

Konfigurieren und Integrieren von APs auf Nicht-SDA-EWC-Switch (C9800-SW)

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Bedingtes Debugging und Radio Active Tracing](#)

[Beispiel für einen erfolgreichen AP-Beitritt](#)

Einleitung

In diesem Dokument wird das Verfahren zur Integration und Bereitstellung eines Access Points (AP) mit einem Embedded Wireless Controller auf einem Catalyst 9000 (Catalyst 9K) Switch (EWC-Switch) in Nicht-SDA-Bereitstellungen beschrieben (es wird kein Cisco DNA Center verwendet).

Voraussetzungen

Anforderungen

Sie müssen folgende Voraussetzungen erfüllen:

- Installieren Sie das Wireless-Unterpaket auf dem Catalyst 9K-Switch, der als Wireless LAN Controller (WLC) fungiert.
- Stellen Sie sicher, dass die Loopback-Schnittstelle so konfiguriert ist, dass sie als Wireless Management Interface (WMI) konfiguriert wird.
- Stellen Sie sicher, dass der GUI-Zugriff auf den Catalyst 9K-Switch aktiviert ist, da eine Konfiguration über die GUI empfohlen wird.

Hinweis: Der EWC-Switch für Nicht-SDA-Bereitstellungen wird nur in Versionen 17.3.x unterstützt.

Verwendete Komponenten

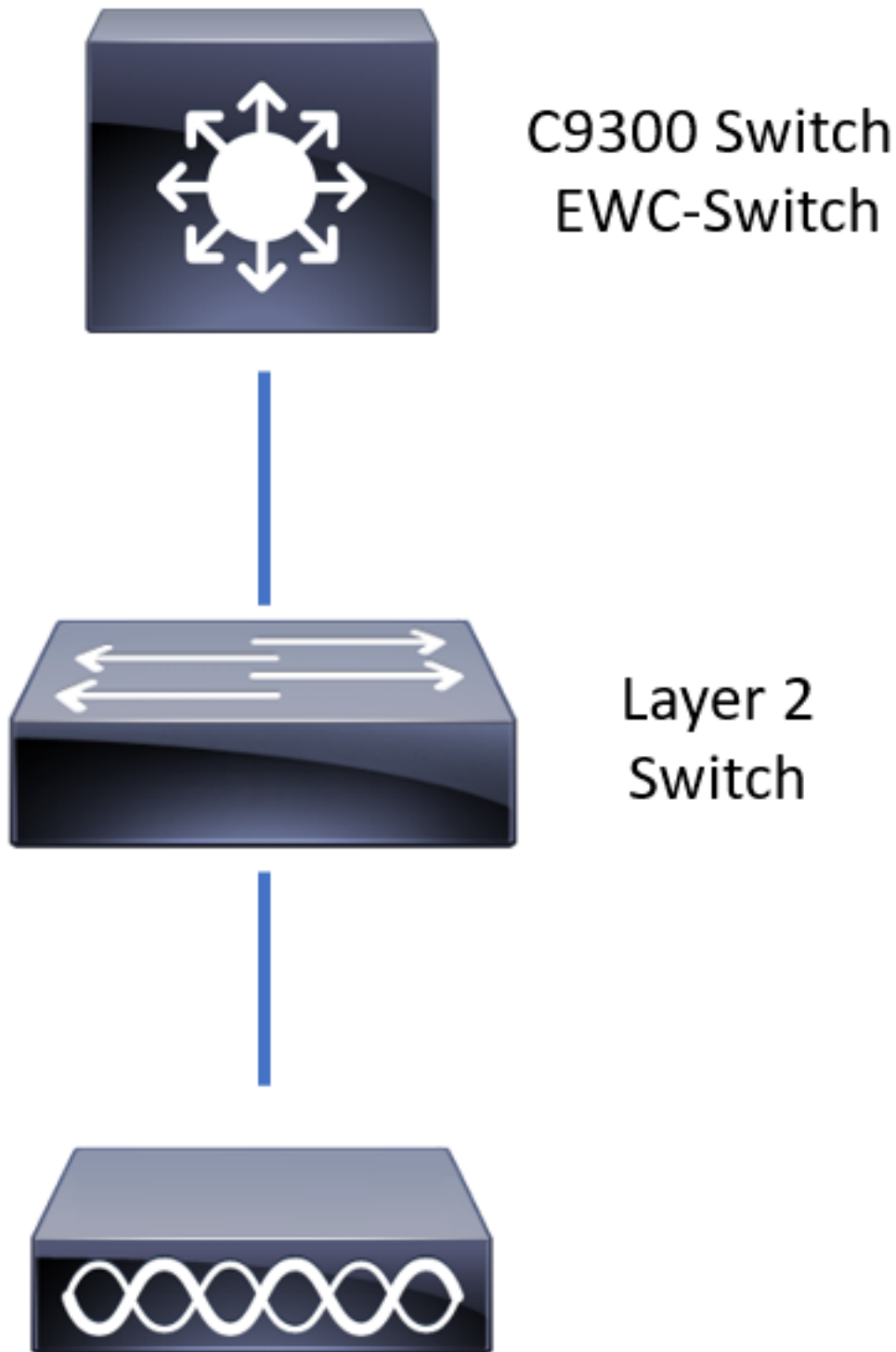
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9300-24P Switch, Cisco IOS® XE Version 17.3.4
- Wireless-Unterpaket für Version 17.3.4
- C9120-AX AP

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

Konfigurieren

Netzwerkdiagramm



APs dürfen direkt mit dem EWC-Switch verbunden werden, dies ist jedoch keine Anforderung. Es wird empfohlen, einen Access Switch zum Anschließen von APs zu verwenden, um bei einem Ausfall des EWC-Switches ein Hochverfügbarkeits-Failover zu ermöglichen.

Konfigurationen

Schritt 1: Konfigurieren Sie den Ländercode für die geografischen Standorte, an denen die Access Points bereitgestellt werden. Dies ist obligatorisch, damit sich die Access Points registrieren können und die Einhaltung der Richtlinien des jeweiligen Landes, in dem sie bereitgestellt werden, sichergestellt ist. Navigieren Sie in der GUI zu **Configuration > Wireless > Access Points**, und

klicken Sie auf die Registerkarte **Country (Land)**. Wählen Sie alle zutreffenden **Ländercodes** aus, um die Zulassungsdomänen der APs abzugleichen.

Hinweis: In den Versionen 17.3.1 bis 17.3.3 listet die EWC-Switch-GUI die Ländercodes auf, wendet jedoch keine Auswahl an, bis ein Ländercode über die CLI hinzugefügt wird, wie in Cisco Bug-ID [CSCvw20478](#) beschrieben. Nachdem ein Ländercode konfiguriert wurde, können Sie über die GUI weitere Ländercodes hinzufügen.

Configuration > Wireless > Access Points

> All Access Points

> 5 GHz Radios

> 2.4 GHz Radios

> Dual-Band Radios

Country

[Click here](#) for list of access point models and protocols supported per country and regulatory domain.

Selected Country MX, US

Apply

Regulatory Domain

802.11a/n/ac: [Indoor: -ABN, Outdoor: -ABN]

802.11b/g/n: [Indoor: -A, Outdoor: -ABN]

Search

	Country Code	Name
<input type="checkbox"/>	MY	Myanmar
<input type="checkbox"/>	MO	Macau
<input type="checkbox"/>	MT	Malta
<input checked="" type="checkbox"/>	MX	Mexico
<input type="checkbox"/>	MY	Malaysia
<input type="checkbox"/>	NG	Nigeria
<input type="checkbox"/>	NL	Netherlands
<input type="checkbox"/>	NO	Norway

CLI-Konfiguration (17.3.1 bis 17.3.3):

```
9300-1#configure terminal
9300-1(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n) [y]: y
9300-1(config)#ap dot11 24ghz shutdown
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n) [y]: y
9300-1(config)#wireless country MX
9300-1(config)#no ap dot11 5ghz shutdown
9300-1(config)#no ap dot11 24ghz shutdown
```

Schritt 2: Aktivieren Sie die Funktion des Wireless Controllers, und konfigurieren Sie das VLAN, in dem sich die APs befinden. Navigieren Sie zu **Configuration > Embedded Wireless Setup**, schieben Sie **Embedded Wireless Setup** auf Enabled, und klicken Sie unter **Location Configuration** auf **+ Add**.

Configuration > Embedded Wireless Setup

Embedded Wireless Setup DISABLED [Apply](#)

Location Configuration

[+ Add](#)

No locations available

Wenn die integrierte Wireless-Einrichtung aktiviert ist, werden diese Befehle per Push an die CLI übertragen. Diese CLIs aktivieren die LISP-Fabric auf dem Catalyst 9000-Switch und dienen somit als Kontrollebenen-/Zuordnungsserver-Knoten, Wireless-Controller mit Loopback als WMI und WLC für die Zuordnung der Kontrollebene, damit die APs und die Clients integriert werden können.

```
9300-1(config)#router lisp
9300-1(config-router-lisp)# locator-table default
9300-1(config-router-lisp)# locator-set rloc_ewlc
9300-1(config-router-lisp-locator-set)# IPv4-interface Loopback0
9300-1(config-router-lisp-locator-set)# auto-discover-rlocs
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# locator-set WLC
9300-1(config-router-lisp-locator-set)#
```

```
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# service ipv4
9300-1(config-lisp-srv-ipv4)# encapsulation vxlan
9300-1(config-lisp-srv-ipv4)# itr map-resolver
```

```
9300-1(config-lisp-srv-ipv4)# etr map-server
```

```
9300-1(config-lisp-srv-ipv4)# etr map-server
```

```
9300-1(config-lisp-srv-ipv4)# etr  
9300-1(config-lisp-srv-ipv4)# sgt  
9300-1(config-lisp-srv-ipv4)# no map-cache away-eids send-map-request  
9300-1(config-lisp-srv-ipv4)# proxy-etr  
9300-1(config-lisp-srv-ipv4)# proxy-itr
```

```
9300-1(config-lisp-srv-ipv4)# map-server  
9300-1(config-lisp-srv-ipv4)# map-resolver  
9300-1(config-lisp-srv-ipv4)# exit-service-ipv4  
9300-1(config-router-lisp)# service ethernet  
9300-1(config-lisp-srv-eth)# itr map-resolver
```

```
9300-1(config-lisp-srv-eth)# itr  
9300-1(config-lisp-srv-eth)# etr map-server
```

```
9300-1(config-lisp-srv-eth)# etr map-server
```

```
9300-1(config-lisp-srv-eth)# etr  
9300-1(config-lisp-srv-eth)# map-server  
9300-1(config-lisp-srv-eth)# map-resolver  
9300-1(config-lisp-srv-eth)# exit-service-ethernet  
9300-1(config-router-lisp)# ipv4 source-locator Loopback0  
9300-1(config-router-lisp)# map-server session passive-open WLC  
9300-1(config-router-lisp)# exit
```

```
9300-1(config)# interface LISP0  
9300-1(config-if)# exit
```

```
9300-1(config)# router lisp  
9300-1(config-router-lisp)# site site_uci  
9300-1(config-router-lisp-site)# description map-server configured from Wireless LAN Controller  
9300-1(config-router-lisp-site)# authentication-key
```

```
9300-1(config-router-lisp-site)# exit-site  
9300-1(config-router-lisp)# exit-router-lisp
```

```
9300-1(config)# ip dhcp relay information option  
9300-1(config)# wireless fabric  
9300-1(config)# wireless management interface Loopback0  
9300-1(config-mgmt-interface)# exit
```

```
9300-1(config)# wireless fabric control-plane default-control-plane
9300-1(config-wireless-cp)# ip address
```

```
9300-1(config-wireless-cp)# exit
```

Schritt 3: Geben Sie im Popup-Fenster, das nach Schritt 2 generiert wird, auf der Registerkarte **Allgemein** den **Standortnamen** und die **AP-Onboarding**-Details wie VLAN und Subnetzmaske ein. Standardmäßig enthält das VLAN-Feld 2045. Es kann eine andere VLAN-ID verwendet werden, die VLAN-ID muss jedoch zwischen 2045 und 4094 liegen und vom Client-Datenverkehr unabhängig sein (kabelgebundene oder Wireless-Clients dürfen dieses VLAN nicht verwenden). Klicken Sie nach Abschluss der Details auf **Apply**

Configuration > Embedded Wireless Setup

Location Configuration

← Back

General Wireless Networks AP Provisioning

Location Name*	EWC-Location	AP Onboarding	
Description	Enter Description	VLAN*	2674
Client Density	Low Typical High	IP Address*	172.16.80.1
		Subnet Mask*	255.255.255.0
		DHCP Server*	172.16.80.1

Apply

Dadurch werden das VLAN für die APs, eine SVI für das AP-VLAN (Standard-Gateway für die APs), der AP-Standort, Richtlinien- und RF-Tags sowie L2- und L3-VNIDs (Virtual Network Identifiers) erstellt. Dies sind die Befehle, die in der CLI als Ergebnis von Schritt 3 angezeigt werden.

```
9300-1(config)# interface LISP0.4097
9300-1(config-subif)# router lisp
9300-1(config-router-lisp)# locator-set rloc_ewlc
9300-1(config-router-lisp-locator-set)# exit-locator-set
9300-1(config-router-lisp)# instance-id 4097
9300-1(config-lisp-inst)# remote-rloc-probe on-route-change
9300-1(config-lisp-inst)# dynamic-eid APONBOARDING_0_2674_4097_8188
9300-1(config-lisp-inst-dyn-eid)# database-mapping 172.16.80.0/24 locator-set rloc_ewlc
9300-1(config-lisp-inst-dyn-eid)# exit-dynamic-eid
9300-1(config-lisp-inst)# service ipv4
9300-1(config-lisp-inst-srv-ipv4)# eid-table default
9300-1(config-lisp-inst-srv-ipv4)# map-cache 172.16.80.0/24 map-request
9300-1(config-lisp-inst-srv-ipv4)# route-export site-registrations
9300-1(config-lisp-inst-srv-ipv4)# distance site-registrations 250
9300-1(config-lisp-inst-srv-ipv4)# map-cache site-registration
9300-1(config-lisp-inst-srv-ipv4)# exit-service-ipv4
9300-1(config-lisp-inst)# exit-instance-id
9300-1(config-router-lisp)# instance-id 8188
9300-1(config-lisp-inst)# remote-rloc-probe on-route-change
9300-1(config-lisp-inst)# service ethernet
```

```

9300-1(config-lisp-inst-srv-eth)# eid-table vlan 2674
9300-1(config-lisp-inst-srv-eth)# database-mapping mac locator-set rloc_ewlc
9300-1(config-lisp-inst-srv-eth)# exit-service-ethernet
9300-1(config-lisp-inst)# exit-instance-id
9300-1(config-router-lisp)# site site_uci
9300-1(config-router-lisp-site)# eid-record instance-id 4097 172.16.80.0/24 accept-more-
specifics
9300-1(config-router-lisp-site)# eid-record instance-id 8188 any-mac
9300-1(config-router-lisp-site)# exit-site
9300-1(config-router-lisp)# exit

9300-1(config)# vlan 2674
9300-1(config-vlan)# name AP_VLAN2674
9300-1(config-vlan)# exit

9300-1(config)# interface Vlan2674
9300-1(config-if)# description APONBOARDING_0_2674_4097_8188
9300-1(config-if)# mac-address 0000.0C9F.FAD1
9300-1(config-if)# ip address 172.16.80.1 255.255.255.0
9300-1(config-if)# ip helper-address 172.16.80.1
9300-1(config-if)# no ip redirects
9300-1(config-if)# ip route-cache same-interface
9300-1(config-if)# no lisp mobility liveness test
9300-1(config-if)# ip directed-broadcast
9300-1(config-if)# lisp mobility APONBOARDING_0_2674_4097_8188
9300-1(config-if)#exit

9300-1(config)# wireless fabric name APONBOARDING_0_2674_4097_8188 12-vnid 8188 13-vnid 4097 ip
172.16.80.0 255.255.255.

```

Schritt 4: Konfigurieren Sie den Catalyst 9K-Switch so, dass er auch als DHCP-Server für das AP-VLAN fungiert, und erstellen Sie entsprechende DHCP-Pools. Navigieren Sie zu **Administration > DHCP Pools**, und klicken Sie auf **+ Hinzufügen**. Legen Sie einen Poolnamen und Netzwerkparameter fest. Stellen Sie sicher, dass das Standard-Gateway auf die SVI-IP-Adresse eingestellt ist. Andernfalls werden die APs teilweise dem Controller hinzugefügt.

Create DHCP Pool
✕

Basic Advanced

DHCP Pool Name* (1-236 Characters)

IP Type

Network*

Subnet Mask*

Starting ip*

Ending ip*

Reserved Only DISABLED

Lease*

(0-365 days)
 (0-23 hours)
 (0-59 minutes)

↶ Cancel

📄 Apply to Device

Create DHCP Pool
✕

Basic
 Advanced

Enable DNS Proxy

Default Router(s) xxx.xxx.xxx.xxx +

IP Address	Remove	
172.16.80.1	✕	^
No items to display		

DNS Server(s) xxx.xxx.xxx.xxx +

IP Address	Remove	
No items to display		

NetBios Name Server(s) xxx.xxx.xxx.xxx +

IP Address	Remove	
No items to display		

Domain cisco.com

DHCP Options List

↶ Cancel

📄 Apply to Device

CLI-Konfiguration:

```
9300-1#configure terminal
9300-1(config)#ip dhcp excluded-address 172.16.80.0 172.16.80.9
9300-1(config)#ip dhcp pool
```

```
9300-1(dhcp-config)#network 172.16.80.0 255.255.255.0
9300-1(dhcp-config)#default-router 172.16.80.1
```

Schritt 5: Konfigurieren Sie den Switch-Port im Zugriffsmodus, und weisen Sie ihn dem zuvor definierten VLAN zu.

```
3850-1(config)#interface
```

```
3850-1(config-if)#switchport mode access
3850-1(config-if)#switchport access vlan
```

Schritt 6: Navigieren Sie zu **Configuration > Embedded Wireless Setup**, und wählen Sie den in Schritt 3 erstellten Standort aus. Klicken Sie auf die Registerkarte **AP Provisioning (AP-Bereitstellung)**, und wählen Sie aus der Liste der verfügbaren APs die APs aus, die bereitgestellt

werden sollen, und klicken Sie auf den blauen Pfeil, um die Liste der **zugeordneten APs** zu ändern. Wenn alle gewünschten Access Points dem jeweiligen Standort zugewiesen wurden, klicken Sie auf **Apply**.

Achtung: Der EWC-Switch ermöglicht die manuelle Tag-Erstellung und -Zuweisung. Dies wird jedoch nicht unterstützt, und die einzige unterstützte Tag-Zuweisung erfolgt über die Standortzuweisung. Auf dem EWC-Switch wird nur ein Standort unterstützt. Daher müssen sich alle Access Points im gleichen Subnetz befinden und demselben Standort zugewiesen sein.

Configuration > Embedded Wireless Setup

Location Configuration

← Back Delete Location

General Wireless Networks **AP Provisioning**

Add/Select APs APs on this Location Apply

Import AP MAC Select File Select CSV File

AP MAC Address

Available AP list Search +

Number of selected APs : 1

<input checked="" type="checkbox"/>	AP MAC	AP Name
<input checked="" type="checkbox"/>	5ce1.7629.2b40	AP5CE1.7629.2B40

1 - 1 of 1 items

Associated AP list Search

Number of selected APs : 0

<input type="checkbox"/>	AP MAC	AP Name	Status
No items to display			

5... items per page

General Wireless Networks **AP Provisioning**

Add/Select APs APs on this Location Apply

Import AP MAC Select File Select CSV File

AP MAC Address

Available AP list Search

Number of selected APs : 0

<input type="checkbox"/>	AP MAC	AP Name
No items to display		

0 items per page

Associated AP list Search

Number of selected APs : 0

<input type="checkbox"/>	AP MAC	AP Name	Status
<input type="checkbox"/>	5ce1.7629.2b40	AP5CE1.7629.2B40	Joined

1 - 1 of 1 items

5... items per page

Mit diesem Schritt wird diese Konfiguration dem EWC-Switch hinzugefügt:

```
9300-1(config)# ap location name EWC-Location
9300-1(config-ap-location)# ap-eth-mac
```

```
9300-1(config-ap-location)# tag policy EWC-Location
9300-1(config-ap-location)# tag rf EWC-Location
```

Der Befehl **ap-eth-mac <AP-MAC-Adresse>** wird für jeden AP wiederholt, der dem Standort hinzugefügt wird. Ein einzelner Standort unterstützt bis zu 500 APs.

Überprüfung

Verwenden Sie diesen Befehl, um die Erstellung und den Status des VLANs für WMI und AP Onboard zu überprüfen.

```
9300-1#show wireless fabric summary
```

```
Fabric Status : Enabled
```

```
Control-plane:
```

```
Name IP-address Key Status
```

```
-----
default-control-plane 172.16.0.1 ciscoeca Up
```

```
Fabric VNID Mapping:
```

```
Name L2-VNID L3-VNID IP Address Subnet Control plane name
```

```
-----
APONBOARDING_0_2674_4097_8188 8188 4097 172.16.80.0 255.255.255.0
```

Überprüfen Sie den AP-Registrierungsstatus mit den folgenden Befehlen:

```
9300-1#show wireless stats ap join summary
```

```
Number of APs: 1
```

```
Base MAC Ethernet MAC AP Name IP Address Status Last Failure Phase Last Disconnect Reason
```

```
-----
ac4a.569c.f560 5ce1.7629.2b40 AP5CE1.7629.2B40 172.16.80.10 Joined Run Tag modified
```

```
9300-1#show fabric ap summary
```

```
Number of Fabric AP : 1
```

```
AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address State
```

```
-----
AP5CE1.7629.2B40 2 9120AXI 5ce1.7629.2b40 ac4a.569c.f560 default location US 172.16.80.10  
Registered
```

Verwenden Sie diesen Befehl, um den VxLAN-Tunnelstatus mit APs zu überprüfen.

```
9300-1#show access-tunnel summary
```

```
Access Tunnels General Statistics:
```

```
Number of AccessTunnel Data Tunnels = 1
```

```
Name RLOC IP(Source) AP IP(Destination) VRF ID Source Port Destination Port
-----
Ac0 172.16.0.1 172.16.80.10 0 N/A 4789
```

```
Name IfId Uptime
-----
Ac0 0x00000069 0 days, 00:20:11
```

Überprüfen Sie mit diesem Befehl die Zuweisung der AP-Tags. APs müssen alle die gleichen Tags haben und **Location** unter **Source (Quelle)** anzeigen.

```
9300-1#show ap tag summary
Number of APs: 1
```

```
AP Name AP Mac Site Tag Name Policy Tag Name RF Tag Name Misconfigured Tag Source
-----
AP5CE1.7629.2B40 5ce1.7629.2b40 default-site-tag EWC-Location EWC-Location No Location
```

Hinweis: In diesem Beispiel ist 172.16.0.1 die Loopback0-IP-Adresse (d. h. die Wireless-Verwaltung), der die APs beitreten. Da es sich um Fabric in a Box handelt, weisen auch alle Fabric-Komponenten darauf hin.

Fehlerbehebung

Bedingtes Debugging und Radio Active Tracing

Aktivieren Sie bedingtes Debuggen, und erfassen Sie die Radio Active (RA)-Ablaufverfolgung zur Fehlerbehebung beim Join-Prozess. RA-Ablaufverfolgungen stellen Ablaufverfolgungen auf Debugebene für alle Prozesse bereit, die mit der angegebenen Bedingung interagieren (in diesem Fall AP-MAC-Adresse). Führen Sie die folgenden Schritte aus, um das bedingte Debuggen zu aktivieren.

Schritt 1: Stellen Sie sicher, dass keine Debugbedingungen aktiviert sind.

```
9300-1#clear platform condition all
```

Schritt 2: Aktivieren Sie die Debug-Bedingung für die AP-MAC-Adresse, die überwacht werden soll.

Standardmäßig beträgt die Überwachungszeit 30 Minuten (1800 Sekunden). Sie können die Debugging-Dauer auf bis zu 2085978494 Sekunden erhöhen.

```
9300-1#debug wireless mac
```

```
9300-1#debug wireless mac
```

Hinweis: Führen Sie zum Debuggen mehrerer Access Points den Befehl `debug wireless mac` für die Funk- und Ethernet-MAC-Adresse jedes Access Points aus. Nur Ethernet-MAC-Debugging zeigt die DTLS-Transaktionen an.

Hinweis: C9800-Debugging funktioniert im Speicher- und Prozessmodell. Das heißt, das Debuggen wird in der Terminalsitzung nicht angezeigt, und alle Protokolle werden intern gepuffert, um später angezeigt zu werden.

Schritt 3: Der Switch-Port des Bounce-AP oder der CAPWAP zum Zurücksetzen des AP von der AP-CLI, um die vollständige Ablaufverfolgung zu erfassen.

Schritt 4: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

```
9300-1#no debug wireless mac
```

```
9300-1#no debug wireless mac
```

Nach Ablauf der Monitorzeit oder manuellem Stoppen der Fehlersuche erzeugt der EWC-Switch eine lokale Datei mit dem Namen:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 5: Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie haben die Möglichkeit, die Datei `ra_trace.log` zur Offline-Analyse auf einen externen Server zu kopieren oder die Ausgabe direkt in der Terminalsitzung anzuzeigen. Offline-Parsing wird aufgrund der Menge der generierten Trace-Logs bevorzugt.

Überprüfen Sie den Namen der RA-Tracing-Datei.

```
9300-1#dir flash: | inc ra_trace
```

Datei auf externen Server kopieren:

```
9300-1#copy flash:ra_trace_MAC_<AP_RADIO_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://
```

```
ra-AP_RADIO_MAC.txt
9300-1#copy flash:ra_trace_MAC_<AP_ETHERNET_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://
```

```
ra-AP_ETHERNET_MAC.txt
```

So zeigen Sie die Ablaufprotokolle einer Terminalsitzung an:

```
9300-1#more flash:ra_trace_MAC_<AP_RADIO_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
9300-1#more flash:ra_trace_MAC_<AP_ETHERNET_MAC>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 6: Wenn die Ursache nicht offensichtlich ist, sammeln Sie die internen Protokolle, die eine ausführlichere Ansicht der Ablaufverfolgungsprotokolle sind. Sie müssen den Client nicht erneut debuggen, da der Befehl Debugprotokolle bereitstellt, die bereits gesammelt und intern gespeichert wurden.

```
9300-1#show logging profile wireless internal filter
```

```
ra-internal-<AP_RADIO_MAC>.txt
9300-1#show logging profile wireless internal filter
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Technical Assistance Center (TAC), um diese Traces zu analysieren.

```
9300-1#copy flash:ra-internal-<AP_RADIO_MAC>.txt tftp://
```

```
ra-internal-<AP_RADIO_MAC>.txt
9300-1#copy flash:ra-internal-<AP_RADIO_MAC>.txt tftp://
```

```
ra-internal-<AP_RADIO_MAC>.txt
```

So zeigen Sie die Ablaufverfolgungsprotokolle in der Terminalsitzung an:

```
9300-1#more flash:ra-internal-<AP_RADIO_MAC>.txt
9300-1#more flash:ra-internal-<AP_ETHERNET_MAC>.txt
```

Schritt 7. Entfernen Sie die Debug-Bedingungen.

Hinweis: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer entfernen, nachdem Sie das Problem behoben haben.

Beispiel für einen erfolgreichen AP-Beitritt

Dies ist die Ausgabe eines erfolgreichen Verbindungsversuchs aus der RA-Ablaufverfolgungsperspektive. Verwenden Sie die Protokollbeispiele, um zu überprüfen, in welcher Phase der Access Point stecken bleibt.

CAPWAP-Erkennungsanfrage und -antwort:

```
2021/09/30 17:49:13.823492 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 IP:172.16.80.10[5264], Discovery Request received
2021/09/30 17:49:13.823519 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 EWLC TAGS payload is not present in discovery request
2021/09/30 17:49:13.823793 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [7353]: (debug): instance :0
port:12289MAC: 0002.0002.ffff
2021/09/30 17:49:13.824314 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 Public IP learnt is FALSE, public IP discovery is FALSE, private IP discovery is
TRUE.
2021/09/30 17:49:13.824414 {wncmgrd_R0-0}{1}: [capwapac-discovery] [7353]: (note): MAC:
ac4a.569c.f560 IP:172.16.80.10[5264], Discovery Response sent
```

DTLS-Handshake für die Zertifikatsvaliditätsprüfung:

```
2021/09/30 17:49:23.259157 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (note): MAC:
ac4a.569c.f560 DTLS session create callback received.
2021/09/30 17:49:23.259393 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: PMTU 576, effective capwap size 416
2021/09/30 17:49:23.259406 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.259406 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (info): DTLS client hello
2021/09/30 17:49:23.260931 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.260931 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (info): DTLS client hello
2021/09/30 17:49:23.267234 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.267332 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.267891 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.270741 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [7770]: (info): Remote Host:
172.16.80.10[5264] MAC: ac4a.569c.f56 Completed cert verification, status:CERT_VALIDATE_SUCCESS
2021/09/30 17:49:23.608757 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
22, handshake
2021/09/30 17:49:23.608990 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
20, change cipher-spec
2021/09/30 17:49:23.609255 {wncd_x_R0-0}{1}: [ewlc-dtls-sess] [7770]: (info): Remote Host:
172.16.80.10[5264] MAC: ac4a.569c.f56 DTLS session established
2021/09/30 17:49:23.609348 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: PMTU 576, effective capwap size 456
2021/09/30 17:49:23.609361 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP:
172.16.80.10[5264] Mac: DTLS session has been established for AP
2021/09/30 17:49:23.650838 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type:
```

23, application data

CAPWAP-Beitrittsanfrage und -antwort:

2021/09/30 17:49:23.650970 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: Capwap message received, type: join_request
2021/09/30 17:49:23.650972 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (note): MAC: ac4a.569c.f560 **Received CAPWAP join request**
2021/09/30 17:49:23.652901 {wncd_x_R0-0}{1}: [rrm-client] [7770]: (ERR): ac4a.569c.f560 Failed to override default values inradio oper for slot 1, reg domain chk status failed
2021/09/30 17:49:23.653789 {wncd_x_R0-0}{1}: [rrm-client] [7770]: (ERR): ac4a.569c.f560 Failed to override default values inradio oper for slot 0, reg domain chk status failed
2021/09/30 17:49:23.653959 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [7770]: (info): ac4a.569c.f560 Retrieved AP SW version: 17.3.4.30, for AP model: C9120AXI-B, AP image type: aplg7, site-tag: default-site-tag
2021/09/30 17:49:23.653967 {wncd_x_R0-0}{1}: [apmgr-db] [7770]: (info): ac4a.569c.f560 Operation state of AP changed to: Registered
2021/09/30 17:49:23.654039 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [7770]: (note): MAC: ac4a.569c.f560 **Successfully processed Join request.** AP name: AP5CE1.7629.2B40, Model: C9120AXI-B, radio slots: 2, rlan slots: 0, site tag name: default-site-tag, **policy tag name: EWC-Location, rf tag name: EWC-Location**
2021/09/30 17:49:23.654112 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [7353]: (note): Msg type :msg->msgtype Priority:1
2021/09/30 17:49:23.654233 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): MAC: ac4a.569c.f560 Join Response generated with MTU 1485. as per MTU payload, update flag: 0
2021/09/30 17:49:23.654311 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (note): MAC: ac4a.569c.f560 **Join processing complete. AP in joined state**

CAPWAP-Konfiguration:

2021/09/30 17:49:23.947851 {wncd_x_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560 Lispagent was triggered during ap join.
2021/09/30 17:49:23.948023 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 **Config status request was processed and Config status response was sent. AP in Configuration state.**
2021/09/30 17:49:23.948157 {wncd_x_R0-0}{1}: [lisp-agent-db] [7770]: (ERR): Invalid source IP address type
2021/09/30 17:49:23.948344 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (note): Map request msg sent successfully for AP vnid 4097
2021/09/30 17:49:23.949993 {wncmgrd_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry
2021/09/30 17:49:23.950130 {wncmgrd_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry
2021/09/30 17:49:24.889682 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data
2021/09/30 17:49:24.889807 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data
2021/09/30 17:49:24.889992 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 **Capwap message received, type: config_status_request**
2021/09/30 17:49:24.890020 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 process config status request
2021/09/30 17:49:24.890045 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 Updating capwap path MTU: 1485 received in config status request
2021/09/30 17:49:24.890048 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [7770]: (info): Session-IP: 172.16.80.10[5264] Mac: ac4a.569c.f560 PMTU 1485, effective capwap size 1368
2021/09/30 17:49:24.890134 {wncd_x_R0-0}{1}: [apmgr-msgelem] [7770]: (info): ac4a.569c.f560 AP domain name is not set in config status
2021/09/30 17:49:24.890135 {wncd_x_R0-0}{1}: [apmgr-msgelem] [7770]: (info): ac4a.569c.f560 AP IPv6 nameserver is not set in config status
[...]
2021/09/30 17:49:24.890818 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [7770]: (info): Session-IP:


```
172.16.80.10[5264] Mac: ac4a.569c.f560 Config status request was processed and Config status response was sent. AP in Configuration state.
2021/09/30 17:49:24.892967 {wncmgrd_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry
2021/09/30 17:49:24.892993 {wncmgrd_R0-0}{1}: [hl-core] [7353]: (debug): Radio change on AP ac4a.569c.f560 not connected to a L1 cache entry
2021/09/30 17:49:24.964085 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [7770]: (debug): DTLS record type: 23, application data
[...]
2021/09/30 17:49:24.964384 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Creating AP ac4a.569c.f560
2021/09/30 17:49:24.964474 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Successfully created AP ac4a.569c.f560
2021/09/30 17:49:24.964479 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Setting capability
2021/09/30 17:49:24.964479 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Updating AP ac4a.569c.f560
2021/09/30 17:49:24.964483 {wncd_x_R0-0}{1}: [ble-d] [7770]: (debug): BLE LTX DB: Successfully updated AP ac4a.569c.f560
[...]
2021/09/30 17:49:25.000954 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): ac4a.569c.f560 AP is in config ready state. Initial configuration will be pushed.
2021/09/30 17:49:25.000972 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): ac4a.569c.f560 Sending FIPS vendor payload config, FIPS status 0
2021/09/30 17:49:25.000975 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): Preparing FIPS config, fips status 0
2021/09/30 17:49:25.000978 {wncd_x_R0-0}{1}: [apmgr-capwap-config] [7770]: (info): Preparing WLANCC config, wlancc status 0
2021/09/30 17:49:25.001064 {wncd_x_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560 AP is in Local mode.
2021/09/30 17:49:25.001064 {wncd_x_R0-0}{1}: [apmgr-ap-global] [7770]: (info): ac4a.569c.f560 Mode update on AP join : AP already in Local mode which matches site configuration
2021/09/30 17:49:25.001081 {wncd_x_R0-0}{1}: [apmgr-db] [7770]: (info): ac4a.569c.f560 Tag process ap wlan config mapping. wlans[0] associated to to AP
```

Wenn sich der Access Point nicht im **lokalen** Modus befindet, wird er neu gestartet, um eine Modusänderung vorzunehmen. Ein ähnliches Protokoll wird auf der EWC-Switch-Konsole ausgegeben:

```
*Sep 29 20:54:07.769: %APMGR_TRACE_MESSAGE-4-WLC_CONFIG_CHECKER_WARNING: Switch 1 R0/0: wncd: config check: The mode of AP ac4a.569c.f560 is changed from Flexconnect to Local.
*Sep 29 20:54:07.769: %APMGR_TRACE_MESSAGE-3-WLC_EXEC_MSG: Switch 1 R0/0: wncd: % Error: AP: AP5CE1.7629.2B40 will go for a reboot due to Mode change from Flexconnect to Local
```

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.