Fehlerbehebung bei einem Lightweight-AP, der einem WLC nicht beitreten kann

Inhalt

Einleitung

In diesem Dokument wird der Prozess zur Erkennung und zum Beitritt von AireOS Wireless LAN-Controllern (WLC) beschrieben.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco AireOS WLCs
- Grundkenntnisse des Lightweight Access Point Protocol (CAPWAP)

Verwendete Komponenten

Der Schwerpunkt dieses Dokuments liegt auf AireOS WLCs. Catalyst 9800 wird darin nicht behandelt, obwohl der Join-Prozess in den meisten Fällen ähnlich verläuft.

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Überblick über den WLC Discovery- und Join-Prozess

In einem Cisco Unified Wireless-Netzwerk müssen die LAPs zunächst einen WLC erkennen und diesem beitreten, bevor sie Wireless-Clients bedienen können.

Daraus ergibt sich jedoch die Frage, wie die LAPs die Management-IP-Adresse des Controllers in einem anderen Subnetz gefunden haben.

Wenn Sie dem LAP über die DHCP-Option 43, DNS-Auflösung (Domain Name System) von, nicht mitteilen Cisco-capwap-controller.local_domain, wo sich der Controller befindet, **oder ihn statisch konfigurieren, weiß das LAP nicht, wo im Netzwerk die Verwaltungsschnittstelle des Controllers zu finden ist.**

Zusätzlich zu diesen Methoden sucht die LAP im lokalen Subnetz automatisch nach Controllern mit einer lokalen Broadcast-Nummer 255.255.255.255. Außerdem speichert die LAP die Management-IP-Adresse ihres Controllers und der Controller, die selbst bei Neustarts als Mobilitäts-Peers vorhanden sind. Sobald der AP jedoch einem anderen WLC beitritt, erinnert er sich nur noch an die IP-Adresse dieses neuen WLC und seiner Mobility Peers und nicht an die vorherigen. Wenn Sie den LAP also an erster Stelle im lokalen Subnetz der Verwaltungsschnittstelle platzieren, findet er die Verwaltungsschnittstelle des Controllers und speichert die Adresse. Das nennt man Priming. Dies hilft Ihnen nicht, den Controller zu finden, wenn Sie später eine LAP austauschen. Cisco empfiehlt daher die Verwendung der DHCP-Option 43 oder der DNS-Methoden.

Die LAPs stellen immer zuerst über eine Erkennungsanforderung eine Verbindung mit der Management-Schnittstellenadresse des Controllers her. Der Controller teilt dem LAP dann die IP-Adresse der Layer-3-AP-Manager-Schnittstelle (die standardmäßig auch die Verwaltungsschnittstelle sein kann) mit, sodass der LAP als Nächstes eine Verbindungsanforderung an die AP-Manager-Schnittstelle senden kann.

Der Access Point führt diesen Vorgang beim Start aus:

- **Der LAP startet und DHCP sendet eine IP-Adresse, wenn ihm zuvor keine statische IP-Adresse zugewiesen wurde.**

- **Der LAP sendet Erkennungsanforderungen über die verschiedenen Erkennungsalgorithmen an die Controller und erstellt eine Controller-Liste. Im Wesentlichen erfasst der LAP so viele Management-Schnittstellenadressen für die Controller-Liste wie möglich über:**

a. **DHCP-Option 43 (gut für globale Unternehmen, bei denen sich Büros und Controller auf verschiedenen Kontinenten befinden).**

b. **DNS-Eintrag für** cisco-capwap-controller (gut für lokale Unternehmen - kann auch verwendet werden, um zu finden, wo brandneue APs beitreten) Wenn Sie CAPWAP verwenden, stellen Sie sicher, dass es einen DNS-Eintrag für cisco-capwap-controller.

- **Management-IP-Adressen von Controllern, die der LAP zuvor speichert.**
- **Eine Layer-3-Übertragung im Subnetz.**
- **Statisch konfigurierte Informationen.**
- **Controller, die in der Mobilitätsgruppe des WLC vorhanden sind, dem der AP zuletzt beigetreten ist**

Aus dieser Liste ist die einfachste Methode für die Bereitstellung, die LAPs im gleichen Subnetz wie die Verwaltungsschnittstelle des Controllers zu haben und den LAPs-Layer-3-Broadcast zu ermöglichen, den Controller zu finden. Diese Methode muss für Unternehmen verwendet werden, die über ein kleines Netzwerk verfügen und keinen lokalen DNS-Server besitzen.

Die nächste einfachste Bereitstellungsmethode ist die Verwendung eines DNS-Eintrags mit DHCP. Sie können mehrere Einträge mit demselben DNS-Namen haben. Dadurch kann die LAP mehrere Controller erkennen. Diese Methode muss von Unternehmen verwendet werden, die alle ihre Controller an einem einzigen Standort haben und über einen lokalen DNS-Server verfügen. Oder, wenn das Unternehmen über mehrere DNS-Suffixe verfügt und die Controller durch Suffixe getrennt sind.

Die DHCP-Option 43 wird von großen Unternehmen zur Lokalisierung der Informationen über das DHCP verwendet. Diese Methode wird von großen Unternehmen mit einem einzigen DNS-Suffix verwendet. Cisco besitzt beispielsweise Gebäude in Europa, Australien und den Vereinigten Staaten. Um sicherzustellen, dass die LAPs nur lokal mit Controllern verbunden werden, kann Cisco keinen DNS-Eintrag verwenden und muss die Informationen der DHCP-Option 43 nutzen, um den LAPs die Management-IP-Adresse ihres lokalen Controllers mitzuteilen.

Schließlich wird die statische Konfiguration für ein Netzwerk ohne DHCP-Server verwendet. Sie können die für die Verbindung mit einem Controller erforderlichen Informationen über den Konsolenport und die AP-CLI statisch konfigurieren. Verwenden Sie den folgenden Befehl, um Controller-Informationen mithilfe der AP-CLI statisch zu konfigurieren:

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Weitere Informationen zur Konfiguration der DHCP-Option 43 auf einem DHCP-Server finden Sie im Konfigurationsbeispiel für die DHCP-Option 43.

- Senden Sie eine Erkennungsanforderung an jeden Controller in der Liste, und warten Sie auf die Antwort zur Controller-Erkennung, die den Systemnamen, die IP-Adressen des AP-Managers, die Anzahl der APs, die bereits an die einzelnen AP-Manager-Schnittstellen angeschlossen sind, und die Gesamtüberkapazität für den Controller enthält.

- Sehen Sie sich die Controller-Liste an, und senden Sie eine Beitrittsanfrage in dieser Reihenfolge an einen Controller (nur wenn der Access Point eine Erkennungsantwort von diesem erhalten hat):

  a. Primärer Controller-Systemname (zuvor auf LAP konfiguriert).

  b. Name des sekundären Controller-Systems (zuvor auf der LAP konfiguriert).

  c. Name des Systems des tertiären Controllers (zuvor für die LAP konfiguriert).

  d. Primärer Controller (sofern für die LAP noch kein primärer, sekundärer oder tertiärer Controller konfiguriert wurde) Früher wusste man immer, welcher Controller ein brandneuer LAPs ist).

  e. Wenn keine der vorherigen Bedingungen erkannt wird, erfolgt der Lastausgleich zwischen Controllern über den Kapazitätsüberschuss in der Erkennungsantwort.

  Wenn zwei Controller über die gleiche Überkapazität verfügen, senden Sie die Verbindungsanforderung an den ersten Controller, der auf die Erkennungsanforderung mit einer Erkennungsantwort geantwortet hat. Wenn ein einzelner Controller über mehrere AP-Manager an mehreren Schnittstellen verfügt, wählen Sie die AP-Manager-Schnittstelle mit der geringsten Anzahl von APs aus.

  Der Controller antwortet auf alle Erkennungsanforderungen ohne Zertifikatsüberprüfung oder WAP-Anmeldeinformationen. Join-Anforderungen müssen jedoch über ein gültiges Zertifikat verfügen, um eine Join-Antwort vom Controller zu erhalten. Erhält der LAP keine Join-Antwort seiner Wahl, versucht er den nächsten Controller in der Liste, es sei denn, der Controller ist ein konfigurierter Controller (primär/sekundär/tertiär).

- Wenn der Access Point die Join-Antwort erhält, überprüft er, ob das Image mit dem des Controllers übereinstimmt. Wenn nicht, lädt der Access Point das Image vom Controller herunter und startet neu, um das neue Image zu laden. Anschließend wird der Vorgang in Schritt 1 erneut gestartet.

- Wenn das System über dasselbe Software-Image verfügt, fordert es die Konfiguration vom Controller an und wechselt in den registrierten Zustand auf dem Controller.

Nach dem Herunterladen der Konfiguration kann der Access Point erneut geladen werden, um die neue Konfiguration anzuwenden. Daher kann es zu einem zusätzlichen Neuladen kommen, was ein normales Verhalten ist.

Debuggen vom Controller

Auf dem Controller gibt es einige **debug** Befehle, mit denen Sie den gesamten Prozess in der CLI anzeigen können:

- **debug capwap events enable**: Zeigt Discovery-Pakete und Join-Pakete an.

- **debug capwap packet enable**: Zeigt Informationen auf Paketebene der Ermittlungs- und Verbindungspakete an.

- **debug pm pki enable**: Zeigt den Zertifikatvalidierungsprozess an.

- **debug disable-all**: Deaktiviert Debugs.

Mit einer Terminalanwendung, die die Ausgabe in einer Protokolldatei, einer Konsole oder Secure Shell (SSH)/Telnet auf dem Controller erfassen und die folgenden Befehle eingeben kann:

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

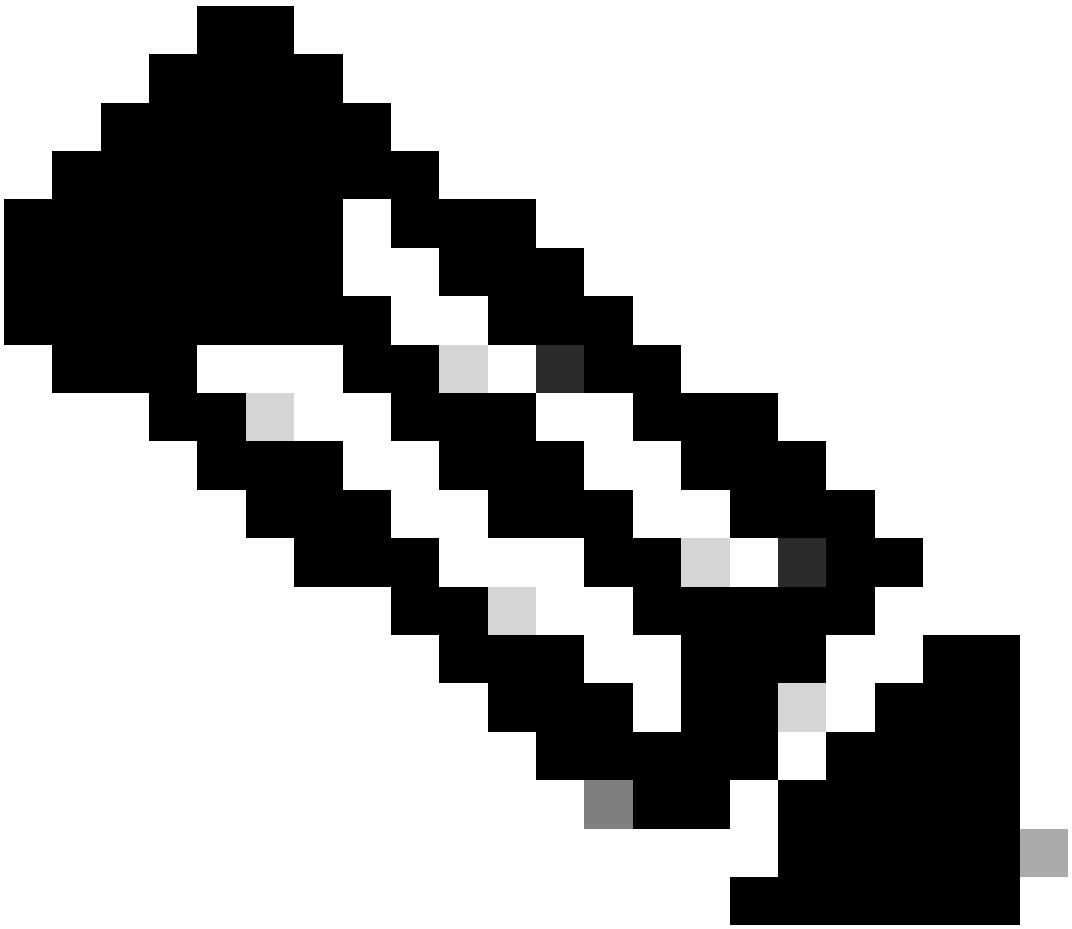
Nachdem die Debugs erfasst wurden, können Sie alle Debugs mit demdebug disable-all Befehl deaktivieren.

Die folgenden Abschnitte zeigen die Ausgabe dieser **debug** Befehle bei der Registrierung des LAP beim Controller.

debug capwap events enable

Dieser Befehl stellt Informationen zu den CAPWAP-Ereignissen und -Fehlern bereit, die beim CAPWAP-Erkennungs- und -Verknüpfungsprozess auftreten.

Dies ist die **debug capwap events enable** Befehlsausgabe für eine LAP, die dasselbe Image wie der WLC hat:



Hinweis: Einige Zeilen der Ausgabe wurden aufgrund von Platzbeschränkungen in die zweite Zeile verschoben.

---

debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317

!--- CAPWAP discovery request sent to the WLC by the LAP.

*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317

!--- WLC responds to the discovery request from the LAP.

*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

!--- LAP sends a join request to the WLC.

*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join

!--- WLC responds with a join reply to the LAP.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure

!--- LAP requests for the configuration information from the WLC.

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99

!--- WLC responds by providing all the necessary configuration information to the LAP.

*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.

!--- LAP is up and ready to service wireless clients.

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- WLC sends all the RRM and other configuration parameters to the LAP.

Wie im vorherigen Abschnitt erwähnt, überprüft ein LAP bei der Registrierung beim WLC, ob er über dasselbe Image wie der Controller verfügt. Wenn sich die Images auf dem LAP und dem WLC unterscheiden, laden die LAPs das neue Image zuerst vom WLC herunter. Wenn die LAP über dasselbe Image verfügt, werden die Konfiguration und andere Parameter weiterhin vom WLC heruntergeladen.

Diese Meldungen werden in der **debug capwap events enable** Befehlsausgabe angezeigt, wenn die LAP im Rahmen des Registrierungsvorgangs ein Image vom Controller herunterlädt:

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Nach Abschluss des Image-Downloads startet die LAP neu, führt die Erkennung aus und führt den Algorithmus erneut aus.

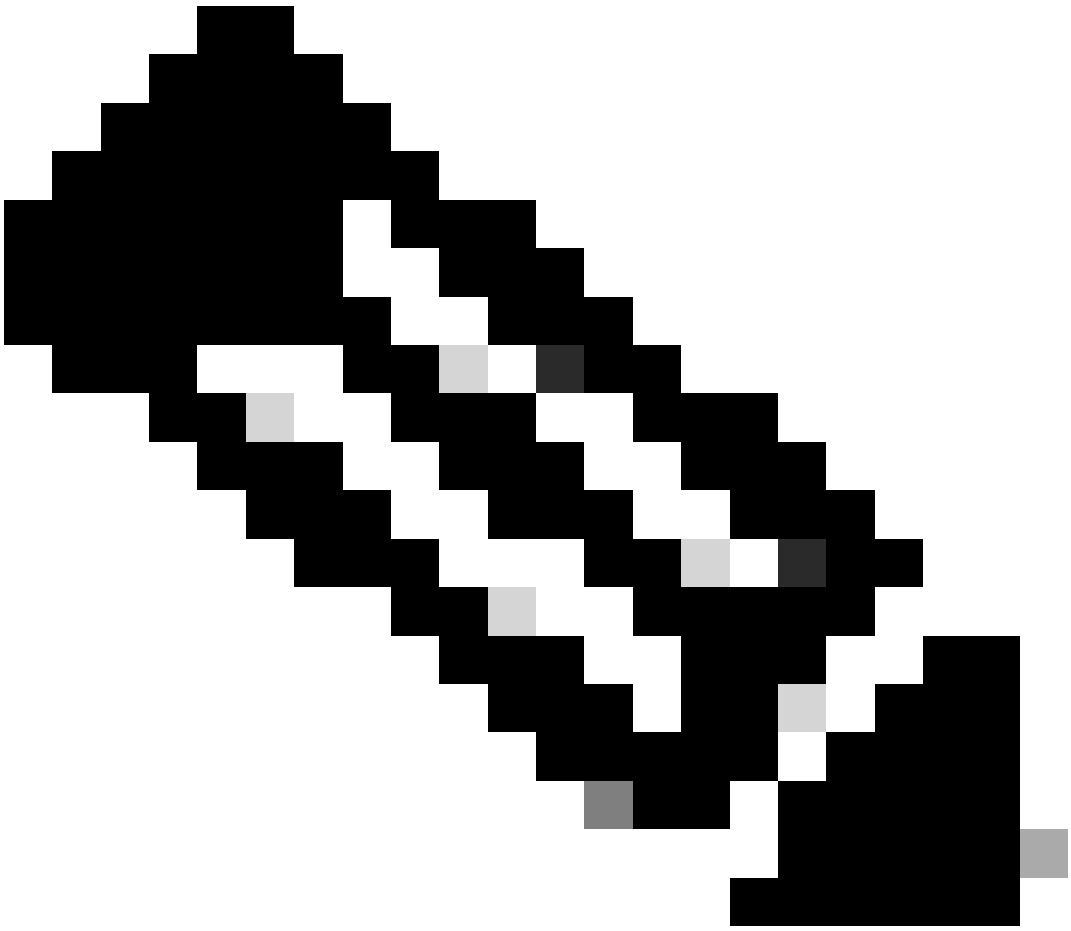
debug pm pki enable

Im Rahmen des Join-Prozesses authentifiziert der WLC jeden LAP durch die Bestätigung, dass sein Zertifikat gültig ist.

Wenn der WAP die CAPWAP-Join-Anforderung an den WLC sendet, bettet er sein X.509-Zertifikat in die CAPWAP-Nachricht ein. Der WAP generiert auch eine zufällige Sitzungs-ID, die ebenfalls in der CAPWAP-Join-Anforderung enthalten ist. Wenn der WLC die CAPWAP-Join-Anforderung empfängt, validiert er die Signatur des X.509-Zertifikats mit dem öffentlichen AP-Schlüssel und überprüft, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde.

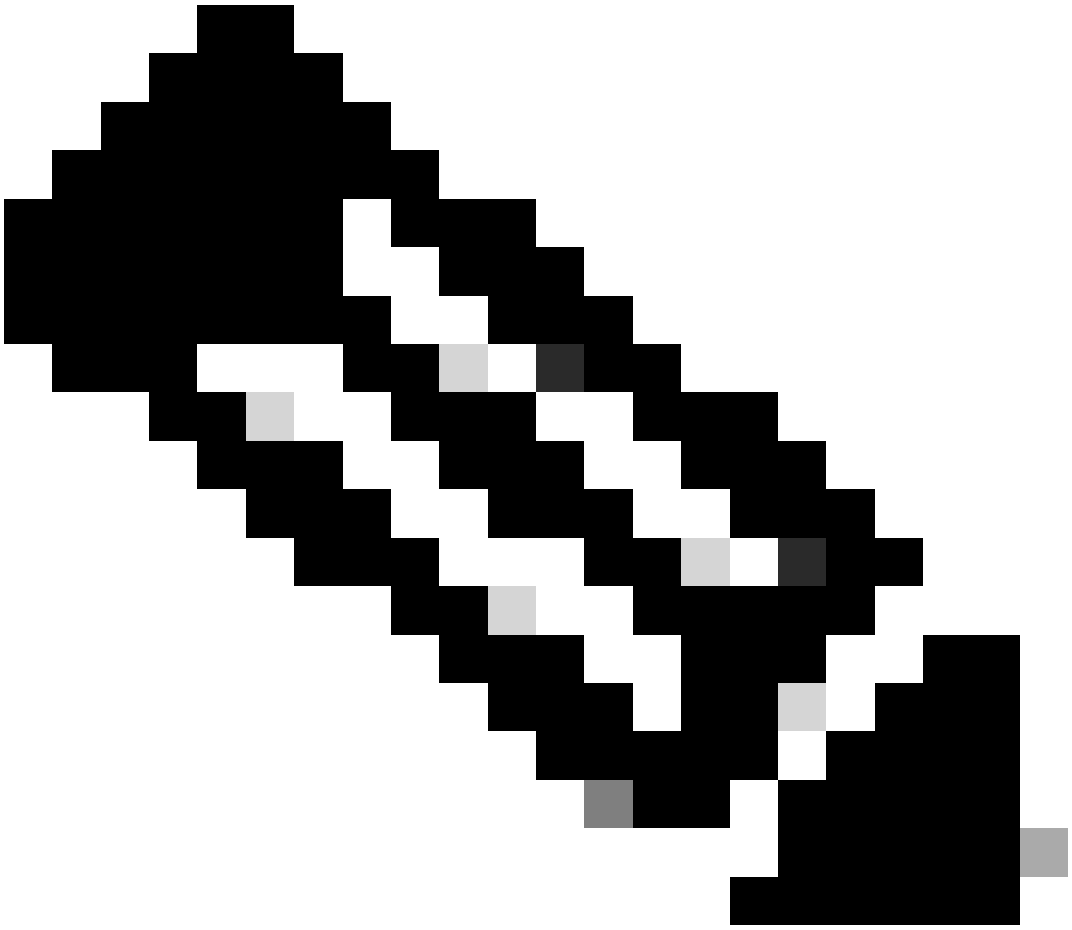
Außerdem wird das Startdatum und die Startzeit für das Gültigkeitsintervall des AP-Zertifikats überprüft und mit dem Datum und der Uhrzeit verglichen (daher muss die Uhr des Controllers in der Nähe des aktuellen Datums und der aktuellen Uhrzeit eingestellt werden). Wenn das X.509-Zertifikat validiert wird, generiert der WLC einen zufälligen AES-Verschlüsselungsschlüssel. Der WLC leitet die AES-Schlüssel an seine Krypto-Engine weiter, damit er zukünftige CAPWAP-Kontrollnachrichten, die mit dem AP ausgetauscht werden, verschlüsseln und entschlüsseln kann. Beachten Sie, dass Datenpakete unverschlüsselt im CAPWAP-Tunnel zwischen der LAP und dem Controller gesendet werden.

Der **debug pm pki enable** Befehl zeigt den Zertifizierungs-Validierungsprozess an, der in der Join-Phase des Controllers stattfindet. Der **debug pm pki enable** Befehl zeigt außerdem den AP-Hashschlüssel beim Join-Prozess an, wenn der AP über ein vom LWAPP-Konvertierungsprogramm erstelltes selbstsigniertes Zertifikat (Self-Signed Certificate, SSC) verfügt. Wenn der Access Point über ein MIC (Manufactured Installed Certificate) verfügt, wird kein Hashschlüssel angezeigt.



Hinweis: Alle APs, die nach Juni 2006 hergestellt wurden, verfügen über ein MIC.

Die folgende Ausgabe des **debug pm pki enable** Befehls wird ausgegeben, wenn sich der LAP mit einem MIC im Controller befindet:



Hinweis: Einige Zeilen der Ausgabe wurden aufgrund von Platzbeschränkungen in die zweite Zeile verschoben.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Debuggen vom Access Point

Wenn die Debug-Meldungen des Controllers keine Join-Anforderung anzeigen, können Sie den Prozess vom Access Point aus debuggen, wenn der Access Point über einen Konsolen-Port verfügt. Mit diesen Befehlen können Sie den AP-Bootvorgang sehen, aber Sie müssen zuerst in den Aktivierungsmodus wechseln (das Standardkennwort lautet Cisco).

- **debug dhcp detail** : Zeigt Informationen zur DHCP-Option 43 an.
- **debug ip udp**: Zeigt alle vom WAP empfangenen und übertragenen UDP-Pakete an.
- debug capwap client event : Zeigt CAPWAP-Ereignisse für den Access Point an.

- **debug capwap client error**: Zeigt CAPWAP-Fehler an.

- **debug dtls client event**: Zeigt DTLS-Ereignisse für den Access Point an.
- **debug dtls error enable**: Zeigt DTLS-Fehler für den Access Point an.
- **undebug all**: Deaktiviert Debug-Vorgänge auf dem Access Point.

Hier ist ein Beispiel für die Ausgabe der debug capwapBefehle. Diese Ausgabe vermittelt einen Eindruck von den Paketen, die der Access Point während des Bootvorgangs sendet, um einen Controller zu erkennen und diesem beizutreten.

```
<#root>

AP can discover the WLC via one of these options :


!--- AP discovers the WLC via option 43


*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set


!--- capwap Discovery Request using the statically configured controller information.


*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set


!--- Capwap Discovery Request sent using subnet broadcast.
```

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

Warum wird LAP nicht zum Controller hinzugefügt?

Überprüfen Sie zunächst die Grundlagen

- Können AP und WLC miteinander kommunizieren?
- Stellen Sie sicher, dass der WAP eine Adresse von DHCP bezieht (prüfen Sie, ob der DHCP-Server die MAC-Adresse des WAP geleast hat).
- Pingen Sie den AP vom Controller.
- Überprüfen Sie, ob die STP-Konfiguration auf dem Switch korrekt ist, damit Pakete an die VLANs nicht blockiert werden.
- Wenn die Pings erfolgreich sind, stellen Sie sicher, dass der Access Point über mindestens eine Methode zum Ermitteln mindestens einer einzelnen WLC-Konsole oder Telnet/SSH im Controller verfügt, um Debug-Vorgänge auszuführen.

-

Bei jedem Neustart des Access Points wird die WLC-Erkennungssequenz initiiert und versucht, den Access Point zu lokalisieren. Starten Sie den AP neu, und überprüfen Sie, ob er dem WLC beitritt.

Im Folgenden sind einige der häufigsten Probleme aufgeführt, aufgrund derer die LAPs nicht dem WLC beitreten.

Problemhinweis: Ablauf von Zertifikaten - FN63942

Die in die Hardware eingebetteten Zertifikate gelten für einen Zeitraum von 10 Jahren nach der Herstellung. Wenn Ihre APs oder Ihr WLC älter als 10 Jahre sind, können abgelaufene Zertifikate zu Verbindungsproblemen mit dem AP führen. Weitere Informationen zu diesem Problem finden Sie in der Problembeschreibung: FN63942.

Mögliche Probleme: Beispiele

Problem 1: Die Controller-Zeit liegt außerhalb des Zertifikatsgültigkeitsintervalls.

Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben:

- Führen Sie debug dtls client error + debug dtls client event Befehle am Access Point aus:

<#root>

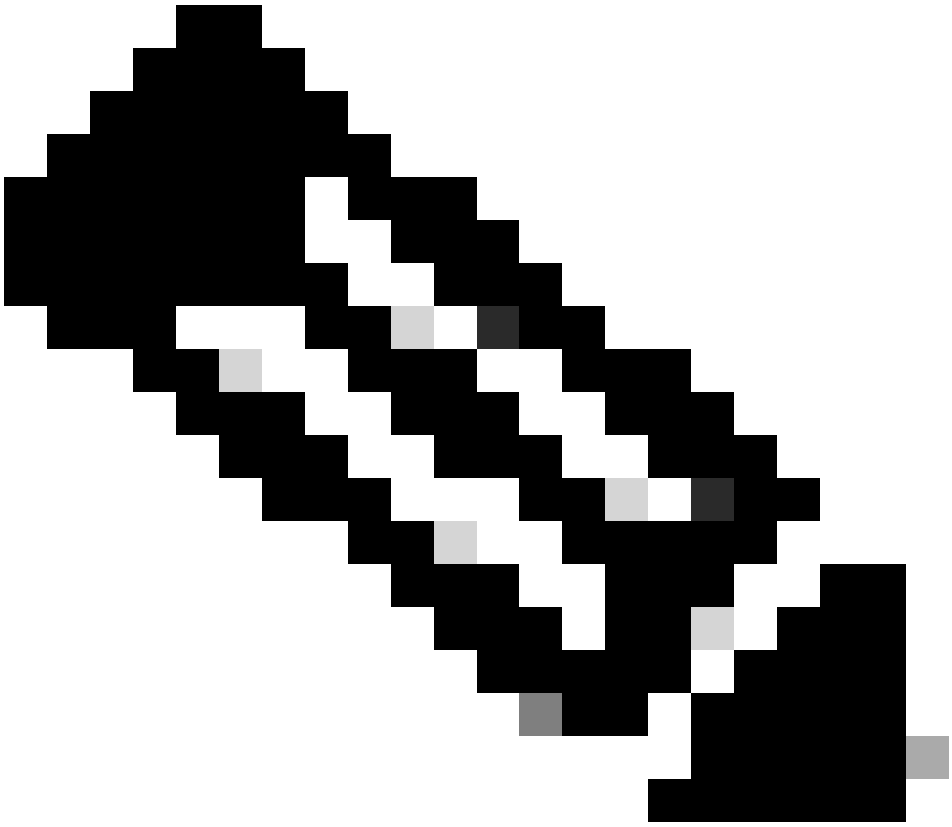
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Diese Informationen zeigen deutlich, dass die Controller-Zeit außerhalb des Zertifikatsgültigkeitsintervalls des AP liegt. Daher kann sich der Access Point nicht beim Controller registrieren. Zertifikate, die im WAP installiert sind, haben ein vordefiniertes Gültigkeitsintervall. Die Controller-Zeit muss so eingestellt werden, dass sie innerhalb des Zertifikatsgültigkeitsintervalls des AP-Zertifikats liegt.

• Geben Sie den **show time** Befehl aus der CLI des Controllers ein, um zu überprüfen, ob das auf dem Controller eingestellte Datum und die Uhrzeit innerhalb dieses Gültigkeitsintervalls liegen. Wenn die Controller-Zeit höher oder niedriger als dieses Gültigkeitsintervall des Zertifikats ist, ändern Sie die Controller-Zeit so, dass sie in dieses Intervall fällt.



Commands > Set Time **Hinweis:** Wenn die Zeit auf dem Controller nicht richtig eingestellt ist, wählen Sie sie im GUI-Modus des Controllers aus, oder geben Sie den Befehl config time in der CLI des Controllers ein, um die Controller-Zeit einzustellen.

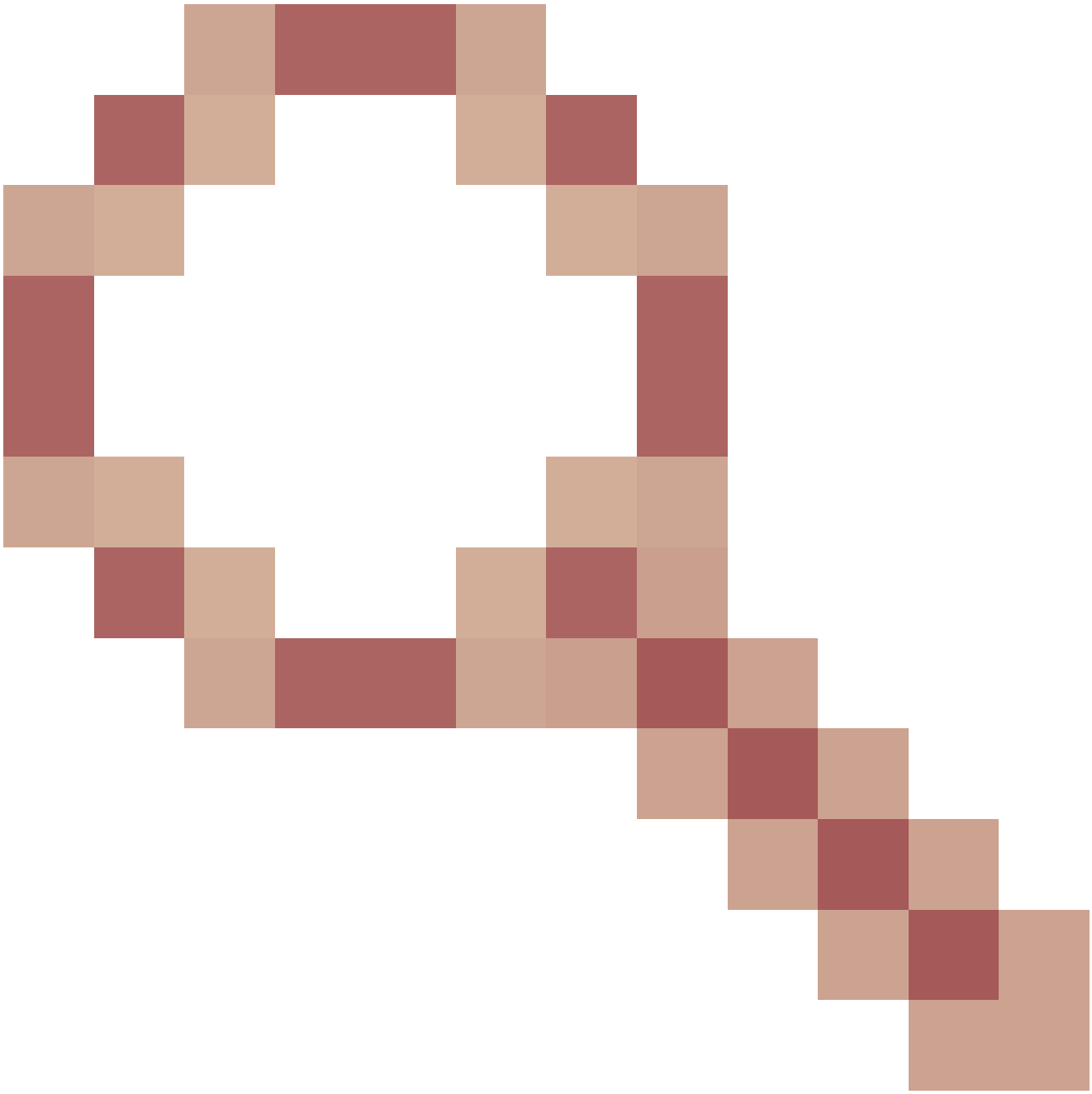
- Überprüfen Sie auf APs mit CLI-Zugriff die Zertifikate mit dem **show crypto ca certificates** Befehl aus der AP-CLI.

Mit diesem Befehl können Sie das im Access Point festgelegte Zertifikatgültigkeitsintervall überprüfen. Hier ein Beispiel:

```
AP00c1.649a.be5c#show crypto ca cert
........................................
........................................
........................................
........................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
..............................
..............................
..............................
```

Die gesamte Ausgabe wird nicht aufgelistet, da mit der Ausgabe dieses Befehls viele Gültigkeitsintervalle verknüpft sein können. Berücksichtigen Sie nur das vom Associated Trustpoint angegebene Gültigkeitsintervall: Cisco_IOS_MIC_cert mit dem entsprechenden AP-Namen im Namensfeld. In diesem Beispiel lautet die Ausgabe `Name: C1200-001563e50c7e`. Dies ist das tatsächliche Gültigkeitsintervall des Zertifikats, das berücksichtigt werden muss.

- Bitte beachten Sie, dass nach Ablauf der Cisco Bug-ID CSCuq19142



LAP/WLC MIC- oder SSC-Lebensdauer ein DTLS-Fehler auftritt: Cisco Bug-ID CSCuq19142.

Problem 2: Diskrepanz im Bereich gesetzlicher Vorschriften

Diese Meldung wird in der **debug capwap events enable** Befehlsausgabe angezeigt:

<#root>

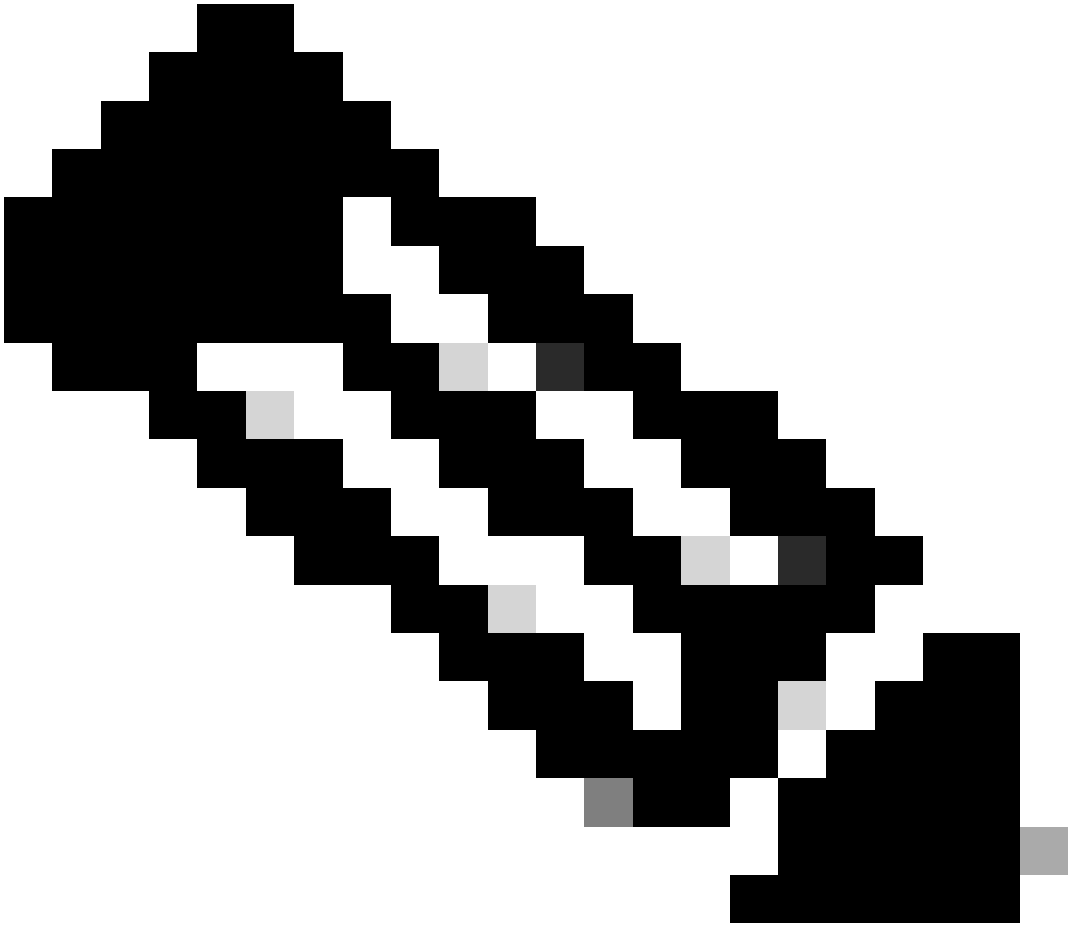
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

Die Meldung weist eindeutig auf eine Diskrepanz im Zulassungsbereich von LAP und WLC hin. Der WLC unterstützt mehrere Zulassungsdomänen, aber jede Zulassungsdomäne muss ausgewählt werden, bevor ein WAP aus dieser Domäne beitreten kann. Beispielsweise kann der WLC, der die Zulassungsdomäne -A verwendet, nur mit APs verwendet werden, die die Zulassungsdomäne -A verwenden (usw.). Wenn Sie APs erwerben, stellen Sie sicher, dass diese denselben Zulassungsbereich nutzen. Erst dann können sich die APs beim WLC registrieren.



Hinweis: 802.1b/g- und 802.11a-Funkmodule müssen sich in derselben Zulassungsdomäne für einen AP befinden.

Problem 3: AP-Autorisierungsliste auf dem WLC aktiviert; LAP nicht in Autorisierungsliste

In solchen Fällen wird die folgende Meldung auf dem Controller in der Ausgabe des debug capwap events enable Befehls angezeigt:

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007:
```

spamRadiusProcessResponse: AP Authorization failure

for 00:0b:85:51:5a:e0

Wenn Sie einen LAP mit einem Konsolenport verwenden, wird diese Meldung angezeigt, wenn Sie den debug capwap client error folgenden Befehl ausführen:

<#root>

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG:
```

No more AP manager IP addresses remain.

Auch dies ist ein deutlicher Hinweis darauf, dass das LAP nicht Teil der AP-Autorisierungsliste auf dem Controller ist.

Sie können den Status der AP-Autorisierungsliste mit dem folgenden Befehl anzeigen:

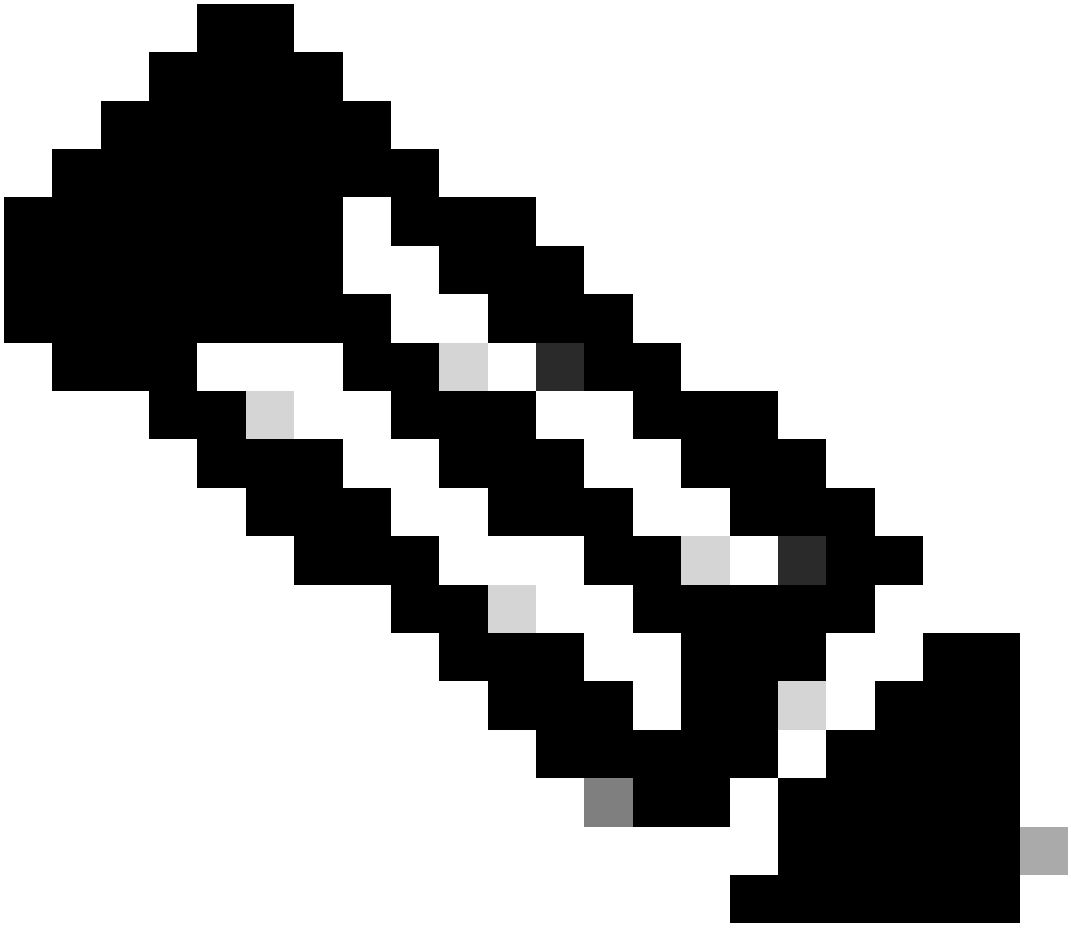
```
<#root>

(Cisco Controller) >

show auth-list

Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Um der AP-Autorisierungsliste eine LAP hinzuzufügen, verwenden Sie den config auth-list add mic <AP MAC Address> Befehl. Weitere Informationen zum Konfigurieren der LAP-Autorisierung finden Sie unter Lightweight Access Point (LAP)-Autorisierung in einem Konfigurationsbeispiel für ein Cisco Unified Wireless Network.

Problem 4: Es liegt ein beschädigtes Zertifikat oder ein beschädigter öffentlicher Schlüssel am AP vor.

Die LAP wird aufgrund eines Zertifikatsfehlers nicht einem Controller hinzugefügt.

Geben Sie die debug capwap errors enable und **debug pm pki enable** Befehle ein. Es werden Meldungen angezeigt, die auf beschädigte Zertifikate oder Schlüssel hinweisen.



Hinweis: Einige Zeilen der Ausgabe wurden aufgrund von Platzbeschränkungen in zweite Zeilen verschoben.

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
from AP 00:0f:24:a9:52:e0

```
.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

Verwenden Sie eine der beiden folgenden Optionen, um das Problem zu beheben:

- MIC AP: Request a Return Materials Authorization (RMA)
- LSC AP - Stellen Sie Ihr LSC-Zertifikat erneut bereit.

Problem 5: Controller empfängt AP-Erkennungsnachricht auf falschem VLAN (Sie sehen die Erkennungsnachricht debuggen, aber nicht Antwort)

Diese Meldung wird in der debug capwap events enable Befehlsausgabe angezeigt:

<#root>

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Diese Meldung bedeutet, dass der Controller eine Ermittlungsanforderung von einer Rundfunk-IP-Adresse mit einer Quell-IP-Adresse erhalten hat, die sich in keinem konfigurierten Subnetz des Controllers befindet. Dies bedeutet auch, dass der Controller derjenige ist, der das Paket verwirft.

Das Problem besteht darin, dass der Access Point nicht die Erkennungsanforderung an die Management-IP-Adresse gesendet hat. Der Controller meldet eine Broadcast-Erkennungsanforderung von einem VLAN, das nicht auf dem Controller konfiguriert ist. Dies tritt in der Regel dann auf, wenn Trunks VLANs zulassen und sie nicht auf Wireless-VLANs beschränken.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Befindet sich der Controller in einem anderen Subnetz, müssen die Access Points für die Controller-IP-Adresse **primiert** werden, oder die Access Points müssen die Controller-IP-Adresse mithilfe einer der Erkennungsmethoden empfangen.

- Der Switch ist so konfiguriert, dass einige VLANs zugelassen werden, die sich nicht auf dem Controller befinden. Beschränken Sie die zulässigen VLANs auf den Trunks.

Problem 6: AP kann dem WLC nicht beitreten, Firewall blockiert erforderliche Ports

Wenn eine Firewall im Unternehmensnetzwerk verwendet wird, stellen Sie sicher, dass diese Ports auf der Firewall aktiviert sind, damit die LAP dem Controller beitreten und mit ihm kommunizieren kann.

Sie müssen diese Ports aktivieren:

- Aktivieren Sie diese UDP-Ports für CAPWAP-Datenverkehr:
  - Daten - 5247
  - Steuerung - 5246
- Aktivieren Sie diese UDP-Ports für den Mobilitätsverkehr:
  - 16666 - 16666
  - 16667 - 16667

- Aktivieren Sie die UDP-Ports 5246 und 5247 für CAPWAP-Datenverkehr.

- TCP 161 und 162 für SNMP (für das Wireless Control System [WCS])

Diese Ports sind optional (abhängig von Ihren Anforderungen):

- UDP 69 für TFTP

- TCP 80 und/oder 443 für HTTP oder HTTPS für GUI-Zugriff

- TCP 23 und/oder 22 für Telnet oder SSH für CLI-Zugriff

Problem 7: Doppelte IP-Adresse im Netzwerk

Dies ist ein weiteres häufiges Problem, das beobachtet wird, wenn der Access Point dem WLC beitreten möchte. Diese Fehlermeldung wird angezeigt, wenn der Access Point versucht, dem Controller beizutreten.

No more AP manager IP addresses remain

Einer der Gründe für diese Fehlermeldung ist, dass im Netzwerk eine doppelte IP-Adresse vorhanden ist, die mit der IP-Adresse des AP-Managers übereinstimmt. In diesem Fall behält der LAP die Einschaltvorgänge bei und kann dem Controller nicht beitreten.

Die Fehlerbeseitigung zeigt, dass der WLC LWAPP-Erkennungsanforderungen von den APs empfängt und eine LWAPP-Erkennungsantwort an die APs sendet.

WLCs empfangen jedoch keine LWAPP-Join-Anfragen von den APs.

Um dieses Problem zu beheben, pingen Sie den AP-Manager von einem verdrahteten Host aus, der sich im gleichen IP-Subnetz befindet wie der AP-Manager. Überprüfen Sie anschließend den ARP-Cache. Wenn eine doppelte IP-Adresse gefunden wird, entfernen Sie das Gerät mit der doppelten IP-Adresse, oder ändern Sie die IP-Adresse auf dem Gerät so, dass es eine eindeutige IP-Adresse im Netzwerk hat.

Der AP kann dann dem WLC beitreten.

Problem 8: LAPs mit Mesh-Image können nicht am WLC teilnehmen

Der Lightweight Access Point ist nicht beim WLC registriert. Im Protokoll wird folgende Fehlermeldung angezeigt:

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
     Type: WLAN USER
```

Dies ist möglich, wenn der Lightweight Access Point mit einem Mesh-Image ausgeliefert wurde und sich im Bridge-Modus befindet. Wenn die LAP mit Mesh-Software bestellt wurde, müssen Sie die LAP zur AP-Autorisierungsliste hinzufügen. Wählen Sie **Security > AP Policies (Sicherheit > AP-Richtlinien**) aus, und fügen Sie **AP** zur Autorisierungsliste hinzu. Anschließend muss der AP beitreten, das Image vom Controller herunterladen und sich im Bridge-Modus beim WLC registrieren. Anschließend müssen Sie den Access Point in den lokalen Modus ändern. Die LAP lädt das Image herunter, startet neu und registriert sich im lokalen Modus wieder am Controller.

Problem 9: Ungültige Adresse für Microsoft DHCP

Access Points können ihre IP-Adressen schnell erneuern, wenn versucht wird, einem WLC beizutreten. Dies kann dazu führen, dass Windows DHCP-Server diese IPs als BAD_ADDRESS markieren, wodurch der DHCP-Pool schnell leer sein könnte. Weitere Informationen finden Sie im Kapitel Client Roaming im Konfigurationshandbuch für Cisco Wireless Controller, Version 8.2.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

- **AP-Join-Prozess mit Catalyst 9800**

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.