排除轻型 AP 无法加入 WLC 的问题

目录

简介

本文档介绍AireOS无线局域网控制器(WLC)发现和加入过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 轻量接入点(LAP)和Cisco AireOS WLC配置的基础知识
- 轻量级无线接入点协议 (CAPWAP) 的基础知识

使用的组件

本文档重点介绍AireOS WLC，并不涵盖Catalyst 9800，尽管加入过程大体相似。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

WLC发现和加入过程概述

在 Cisco 统一无线网络中，LAP 必须首先发现并加入 WLC 才能用于无线客户端。

但是，这会带来一个问题：当控制器位于不同子网时，LAP如何查找控制器的管理IP地址？

如果未通过DHCP选项43、域名系统(DNS)解析Cisco-capwap-controller.local_domain告知LAP控制器的位置或对其进行静态配置，则**LAP不会知道在网络中的哪个位置查找控制器的管理接口。**

除这些方法之外，LAP 会自动在本地子网上查找使用 255.255.255.255 这一本地广播地址的控制器。此外，LAP会记住其控制器的管理IP地址，即使在重新启动后，控制器也会显示为移动对等体。但是，当AP加入另一个WLC时，它只记住该新WLC及其移动对等体的IP，而不记得之前的移动对等体。因此，如果您将LAP放在管理接口的本地子网上，它会查找控制器管理接口并记住该地址。这称为引爆。如果您在稍后替换 LAP，此过程不会帮助您找到控制器。因此，Cisco建议使用DHCP选项43或DNS方法。

LAP 始终会首先使用发现请求连接至控制器的管理接口地址。然后，控制器会向 LAP 告知第 3 层 AP 管理器接口（默认情况下也可以是管理接口）的 IP 地址，以便 LAP 随后可以将加入请求发送至 AP 管理器接口。

AP 在启动时会经历以下过程：

- **LAP 启动并使用 DHCP 协议获取一个 IP 地址（如果之前未分配静态 IP 地址）。**
- **LAP 通过各种发现算法向控制器发送发现请求，构建一个控制器列表。本质上，LAP 可以通过以下选项了解控制器列表的尽可能多的管理接口地址：**

a. **DHCP选项43（适用于办公室和控制器位于不同大陆的全球性公司）。**

cisco-capwap-controller

- **的DNS条目（对本地企业有好处-也可用于查找新AP加入的位置）如果使用CAPWAP，请确保有一个用于** cisco-capwap-controller的DNS条目。
- **LAP 之前记住的控制器的管理 IP 地址.**
- **子网上的第 3 层广播.**
- **静态配置的信息.**
-

控制器出现在 AP 最后加入的 WLC 的移动组中.

在此列表中，最简单的部署方法是将 LAP 放在与控制器管理接口相同的子网中，并允许 LAP 第 3 层广播查找控制器。此方法必须用于拥有小型网络且没有本地DNS服务器的公司。

第二简单的部署方法是将 DNS 条目与 DHCP 结合使用。可以为同一 DNS 名称建立多个条目。这样一来，LAP 就能发现多个控制器。此方法必须由所有控制器位于同一位置并拥有本地DNS服务器的公司使用。或者，拥有多个 DNS 后缀，各控制器由后缀分隔的公司。

大型公司使用DHCP选项43通过DHCP对信息进行本地化。此方法适用于拥有单个 DNS 后缀的大型企业。例如，Cisco 在欧洲、澳大利亚和美国拥有办公楼。为确保 LAP 仅在本地加入控制器，Cisco 不能使用 DNS 条目，必须使用 DHCP option 43 信息告诉 LAP 本地控制器的管理 IP 地址是什么。

最后，静态配置用于不含 DHCP 服务器的网络。您可以通过控制台端口和AP的CLI静态配置加入控制器所需的信息。有关如何使用AP CLI静态配置控制器信息的信息，请使用以下命令：

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

有关如何在DHCP服务器上配置DHCP option 43的信息，请参阅DHCP option 43配置示例

- 向列表上的每个控制器发送发现请求，并等待控制器发现应答，该应答中包含系统名称、AP管理器IP地址、已连接到每个AP管理器接口的AP数量以及控制器的整体过剩容量。
- 查看控制器列表并按以下顺序向控制器发送加入请求（仅在 AP 收到控制器的发现回应后进行）：

a. 主控制器系统名称（以前在LAP上配置）。

b. 辅助控制器系统名称（先前在LAP上配置）。

c. 第三控制器系统名称（先前在LAP上配置）。

d. 主控制器(如果LAP先前未配置任何主、辅助或第三控制器名称。用于始终知道哪个控制器是全新的LAP加入)。

e. 如果未看到任何上述情况，请使用发现响应中的超额容量值在控制器之间实现负载均衡。

如果两个控制器的过剩能力相同，则向通过发现响应响应发现请求的第一个控制器发送加入请求。如果单个控制器在多个接口上有多个 AP-manager，请选择包含 AP 数量最少的 AP-manager 接口。

控制器响应所有发现请求，而不使用证书检查或AP凭证。但是，加入请求必须具有有效证书才能从控制器获得加入响应。如果LAP没有收到来自其选择的加入响应，则LAP会尝试列表中的下一个控制器，除非控制器是已配置的控制器（主/辅助/第三）。

- 如果收到加入回应，AP 将进行检查以确保它与控制器具有相同的映像。否则，AP 将从控制器下载映像并重新启动以加载此新映像，然后从步骤 1 开始重新执行该过程。
- 如果它有同一个软件映像，将向控制器请求配置并在控制器上转入已注册状态。

下载配置后，AP可再次重新加载以应用新配置。因此，可能会发生额外的重新加载，这是正常行为。

从控制器进行调试

可以使用控制器上的一些**debug** 命令在CLI上查看此完整过程：

- **debug capwap events enable**:显示发现数据包和加入数据包。
- **debug capwap packet enable**:显示发现和加入数据包的数据包级别信息。
- **debug pm pki enable**:显示证书验证过程。
- **debug disable-all**:关闭调试。

使用可将输出捕获到日志文件的终端应用，在控制台中或通过安全外壳 (SSH)/Telnet 连接至控制器，并输入以下命令：

<#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

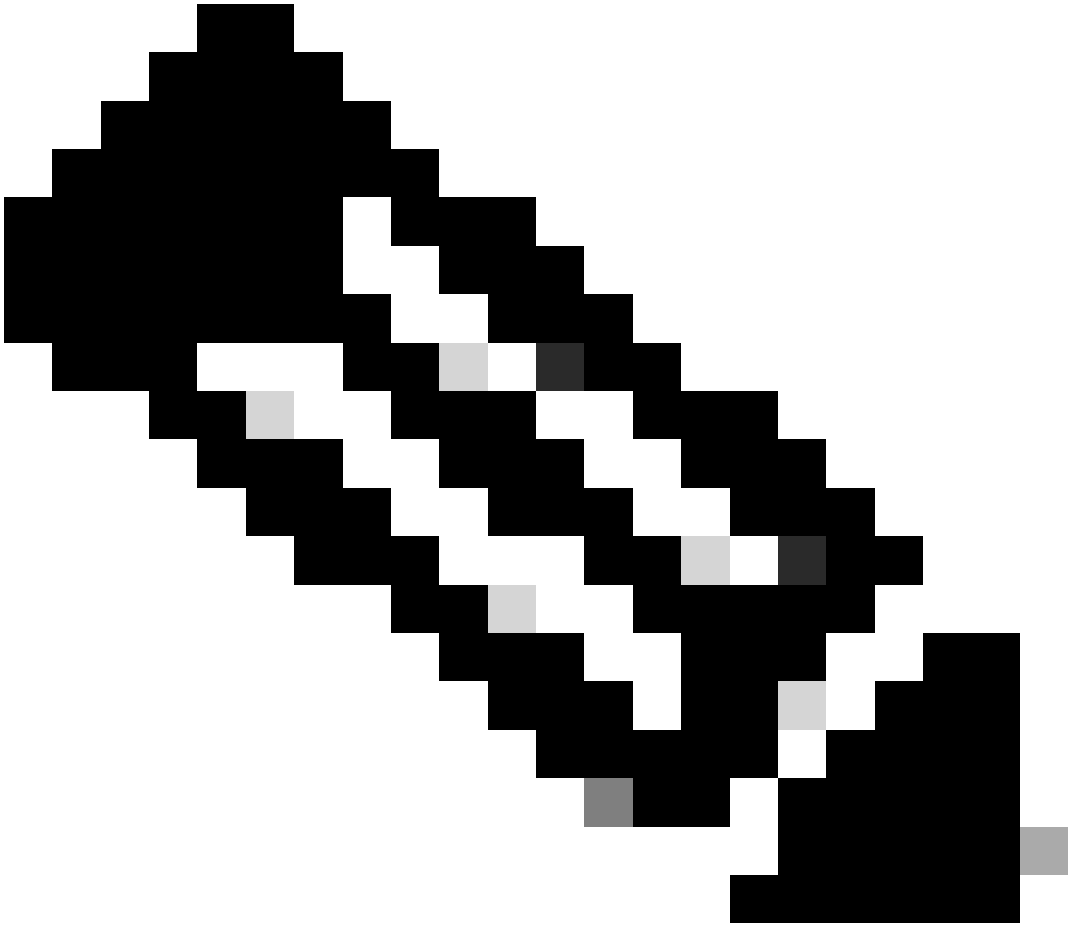
在捕获到这些debug命令后，可以使用debug disable-all命令禁用所有调试。

接下来的部分显示了LAP向控制器进行注册时，这些**debug** 命令的输出。

debug capwap events enable

此命令提供有关CAPWAP发现和加入过程中发生的CAPWAP事件和错误的信息。

以下是针对与WLC具有相同映像的LAP的**debug capwap events enable** 命令的输出：



注意：由于空间限制，输出中的某些行已移至第二行。

<#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.

如之前部分中所述，一旦 LAP 向 WLC 进行注册，它将会检查以确定自己是否与控制器具有相同的映像。如果 LAP 上的映像与 WLC 上的映像不同，那么 LAP 将首先从 WLC 中下载新映像。如果 LAP 与 WLC 具有相同的映像，它将继续从 WLC 中下载配置和其他参数。

如果LAP在注册过程中从控制器中下载映像，您将在**debug capwap events enable** 的命令输出中看到以下消息：

```
*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
```

映像下载完成后，LAP将重新启动并再次运行发现并加入算法。

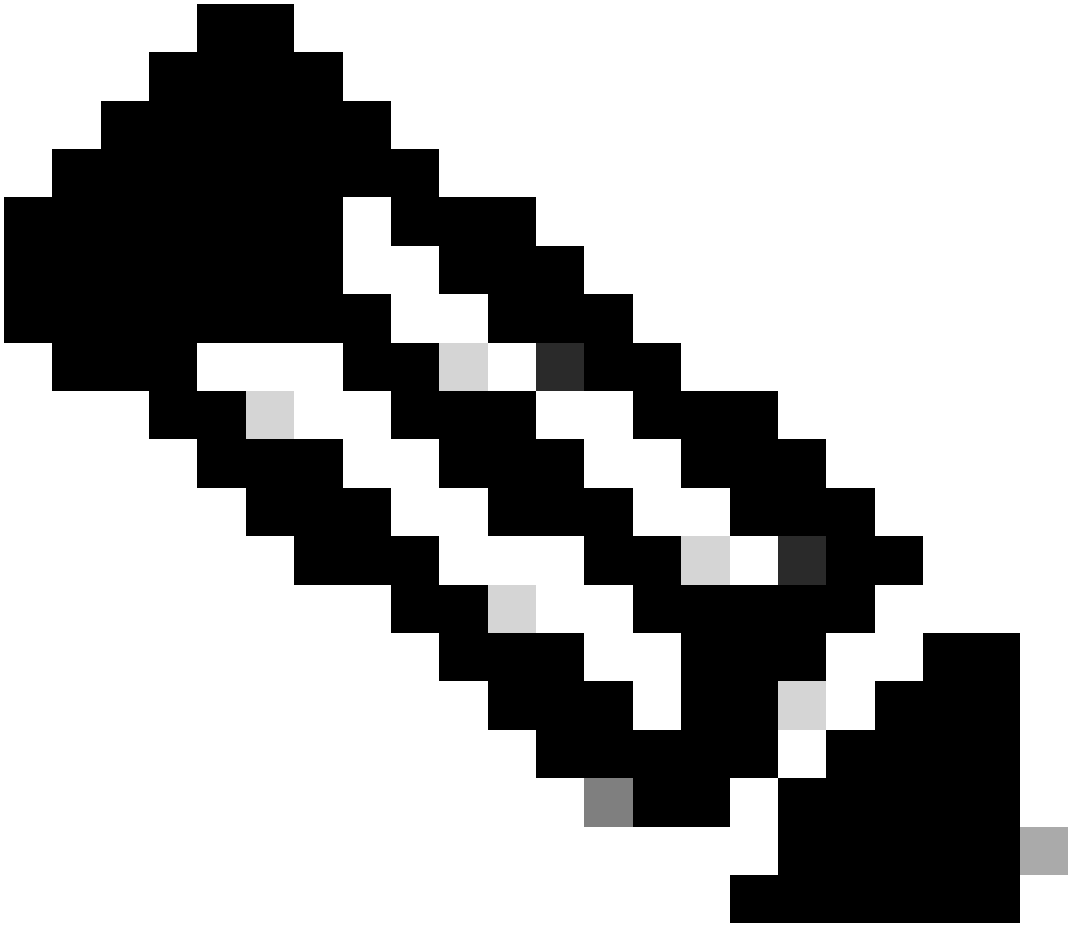
debug pm pki enable

作为加入过程的一部分，WLC通过确认每个LAP的证书有效对其进行身份验证。

当向 WLC 发送 CAPWAP 加入请求时，AP 会将其 X.509 证书嵌入到 CAPWAP 消息中。AP 还会生成一个随机会话 ID，该会话 ID 也包含在 CAPWAP 加入请求中。当WLC收到CAPWAP加入请求时，它将使用AP公钥验证X.509证书的签名，并检查证书是否由受信任的证书颁发机构颁发。

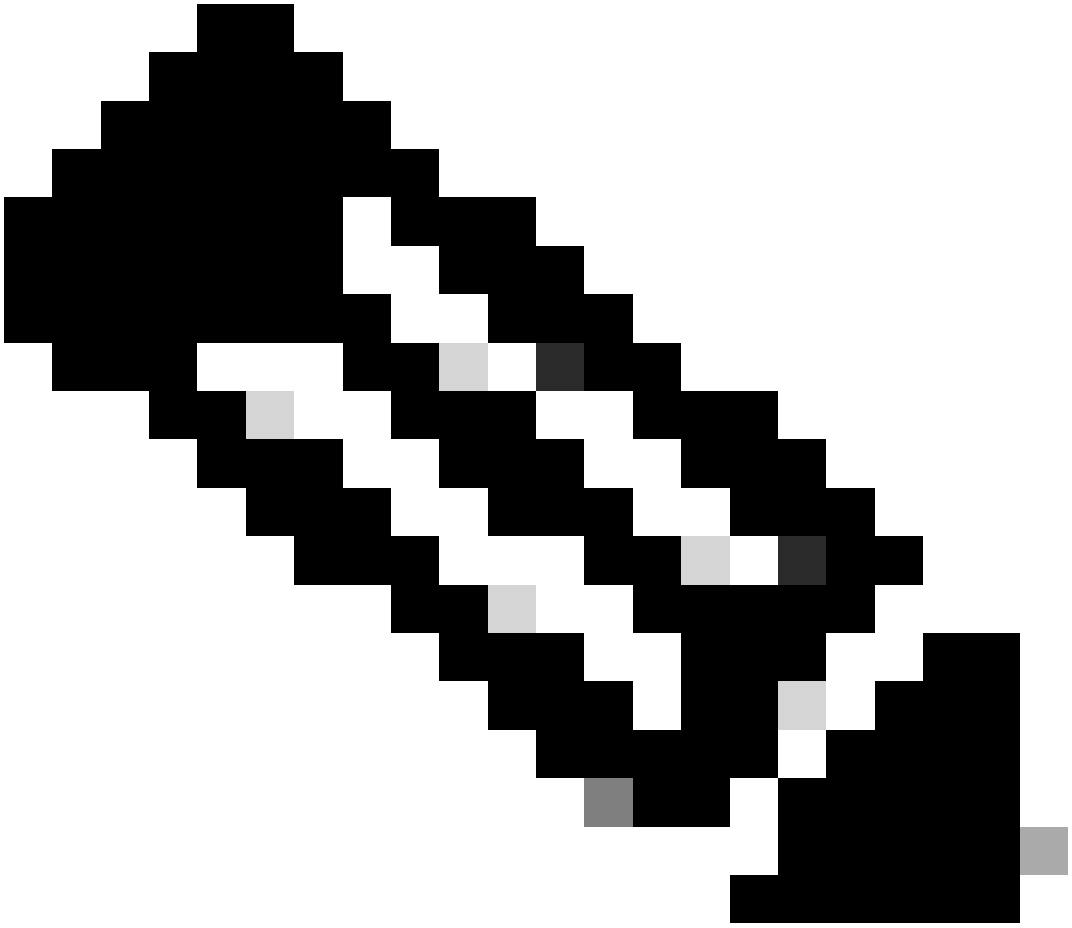
它还查看AP证书有效间隔的开始日期和时间，并将该日期和时间与其自己的日期和时间进行比较（因此，控制器时钟需要设置为接近当前日期和时间）。如果 X.509 证书通过验证，WLC 将生成一个随机的 AES 加密密钥。WLC将AES密钥插入其加密引擎，以便可以加密和解密将来与AP交换的CAPWAP控制消息。请注意，数据包在 LAP 与控制器之间的 CAPWAP 隧道中以明文形式发送。

debug pm pki enable 命令显示在控制器的加入阶段发生的认证验证过程。如果AP有LWAPP转换程序创建的自签名证书(SSC)，**debug pm pki enable** 命令还会在加入进程中显示AP哈希键。如果AP具有已制造安装证书(MIC)，则您看不到哈希密钥。



注意：2006年6月以后生产的所有接入点都有一个MIC。

以下是带有MIC的LAP加入控制器时**debug pm pki enable** 命令的输出：



注意：由于空间限制，输出中的某些行已移至第二行。

<#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

从 AP 进行调试

如果控制器调试未指示加入请求，则在AP具有控制台端口时可以从AP调试进程。您可以使用这些命令查看AP启动过程，但必须首先进入启用模式（默认口令为Cisco）。

- **debug dhcp detail** :显示 DHCP 选项 43 信息。
- **debug ip udp**：显示AP接收和传输的所有UDP数据包。
- debug capwap client event :显示 AP 的 capwap 事件。
- **debug capwap client error**:显示 AP 的 capwap 错误。
- **debug dtls client event**:显示 AP 的 DTLS 事件。

- **debug dtls error enable**:显示 AP 的 DTLS 错误。
- **undebug all**:在 AP 上禁用调试。

下面是debug capwap命令的输出示例。此部分输出提供AP在引导过程中发送的数据包的信息，以发现和加入控制器。

```
<#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 未加入控制器的原因是什么？

先从基本原因查起

- AP 能否与 WLC 通信？
- 确保AP从DHCP获取地址（检查DHCP服务器租用AP的MAC地址）。
- 从控制器对AP执行ping操作。
- 检查交换机上的STP配置是否正确，这样不会阻止发送到VLAN的数据包。
- 如果 ping 成功，确保 AP 至少可以通过一种方法发现至少一个可进入控制器的单个 WLC 控制台或 telnet/ssh 以运行调试。
- 每次重新启动时，AP 都会启动 WLC 发现序列并尝试定位 AP。重新启动 AP 并检查其是否加入 WLC。

下面列出了 LAP 未加入 WLC 的一些常见原因。

现场通知：证书过期- FN63942

硬件中嵌入的证书的有效期为自制造之日起 10 年。如果您的AP或WLC的期限超过10年，过期的证书可能会导致AP加入问题。有关此问题的详细信息，请查看field notice：Field Notice： FN63942。

要查找的潜在问题：示例

问题1：控制器时间超出了证书有效间隔

要对此问题进行故障排除，请完成以下步骤：

- 在AP上发出debug dtls client error + debug dtls client event命令：

<#root>

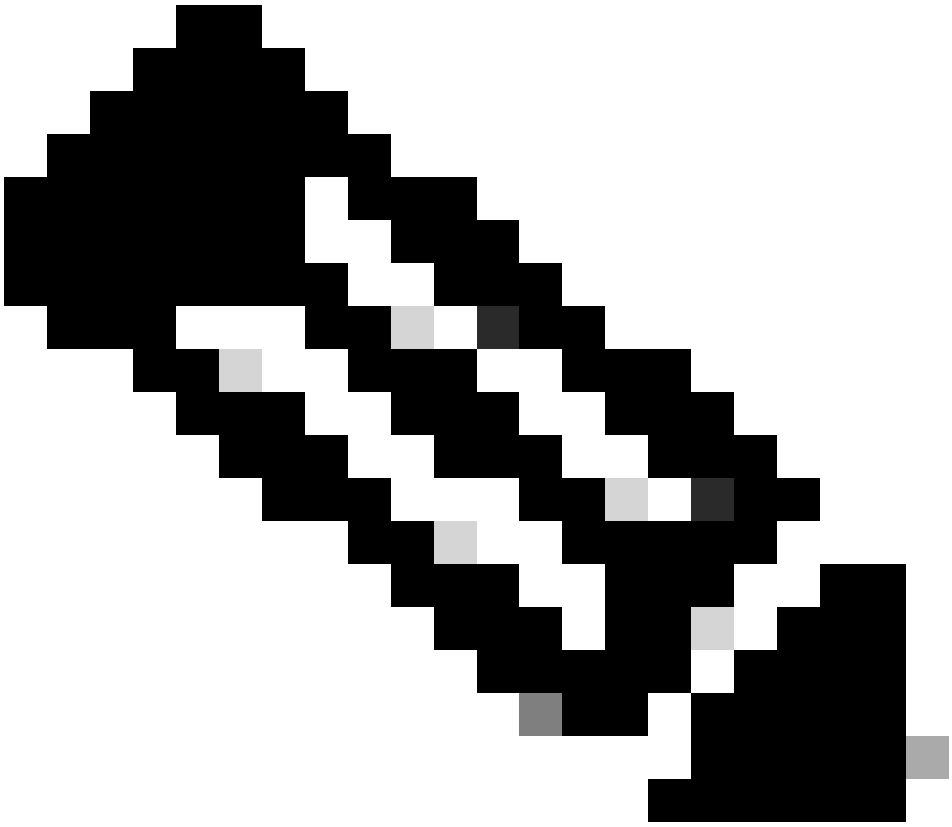
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

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
```

此信息清楚地显示控制器时间不在AP的证书有效间隔内。因此，AP 无法注册到控制器。AP 上安装的证书具有预定义的有效间隔。必须设置控制器时间，使其在AP证书的证书有效间隔内。

- 从控制器的CLI发出 **show time** 命令，以便验证控制器上的日期和时间设置是否在此有效间隔内。如果控制器时间不在此有效间隔内，则请更改控制器时间使其处在有效间隔内。



注意：如果控制器上的时间设置不正确，请在控制器的GUI模式下选择Commands > Set Time，或在控制器的CLI中发出config time命令来设置控制器时间。

- 在可以访问CLI的AP上，请从AP的CLI中使用**show crypto ca certificates** 命令对证书进行验证。

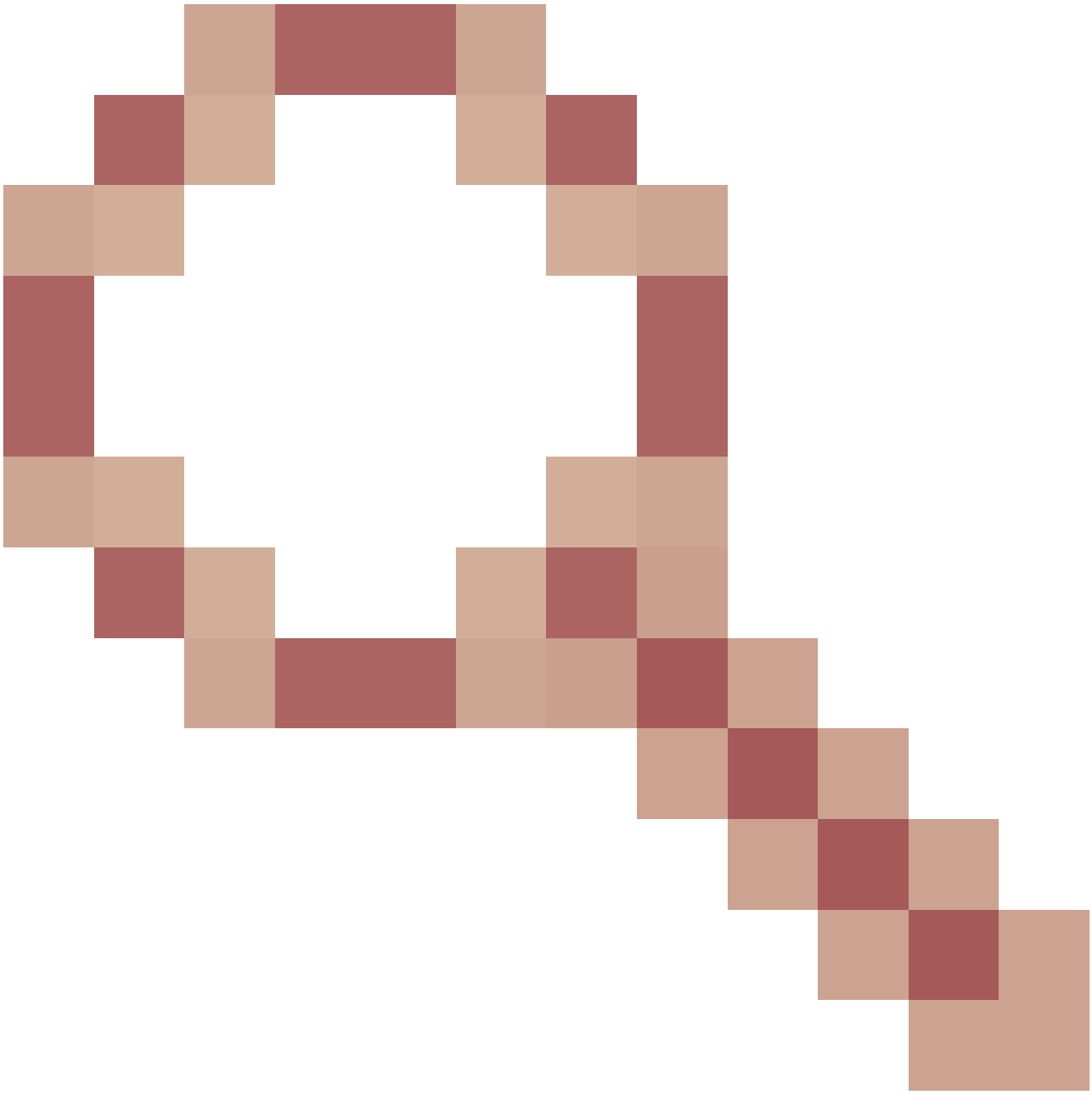
通过此命令，您可以确认 AP 上的证书有效间隔设置。示例如下：

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

未列出整个输出，因为可能存在许多与此命令输出关联的有效间隔。仅考虑关联信任点指定的有效间隔：Cisco_IOS_MIC_cert和名称字段中的相关AP名称。在此示例输出中，对应代码为Name： C1200-001563e50c7e。这是要考虑的实际证书有效间隔。

- 请参阅思科漏洞ID CSCuq19142



LAP/WLC MIC或SSC有效期到期导致DTLS故障：思科漏洞ID CSCuq19142。

问题2：管制范围不匹配

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

<#root>

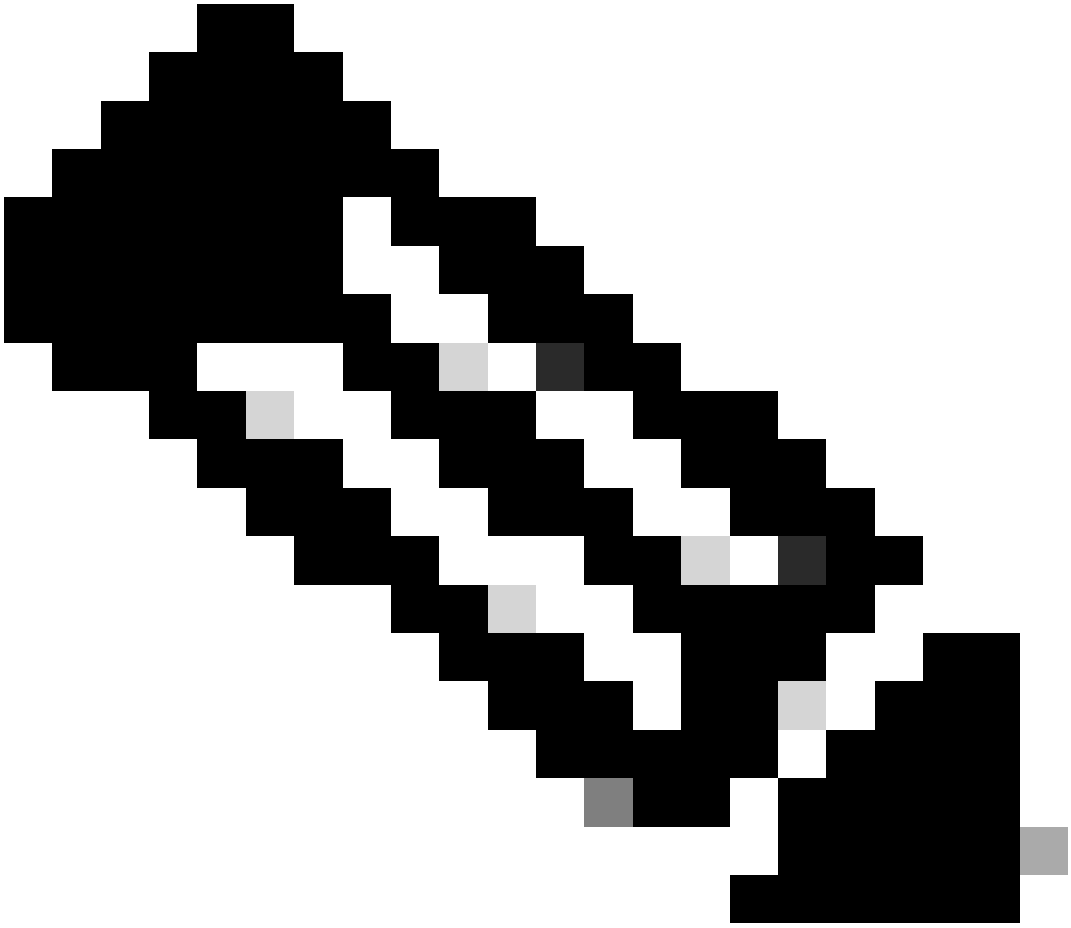
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***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的管制域不匹配。WLC支持多个管制域，但必须先选择每个管制域，AP才能从该域加入。例如，使用管理域 A 的 WLC 只能与使用管理域 A 的 AP 结合使用（以此类推）。当您购买AP时，请确保它们共享相同的管制范围。只有这样 AP 才能登记到 WLC。



注意：对于单个AP，802.1b/g和802.11a无线电必须在同一管制域中。

问题3：WLC上启用了AP授权列表；LAP不在授权列表中

在此类情况下，您将在控制器上debug capwap events enable命令的输出中看到此消息：

<#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

如果使用带有控制台端口的LAP，在您发出debug capwap client error命令时将会看到此消息：

```
<#root>

APO01d.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.

这再次明确表明LAP不属于控制器上的AP授权列表。

您可以使用以下命令查看AP授权列表的状态：

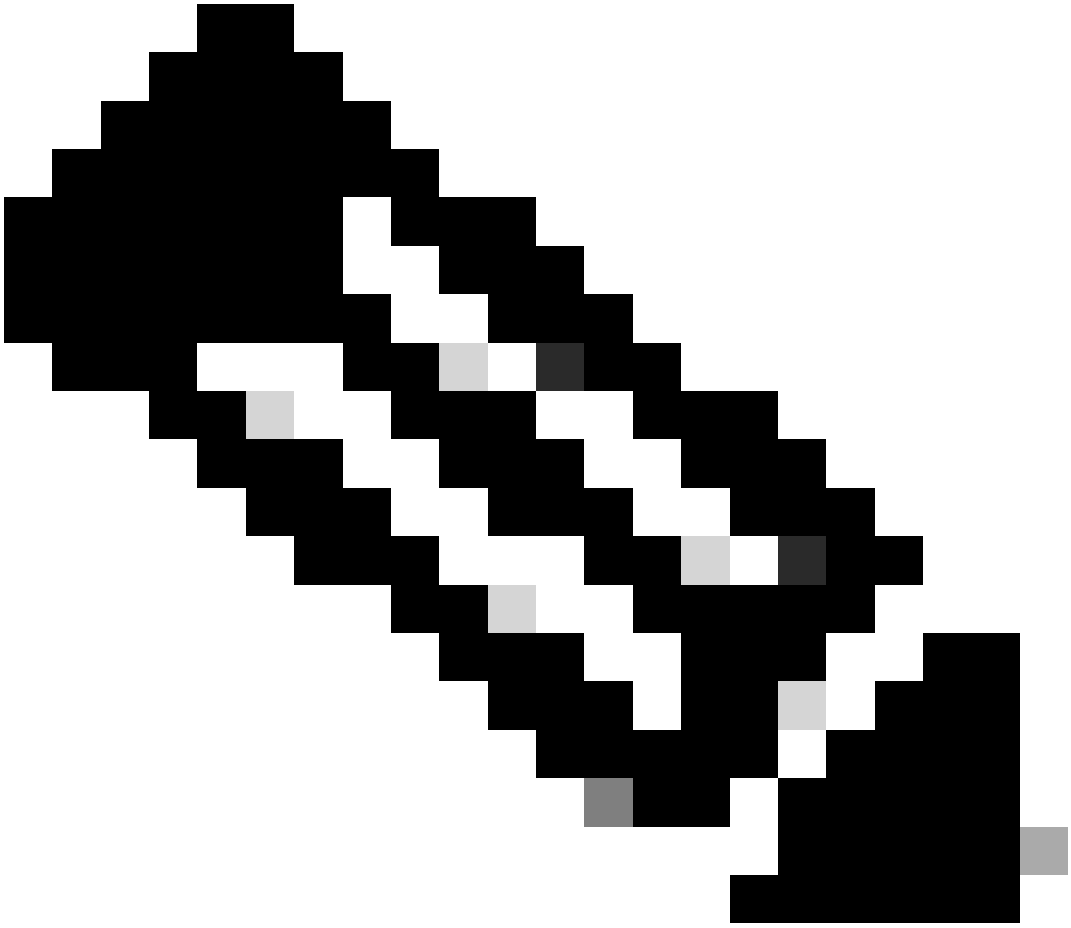
```
<#root>

(Cisco Controller) >

show auth-list

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

要将LAP添加到AP授权列表中，请使用config auth-list add mic <AP MAC Address> 命令。有关如何配置 LAP 授权的更多信息，请参阅思科统一无线网络配置示例中的轻量级无线接入点 (LAP) 授权。

问题4：AP上的证书或公钥损坏

由于证书存在问题，LAP 不会加入控制器。

发出debug capwap errors enable和**debug pm pki enable** 命令。您将看到指出证书或密钥损坏的消息。



注意：由于空间限制，输出的部分内容已移至第二行。

<#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
```

使用以下两个选项之一来解决此问题：

- MIC AP -请求退货授权(RMA)。
- LSC AP - 重新调配 LSC 证书.

问题5：控制器接收错误VLAN上的AP发现消息（您会看到发现消息debug，但不会看到响应）

您可以在debug capwap events enable命令输出中看到此消息：

<#root>

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

此消息表示控制器收到广播IP地址的发现请求，该广播IP地址的源IP地址不在控制器上任何已配置的子网中。这也意味着丢弃数据包的是控制器。

问题在于AP不是向管理IP地址发送发现请求的设备。控制器报告来自控制器上未配置的VLAN的广播发现请求。当TRUNK允许VLAN且未将其限制为无线VLAN时，通常会发生这种情况。

要解决此问题，请完成以下步骤：

- 如果控制器在其他子网上，必须针对控制器的IP地址预先准备 AP，否则，AP必须使用发现方法之一接收控制器IP地址。
- 交换机配置为允许一些VLAN不在控制器上。在 trunk 上限制允许的 VLAN。

问题6：AP无法加入WLC，防火墙阻塞必要的端口

如果企业网络中使用了防火墙，请确保在防火墙上启用这些端口，LAP才能加入控制器并与控制器通信。

您必须启用以下端口：

- 为 CAPWAP 流量启用以下 UDP 端口：
  - 数据 - 5247
  - 控制 - 5246
- 为移动性流量启用如下 UDP 端口：
  - 16666 - 16666
  - 16667 - 16667
- 为 CAPWAP 流量启用 UDP 端口 5246 和 5247。

- 用于 SNMP 的 TCP 161 和 162（适用于 Wireless Control System [WCS]）

这些端口是可选的（取决于您的要求）：

- UDP 69，用于 TFTP
- TCP 80 和/或 443，用于通过 HTTP 或 HTTPS 的 GUI 访问
- TCP 23 和/或 22，用于通过 Telnet 或 SSH 的 CLI 访问

问题7：网络中的IP地址重复

这是当AP尝试加入WLC时看到的另一个常见问题。当AP尝试加入控制器时，您可以看到此错误消息。

<#root>

No more AP manager IP addresses remain

导致出现此错误消息的一个原因是，网络中存在与 AP manager IP 地址完全一致的重复的 IP 地址。在这种情况下，LAP将保持重新通电启动状态，无法加入控制器。

调试显示WLC从AP接收LWAPP发现请求，并将LWAPP发现响应传输到AP。

不过，WLC 不会接收 AP 发出的 LWAPP 加入请求。

为了对此问题进行故障排除，请从 AP manager 所在 IP 子网上的一台有线主机对 AP manager 执行 ping 操作。然后，请检查 ARP 缓存。如果找到重复的IP地址，请删除具有重复IP地址的设备，或更改设备的IP地址，使其在网络中具有唯一的IP地址。

然后，AP 就可以加入 WLC 了。

问题8：具有网状映像的LAP无法加入WLC

轻量级无线接入点不会向 WLC 注册。日志显示此错误消息:

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

如果轻量级无线接入点随附网状网映像并处于桥接模式，则可能会发生此问题。如果 LAP 与网状网软件一同订购，则需要将 LAP 添加到 AP 授权列表中。依次选择安全性 > AP 策略，并将 AP 添加到授权列表中。然后，AP必须加入，从控制器下载映像，然后在桥接模式下注册到WLC。然后，您需要将 AP 更改为本地模式。LAP下载映像、重新启动，并以本地模式注册回控制器。

问题9：Microsoft DHCP地址错误

当尝试加入WLC时，接入点可以快速更新其IP地址，这会导致Windows DHCP服务器将这些IP标记为BAD_ADDRESS，从而快速耗尽DHCP池。 有关详细信息，请参阅Cisco无线控制器配置指南8.2版的客户端漫游一章。

相关信息

- **思科技术支持和下载**
- **AP与Catalyst 9800的连接过程**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。