsanfragen akzeptiert werden. Anmerkung: Diese Einstellung ist standardmäßig deaktiviert und kann CAPWAP-Erkennungsanfragen ablehnen, die speziell von APs mit globaler Verwendung im Day-0-Modus gesendet werden. Aktivieren Sie diese Einstellung im Standard-AP-Join-Profil. Dieses Profil wird verwendet, wenn der Access Point zu Beginn dem Controller beitrifft.

```
<#root>
```

```
CW9800(config)#
```

```
ap profile default-ap-profile
```

```
CW9800(config-ap-profile)#capwap-discovery onboarding ?
```

```
all          Configure automatic CAPWAP onboarding from Meraki based on both unicast and broadcast o
```

```
unicast     Configure automatic CAPWAP onboarding from Meraki based on unicast discovery request or
```

- Erfolgreiche Antwort, aber nicht unterstützte Version - Der antwortende WLC läuft nicht auf Version 17.15.02 oder höher:

```
<#root>
```

```
| [2000-01-01 00:15:07.101] [offline-migration] forcing DHCP renew
| [2000-01-01 00:15:07.102] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:15:12.150] [offline-migration] migration decision
| [2000-01-01 00:15:12.150] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:15:12.150] [offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:15:12.151] [offline-migration][v6] no WLC IP in DHCP option 52
| [2000-01-01 00:15:12.151] [offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:15:17.193]
```

```
[offline-migration][v4][capwap-12] 1 WLC(s) detected (unsupported)
```

```
| [2000-01-01 00:15:17.283]
```

```
[offline-migration][v4][capwap-12] - unsupported - 10.127.197.196 - 17.12.4.22
```

## AP schließt Beitrittsphase nicht ab

Sobald der AP erfolgreich in den CATALYST-Modus konvertiert wurde, wird für die Verbindung mit dem Wireless LAN Controller 9800 dasselbe Verbindungsverfahren wie für andere Catalyst APs verwendet. Probleme können in drei Phasen auftreten:

- CAPWAP-Erkennungsphase

- Etablierungsphase des DTLS-Tunnels
- Teilnahmephase

Wenden Sie denselben Fehlerbehebungsansatz an, indem Sie auf [Erläuterung des AP-Beitrittsprozesses beim Catalyst 9800 WLC](#).

## Fehler bei der Auflösung der AP-Zulassung

Der Access Point der Serie CW917x verfügt über keinen vordefinierten Zulassung. Der Ländercode kann auf Zugangspunkten der Serie CW917x nicht manuell über den Controller konfiguriert werden. Stattdessen bestimmt der WAP automatisch den Ländercode mithilfe verschiedener Methoden wie Näherungserkennung (RF und CDP/LLDP), GPS/GNSS und der RAF-Datei auf dem WLC.

### AP-Support nach Land (jeweilige Version)

Überprüfen Sie vor der Fehlerbehebung im Zulassungsbereich, ob das jeweilige Zugangspunktmodell der Serie CW917x in dem Land unterstützt wird, das Sie für Ihre Version des 9800-Controllers konfigurieren möchten. Wenn das Land nicht unterstützt wird, bleiben beide Funkgeräte inaktiv.

Sie können die Länder-zu-Kanal-Zuordnung in der technischen Referenz für Ihr spezifisches AP-Modell und die WLC-Version in der [Access Point Feature Matrix](#) überprüfen und überprüfen, ob die Unterstützung für ein bestimmtes Land in der spezifischen Controller-Version für Access Points der Serie CW917x verfügbar ist.

Darüber hinaus können Sie das Dokument nachlesen, in dem die Zulassungsphase für die CW917x APs [von Cisco CW917x Wi-Fi 7 Access Point-Ländercodes und -phasen für die](#) einzelnen Länder beschrieben wird.

Wenn Sie sichergestellt haben, dass Ihr Land von der WLC-Version für den Access Point der Serie CW917x unterstützt wird, überprüfen Sie, ob der Access Point seine Zulassung mit einer der unterstützten Methoden auflösen kann. Wenn der Access Point den Zulassungsbereich nicht auflöst, wird der Status des Access Points angezeigt:

```
<#root>
```

```
WLC#
```

```
show ap summary
```

```
Number of APs: 2
```

CC = Country Code  
RD = Regulatory Domain

AP Name        Slots        AP Model        Ethernet MAC        Radio MAC

CC    RD

IP Address	State	Location					
LAB-9136	4	C9136I-ROW	aaaa.bbbb.cccc	aaaa.bbbb.cccc	IN	-RW	10.127.197.153
LAB-CW9172	3	CW9172H	aaaa.bbbb.cccc	aaaa.bbbb.cccc			

--    -UN

10.127.197.152    Registered    default location

<#root>

WLC#

show ap config general | in AP\_NAME | Country

Cisco AP Name : AP\_NAME  
Regulatory Domain Allowed by Country : 802.11bg:-A^ 802.11a:-DN^ 802.11 6GHz:  
AP Country Code

: - >> No Country Code resolved

## Verwenden von Proximity

Wi-Fi 7-APs im weltweiten Modus können den Ländercode bestehender älterer APs oder mit demselben WLC verbundener Wi-Fi 7-APs auf dem Stockwerk oder von APs, die als CDP/LLDP-Nachbarn erkannt wurden, auflösen. Die auf Proximity basierende Erkennung kann entweder die RF-basierte Erkennung oder die CDP/LLDP-Nachbarerkennung verwenden. Wenn der WLAN-7-WAP den benachbarten WAP nicht über Proximity erkennen kann, wird der Fehler angezeigt:

<#root>

[\*06/28/2026 15:24:36.7773]

Sending proximity\_request payload

[\*06/28/2026 15:24:36.7787]

SinglePID Proximity resolution: Country Code not available

```
[*06/28/2026 15:24:36.7795] SinglePID Regulatory Blob resolution: Country Code not available  
[*06/28/2026 15:25:35.8011] Sending proximity_request payload  
[*06/28/2026 15:25:35.8025] SinglePID Proximity resolution: Country Code not available  
[*06/28/2026 15:25:35.8031] SinglePID Regulatory Blob resolution: Country Code not available
```

## RF-basiert

Damit diese Methode funktioniert, positionieren Sie den Access Point mit aufgelöstem Ländercode und Wi-Fi 7 AP-Zulassung in der Nähe, damit dieser benachbarte Ermittlungspakete austauschen kann. Dieser Access Point muss mit demselben WLC verbunden sein, dessen Ländercode bereits aufgelöst wurde. Diese Pakete werden über das 2,4-GHz-Funkmodul ausgetauscht. Stellen Sie daher sicher, dass das 2,4-GHz-Funkmodul auf dem Ziel-AP aktiviert ist (dem AP, von dem der Ländercode aufgelöst werden soll).

## CDP-/LLDP-basiert

Der CDP/LLDP-basierte Erkennungsmechanismus wird verwendet, wenn ein voll funktionsfähiger Access Point mit einem aufgelösten Ländercode und ein Wi-Fi 7-Access Point im weltweiten Modus (ohne Ländercode) mit demselben Switch und demselben WLC verbunden sind.

Um diese Methode zu verwenden, stellen Sie Folgendes sicher:

- Beide APs sind mit demselben Switch verbunden.
- Beide APs sind mit demselben WLC verbunden.
- Ein Access Point verfügt über eine aufgelöste Ländervorwahl und ist aktiv für Kunden zuständig.
- Der WLAN-7-Zugangspunkt befindet sich im weltweiten Modus und erfordert einen Ländercode.



Anmerkung: Die CDP-/LLDP-basierte Erkennung wird ab Cisco IOS XE 17.15.4 und 17.18.1 unterstützt. Stellen Sie sicher, dass auf Ihrem WLC eine dieser unterstützten Versionen oder höher ausgeführt wird.

---

## Verwenden der RAF-Datei

Wenn die Proximity-Methode die Zulassungsdomäne nicht auflösen kann, können Sie alternativ die RAF (Regulatory Domain Authorization File) aus dem Meraki Dashboard verwenden. Gehen Sie dazu folgendermaßen vor:

1. Setzen Sie den Wi-Fi 7 AP über einen Cloud-AP in Anspruch, und fügen Sie ihn Ihrem Netzwerk hinzu. Beachten Sie, dass der Access Point nicht über eine Netzwerkverbindung zum hinzuzufügenden Meraki Dashboard verfügen muss.
2. Konfigurieren Sie den erforderlichen Ländercode für den Access Point im Netzwerk, in dem der Access Point beansprucht wurde.
3. Laden Sie die Datei für die Zulassung vom Controller herunter, und laden Sie sie hoch. Die Datei muss die Seriennummer, die MAC-Adresse und den Ländercode des APs enthalten.

<#root>

!! Verify the data on RAF File !!

WLC#

show ap regulatory activation all

Regulatory Activation file Meta-data

-----  
Date Created : 06/30/2026 08:12:41

Created By : shchoube@cisco.com

Device count : 2

Organization Id : 1780642

AP MAC	Serial Number	Country code
AP1_MAC	AP1_SN	IN
AP2_MAC	AP2_SN	US

4. Wenn Sie demselben Controller neue APs hinzufügen, die andere Ländercodes erfordern, platzieren Sie diese in separaten Netzwerken im Meraki Dashboard. Dadurch wird sichergestellt, dass die Ländercodeeinstellungen sich nicht gegenseitig überschreiben.

## AP aufgrund von Lizenzproblemen nicht konform

Wenn ein Access Point dem richtigen Ländercode beitrifft, kann er dennoch ein Compliance-Problem melden, wenn er nicht lizenziert ist. Wi-Fi 7 APs werden einer Konformitätsprüfung unterzogen und erfordern Cisco Wireless-Lizenzen (CW). Im Gegensatz dazu verwenden frühere APs, die keine Wi-Fi-7-Access Points sind, AIR-Lizenzen und erfordern keine Compliance-Prüfung.

<#root>

WLC#

```
show ap summary license
```

For AIR licenses, per AP tracking of license state is unavailable. Please use "show license summary" to Policy allowed state means device is deemed compliant due to a policy downloaded from licensing authority

AP Name	AP Model	AP MAC	License Type	License State	Non Compliance Reason
AP1	CW9172H	xxxx.xxxx.xxxx	CW	Non Compliant	Never Licensed
AP2	CW9176I	xxxx.xxxx.xxxx	CW	Non Compliant	Never License

WLC#

```
show license summary
```

Account Information:

Smart Account: <none>

Virtual Account: <none>

License Usage:

License Entitlement Tag Count Status

-----  
cisco-wireless-advan... (CNS\_CW\_A) 2 IN USE

!! Check the current level of license configured on WLC for WiFi7AP !!

WLC#

```
show version | in License Level
```

License Level: adventerprise

AIR License Level: AIR Network Essentials addon AIR DNA Essentials

Next reload AIR License Level: AIR Network Essentials addon AIR DNA Essentials

Cisco Wireless License Level: Cisco Wireless Advantage

Next reload Cisco Wireless License Level: Cisco Wireless Advantage

Stellen Sie bei diesem Problem sicher, dass auf dem 9800 WLC die richtige Lizenzstufe für die Verwendung mit den Wi-Fi7-APs konfiguriert ist. Für Wi-Fi7-APs sind CW-Lizenzen erforderlich:

1. Cisco Wireless Essentials
2. Vorteile von Cisco Wireless

Wenn APs nicht lizenziert sind, beheben Sie die Smart Licensing-Probleme auf dem 9800 WLC über [Konfigurieren und Fehlerbehebung für Smart Licensing auf dem Catalyst 9800](#).

## Protokollsammlung

Protokolle von WLC

- Aktivieren Sie `term exec prompt timestamp`, um einen Zeitverweis für alle Befehle zu erhalten.
- `show`-Befehle:
  - `show ap summary` | i Anzahl der APs
  - `sh log` | i AP-Ereignis:
  - Anzeigen der AP-Verfügbarkeit
  - `show ap cdp neighbor`
  - Wireless-Zustandsübersicht anzeigen
  - Anzeige der Wireless-Zustandszuordnung
  - Zusammenfassung der Wireless-Zuordnungszuordnung anzeigen
  - Wireless-Zertifizierungskonfiguration anzeigen
  - Wireless-Management-Vertrauenspunkt anzeigen
  - Wireless-DTLS-Verbindungen anzeigen
  - `show logging profile wireless start last X days filter mac <radio-or-ethernet-AP-mac>`
  - `show ap regulatorische aktivierung alle`
  - `show ap config general`
  - `Show tech-support wireless`
- Radio Active Trace:
  - `debugging wireless AP_MAC {aaa.bbb.cccc} {Überwachungszeit} {N Sekunden} !!` Die Einstellung der Zeit erlaubt es uns, Traces für bis zu 24 Tage zu aktivieren.
  - Kein Debuggen Wireless AP\_MAC {aaa.bbb.cccc} !! So deaktivieren Sie das Debuggen

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



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

---

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

`# klare Plattformbedingung alle !!`

`# underbug all !!`

Über GUI:

Schritt 1: Navigieren Sie zu Fehlerbehebung > Radioaktive Verfolgung.

Schritt 2: Klicken Sie auf Hinzufügen, und geben Sie die AP-MAC-Adresse ein.

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

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

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

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

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

- Integrierte Paketerfassung gefiltert nach AP-IP-Adressen-ACL:

!! Erstellen einer ACL !!

```
ip access-list extended CAP-FILTER
```

```
permit ip host <AP_IP> any
```

```
permit ip any host <AP_IP>
```

!! Paketerfassung konfigurieren !!

MYCAP-Schnittstelle Po1 überwachen, beide

MYCAP-Puffer mit kreisförmiger Größe 100 erfassen

```
monitor capture MYCAP access-list CAP-FILTER monitor capture MYCAP match  
any/ipv4/ipv6.MAC !!
```

MYCAP Start überwachen !!

!!Vervielfältigen

MYCAP-Stopp überwachen

MYCAP-Exportflash überwachen:|tftp:|http:.../filename.pcap

Protokolle vom Access Point

## AP im Meraki-Modus

- offline-migration-info um aktuelle Protokolle und den Status des Migrationsversuchs abzurufen.

## AP im Catalyst-Modus

- Technologie anzeigen !! Sammeln Sie Show-Tech, um alle Konfigurationsdetails und Funkstatistiken für den Access Point zu erhalten.
- dtls-Verbindung anzeigen !! Zertifikate, Ports und Chiffren, Versionen für DTLS prüfen
- Terminalmonitor und Protokollierungskonsole bei SSH-Zugriff zur Aktivierung der Konsolenprotokollierung und -anzeige
- Grundlegende Debug-Funktionen
  - debug capwap client event
  - debug capwap client error
  - debuggen dtls-Clientfehler
  - debuggen dtls-Clientereignis
- Erweiterte Debugging-Optionen
  - debuggen capwap client keepalive
  - debug capwap client pmtu
  - debug capwap client payload
  - Debug Capwap-Clientdetails

## Protokolle vom mit dem AP verbundenen Uplink-Switch

- Eingebettete Paketerfassung am Port des AP-Anschlusses
  - monitor capture mycap interface <AP\_Connected\_Port> beide
  - mycap-Übereinstimmung der Monitorerfassung mit allen
  - Größe des Monitorerfassungspuffers 50
  - überwachen erfassen mycap-Datei Speicherort flash:mycap.pcap
  - mycap Start/Stopp überwachen
  - show monitor-Erfassungsdatei flash:mycap.pcap
- Switched Port Analyzer (SPAN-Erfassung)
  - Überwachungssitzung 1 Quellschnittstelle <AP\_Connected\_Port>
  - monitor session 1 destination interface x/x/x encapsulation replicate >>>> — Der

Port, an dem der PC mit Wireshark verbunden ist.

---



Anmerkung: Wenn ein Drittanbieter-Switch verwendet wird, erfassen Sie einen Port-SPAN oder eine gleichwertige Paketerfassung auf dem Uplink-Switch-Port.

---

## Zugehörige Informationen

- [Bereitstellungsleitfaden für Cisco Wireless Access Points der Serie CW917x](#)

## Informationen zu dieser Übersetzung

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