

# Konfigurieren einer Punkt-zu-Punkt-Mesh-Verbindung mit Ethernet-Bridging auf einem integrierten Wireless-Controller mit C9124 Access Points

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Ethernet-Bridging](#)

[Integrierter Wireless Controller am Catalyst Access Point](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Switch-Konfigurationen](#)

[EWC- und RAP-Konfiguration](#)

[MAP konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Nützliche Befehle](#)

[Beispiel 1: RAP empfängt Adjacency von MAP und setzt die Authentifizierung durch](#)

[Beispiel 2: MAP-MAP-Adresse nicht zum WLC hinzugefügt oder falsch hinzugefügt](#)

[Beispiel 3: RAP verliert MAP](#)

[Tipps, Tricks und Empfehlungen](#)

[Referenzen](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration von P2P Mesh Link mit Ethernet Bridging auf Embedded Wireless Controller (eWC) mit C9124 Access Points beschrieben.

## Voraussetzungen

### Anforderungen

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

- Cisco Wireless LAN Controller (WLC) 9800

- Cisco Catalyst Access Points (APs)
- Integrierter Wireless Controller auf Catalyst Access Points
- Mesh-Technologie.

## Verwendete Komponenten

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

- EWC IOS® XE 17.12.2
- 2 APs C9124.
- 2 Power Injectors AIR-PWRINJ-60RGD1.
- 2 Switches;
- 2 Laptops
- 1 x AP C9115

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

## Hintergrundinformationen

### Ethernet-Bridging

Die Mesh-Netzwerklösung, die Teil der Cisco Unified Wireless Network-Lösung ist, ermöglicht es zwei oder mehr Cisco Mesh Access Points (im Folgenden als Mesh Access Points bezeichnet), über einen oder mehrere Wireless-Hops miteinander zu kommunizieren, um mehrere LANs zu verbinden oder die Wi-Fi-Abdeckung zu erweitern.

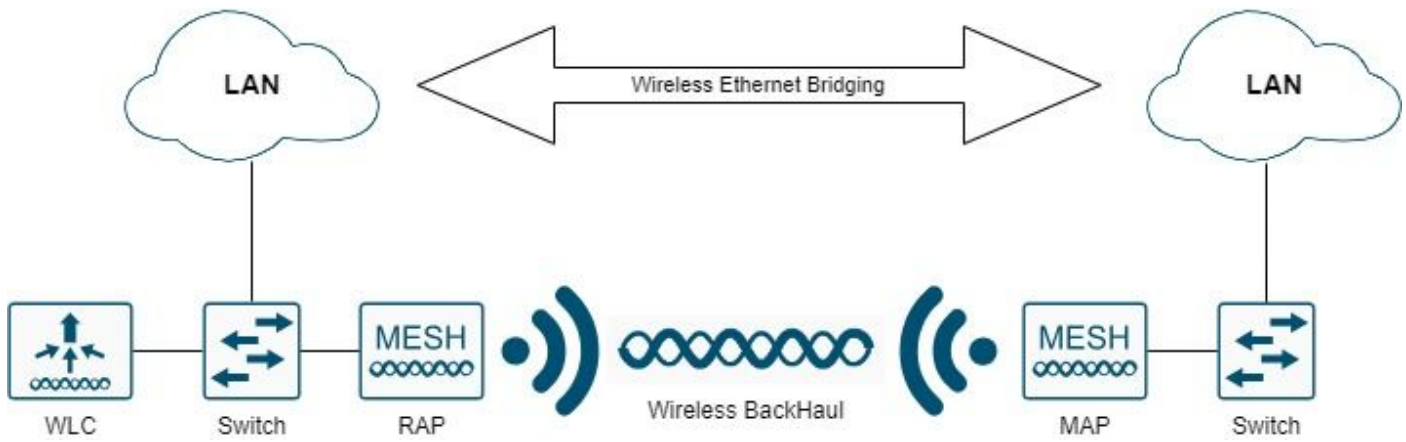
Die Mesh-Access Points von Cisco werden von jedem in der Mesh-Netzwerklösung implementierten Cisco Wireless LAN-Controller aus konfiguriert, überwacht und betrieben.

Die unterstützten Mesh-Netzwerkösungen sind einer von drei allgemeinen Typen:

- Point-to-Point-Bereitstellung
- Point-to-Multipoint-Bereitstellung
- Mesh-Bereitstellung

Der Schwerpunkt dieses Dokuments liegt auf der Konfiguration von Punkt-zu-Punkt-Mesh-Bereitstellung und Ethernet-Bridging auf demselben System.

Bei einer Point-to-Point-Mesh-Bereitstellung ermöglichen die Mesh Access Points einen Wireless-Zugriff und ein Backhaul für Wireless-Clients. Außerdem können sie gleichzeitig das Bridging zwischen einem LAN und einer Terminierung zu einem Remote-Ethernet-Gerät oder einem anderen Ethernet-LAN unterstützen.



Wireless Ethernet-Bridging

Weitere Informationen [zu](#) diesen Bereitstellungsarten finden Sie im [Mesh-Bereitstellungsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800](#).

Der Outdoor Mesh AP der Cisco Catalyst Serie 9124 ist ein Wireless-Gerät für den Wireless-Client-Zugriff und das Punkt-zu-Punkt-Bridging, Punkt-zu-Mehrpunkt-Bridging und Punkt-zu-Mehrpunkt-Mesh-Wireless-Konnektivität.

Der Access Point für den Außenbereich ist eine eigenständige Einheit, die an einer Wand oder einem Überhang, an einem Dachmast oder an einem Laternenmast montiert werden kann.

Sie können den C9124 in einer der folgenden Mesh-Rollen betreiben:

- Access Point (RAP) auf dem Dach
- Mesh Access Point (MAP)

RAPs sind mit einem Wireless LAN Controller von Cisco verbunden. Sie nutzen die Wireless-Backhaul-Schnittstelle für die Kommunikation mit in der Nähe befindlichen MAPs. RAPs sind der übergeordnete Knoten zu einem Bridge- oder Mesh-Netzwerk und verbinden ein Bridge- oder Mesh-Netzwerk mit dem kabelgebundenen Netzwerk. Es kann also nur einen RAP für ein Bridge- oder Mesh-Netzwerksegment geben.

MAPs haben keine Kabelverbindung zu einem Cisco Wireless LAN Controller. Sie können vollständig drahtlos sein und Clients unterstützen, die mit anderen MAPs oder RAPs kommunizieren, oder sie können verwendet werden, um eine Verbindung zu Peripheriegeräten oder einem kabelgebundenen Netzwerk herzustellen.

## Integrierter Wireless Controller am Catalyst Access Point

Der Cisco Embedded Wireless Controller (EWC) für Catalyst Access Points ist ein softwarebasierter Controller, der in Cisco Catalyst 9100 Access Points integriert ist.

In einem Cisco EWC-Netzwerk wird ein Zugangspunkt (Access Point, AP), der die Wireless-Controller-Funktion ausführt, als aktiver Zugangspunkt festgelegt.

Die anderen Zugangspunkte, die von diesem aktiven Zugangspunkt verwaltet werden, werden als

untergeordnete Zugangspunkte bezeichnet.

Das aktive EBR hat zwei Aufgaben:

- Es fungiert als Wireless LAN Controller (WLC) zur Verwaltung und Steuerung der untergeordneten APs. Die untergeordneten APs dienen als Lightweight Access Points zur Bedienung von Clients.
- Er dient als Access Point für Clients.

Eine Produktübersicht zu EWC für APs finden Sie im [Datenblatt](#) zu [Cisco Embedded Wireless Controller auf Catalyst Access Points](#).

Nähere Informationen zur Bereitstellung von EWC in Ihrem Netzwerk finden Sie im [Whitepaper Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\)](#).

Dieses Dokument konzentriert sich auf C9124 als EWC und geht davon aus, dass sich bereits ein AP 9124 im EWC-Modus befindet.

## Konfigurieren

### Netzwerkdiagramm


Alle Geräte in diesem Netzwerk befinden sich im Subnetz 192.168.100.0/24, mit Ausnahme der Laptops in VLAN 101 mit Subnetz 192.168.101.0/25.

Die Verwaltungsschnittstelle des EWC-AP (WLC) ist nicht markiert, und das native VLAN an den Switch-Ports ist auf VLAN 100 festgelegt.

AP9124\_RAP übernimmt die Rolle eines eWLC und Root Access Point (RAP), während AP9124\_MAP die Rolle eines Mesh Access Point (MAP) übernimmt.

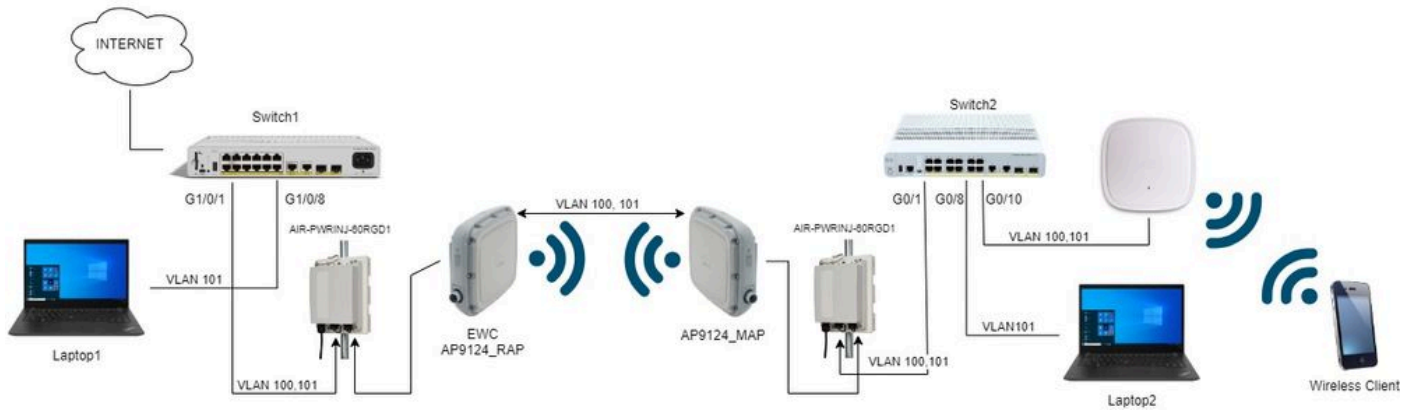
In dieser Übung wird ein AP C9115 ebenfalls hinter dem MAP platziert, um zu zeigen, dass APs über eine Mesh-Verbindung einem WLC beitreten können.

Diese Tabelle enthält die IP-Adressen aller Geräte im Netzwerk:

 Hinweis: Das Tagging der Management-Schnittstelle kann Probleme verursachen, wenn der Access Point dem internen WLC-Prozess beitrifft. Wenn Sie sich entscheiden, die Management-Schnittstelle zu taggen, stellen Sie sicher, dass der kabelgebundene Infrastrukturtteil entsprechend konfiguriert ist.

"Slot0:"	IP-Adresse
Standardgateway	Statisch auf VLAN 100: 192.168.100.1
Laptop1	DHCP in VLAN 101
Laptop2	DHCP in VLAN 101
Switch1 (DHCP-Server)	VLAN 100 SVI: Statisch auf VLAN 100: 192.168.100.1 (DHCP-Server)

Switch1 (DHCP-Server)	VLAN 101 SVI: Statisch auf VLAN 101: 192.168.101.1 (DHCP-Server)
Switch2	VLAN 100 SVI: DHCP auf VLAN 100
Switch2	VLAN 101 SVI: DHCP auf VLAN 101
9124EWC	Statisch auf VLAN 100: 192.168.100.40
AP9124 RAP	DHCP auf VLAN 100
AP9124-MAP	DHCP auf VLAN 100
AP 9115	DHCP auf VLAN 100



Netzwerkdiagramm



Hinweis: Die Stromversorgung der C9124 APs erfolgt mit AIR-PWRINJ-60RGD1 gemäß den Richtlinien im [Cisco Catalyst 9124AX Series Outdoor Access Point Hardware Installation Guide](#).

---

## Konfigurationen

In diesem Dokument wird davon ausgegangen, dass bereits ein AP 9124 mit EWC vorhanden ist, wobei die Erstbereitstellung gemäß dem [Whitepaper Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\) erfolgt ist](#).

Weitere Tipps und Tricks zum Konvertierungsprozess finden Sie im Dokument [Convert Catalyst 9100 Access Points to Embedded Wireless Controller \(Catalyst 9100 Access Points in Embedded Wireless Controller konvertieren\)](#).

### Switch-Konfigurationen

Nachfolgend sind die für die Switches relevanten Konfigurationen aufgeführt.

Switch-Ports, an denen APs angeschlossen sind, befinden sich im Trunk-Modus, wobei das native VLAN auf 100 festgelegt ist und VLAN 101 ermöglicht.

Beim Staging der APs müssen Sie den MAP als MAP konfigurieren. Daher müssen Sie dafür sorgen, dass der AP über Ethernet dem eWC beitrifft. Hier wird der Switch1-Port G1/0/2 für das Staging der MAP verwendet. Nach dem Staging wird die MAP zu Switch2 verschoben.

Switch-Ports, an die Laptops angeschlossen sind, werden als Access-Ports im VLAN 101 konfiguriert.

Switch1:

```
ip dhcp excluded-address 192.168.101.1 192.168.101.10
ip dhcp excluded-address 192.168.100.1 192.168.100.10
!
ip dhcp pool AP_VLAN100
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 192.168.1.254
!
ip dhcp pool VLAN101
network 192.168.101.0 255.255.255.0
default-router 192.168.101.1
dns-server 192.168.1.254
!
interface GigabitEthernet1/0/1
description AP9124_RAP (EWC)
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet1/0/2
description AP9124_MAP_Staging
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet1/0/8
description laptop1
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
```

Switch 2:

```
interface GigabitEthernet0/1
description AP9124_MAP
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet0/8
```

```

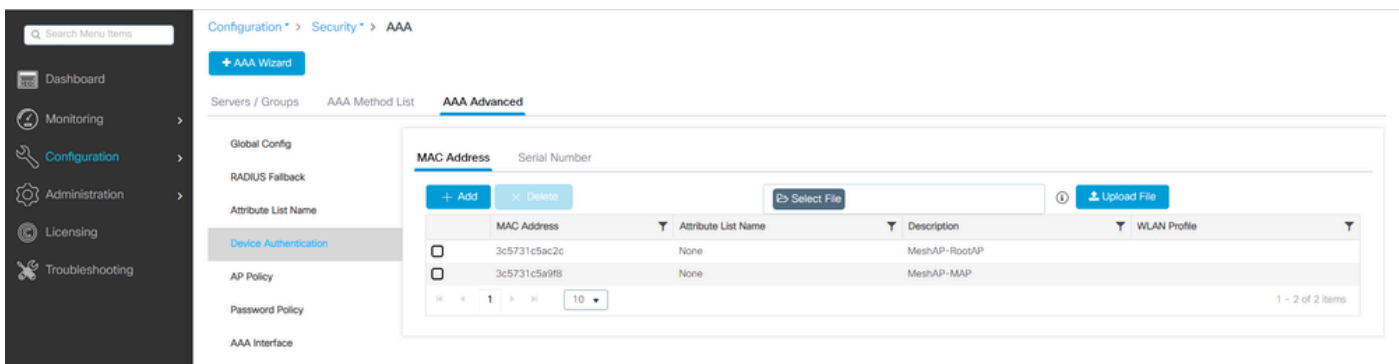
description laptop2
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
interface GigabitEthernet0/1
description AP9115
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end

```

## EWC- und RAP-Konfiguration

Nach der Day0-Konfiguration des EWC AP muss sich der eingebettete AP selbst anschließen.

1. Fügen Sie die Ethernet-MAC-Adressen des Root-AP und des Mesh-AP zur Geräteauthentifizierung hinzu. Gehen Sie zu Configuration > Security > AAA > AAA Advanced > Device Authentication, und klicken Sie auf die Schaltfläche und dann auf die Schaltfläche und klicken Sie auf die Schaltfläche und fügen Sie Folgendes hinzu:



MAC-Adressen bei der Geräteauthentifizierung

## CLI-Befehle:

```

9124EWC(config)#username 3c5731c5ac2c mac description MeshAP-RootAP
9124EWC(config)#username 3c5731c5a9f8 mac description MeshAP-MAP

```

Die Ethernet-MAC-Adresse kann durch Ausführen der Option "show controller wired 0" (Controller mit 0 anzeigen) über die AP-CLI bestätigt werden. Beispiel vom Root-AP:

```

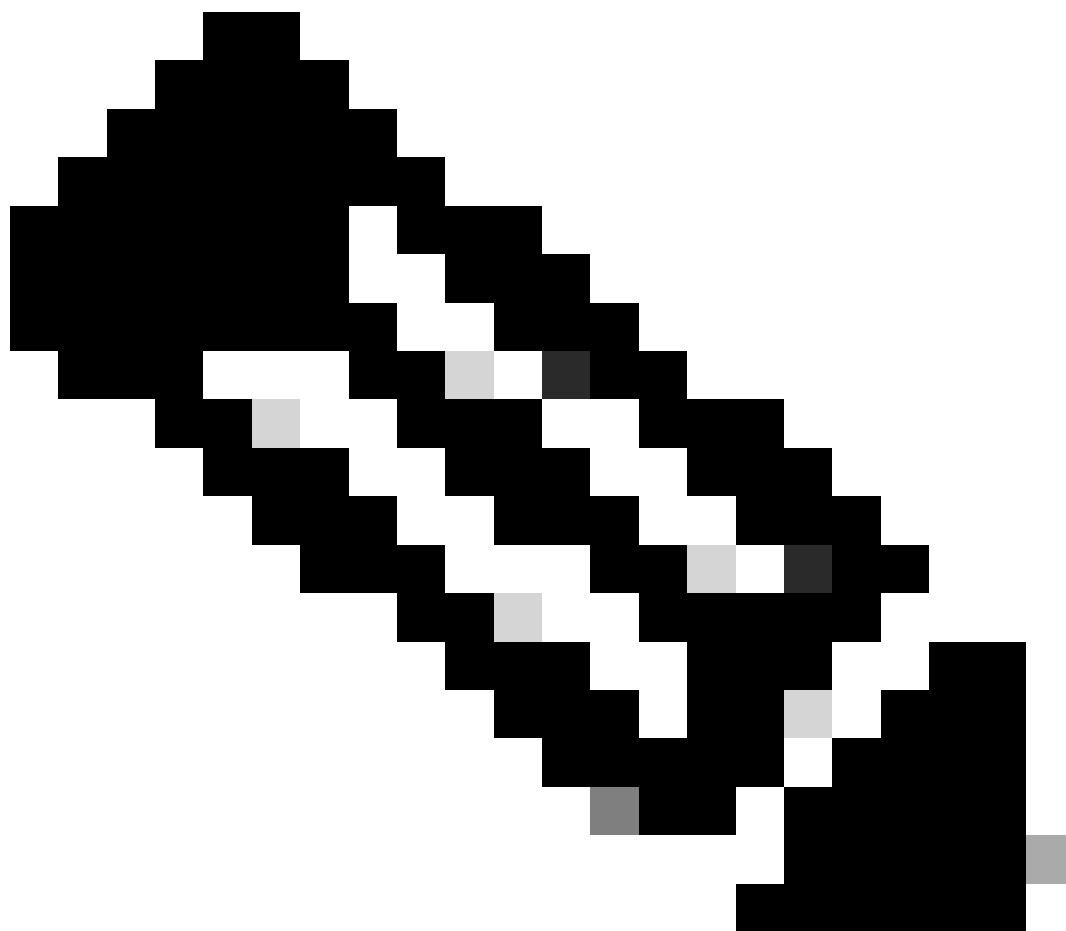
AP3C57.31C5.AC2C#show controllers wired 0
wired0 Link encap:Ethernet HWaddr 3C:57:31:C5:AC:2C

```



Der Zugriff auf die zugrunde liegende AP-Shell kann mit dem Befehl "wireless ewc-ap ap shell username x" wie folgt abgeschlossen werden:

```
9124EWC#wireless ewc-ap ap shell username admin
[...]
admin@192.168.255.253's password:
AP3C57.31C5.AC2C>en
Password:
AP3C57.31C5.AC2C#
AP3C57.31C5.AC2C#logout
Connection to 192.168.255.253 closed.
9124EWC#
```



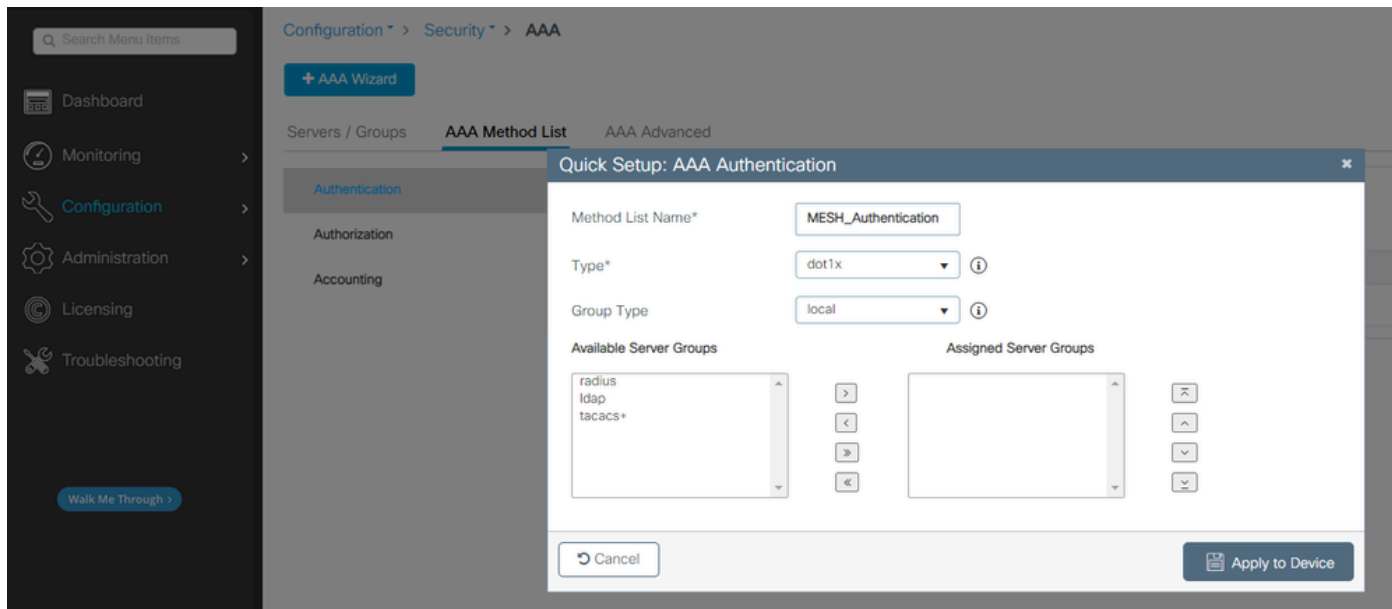
Hinweis: Dieser Befehl entspricht dem Befehl apciscoshell, der zuvor bei Mobility Express-Controllern verfügbar war.

Wenn der Benutzername und das Kennwort für die AP-Verwaltung im AP-Profil nicht

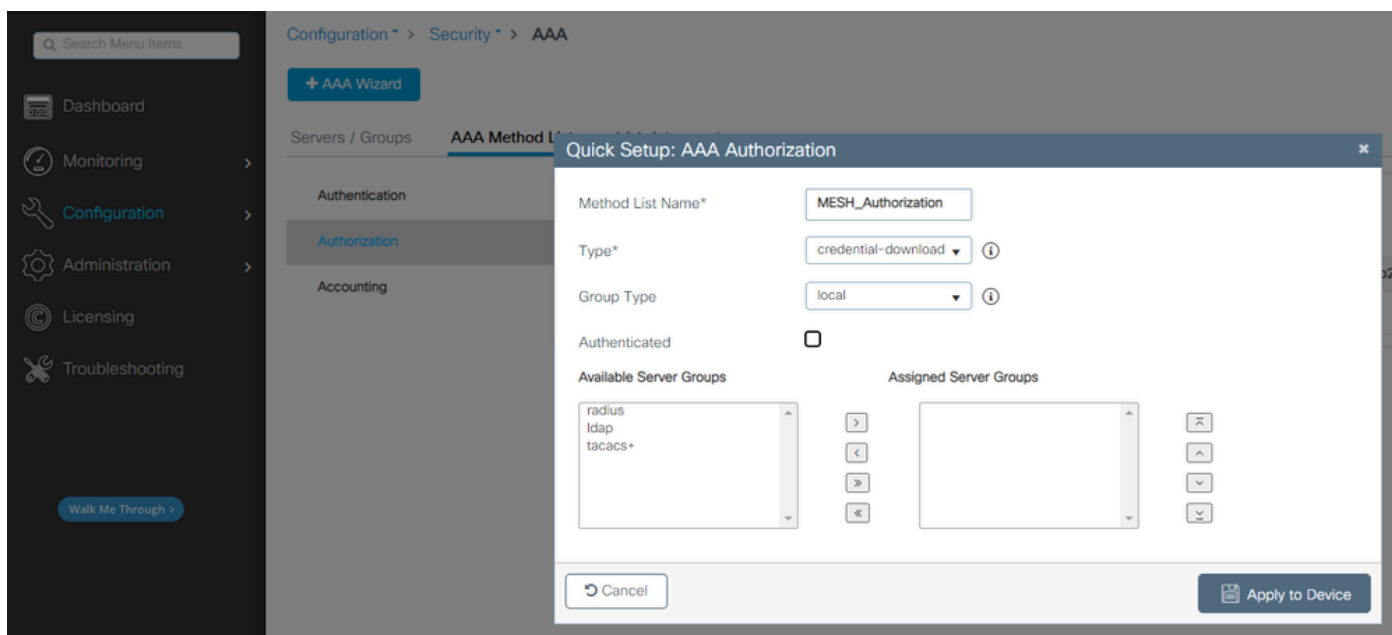
---

angegeben sind, verwenden Sie stattdessen den Standardbenutzernamen Cisco und das Standardkennwort Cisco.

## 2. Authentifizierungs- und Autorisierungsmethoden hinzufügen:



Liste der Authentifizierungsmethoden

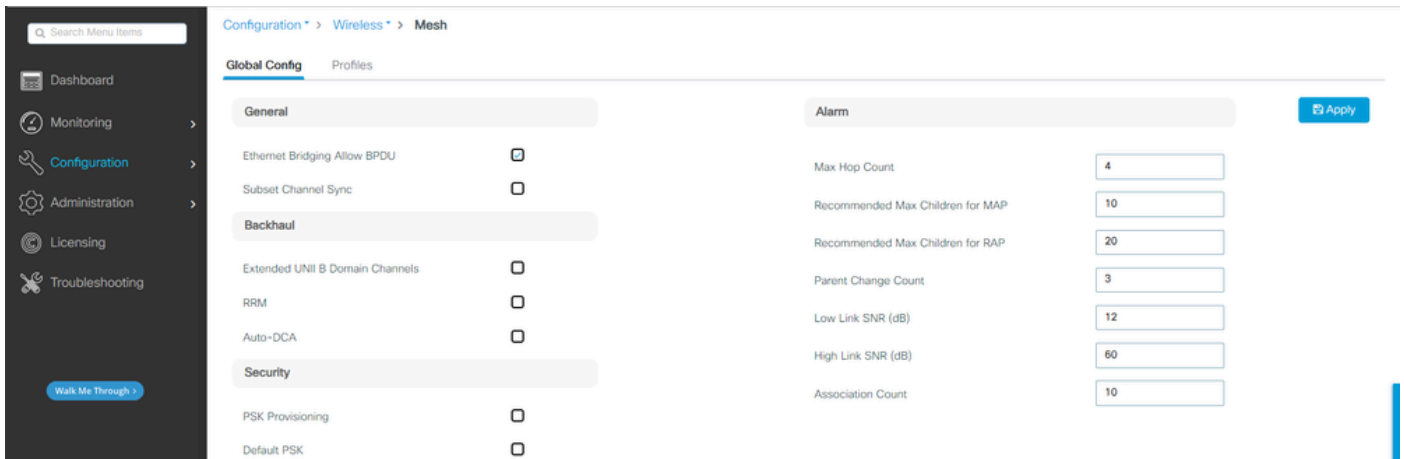


Liste der Autorisierungsmethoden

## CLI-Befehle:

```
9124EWC(config)#aaa authentication dot1x MESH_Authentication local
9124EWC(config)#aaa authorization credential-download MESH_Authentication local
```

3. Gehen Sie zu Konfiguration > Wireless > Mesh. Da die Konfiguration in diesem Dokument Ethernet-Bridging erfordert, aktivieren Sie Ethernet-Bridging erlauben BPDUs:



Ethernet-Bridging BPDUs zulassen

CLI-Befehle:

```
9124EWC(config)#wireless mesh ethernet-bridging allow-bdpu
```



Hinweis: Standardmäßig leiten die Mesh-APs keine BPDUs über die Mesh-Verbindung weiter.

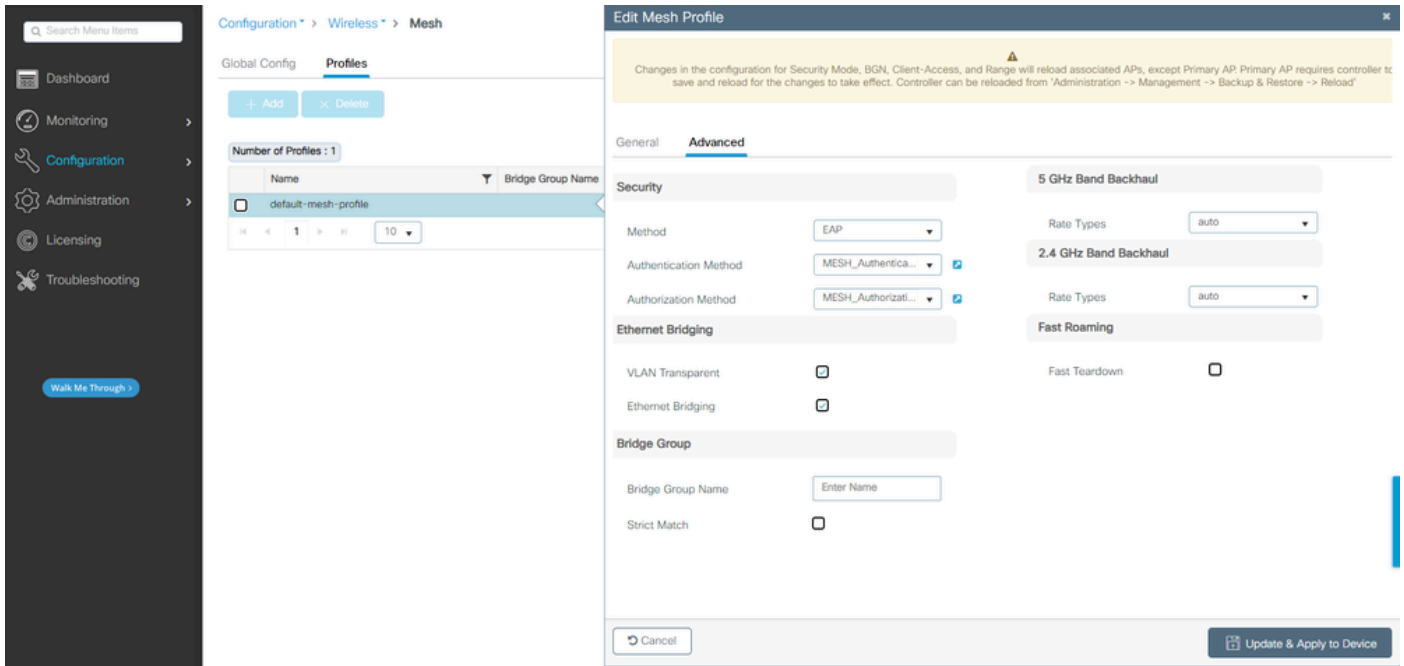
Wenn Sie keine redundante Verbindung zwischen den beiden Standorten haben, wird sie nicht benötigt.

Wenn redundante Verbindungen vorhanden sind, müssen Sie BPDUs zulassen. Andernfalls besteht die Gefahr, dass eine STP-Schleife im Netzwerk erstellt wird.

---

4. Konfigurieren Sie das Standard-Mesh-Profil, in dem Sie die zuvor konfigurierten AAA-Authentifizierungs- und Autorisierungsmethoden auswählen. Klicken Sie auf das Standard-Mesh-Profil, und bearbeiten Sie es.

Wechseln Sie zur Registerkarte Erweitert, und wählen Sie die Authentifizierungs- und Autorisierungsmethoden aus. Aktivieren Sie Option Ethernet Bridging.



Standard-Mesh-Profil bearbeiten

## CLI-Befehle:

```

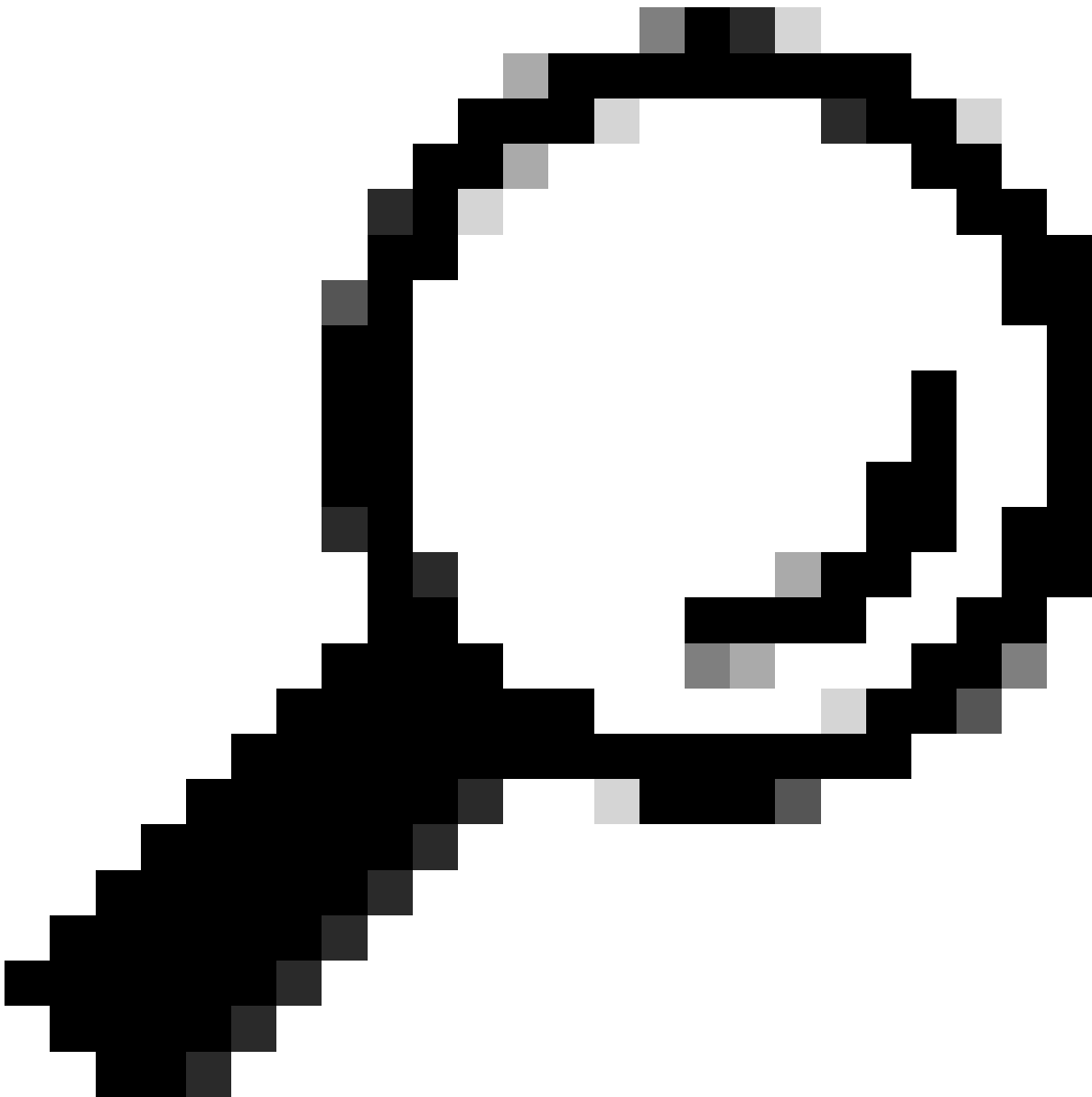
9124EWC(config)#wireless profile mesh default-mesh-profile
9124EWC(config-wireless-mesh-profile)#description "default mesh profile"
9124EWC(config-wireless-mesh-profile)#ethernet-bridging
9124EWC(config-wireless-mesh-profile)#ethernet-vlan-transparent
9124EWC(config-wireless-mesh-profile)#method authentication MESH_Authentication
9124EWC(config-wireless-mesh-profile)#method authorization MESH_Authorization

```

## Besonderer Hinweis auf die Option VLAN Transparent:

Diese Funktion legt fest, wie ein Mesh-Access Point VLAN-Tags für den über Ethernet überbrückten Datenverkehr behandelt:

- Wenn VLAN Transparent aktiviert ist, werden VLAN-Tags nicht verarbeitet, und Pakete werden als nicht markierte Pakete überbrückt.
  - Wenn VLAN Transparent aktiviert ist, ist keine Konfiguration von Ethernet-Ports erforderlich. Der Ethernet-Port übergibt sowohl getaggte als auch ungetaggte Frames, ohne die Frames zu interpretieren.
- Wenn VLAN Transparent deaktiviert ist, werden alle Pakete entsprechend der VLAN-Konfiguration am Port verarbeitet (Trunk-, Zugriffs- oder Normalmodus).
  - Wenn für den Ethernet-Port der Trunk-Modus eingestellt ist, muss Ethernet-VLAN-Tagging konfiguriert werden.



Tipp: Um AP VLAN Tagging zu verwenden, müssen Sie das Kontrollkästchen VLAN Transparent deaktivieren.

Wenn Sie kein VLAN Tagging verwenden, bedeutet dies, dass RAP und MAP auf nativen VLANs konfiguriert auf den Trunk-Ports sind. In diesem Fall müssen Sie VLAN Transparent aktivieren, wenn sich andere Geräte hinter MAP im nativen VLAN (hier VLAN 100) befinden sollen.

---

5. Der interne AP tritt dem EWC bei und Sie können den AP-Join-Status mit dem Befehl "show ap summary" überprüfen:

```

9124EwC#show ap summary
Number of APs: 1

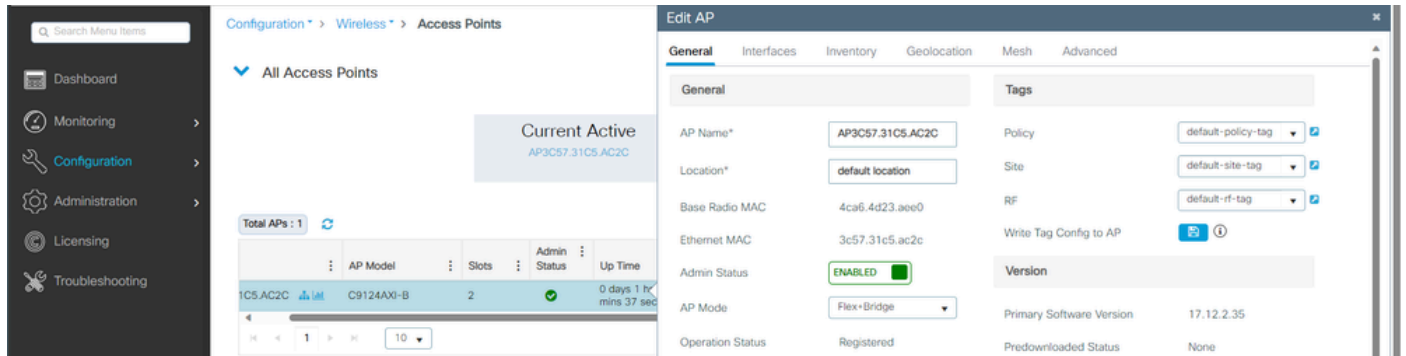
CC = Country Code
RD = Regulatory Domain

AP Name           Slots AP Model           Ethernet MAC           Radio MAC           CC           RD           IP Address           State           Location
-----
AP3C57.31C5.AC2C  2           C9124AXI-B           3c57.31c5.ac2c     4ca6.4d23.aee0     US           -8           192.168.100.11     Registered     default location

```

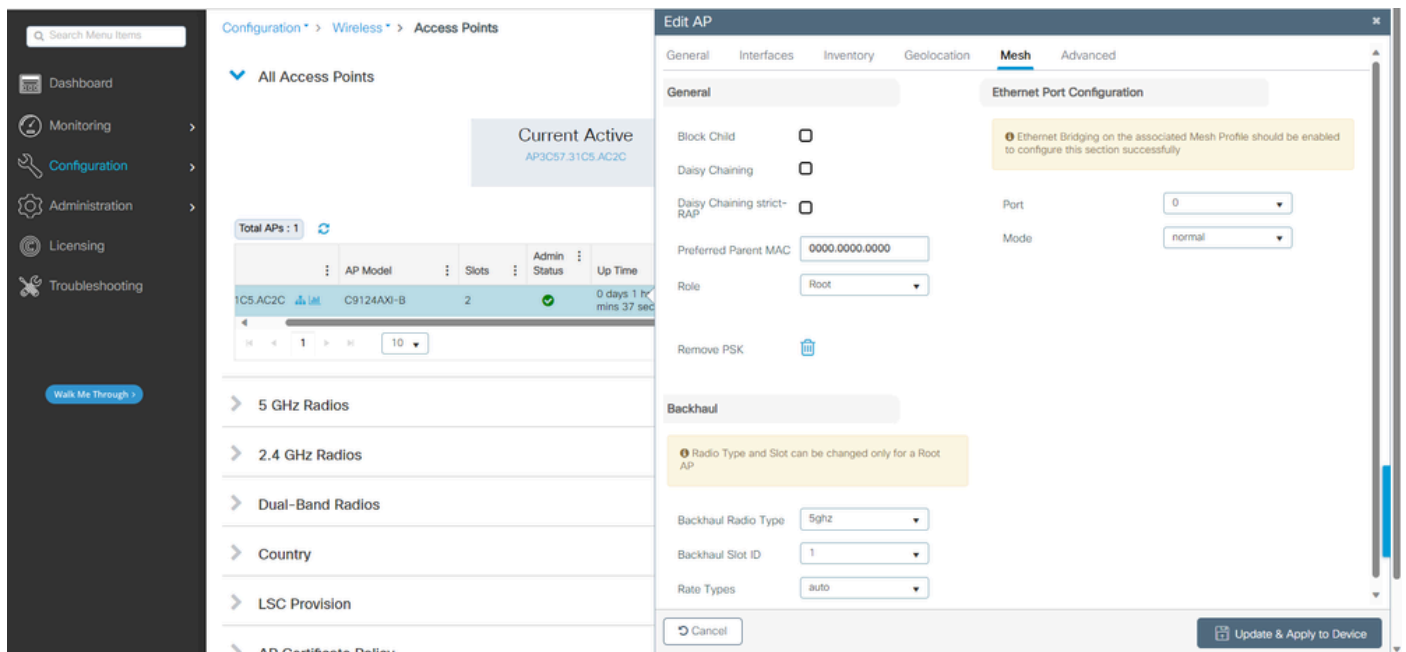
show ap summary

Sie können auch sehen, dass der Access Point über die GUI verbunden wird, wobei der Access Point als Flex+Bridge-Modus angezeigt wird. Sie können den Namen des Access Points jetzt ändern. In dieser Konfiguration wird der Name AP9124\_RAP verwendet:



AP - Allgemeine Details

Sie können die Geolocation bearbeiten und dann auf der Registerkarte Mesh sicherstellen, dass ihre Rolle als Root-AP konfiguriert ist und die Ethernet-Port-Konfiguration auf Trunk mit den entsprechenden VLAN-IDs festgelegt ist:



Wurzel der Mesh-Rolle

Edit AP
✕

---

General
Interfaces
Inventory
Geolocation
Mesh
Advanced

**General**

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Remove PSK

**Ethernet Port Configuration**

*ⓘ* Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port

Mode

Native VLAN ID\*

Allowed VLAN IDs

**Backhaul**

*ⓘ* Radio Type and Slot can be changed only for a Root AP

Backhaul Radio Type

Backhaul Slot ID

Rate Types

↶ Cancel

Update & Apply to Device

Ethernet-Port-Konfiguration

## MAP konfigurieren

Es ist jetzt an der Zeit, sich dem 9124 MAP anzuschließen.

1. Schließen Sie den MAP AP zum Staging an den Switch1 an. Der Access Point wird dem EWC hinzugefügt und in der Liste der Access Points angezeigt. Ändern Sie seinen Namen in einen Namen wie AP9124\_MAP, und konfigurieren Sie ihn auf der Registerkarte Mesh als Mesh Role. Klicken Sie auf Aktualisieren und auf Gerät anwenden:



The screenshot displays a network management interface with two main panes. The left pane, titled 'Configuration > Wireless > Access Points', shows a list of 'All Access Points'. A 'Current Active' status box is visible above the table. The table lists two APs: AP9124\_MAP and AP9124\_RAP, both of model C9124AXI-B with 2 slots and active status. Below the table are expandable sections for '5 GHz Radios', '2.4 GHz Radios', 'Dual-Band Radios', 'Country', and 'LSC Provision'. The right pane, titled 'Edit AP', shows configuration options for the 'Mesh' profile. It includes sections for 'General' (Block Child, Daisy Chaining, etc.), 'Ethernet Port Configuration' (Port, Mode, Native VLAN ID, Allowed VLAN IDs), and 'Backhaul' (Backhaul Radio Type, Slot ID, Rate Types). A 'Cancel' button is at the bottom left, and an 'Update & Apply to Device' button is at the bottom right.

### MAP-Konfiguration

2. Trennen Sie den Access Point von Switch1, und stellen Sie die Verbindung zu Switch2 her, wie im Netzwerkdiagramm dargestellt. Der MAP wird über eine Wireless-Schnittstelle und den RAP in das EWC integriert.



Hinweis: Wenn die APs über einen Power Injector mit Strom versorgt werden, fällt der Access Point nicht aus. Wenn sich die Konfiguration in einer kontrollierten Umgebung befindet, ist der Switch2 physisch in der Nähe, und wir können das Kabel einfach von einem Switch zum anderen verlegen.

---

Sie können ein Konsolenkabel an den AP anschließen und sehen, was über die Konsole geschieht. Hier sind einige wichtige Nachrichten gesehen.

---

Hinweis: Ab Version 17.12.1 wird die Standardkonsolenbaudrate der 802.11AX-APs von 9600 bps auf 115200 bps geändert.

---

MAP verliert Verbindung zu EWC:

AP9124\_MAP#

```
[*01/11/2024 14:08:23.0214] chatter: Device wired0 notify state change link DOWN
[*01/11/2024 14:08:28.1474] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:28.1474]
[*01/11/2024 14:08:31.1485] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:31.1486]
[*01/11/2024 14:08:33.4214] chatter: Device wired0 notify state change link UP
[*01/11/2024 14:08:34.1495] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:34.1495]
[*01/11/2024 14:08:37.1505] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=84, M
[*01/11/2024 14:08:37.1505]
[*01/11/2024 14:08:40.1515] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=84, M
[*01/11/2024 14:08:40.1515]
```

```
[*01/11/2024 14:08:43.1524] Max retransmission count exceeded, going back to D
[...]
[*01/11/2024 14:08:48.1537] CRIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Blocklist
[*01/11/2024 14:08:48.1538] CRIT-MeshWiredAdj[0][3C:57:31:C5:A9:F8]: Remove as
[*01/11/2024 14:08:48.1539] CRIT-MeshLink: Link Down Block Root port Mac: 3C:5
[*01/11/2024 14:08:48.1542] CRIT-MeshWiredBackhaul[0]: Remove as uplink
```

MAP wechselt über Wireless in den Erkennungsmodus und findet den RAP über Radio Backhaul auf Kanal 36, findet den EWC und schließt sich ihm an:

```
[*01/11/2024 14:08:51.3893] CRIT-MeshRadioBackhaul[1]: Set as uplink
[*01/11/2024 14:08:51.3894] CRIT-MeshAwppAdj[1][4C:A6:4D:23:AE:F1]: Set as Par
[*01/11/2024 14:08:51.3915] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (mon0)
[*01/11/2024 14:08:51.3926] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (apbh
[*01/11/2024 14:08:51.4045] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (apbhr0)
[*01/11/2024 14:08:51.4053] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (mon0)
[*01/11/2024 14:08:53.3898] CRIT-MeshLink: Set Root port Mac: 4C:A6:4D:23:AE:F
[*01/11/2024 14:08:53.3904] Mesh Reconfiguring DHCP.
[*01/11/2024 14:08:53.8680] DOT11_UPLINK_EV: wgb_uplink_set_port_authorized: c
[*01/11/2024 14:08:53.9232] CRIT-MeshSecurity: Mesh Security successful auther
[...]
[*01/11/2024 14:09:48.4388] Discovery Response from 192.168.100.40
[*01/11/2024 14:09:59.0000] Started wait dtls timer (60 sec)
[*01/11/2024 14:09:59.0106]
[*01/11/2024 14:09:59.0106] CAPWAP State: DTLS Setup
[*01/11/2024 14:09:59.0987] dtls_verify_server_cert: Controller certificate ve
[*01/11/2024 14:09:59.8466]
[*01/11/2024 14:09:59.8466] CAPWAP State: Join
[*01/11/2024 14:09:59.8769] Sending Join request to 192.168.100.40 through po
[*01/11/2024 14:10:04.7842] Sending Join request to 192.168.100.40 through po
[*01/11/2024 14:10:04.7953] Join Response from 192.168.100.40, packet size 139
[...]
[*01/11/2024 14:10:06.6919] CAPWAP State: Run
[*01/11/2024 14:10:06.8506] AP has joined controller 9124EWC
[*01/11/2024 14:10:06.8848] Flexconnect Switching to Connected Mode!
[...]
```

MAP wird nun über RAP mit dem EWC verbunden.

AP C9115 kann jetzt eine IP-Adresse im VLAN 100 abrufen und am EWC teilnehmen:



Warnung: Beachten Sie, dass VLAN 100 das native Switch-Port-VLAN für den Trunk ist. Damit der Datenverkehr vom Access Point im VLAN 100 den WLC im VLAN 100 erreicht, muss für die Mesh-Verbindung VLAN Transparent aktiviert sein. Dies wird im Abschnitt "Ethernet Bridging" des Mesh-Profiles durchgeführt.

---

```
[*01/19/2024 11:40:55.0710] ethernet_port wired0, ip 192.168.100.14, netmask 255.255.255.255
[*01/19/2024 11:40:58.2070]
[*01/19/2024 11:40:58.2070] CAPWAP State: Init
[*01/19/2024 11:40:58.2150]
[*01/19/2024 11:40:58.2150] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2400] Discovery Request sent to 192.168.100.40, discovered
[*01/19/2024 11:40:58.2530] Discovery Request sent to 255.255.255.255, discovered
[*01/19/2024 11:40:58.2600]
[*01/19/2024 11:40:58.2600] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2670] Discovery Response from 192.168.100.40
[*01/19/2024 11:40:58.2670] Found Configured MWAR '9124EWC' (respIdx 1).
[*01/19/2024 15:13:56.0000] Started wait dtls timer (60 sec)
[*01/19/2024 15:13:56.0070]
[*01/19/2024 15:13:56.0070] CAPWAP State: DTLS Setup
```

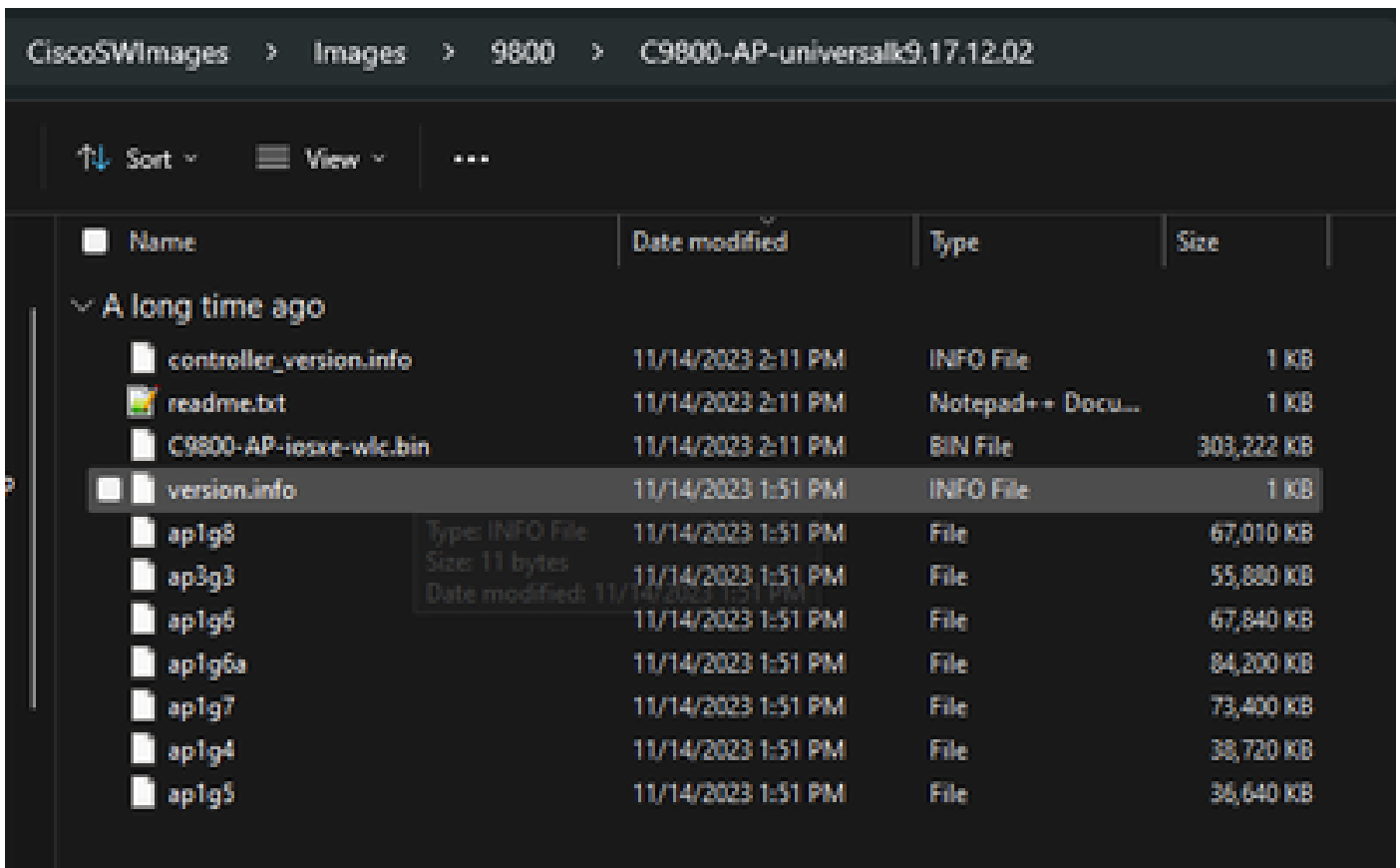
```

[...]
[*01/19/2024 15:13:56.1660] dtls_verify_server_cert: Controller certificate ve
[*01/19/2024 15:13:56.9000] sudi99_request_check_and_load: Use HARSA SUDI cert
[*01/19/2024 15:13:57.2980]
[*01/19/2024 15:13:57.2980] CAPWAP State: Join
[*01/19/2024 15:13:57.3170] shared_setenv PART_BOOTCNT 0 &> /dev/null
[*01/19/2024 15:13:57.8620] Sending Join request to 192.168.100.40 through po
[*01/19/2024 15:14:02.8070] Sending Join request to 192.168.100.40 through po
[*01/19/2024 15:14:02.8200] Join Response from 192.168.100.40, packet size 139
[*01/19/2024 15:14:02.8200] AC accepted previous sent request with result code
[*01/19/2024 15:14:03.3700] Received wlcType 2, timer 30
[*01/19/2024 15:14:03.4440]
[*01/19/2024 15:14:03.4440] CAPWAP State: Image Data
[*01/19/2024 15:14:03.4440] AP image version 17.12.2.35 backup 17.9.4.27, Cont
[*01/19/2024 15:14:03.4440] Version is the same, do not need update.
[*01/19/2024 15:14:03.4880] status 'upgrade.sh: Script called with args:[NO_UP
[*01/19/2024 15:14:03.5330] do NO_UPGRADE, part2 is active part
[*01/19/2024 15:14:03.5520]
[*01/19/2024 15:14:03.5520] CAPWAP State: Configure
[*01/19/2024 15:14:03.5600] Telnet is not supported by AP, should not encode t
[*01/19/2024 15:14:03.6880] Radio [1] Administrative state DISABLED change to
[*01/19/2024 15:14:03.6890] Radio [0] Administrative state DISABLED change to
[*01/19/2024 15:14:03.8670]
[*01/19/2024 15:14:03.8670] CAPWAP State: Run
[*01/19/2024 15:14:03.9290] AP has joined controller 9124EWC
[*01/19/2024 15:14:03.9310] Flexconnect Switching to Connected Mode!

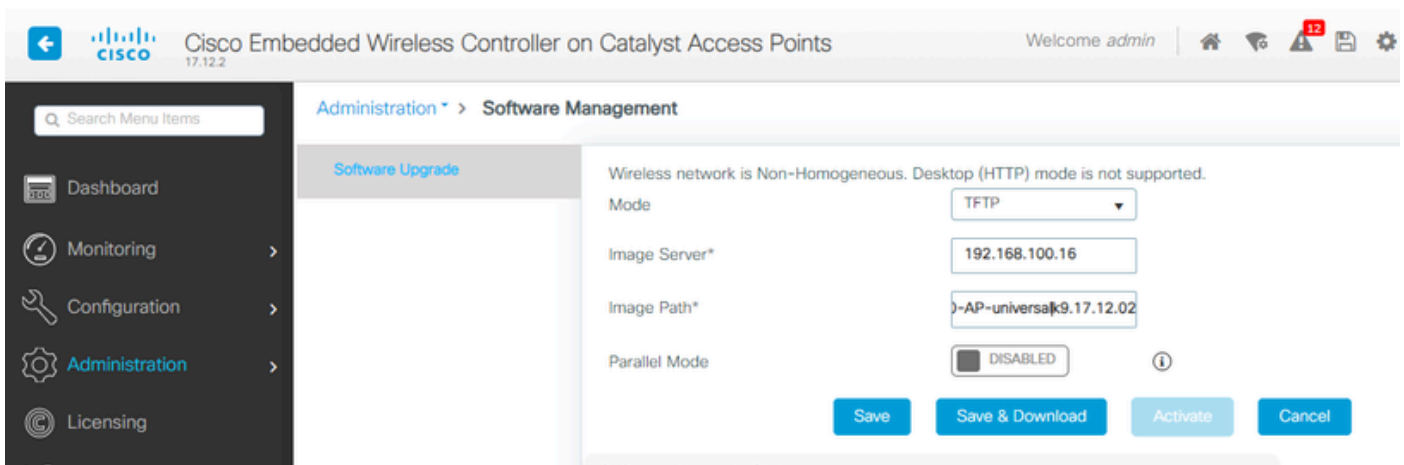
```

Da es sich um einen EWC-AP handelt, enthält er nur das AP-Image, das seinem eigenen Modell entspricht (hier läuft ein C9124 auf ap1g6a). Wenn Sie einem anderen AP-Modell beitreten, haben Sie ein nicht homogenes Netzwerk.

Wenn sich der Access Point unter diesen Bedingungen nicht in derselben Version befindet, muss er dieselbe Version herunterladen. Stellen Sie deshalb sicher, dass Sie über einen gültigen TFTP/SFTP-Server und -Speicherort mit den AP-Images verfügen, die im Verzeichnis EWC > Administration > Software Management (EWC > Administration > Softwareverwaltung) konfiguriert sind:



TFTP-Server mit Ordner "AP-Bilder"



AP-Bilder

Der AP wird in der AP-Liste angezeigt, und Sie können ein PolicyTag zuweisen:

Cisco Embedded Wireless Controller on Catalyst Access Points

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Current Active  
AP9124\_RAP

Total APs : 3

AP Name	AP Model	Slots	Admin Status	Up Time
AP9115	C9115AXE-B	2	✓	0 days 0 hrs mins 36 secs
AP9124_MAP	C9124AXI-B	2	✓	8 days 6 hrs mins 37 secs
AP9124_RAP	C9124AXI-B	2	✓	8 days 6 hrs mins 40 secs

5 GHz Radios

Edit AP

General Interfaces Inventory Geolocation ICap Advanced

General

AP Name\* AP9115

Location\* default location

Base Radio MAC 1cd1.e079.66e0

Ethernet MAC 84f1.47b3.2cdc

Admin Status ENABLED

AP Mode Flex

Operation Status Registered

Fabric Status Disabled

CleanAir NSI Key

LED Settings

LED State ENABLED

Tags

Policy LocalSWTag

Site default-site-tag

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.12.2.35

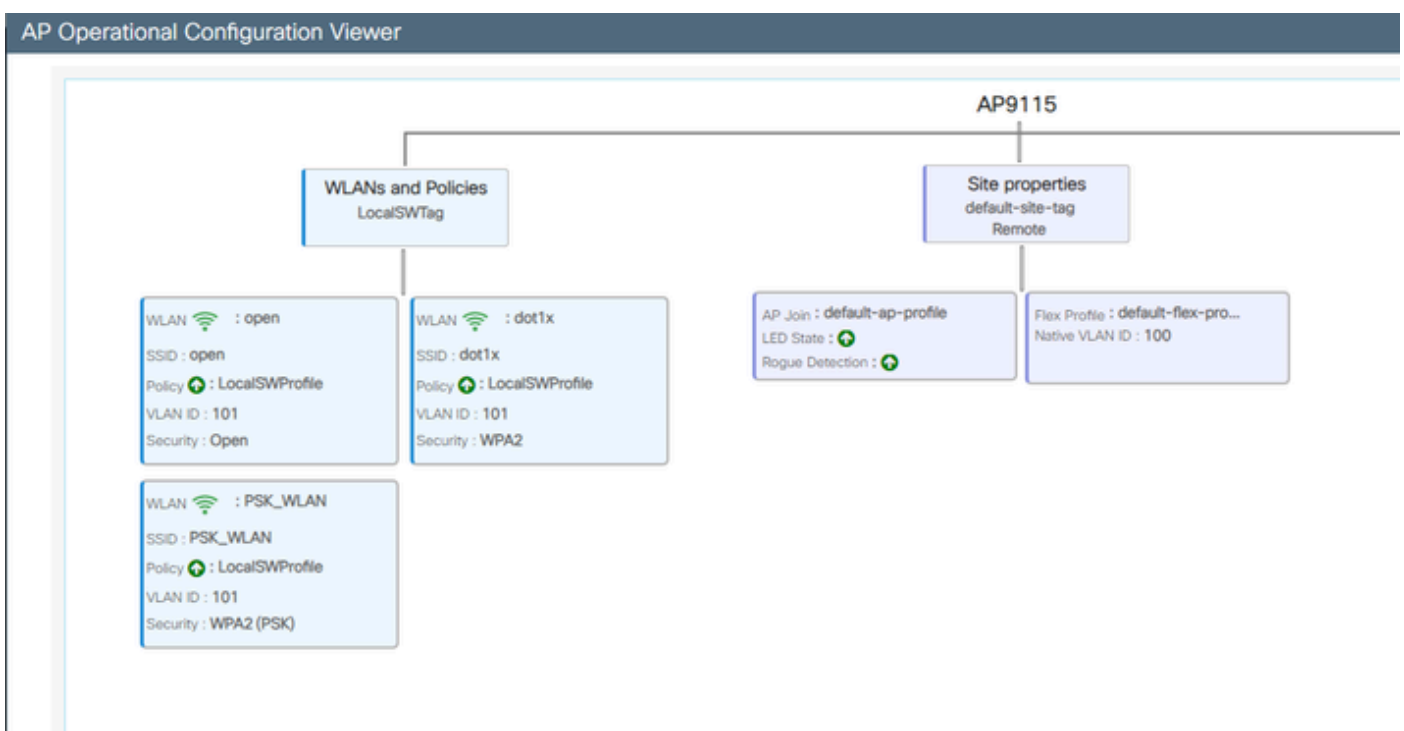
Predownloaded Status Predownloading

Predownloaded Version 0.0.0.0

Next Retry Time 0

Boot Version 1.1.2.4

AP-Liste mit 9115-Details



AP-Betriebsanzeige

## Überprüfung

Sie können den Mesh-Tree über die GUI sehen, die auch die Ausgabe von CLI liefert, wenn Sie den Befehl "show wireless mesh ap tree" verwenden. Gehen Sie auf der GUI zu Monitoring > Wireless > Mesh:



Monitoring > Wireless > Mesh

AP Convergence

Global Stats

Number of Bridge APs	0	Number of Flex+Bridge APs	2
Number of RAPs	0	Number of Flex+Bridge RAPs	1
Number of MAPs	0	Number of Flex+Bridge MAPs	1

Tree

```

AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
-----
[Sector 1]
-----
AP9124_RAP [0, 0, Default, (36), 0000.0000.0000, 3%, 0]
|-AP9124_MAP [1, 73, Default, (36), 0000.0000.0000, 3%, 0]
Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
(*) Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller

```

## Mesh-AP-Struktur

Auf dem RAP und MAP können Sie den Mesh-Backhaul mit dem Befehl "show mesh backhaul" überprüfen:

```

AP9124_RAP#show mesh backhaul
Wired Backhaul: 0 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
0 16 TRUE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16 0 T/F: T F T T F T Filtered

-----

Wired Backhaul: 1 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
1 Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16 0 T/F: F F F F F F Filtered

-----

Radio Backhaul: 0 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
2 INITIAL ACCESS UP Invalid FALSE FALSE TRUE FALSE FALSE ALLOWED RADIO

No Radio Adjacency Exists

-----

Radio Backhaul: 1 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
3 MAINT DOWNLINK UP Invalid FALSE TRUE FALSE FALSE TRUE ALLOWED RADIO
Mesh AMPP Radio adjacency info
Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W),
BlockListed(B), Authenticated(A), HTC capable(H), VHTCapable(V)
OldParent(O), BGScan(S)
Address Cost RawCost LinkCost ReportedCost Snr BCount Ch Width Bgn Flags: P O C N R W B A H V S Reject reason
4C:A6:4D:23:9D:51 Invalid Invalid 0 0 76 0 36 20 MHz - (T/F): F F T F T F F T T T F -

```

## RAP Show Mesh-Backhaul

```

AP9124_MAP#show mesh backhaul
Wired Backhaul: 0 [3C:57:31:C5:A9:F8]
idx Cost Uplink InterfaceType
0 Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:A9:F8 16 16 32 T/F: F F T F T T Blocklisted: GW UNREACHABLE

-----

Wired Backhaul: 1 [3C:57:31:C5:A9:F8]
idx Cost Uplink InterfaceType
1 Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:A9:F8 16 16 0 T/F: F F F F F F Filtered

-----

Radio Backhaul: 0 [4C:A6:4D:23:9D:51]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
2 INITIAL ACCESS UP Invalid FALSE FALSE TRUE FALSE FALSE ALLOWED RADIO

No Radio Adjacency Exists

-----

Radio Backhaul: 1 [4C:A6:4D:23:9D:51]
Hops to Root: 1
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
3 MAINT UPLINK UP 217 TRUE TRUE FALSE FALSE TRUE ALLOWED RADIO
Mesh AWPP Radio adjacency info
Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W),
BlockListed(B), Authenticated(A), HTC capable(H), VHTCapable(V)
OldParent(O), BGScan(S)
Address Cost RawCost LinkCost ReportedCost Snr BCount Ch Width Bgn Flags: P O C N R W B A H V S Reject reason
4C:A6:4D:23:AE:F1 217 272 256 16 70 0 36 20 MHz - (T/F): T F F T T T F T T T F -

-----

AP9124_MAP#

```

MAP Mesh-Backhaul anzeigen

Sie können die Konfiguration des Mesh-VLAN-Trunking auf der AP-Seite überprüfen:

```

AP9124_RAP#show mesh ethernet vlan config static
Static (Stored) ethernet VLAN Configuration

```

```

Ethernet Interface: 0
Interface Mode: TRUNK
Native Vlan: 100
Allowed Vlan: 101,

```

```

Ethernet Interface: 1
Interface Mode: ACCESS
Native Vlan: 0
Allowed Vlan:

```

Ethernet Interface: 2  
Interface Mode: ACCESS  
Native Vlan: 0  
Allowed Vlan:

Laptop2, der an Switch2 angeschlossen ist, hat von VLAN 101 eine IP-Adresse erhalten:

```
C:\Users\luke>ipconfig

Windows IP Configuration

Ethernet adapter usb_xhci:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 192.168.101.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.101.1
```

Der Laptop1 auf Switch1 empfing eine IP von VLAN 101:

Ethernet adapter Ethernet 6\_White:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::d1d6:f607:ff02:4217%18
IPv4 Address. . . . . : 192.168.101.13
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.101.1
```

```
C:\Users\tantunes>ping 192.168.101.12 -i 192.168.101.13
```

```
Pinging 192.168.101.12 with 32 bytes of data:
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
Reply from 192.168.101.12: bytes=32 time=7ms TTL=128
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
```

```
Ping statistics for 192.168.101.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 7ms, Average = 5ms
```



Hinweis: Beachten Sie, dass zum Testen von ICMP zwischen Windows-Geräten ICMP auf der System-Firewall zugelassen werden muss. Standardmäßig blockieren Windows-Geräte ICMP in der System-Firewall.

---

Ein weiterer einfacher Test zur Überprüfung des Ethernet-Bridging besteht darin, SVI für VLAN 101 auf beiden Switches bereitzustellen und Switch2 SVI auf DHCP zu setzen. Switch2 SVI für VLAN 101 erhält IP von VLAN 101 und Sie können Switch 1 VLAN 101 SVI für die Prüfung der VLAN 101-Konnektivität pingen:

```
<#root>
```

```
Switch2#show ip int br
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned YES NVRAM up down
Vlan100 192.168.100.61 YES DHCP up up
```

```
Vlan101 192.168.101.11 YES DHCP up up
```

```
GigabitEthernet0/1 unassigned YES unset up up
[...]
Switch2#
Switch2#ping 192.168.101.1 source 192.168.101.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.101.11
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
Switch2#
```

<#root>

```
Switch1#sh ip int br
Interface IP-Address OK? Method Status Protocol
Vlan1 192.168.1.11 YES NVRAM up up
Vlan100 192.168.100.1 YES NVRAM up up
```

```
Vlan101 192.168.101.1 YES NVRAM up up
```

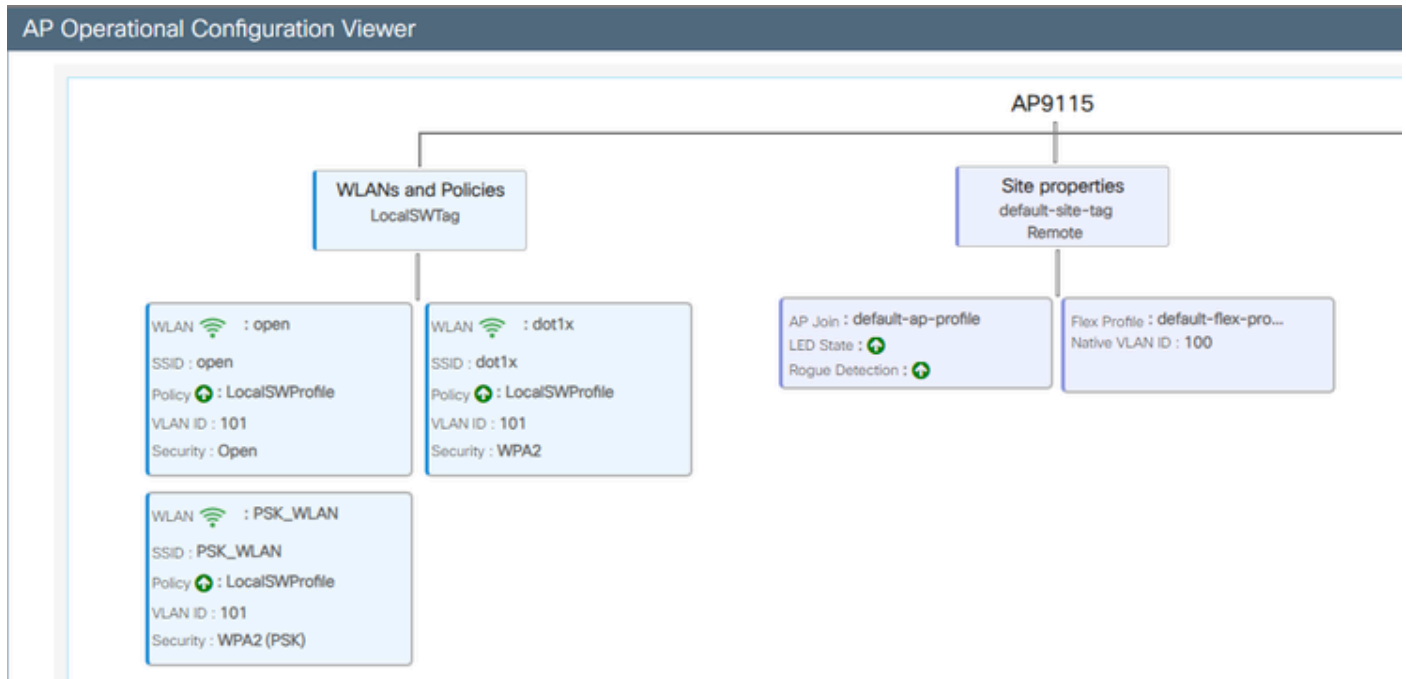
```
GigabitEthernet1/0/1 unassigned YES unset up up
[...]
Switch1#ping 192.168.101.11 source 192.168.101.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.11, timeout is 2 seconds:
Packet sent with a source address of 192.168.101.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
Switch1#
```

Der lokale Modus AP C9115 ist ebenfalls dem EWC beigetreten:

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode
AP9115	C9115AXE-B	2	✓	0 days 0 hrs 35 mins 30 secs	192.168.100.14	1cd1.e079.66e0	84f1.47b3.2cdc	Flex
AP9124_MAP	C9124AXI-B	2	✓	0 days 0 hrs 52 mins 59 secs	192.168.100.12	4ca6.4d23.9d40	3c57.31c5.a9f8	Flex+Bridge
AP9124_RAP	C9124AXI-B	2	✓	0 days 2 hrs 46 mins 57 secs	192.168.100.11	4ca6.4d23.aee0	3c57.31c5.ac2c	Flex+Bridge

AP 9115 mit EWC verbunden

Es wurden drei offene, PSK- und dot1x-WLANs erstellt, die einem Richtlinienprofil mit dem in den Zugriffsrichtlinien definierten VLAN 101 zugeordnet sind:



AP9115 - Betriebskonfiguration

Wireless-Clients können sich mit den WLANs verbinden:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 2 out of 2 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Site ID	SSID	WLAN ID	Client Type	State
9294-828a-e572	192.168.101.14	fe80:9294-828a-e572	AP9115	1	open	4	WLAN	Run
wc0a-3434-216c	192.168.101.15	fe80:wc0a-3434-216c	AP9115	1	PSK_WLAN	5	WLAN	Run

## Fehlerbehebung

In diesem Abschnitt werden nützliche Befehle sowie einige Tipps, Tricks und Empfehlungen vorgestellt.

Nützliche Befehle

Auf RAP/MAP:

```
AP9124_RAP#show mesh
adjacency          MESH Adjacency
backhaul           MESH backhaul
bgscan             MESH Background Scanning
channel            MESH channels
client-debug-filter MESH client debugging filter set
config             MESH config parameter
convergence        MESH convergence info
dfs                MESH dfs information
dhcp               Flex-mesh Internal DHCP Server
ethernet           show mesh ethernet bridging
forwarding         MESH Forwarding
history            MESH history of events
least-congested-scan Mesh least congested channel scan
linktest           MESH linktest stats
nat                Flex-mesh NAT/PAT
res                MESH RES info
security           MESH Security Show
stats              MESH stats
status             MESH status
stp                MESH daisychain STP info
timers             MESH Adjacency timers
```

```
AP9124_RAP#debug mesh
  adjacency      MESH adjacency debugs
  ap-link        MESH link debugs
  bg-scan        Mesh background scanning debugs
  channel        MESH channel debugs
  clear          RESET all MESH debugs
  client         Debug mesh clients
  convergence    MESH convergence debugs
  dhcp           MESH Internal DHCP debugs
  dump-pkts      Dump mesh packets
  events         MESH events
  filter         MESH debug filter
  forward-mcast  Mesh forwarding mcast debugs
  forward-table  Mesh forwarding table debugs
  history        MESH history of events
  level          Enable different mesh debug levels
  linktest       Mesh linktest debugs
  nat            Mesh NAT debugs
  path-control   MESH path-control debugs
  port-control   MESH port-control debugs
  security       MESH security debugs
  stp            MESH daisychain STP debugs
  wpa_suplicant Mesh WPA_SUPPLICANT debugs
  wstp           MESH WSTP debugs
```

RAP/MAP-Debug-Mesh-Optionen

Auf WLC:



```

9124ENC#show wireless mesh ?
airtime-fairness    Shows Mesh AP Airtime Fairness information
ap                  Shows mesh AP related information
cac                 Shows Mesh AP cac related information
config              Show mesh configurations
convergence          Show mesh convergence details.
ethernet            Show wireless mesh ethernet
neighbor            Show neighbors of all connected mesh Aps
persistent-ssid-broadcast Shows Mesh AP persistent ssid broadcast
information
rrm                  Show wireless mesh rrm information

```

Wireless Mesh anzeigen

Für die Fehlersuche auf dem WLC ist es am besten, RadioActive trace mit der MAC-Adresse des MAP/RAP zu verwenden.

Beispiel 1: RAP empfängt Adjacency von MAP und setzt die Authentifizierung durch

<#root>

AP9124\_RAP#show debug

mesh:

adjacent packet debugging is enabled

event debugging is enabled

mesh linktest debug debugging is enabled

```

Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshRadio
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshAwppA
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9560] EVENT-MeshAwppA
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9570] CLSM[4C:A6:4D:2
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9588] EVENT-MeshRadio
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9592] EVENT-MeshLink
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9600] EVENT-MeshSecur
Jan 16 14:47:05 AP9124_RAP kernel: [*01/16/2024 14:47:05.1008] EVENT-MeshSecur
Jan 16 14:47:05 AP9124_RAP kernel: [*01/16/2024 14:47:05.1011] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1172] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2033] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecur

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:

```

```

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2144] EVENT-MeshLink
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2146] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2147] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwppA
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3576] EVENT-MeshRadio
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadio
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadio

```

Beispiel 2: MAP-MAP-Adresse nicht zum WLC hinzugefügt oder falsch hinzugefügt

<#root>

```

Jan 16 14:52:13 AP9124_RAP kernel: [*01/16/2024 14:52:13.6402] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7407] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7408] EVENT-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7409] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7411] EVENT-MeshLink
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7419] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7583] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7586] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7586] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7620] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7620] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] 0x3c 0x57 0x31
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] 0xff 0xff 0xff
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] 0xaa 0xff 0x00
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] 0xaa 0xff 0xaa
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7636] EVENT-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7637] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7642] EVENT-MeshLink
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7642] EVENT-MeshSecur

```

Beispiel 3: RAP verliert MAP

<#root>

```
Jan 16 14:48:58 AP9124_RAP kernel: [*01/16/2024 14:48:58.9929] INFO-MeshRadio
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.2889] INFO-MeshAwppAc
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.7894] INFO-MeshAwppAc
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.9931] INFO-MeshRadio
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.9932] INFO-MeshRadio
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.2891] INFO-MeshAwppAc
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.7891] INFO-MeshAwppAc
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.9937] INFO-MeshRadio
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.9938] INFO-MeshRadio
Jan 16 14:49:01 AP9124_RAP kernel: [*01/16/2024 14:49:01.2891] INFO-MeshAwppAc

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5480] EVENT-MeshAwppAc

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5481] EVENT-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5481] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5488] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5489] INFO-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5501] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5501] EVENT-MeshAdj[1

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5502] EVENT-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5511] EVENT-MeshLink
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5512] EVENT-MeshSecur
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5513] EVENT-MeshLink
```

## Tipps, Tricks und Empfehlungen

- Durch ein Upgrade von MAP und RAP auf dieselbe Image-Version über das Kabel vermeiden wir, dass Bilder per Funk heruntergeladen werden (was in "schmutzigen" HF-Umgebungen problematisch sein kann).
- Es wird dringend empfohlen, das Setup vor der Bereitstellung vor Ort in einer kontrollierten Umgebung zu testen.
- Wenn Sie Ethernet-Bridging mit Windows-Laptops auf beiden Seiten testen, beachten Sie, dass Sie ICMP auf der System-Firewall zulassen müssen, um ICMP zwischen Windows-Geräten zu testen. Standardmäßig blockieren Windows-Geräte ICMP in der System-Firewall.
- Wenn APs mit externen Antennen verwendet werden, überprüfen Sie im Bereitstellungsleitfaden, welche Antennen kompatibel sind und an welchen Port angeschlossen werden soll.
- Um den Datenverkehr von verschiedenen VLANs über die Mesh-Verbindung zu

überbrücken, muss die Funktion "VLAN Transparent" deaktiviert werden.

- Erwägen Sie einen lokalen Syslog-Server für die APs, da dieser sonst nur über eine Konsolenverbindung Debuginformationen bereitstellen kann.

## Referenzen

[Datenblatt: Cisco Embedded Wireless Controller auf Catalyst Access Points](#)

[Cisco Embedded Wireless Controller auf Catalyst Access Points \(EWC\) - Whitepaper](#)

[Konfigurieren der Punkt-zu-Punkt-Mesh-Verbindung mit Ethernet-Bridging auf Mobility Express-APs](#)

## 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.