疑難排解輕量型 AP 無法加入 WLC 的問題

目錄

簡介

必要條件

- 需求
- 採用元件
- 慣例

WLC發現和加入過程概述

從控制器偵錯

- debug capwap events enable
- debug pm pki enable

從 AP 進行偵錯

LAP未加入控制器，為什麼？

- 首先檢查基本資訊

現場通知：證書過期- FN63942

要查詢的潛在問題：示例

- 問題1：控制器時間超出證書有效間隔
- 問題2：監管域不匹配
- 問題3：在WLC上啟用了AP授權清單；LAP不在授權清單中
- 問題4：AP上的證書或公鑰損壞
- 問題5：控制器在錯誤的VLAN上接收到AP發現消息（您會看到發現消息調試，但沒有響應）
- 問題6：AP無法加入WLC，防火牆阻塞了必要的埠
- 問題7：網路中的IP地址重複
- 問題8：具有網狀映像的LAP無法加入WLC
- 問題9：Microsoft DHCP地址錯誤

相關資訊

簡介

本檔案將說明AireOS無線LAN控制器(WLC)探索和加入程式。

必要條件

需求

思科建議您瞭解以下主題：

- 關於輕型存取點(LAP)和Cisco AireOS WLC配置的基本知識
- Lightweight Access Point Protocol (CAPWAP) 的基本知識

採用元件

本文檔重點介紹AireOS WLC，並不包括Catalyst 9800，儘管加入過程大體相似。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

WLC發現和加入過程概述

在Cisco統一無線網路中，LAP必須先發現並加入WLC，然後才能為無線客戶端提供服務。

但是，這會產生一個問題：當控制器位於不同的子網時，LAP如何找到控制器的管理IP地址？

如果您未通過DHCP選項43、域名系統(DNS)解析Cisco-capwap-controller.local_domain告知LAP控制器的位置，**或者未進行靜態配置，則LAP不知道在網路中的**哪個位置可以找到控制器的管理介面。

除了這些方法外，LAP還會自動在本地子網中查詢具有255.255.255.255本地廣播的控制器。此外，**LAP會記住其控制器的管理IP地址，並且即使在重新啟動期間，**控制器仍顯示為移動對等體。但是，**當該AP加入另一個WLC時，**它只記得該新**WLC及其移動對等體的IP，而不記得上一個移動體的IP。因此，如果**您將**LAP放在管理介面的本地子網上，**它會查詢控制器管理介面並記住該地址。這叫做促發作用。如果您稍後更換**LAP，這不會有助於找到控制器。因此，Cisco建議使用DHCP option 43或DNS方法。**

LAP 一律會先透過探索要求連線至控制器的管理介面位址。然後，控制器會向 LAP 告知第 3 層 AP 管理程式介面（依預設也可以是管理介面）IP 位址，以便 LAP 接著將加入要求傳送給 AP 管理程式介面。

AP 在啟動時會逐步完成下列程序：

- **如果LAP之前未分配靜態IP地址，則引導並DHCP作為IP地址。**
- **LAP透過各種發現演算法向控制器傳送發現請求，並構建控制器清單。**基本上，**LAP透過以下方式獲取儘可能多的控制器清單管理介面地址：**

a. **DHCP選項43（適用於辦公室與控制器位於不同大陸的全球性公司）。**

cisco-capwap-controller

- **的DNS條目（對本地企業有好處-也可用於查詢新AP加入的位置）如果使用CAPWAP，請確保** cisco-capwap-controller**有一個**DNS條目。
- **LAP以前記憶的控制器的管理IP地址。**
- **子網上的第3層廣播。**
- **靜態配置的資訊。**
-

控制器出現在 AP 最後加入的 WLC 行動群組中.

在此清單中，最簡單的部署方式是將 LAP 置於與控制器管理介面相同的子網路上，並允許 LAP 第 3 層廣播尋找控制器。此方法必須用於擁有小型網路且沒有本地DNS伺服器的公司。

下一個最簡單的部署方法是使用DNS條目與DHCP。您可以有多個**DNS名稱相同的條目。這允許LAP發現多個控制器。此方法必須由所有控制器位於單一位置並擁有本地DNS伺服器的公司使用。或者，如果公司有多個DNS字尾，並且控制器用字尾隔離。**

大型公司使用DHCP選項43將DHCP的資訊在地化。此方法供具有單一DNS尾碼的大型企業使用。例如，思科在歐洲、澳洲和美國擁有建築。為了確保LAP僅本地加入控制器，Cisco不能使用DNS條目，必須使用DHCP option 43資訊告知LAP其本地控制器的管理IP地址。

最後，靜態配置用於沒有DHCP伺服器的網路。您可以透過控制檯埠和**AP的CLI靜態配置加入控制器所需的資訊。有關如何使用AP CLI靜態配置控制器資訊的資訊，請使用此命令：**

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

有關如何在DHCP伺服器上配置DHCP option 43的資訊，請參閱DHCP option 43配置示例

- 向清單上的每個控制器傳送發現請求，並等待控制器發現應答，該應答包含系統名稱、AP管理器IP地址、已連線到每個AP管理器介面的AP數量以及控制器的整體過剩容量。
- 檢視控制器清單，並按以下順序向控制器傳送加入請求（僅當無線存取點收到來自它的發現回覆時）：

a. 主控制器系統名稱（先前在LAP上配置）。

b. 輔助控制器系統名稱（先前在LAP上配置）。

c. 第三級控制器系統名稱（先前在LAP上配置）。

d. 主控制器(如果之前未使用Primary、Secondary或Tertiary控制器名稱配置LAP。用於始終知道哪個控制器是新的LAP加入)。

e. 如果看不到之前的情況，則使用發現響應中的超量容量值來平衡各控制器的負載。

如果兩個控制器具有相同的超額容量，則將加入請求傳送到響應發現請求的第一個控制器，該控制器具有發現響應。如果單個控制器在多個介面上有多個AP管理器，請選擇具有最少數量AP的AP管理器介面。

控制器響應所有發現請求，而不使用證書檢查或AP憑據。但是，加入請求必須具有有效的證書，才能從控制器獲得加入響應。如果LAP沒有收到來自其選擇的加入響應，則LAP會嘗試清單中的下一個控制器，除非該控制器是已配置的控制器（主/輔助/第三）。

- 收到加入回覆時，AP會進行檢查以確保其映像與控制器的映像相同。否則，AP會從控制器下載映像並重新啟動以載入新映像，並從步驟1重新開始整個過程。

- 如果它有相同的軟體映像，則從控制器請求配置並進入控制器上的註冊狀態。

下載配置後，AP可以再次重新載入以應用新配置。因此，可能會發生額外重新載入，這是正常行為。

從控制器偵錯

可以使用控制器上的一些**debug** 命令在CLI上檢視此整個過程：

- **debug capwap events enable**:顯示探索封包和加入封包。

- **debug capwap packet enable**:顯示探索和加入封包的封包層級資訊。

- **debug pm pki enable**:顯示憑證驗證程序。

- **debug disable-all**:關閉偵錯。

藉由可將輸出擷取至記錄檔的終端應用程式，透過主控台或使用安全殼層 (SSH)/Telnet 連線至您的控制器，然後輸入以下命令：

<#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

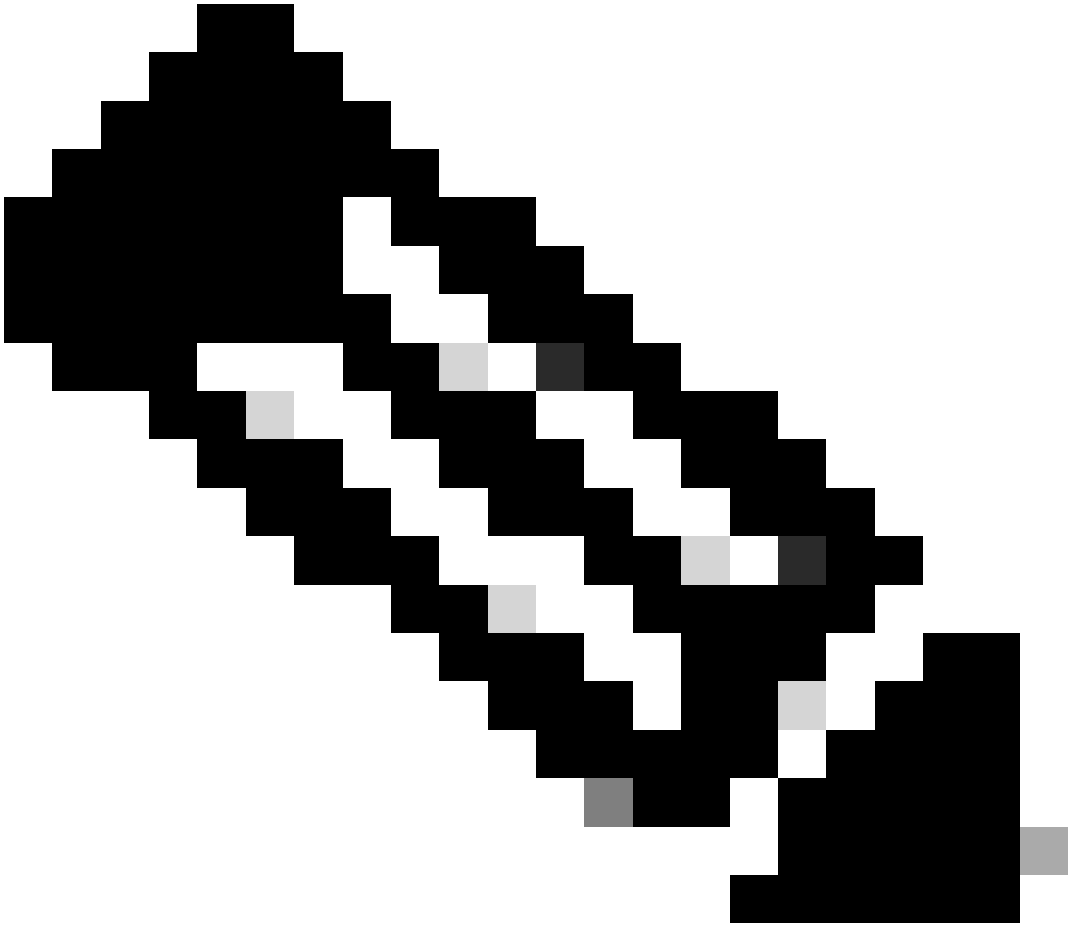
在捕獲到這些debug命令後，可以使用debug disable-all命令停用所有調試。

接下來的部分顯示了LAP向控制器進行註冊時，這些**debug** 命令的輸出。

debug capwap events enable

此命令提供有關CAPWAP發現和加入過程中發生的CAPWAP事件和錯誤的資訊。

以下是針對與WLC具有相同映像的LAP的**debug capwap events enable** 命令的輸出：



註：由於空間限制，某些輸出行已移至第二行。

<#root>

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.

如上一節中所述，一旦LAP註冊到WLC，它將檢查其映像是否與控制器相同。如果LAP和WLC上的映像不同，LAP將首先從WLC下載新映像。如果LAP具有相同的映像，它將繼續從WLC下載配置和其他引數。

如果LAP在註冊過程中從控制器中下載映像，您將在**debug capwap events enable** 的命令輸出中看到以下消息：

```
*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
```

映像下載完成後，LAP將重新啟動並運行發現，然後再次加入演算法。

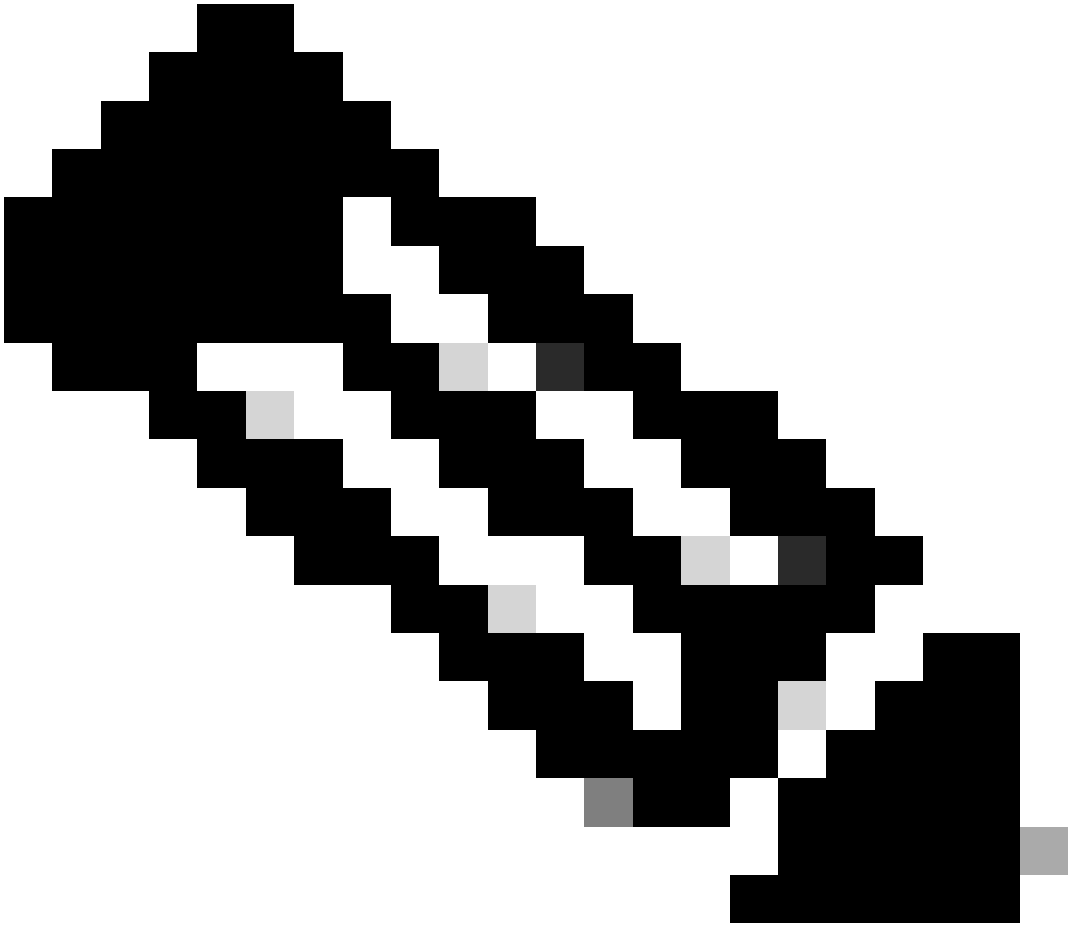
debug pm pki enable

作為加入過程的一部分，WLC透過確認每個LAP的證書有效對其進行身份驗證。

當 AP 將 CAPWAP 加入要求傳送至 WLC 時，它會將其 X.509 憑證內嵌到 CAPWAP 訊息中。AP 也會產生同樣包含在 CAPWAP 加入要求中隨機工作階段 ID。WLC收到CAPWAP加入請求後，會使用AP公鑰驗證X.509證書的簽名，並檢查證書是否由受信任的證書頒發機構頒發。

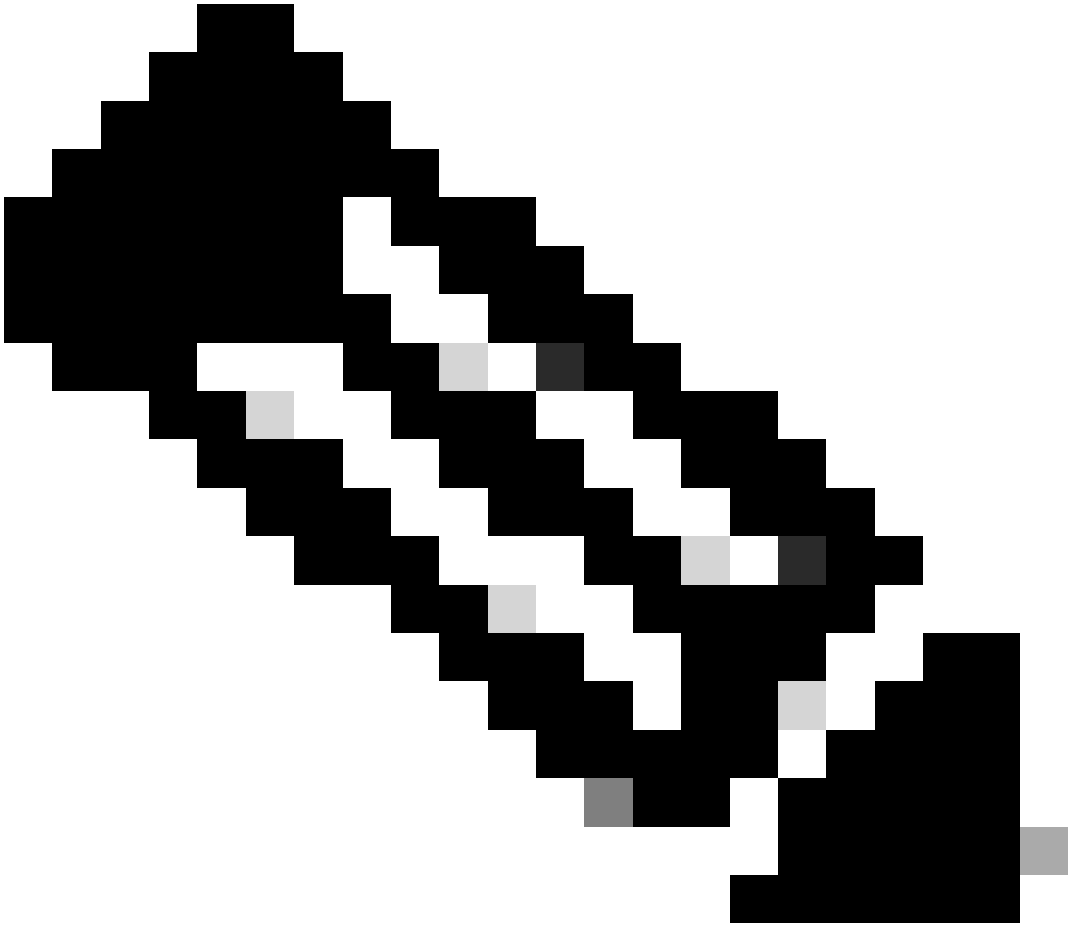
它還檢視AP證書有效間隔的開始日期和時間，並將該日期和時間與其自己的日期和時間進行比較（因此，控制器時鐘需要設定為接近當前日期和時間）。如果X.509憑證已驗證，則WLC會產生隨機AES加密金鑰。WLC將AES金鑰插入其加密引擎，以便加密和解密將來與AP交換的CAPWAP控制消息。請注意，資料封包會以純文字傳入 LAP 與控制器之間的 CAPWAP 通道。

debug pm pki enable 命令顯示在控制器的加入階段發生的認證驗證過程。如果AP有LWAPP轉換程式建立的自簽名證書(SSC)，**debug pm pki enable** 命令還會在加入進程中顯示AP雜湊鍵。如果AP具有已製造的安裝證書(MIC)，則您看不到雜湊金鑰。



註：在2006年6月以後製造的所有AP都具有MIC。

以下是帶有MIC的LAP加入控制器時**debug pm pki enable** 命令的輸出：



註：由於空間限制，某些輸出行已移至第二行。

<#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

從 AP 進行偵錯

如果控制器調試未指示加入請求，則可以在存取點具有控制檯埠時從AP調試進程。您可以使用這些命令檢視AP啟動過程，但必須首先進入啟用模式（預設口令為Cisco）。

- **debug dhcp detail** :顯示 DHCP 選項 43 資訊。
- **debug ip udp**：顯示AP接收和傳輸的所有UDP資料包。
- debug capwap client event :顯示 AP 的 CAPWAP 事件。
- **debug capwap client error**:顯示 AP 的 CAPWAP 錯誤。
- **debug dtls client event**:顯示 AP 的 DTLS 事件。

- **debug dtls error enable**:顯示 AP 的 DTLS 錯誤。
- **undebug all**:停用 AP 上的偵錯。

下面是debug capwap命令的輸出示例。此部分輸出提供AP在引導過程中傳送的資料包以發現和加入控制器的資訊。

```
<#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
```

LAP未加入控制器，為什麼？

首先檢查基本資訊

- AP和WLC能否通訊？
- 確保AP從DHCP獲取地址（檢查DHCP伺服器租用AP的MAC地址）。
- 從控制器對AP執行ping操作。
- 檢查交換機上的STP配置是否正確，以便不會阻止發往VLAN的資料包。
- 如果ping成功，請確保AP至少有一種方法，用於發現至少一個WLC控制檯或telnet/ssh到控制器以運行調試。
- 每當 AP 重新開機時，它都會初始化 WLC 探索序列並嘗試尋找 AP。將 AP 重新開機並檢查其是否已加入 WLC。

下面是LAP不加入WLC的一些常見問題。

現場通知：證書過期- FN63942

製造後，內嵌於硬體中的憑證有效期限為 10 年。如果您的AP或WLC使用時間超過10年，則過期的證書可能會導致AP加入問題。有關此問題的詳細資訊，請參閱此現場通知：現場通知：FN63942。

要查詢的潛在問題：示例

問題1：控制器時間超出證書有效間隔

完成以下步驟以對此問題進行故障排除：

- 在AP上發出debug dtls client error + debug dtls client event命令：

<#root>

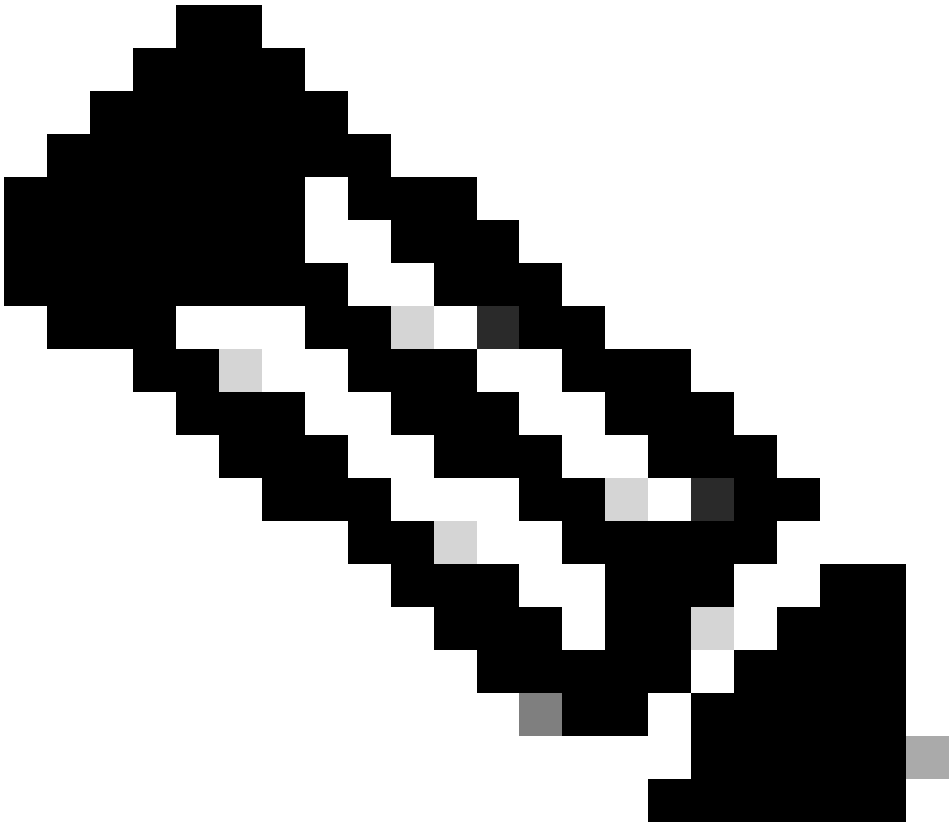
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

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
```

此資訊清楚地顯示控制器時間不在AP的證書有效間隔內。因此，AP無法註冊到控制器。AP中安裝的證書具有預定義的有效間隔。必須設定控制器時間，以使其在AP證書的證書有效間隔內。

- 從控制器的CLI發出 **show time** 命令，以便驗證控制器上的日期和時間設定是否在此有效間隔內。如果控制器時間高於或低於此證書有效間隔，請將控制器時間更改為在此間隔內。



注意：如果控制器上的時間設定不正確，請在控制器的GUI模式下選擇Commands > Set Time，或在控制器的CLI中發出config time命令來設定控制器時間。

- 在可以訪問CLI的AP上，請從AP的CLI中使用**show crypto ca certificates** 命令對證書進行驗證。

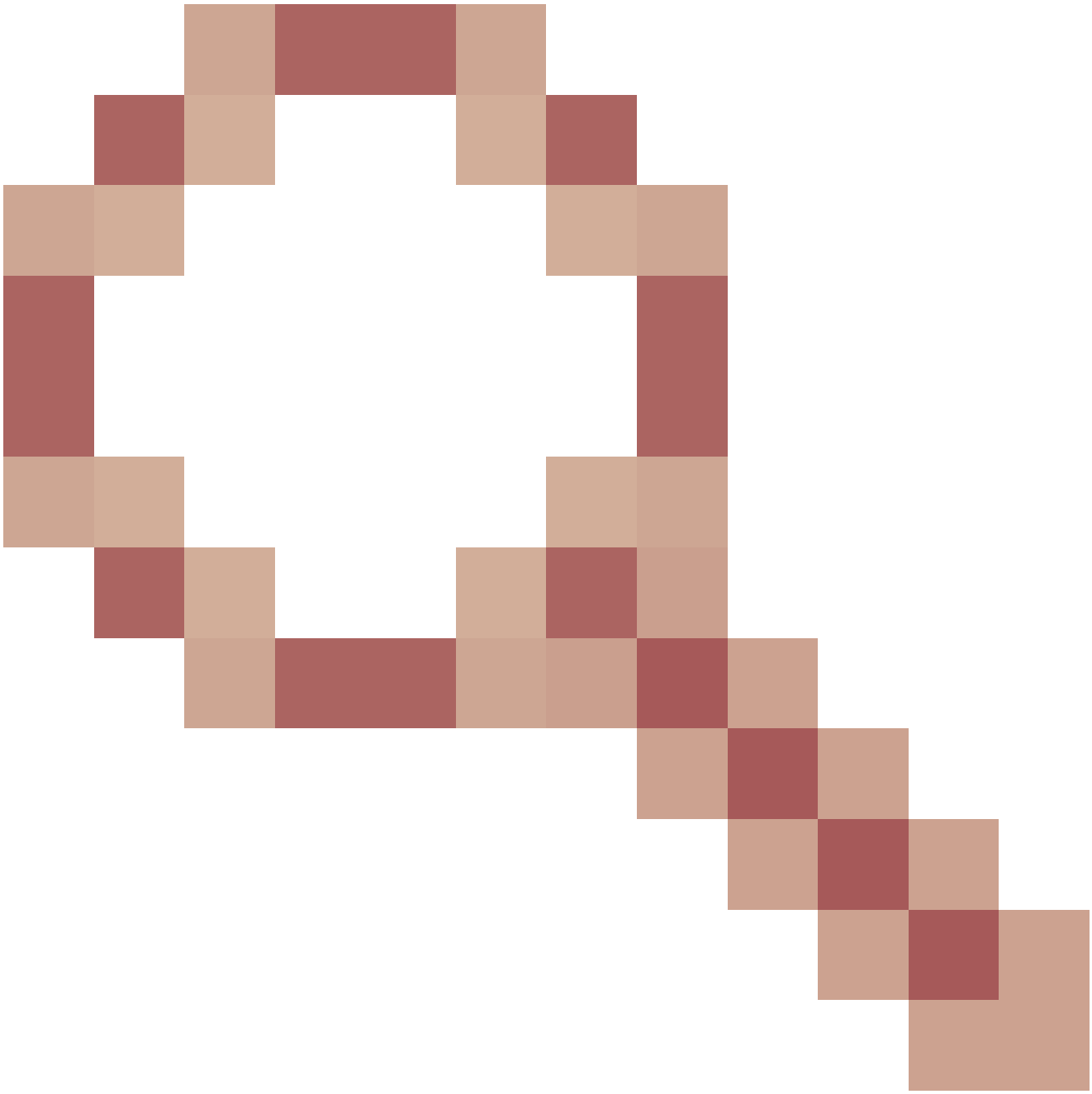
此命令允許您驗證在AP中設定的證書有效間隔。範例如下：

```
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:
.................................
.................................
.....................................
```

未列出整個輸出，因為可能存在許多與此命令輸出關聯的有效間隔。僅考慮關聯信任點指定的有效間隔：Cisco_IOS_MIC_cert和名稱欄位中的相關AP名稱。在此示例輸出中，對應代碼為Name： C1200-001563e50c7e。這是要考慮的實際憑證有效間隔。

- 請參閱思科漏洞ID CSCuq19142



LAP/WLC MIC或SSC有效期到期導致DTLS故障： 思科漏洞ID CSCuq19142.

問題2：監管域不匹配

您可以在**debug capwap events enable** 命令輸出中看到此消息：

<#root>

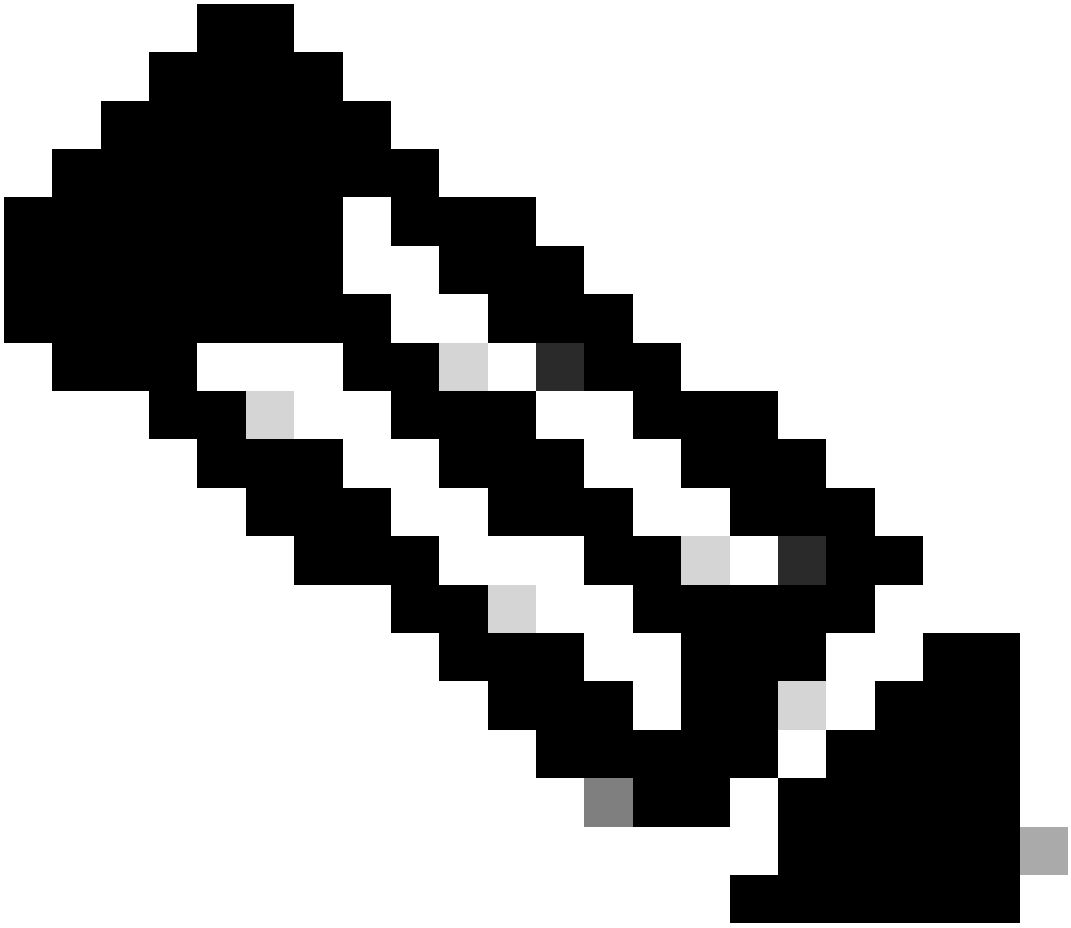
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***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

此消息清楚地表明LAP和WLC的監管域不匹配。WLC支援多個管制域，但必須先選擇每個管制域，AP才能從該域加入。例如，使用管制域-A的WLC只能與使用管制域-A（等）的AP一起使用。購買AP時，請確保它們共用相同的監管域。只有這樣，AP才能註冊到WLC。



注意：對於單個AP，802.1b/g和802.11a無線電必須在同一管制域中。

問題3：在WLC上啟用了AP授權清單；LAP不在授權清單中

在此類情況下，您將在控制器上debug capwap events enable命令的輸出中看到此消息：

<#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

如果使用帶有控制檯埠的LAP，在您發出debug capwap client error命令時將會看到此消息：

```
<#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.

這再次清楚地表明LAP不是控制器上AP授權清單的一部分。

您可以使用此命令檢視AP授權清單的狀態：

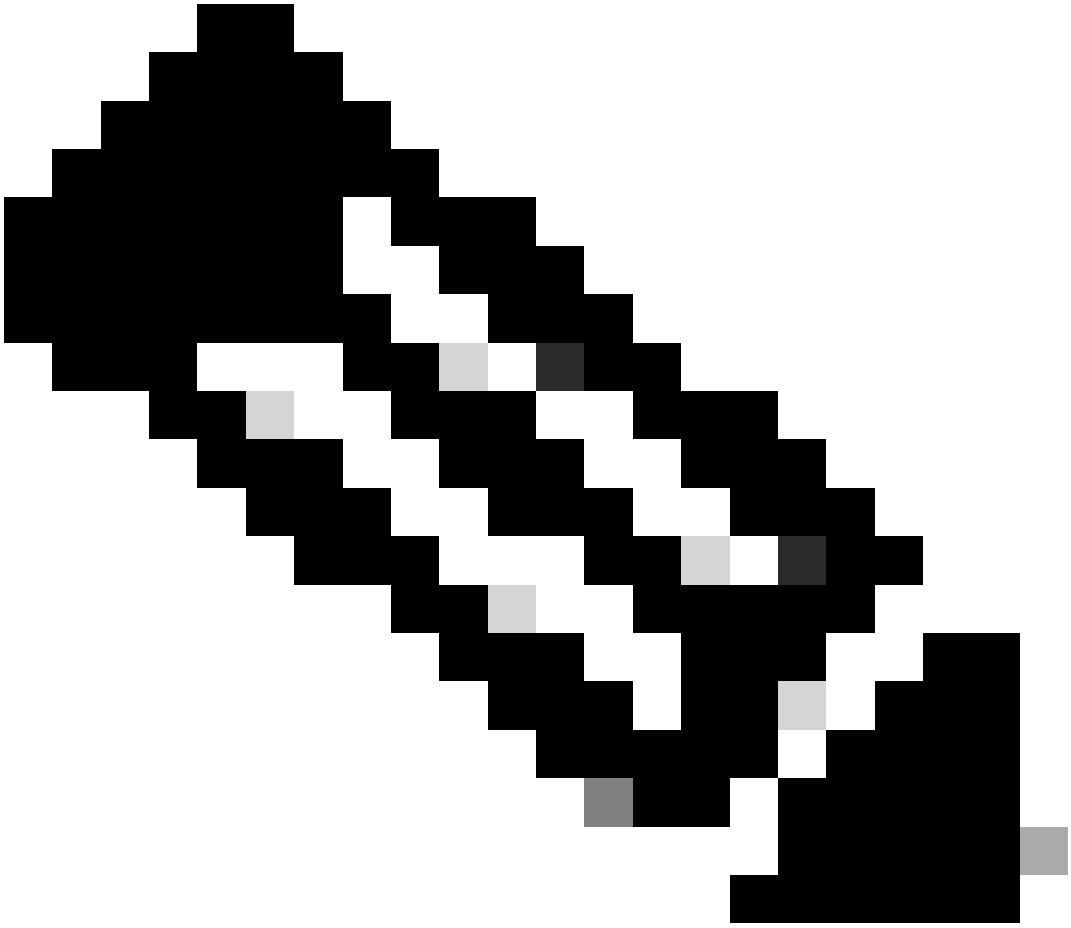
```
<#root>

(Cisco Controller) >

show auth-list

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

要將LAP增加到AP授權清單中，請使用config auth-list add mic <AP MAC Address> 命令。如需有關如何設定 LAP 授權的詳細資訊，請參閱思科整合無線網路組態範例中的 Lightweight Access Point (LAP) 授權。

問題4：AP上的證書或公鑰損壞

由於證書問題，LAP未加入控制器。

發出debug capwap errors enable和**debug pm pki enable** 命令。您會看到指示已損壞的證書或金鑰的消息。



注意：由於空間限制，部分輸出內容已移至第二行。

<#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
```

請使用以下兩個選項之一來解決問題：

- MIC AP -請求退貨授權(RMA)。
- LSC AP -重新設定LSC證書。

問題5：控制器在錯誤的VLAN上接收到AP發現消息（您會看到發現消息調試，但沒有響應）

您可以在debug capwap events enable命令輸出中看到此消息：

<#root>

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

此訊息表示控制器收到來自廣播IP位址（其來源IP位址不在控制器上任何已設定子網路中）的探索要求。這也表示控制器是捨棄封包的控制器。

問題在於AP不是向管理IP地址傳送發現請求的AP。控制器報告來自控制器上未配置的VLAN的廣播發現請求。當中繼允許VLAN且未將其限制為無線VLAN時，通常會發生這種情況。

要解決此問題，請完成以下步驟：

- 如果控制器在其他子網上，必須針對控制器的IP地址**預先準備** AP，否則，AP必須使用其中一個發現方法接收控制器IP地址。

- 交換器設定為允許某些VLAN不在控制器上。限制中繼上允許的VLAN。

問題6：AP無法加入WLC，防火牆阻塞了必要的埠

如果在企業網路中使用防火牆，請確定防火牆上已啟用這些連線埠，LAP才能加入並與控制器通訊。

您必須啟用以下連線埠：

- 為CAPWAP流量啟用以下UDP埠：
  - 資料- 5247
  - 控制- 5246
- 為移動流量啟用以下UDP埠：
  - 16666 - 16666
  - 16667 - 16667
- 為CAPWAP流量啟用UDP埠5246和5247。

- 用於SNMP的TCP 161和162（用於無線控制系統[WCS]）

這些埠是可選的（取決於您的要求）：

- 用於TFTP的UDP 69

- TCP 80和/或443用於HTTP或HTTPS用於GUI訪問

- TCP 23和/或22用於Telnet或SSH，用於CLI訪問

問題7：網路中的IP地址重複

這是AP嘗試加入WLC時出現的另一個常見問題。當AP嘗試加入控制器時，您可以看到此錯誤消息。

No more AP manager IP addresses remain

出現此錯誤消息的原因之一是，網路上有重複的IP地址與AP管理器IP地址匹配。在這種情況下，LAP會保持電源循環啟動且無法加入控制器。

調試顯示，WLC從AP接收LWAPP發現請求，並將LWAPP發現響應傳輸到AP。

但是，WLC不會從AP接收LWAPP加入請求。

要解決此問題，請從與AP管理器位於同一IP子網的有線主機ping AP管理器。然後，檢查ARP快取。如果找到重複的IP地址，請刪除具有重複IP地址的裝置，或者更改裝置上的IP地址，使其在網路中具有唯一的IP地址。

然後，AP可以加入WLC。

問題8：具有網狀映像的LAP無法加入WLC

Lightweight Access Point 未向 WLC 註冊。記錄顯示此錯誤訊息:

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

如果 Lightweight Access Point 配備網狀映像且處於橋接模式，就可能出現此情況。如果訂購的 LAP 具有網狀軟體，則必須將 LAP 新增至 AP 授權清單。選擇「安全性 > AP 原則」，然後將 AP 新增至「授權清單」。然後，AP必須加入，從控制器下載映像，然後在網橋模式下註冊到WLC。接著，您必須將 AP 變更為本機模式。LAP下載映像、重新啟動，並以本地模式註冊回控制器。

問題9：Microsoft DHCP地址錯誤

嘗試加入WLC時，存取點可以快速更新其IP地址，這可以導致Windows DHCP伺服器將這些IP標籤為BAD_ADDRESS，從而快速耗盡DHCP池。 有關詳細資訊，請參閱思科無線控制器配置指南8.2版中的客戶端漫遊一章。

相關資訊

- **思科技術支援與下載**
- **使用Catalyst 9800的AP加入過程**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。