排除轻量接入点无法加入无线 LAN 控制器的故障

目录

简介

本文给予无线局域网控制器(WLC)发现号的概述和加入进程。本文在某些也提供信息问题一轻量级

接入点(LAP)为什么不能加入WLC和如何排除故障问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 有关 LAP 和 Cisco WLC 配置的基本知识
- 有关轻量接入点协议 (LWAPP) 的基本知识

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

无线局域网控制器(WLC)发现号的概述和加入进程

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。

最初，控制器仅在第 2 层模式下运行。在第 2 层模式下，LAP 应与管理接口在同一子网上，控制器上不存在第 3 层模式 AP-manager 接口。拉普与使用仅第2层封装的控制器联络(以太网封装)并且不动态主机配置协议(DHCP) IP地址。

在开发控制器的第 3 层模式时，引入了一个新的名为 AP-manager 的第 3 层接口。在第 3 层模式下，LAP 首先会使用 DHCP 协议获取一个 IP 地址，然后使用 IP 地址将它们的发现请求发送到管理接口（第 3 层）。这样一来，LAP 将可以与控制器的管理接口在不同的子网上。第 3 层模式是当前的主导模式。一些控制器和 LAP 只能执行第 3 层模式。

然而，这也带来了一个新问题：当控制器与 LAP 在不同的子网上时，LAP 是如何找到控制器的管理 IP 地址的？

在第 2 层模式下，上述两者需要在同一子网中。在第 3 层模式下，从本质上看，控制器和 LAP 在网络中就是藏与找的关系。如果您不通过 DHCP option 43、“Cisco-lwapp-controller@local_domain”的 DNS 解析或静态配置 LAP 告诉 LAP 控制器的位置，LAP 将不会知道该到网络中的哪一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 会记住其在重新启动过程中加入的所有控制器的管理 IP 地址。因此，如果您首次将 LAP 放到管理接口的本地子网上，它将查找控制器的管理接口并记住此地址。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 推荐使用 DHCP option 43 或 DNS 方法。

当 LAP 发现控制器时，它们不知道控制器是在第 2 层模式下还是在第 3 层模式下。因此，LAP 总是连接到首先响应发现请求的控制器的管理接口地址。然后控制器会在发现回应中告诉 LAP 它处于哪种模式下。如果控制器在第 3 层模式下，发现回应将包含第 3 层 AP-manager IP 地址，以便 LAP 可以在接下来向 AP-manager 接口发送加入请求。

注意： 默认情况下，管理接口和 AP-manager 接口在配置期间在其 VLAN 上处于未标记状态。如果这些接口处于已标记状态，请确保在同一 VLAN 上对这些接口进行了标记，以便能够正确接收发现和加入 WLC 的响应。

LWAPP AP 在启动第 3 层模式时执行此过程：

1. 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）。
2. 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：DHCP option 43（特别适合于办公室和控制器分布于不同的大陆的跨国公司）Cisco-capwap 控制器的 DNS 条目（特别适合于本地企业 - 也可用于查找全新 AP 的加入位置）**注意：** 如果您使用 CAPWAP，请确保有一个与 Cisco-capwap 控制器对应的 DNS 条目。LAP 之前记住的控制器的管理 IP 地址子网上的第 3 层广播空中配置静态配置的信息从此列表，使用的最容易的方法部署将有相同子网的拉普作为控制器的管理接口和允许LAPâ s第3层广播查找控制器。应将此方法用于拥有小型网络但没有本地 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。此方法适用于所有控制器均在单个位置且拥有本地 DNS 服务器的公司。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 option 43 来通过 DHCP 本地化信息。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。您能静态配置必要的信息通过控制台端口和APâ s CLI加入控制器。有关使用 AP CLI 静态配置控制器信息的信息，请参阅使用接入点 CLI 手动配置控制器信息。有关 LAP 用于查找控制器的不同发现算法的详细说明，请参阅向 WLC 注册 LAP。有关在 DHCP 服务器上配置 DHCP option 43 的信息，请参阅用于轻量 Cisco Aironet 接入点配置的 DHCP OPTION 43 示例。
3. 向列表中列出的每个控制器发送发现请求，然后等待控制器的发现回应，其中包含系统名称、AP-manager IP 地址、已连接到各 AP-manager 接口的 AP 数量以及控制器的总体过剩能力。
4. 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）：主控制器系统名称（之前在 LAP 上配置的）辅助控制器系统名称（之前在 LAP 上配置的）第三控制器系统名称（之前在 LAP 上配置的）主控制器（如果之前未使用任何主，辅助或第三控制器名称对 LAP 进行配置。用于时时掌握哪一控制器带来全新的 LAP 加入）如果您看不到上述任何信息，请在发现响应中使用过剩能力跨控制器配置负载均衡。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。控制器将响应所有发现请求，而不检查证书或 AP 证书。不过，加入请求必须具有有效的证书才能获得控制器的加入响应。如果 LAP 未从其选择的控制器接收到加入响应，它将尝试从列表中的下一个控制器获取，除非控制器是一个已配置控制器（主/辅助或第三控制器）。
5. 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。
6. 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。在您下载配置后，AP 可能会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

为使您能在 CLI 上看到这一完整的过程，可以使用控制器上的一些 **debug** 命令。

- **调试lwapp事件enableâ** 显示发现信息包和加入数据包。
- **调试lwapp数据包enableâ** 显示数据包发现和加入数据包的级别信息。
- **调试下午pki enableâ** 显示证书确认进程。
- **调试禁用allâ** 关闭调试。

使用能获取输出到日志文件、控制台或安全壳SSH /Telnet到您的控制器的一终端的应用程序，和请

输入这些命令：

config session timeout 120 config serial timeout 120 show run-config (and spacebar thru to collect all) **debug mac addr** <*ap-mac-address*> (in xx:xx:xx:xx:xx format) **debug client** <*ap-mac-address*> **debug lwapp events enable debug lwapp errors enable debug pm pki enable**

在捕获到这些 debug 命令后，可以使用 **debug disable-all** 命令关闭所有调试。

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 lwapp events enable

此命令提供有关 LWAPP 发现和加入过程中发生的 LWAPP 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 lwapp events enable** 命令的输出：

注意： 由于空间有限，此输出的一些行被拆分为两行显示。

debug lwapp events enable Wed Oct 24 16:59:35 2007: 00:0b:85:5b: fb:d0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:5b: fb:d0 to 00:0b:85:33:52:80 on port '2' *!--- LWAPP discovery request sent to the WLC by the LAP.* Wed Oct 24 16:59:35 2007: 00:0b:85:5b:fb:d0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2 *!--- WLC responds to the discovery request from the LAP.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2' *!--- LAP sends a join request to the WLC.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 AP ap:5b:fb:d0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:5B:FB:D0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 LWAPP Join-Request MTU path from AP 00:0b:85:5b:fb:d0 is 1500, remote debug mode is 0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully added NPU Entry for AP 00:0b:85:5b:fb:d0 (index 55) Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0 AP IP: 10.77.244.219, AP Port: 49085, next hop MAC: 00:0b:85:5b:fb:d0 Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:5b:fb:d0 *!--- WLC responds with a join reply to the LAP.* Wed Oct 24 16:59:46 2007: 00:0b:85:5b:fb:d0 Register LWAPP event for AP 00:0b:85:5b:fb:d0 slot 0 -- LAP registers with the WLC Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 *!--- LAP requests for the configuration information from the WLC.* Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Updating IP info for AP 00:0b:85:5b:fb:d0 -- static 1, 10.77.244.219/255.255.255.224, gtw 10.77.244.220 Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -AB Wed Oct 24 16:59:48 2007: Send AP Timesync of 1193245188 source MANUAL Wed Oct 24 16:59:48 2007: spamEncodeDomainSecretPayload:Send domain secret TSWEBRET<0d,59,aa,b3,7a,fb,dd,b4,e2,bd,b5,e7,d0,b2,52,4d,ad,21,1a,12> to AP 00:0b:85:5b:fb:d0 Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Config-Message to AP 00:0b:85:5b:fb:d0 *!--- WLC responds by providing all the necessary configuration information to the LAP.* Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'eap fast' Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'webauth' Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'eap fast' Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'WPA' Wed Oct 24 16:59:48 2007: Running spamEncodeCreateVapPayload for SSID 'webauth' . . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:5b:fb:d0 . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP Up event for AP 00:0b:85:5b:fb:d0 slot 0! *!--- LAP is up and ready to service wireless clients.* Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5b:fb:d0 . . . Wed Oct 24 16:59:48 2007: 00:0b:85:5b:fb:d0 Received LWAPP RRM_CONTROL_RES from AP 00:0b:85:5b:fb:d0 *!--- 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 lwapp events enable** 的命令输出中看到以下消息：

```
Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from AP
00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES from
AP 00:0b:85:5b:fb:d0 Wed Oct 24 17:49:40 2007: 00:0b:85:5b:fb:d0 Received LWAPP IMAGE_DATA_RES
from AP 00:0b:85:5b:fb:d0
```

在映像下载完成后，LAP 将重新启动并将再次运行发现和加入算法。

debug pm pki enable

作为加入过程的一部分，WLC 会验证每个 LAP 的证书是否有效。

当 AP 向 WLC 发送 LWAPP 加入请求时，它会将其 X.509 证书嵌入到 LWAPP 消息中。AP 还会生成一个随机会话 ID，同样包含在 LWAPP 加入请求中。当 WLC 收到 LWAPP 加入请求时，它会使用 AP 的公钥对 X.509 证书的签名进行验证并检查证书是否由受信任的证书颁发机构颁发。

它也查看开始的日期和时间为AP证书有效性间隔并且与其自己的日期和时间(因此controllerâ s时钟比较日期和时间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 可以为其加密引擎查明 AES 密钥，以便可能加密和解密将来与 AP 交换的 LWAPP 控制消息。注意，数据包在 LWAPP 与控制器之间的隧道空闲时在两者之间进行发送。

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。**enable命令调试下午的pki**在加入进程中也将显示AP哈希密钥，如果AP有LWAPP转换程序(SSC)创建的一自签名证书。如果AP有一制作的预装证书(MIC)，您将看不到哈希密钥。

注意： 2006 年 6 月之后制造的所有 AP 都有 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： 由于空间有限，此输出的一些行被拆分为两行显示。

```
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: locking ca cert table
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b8591c3c0, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: <issuer>  C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca, MAILTO=support@airespace.com
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:91:c3:c0
Thu Oct 25 13:52:59 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 2d812f0c
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
```

Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: called to get cert for CID 20f00bf3
Thu Oct 25 13:52:59 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: calling x509_decode()
Thu Oct 25 13:52:59 2007: ssphmUserCertVerify: **user cert verfied using >bsnOldDefaultCaCert<** Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: **ValidityString (current): 2007/10/25/13:52:59** Thu
Oct 25 13:52:59 2007: sshpmGetIssuerHandles: **AP version is 0x400d900, sending Cisco ID cert...**
Thu Oct 25 13:52:59 2007: sshpmGetCID: called to evaluate <cscoDefaultIdCert> Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25
13:52:59 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59
2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 2, ID cert >bsnSslWebadminCert< Thu Oct 25 13:52:59 2007:
sshpmGetCID: comparing to row 3, ID cert >bsnSslWebauthCert< Thu Oct 25 13:52:59 2007:
sshpmGetIssuerHandles: **Airespace ID cert ok; sending it...** Thu Oct 25 13:52:59 2007:
sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 0, CA cert >bsnOldDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 1, CA cert >bsnDefaultRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID:
comparing to row 2, CA cert >bsnDefaultCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing
to row 3, CA cert >bsnDefaultBuildCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row
4, CA cert >cscoDefaultNewRootCaCert< Thu Oct 25 13:52:59 2007: sshpmGetCID: comparing to row 5,
CA cert >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCID: comparing to row 0, ID
cert >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromHandle: calling
sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: called
to get cert for CID 156af135 Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 0,
certname >bsnOldDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
1, certname >bsnDefaultRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 2, certname >bsnDefaultCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to
row 3, certname >bsnDefaultBuildCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing
to row 4, certname >cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID:
comparing to row 5, certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007:
sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03
2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID() with CID 0x156af135 Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: called to get cert for CID 156af135 Thu Oct 25 13:53:03
2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Thu Oct 25
13:53:03 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Thu Oct
25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 3, certname >bsnDefaultBuildCert< Thu
Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 4, certname
>cscoDefaultNewRootCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row 5,
certname >cscoDefaultMfgCaCert< Thu Oct 25 13:53:03 2007: sshpmGetCertFromCID: comparing to row
0, certname >bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: called to
encrypt 16 bytes Thu Oct 25 13:53:03 2007: ssphmPublicKeyEncrypt: successfully encrypted, out is
192 bytes Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for CID 156af135 Thu Oct
25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert< Thu Oct 25 13:53:03 2007: sshpmGetOpensslPrivateKeyFromCID: match in row 0
Thu Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 172 bytes Thu
Oct 25 13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 24 bytes Thu Oct 25
13:53:03 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 192 Thu Oct 25 13:53:03
2007: sshpmPrivateKeyEncrypt: encrypted bytes: 384 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: called with 0xae0c358 Thu Oct 25 13:53:03 2007:
sshpmFreePublicKeyHandle: **freeing public key**

对于带有 SSC 的 LAP，**debug pm pki enable** 的命令输出将如下所示。注意，在此输出中也可以看到 SSC 哈希。

注意： 由于空间有限，此输出的一些行被拆分为两行显示。

```
(Cisco Controller) > debug pm pki enable Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate
<bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
cscoDefaultMfgCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert< Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on
Public Key Data Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122
300d06092a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003
82010f003082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd
7d406ea0cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0
39f2bff7ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3
9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb
058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce
cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e
c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e
c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db
251e2e079cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc
1a61502dc54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490
881e3e3102d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b
d514795f7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693
f9f6c5cb88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f
76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3
b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f
de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8
eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301
0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This is the actual SSC key-hash value. Mon May 22
06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode
is 0
```

从 LAP 进行调试

如果控制器调试未指出加入请求，那么只要 LAP 有一个控制台端口，您就可以从 LAP 调试过程。您可以随这些命令看到 LAP 启动过程，不过您必须首先进入启用模式（默认口令是 Cisco）：

- **debug dhcp detailâ** 显示DHCP选项43信息。
- **debug ip udpâ** 显示加入/发现信息包对控制器以及DHCP和DNS查询(所有这些是UDP数据包。波尔特12223是controllerâ s源端口)。
- **调试lwapp客户端eventâ** 显示AP的LWAPP事件。
- **undebug allâ** 禁用在AP的调试。

以下是 **debug ip udp** 命令的输出示例。这一部分输出说明了 LAP 在启动过程中为发现和加入控制器而发送的数据包的信息。

```
UDP: sent src=10.77.244.199(20679), dst=10.77.244.208(12223)
!--- LWAPP Discovery Request sent to a controller to which !--- the AP was previously registered
to. UDP: sent src=10.77.244.199(20679), dst=172.16.1.50(12223) !--- LWAPP Discovery Request
using the statically configured controller information. UDP: sent src=10.77.244.199(20679),
dst=255.255.255.255(12223) !--- LWAPP Discovery Request sent using subnet broadcast. UDP: sent
src=10.77.244.199(20679), dst=172.16.1.51(12223) !--- LWAPP Join Request sent to AP-Manager
interface on statically configured controller.
```

避免与 DHCP 相关的问题

使用 DHCP 查找 IP 地址的 LAP 在启动 WLC 发现过程之前可能无法接收 DHCP 地址，原因是与 DHCP 相关的参数配置不正确。此部分说明 DHCP 如何与 WLC 一起使用，以及如何提供一些最佳实践来避免与 DHCP 相关的问题。

对于 DHCP，控制器像具有 IP 地址的路由器一样运行。也就是说，它填写网关 IP 地址然后直接通过单播数据包将请求转发到 DHCP 服务器。

当 DHCP 所提供的信息回到控制器时，会将 DHCP 服务器 IP 地址更改为它的虚拟 IP 地址。这样做的原因是，当 Windows 在 AP 之间进行漫游时，它要做的第一件事就是尝试联系 DHCP 服务器并更新其地址。

当 DHCP 服务器的地址为 1.1.1.1（控制器上典型的虚拟 IP 地址）时，控制器可以拦截该数据包并快速对 Windows 做出响应。

这也是所有控制器上的虚拟 IP 地址都相同的原因。如果 Windows 便携式计算机漫游到另一控制器上的 AP，它将尝试联系该控制器上的虚拟接口。由于移动性事件和上下文转移的存在，Windows 客户端漫游到的新控制器已具备再次响应 Windows 所需的全部信息。

如果要在控制器上使用内部 DHCP 服务器，只需将管理 IP 地址作为 DHCP 服务器放在为子网创建的动态接口上即可。然后将该接口分配给 WLAN。

控制器在每个子网上都需要一个 IP 地址的原因是，这样它才能在 DHCP 请求中填充 DHCP 网关地址。

在您为 WLAN 配置 DHCP 服务器时，应注意以下几点：

1. DHCP 服务器的 IP 地址不应属于控制器上的任何动态子网。它将被拦截，但可以使用以下命令进行覆盖：
   config network mgmt-via-dynamic-interface on version 4.0 only (command not available in version 3.2)
2. 控制器将使用其在该接口上的 IP 地址，通过单播从动态接口转发 DHCP（用较新的代码）。确保所有防火墙都允许此地址到达 DHCP 服务器。
3. 确保 DHCP 服务器的响应可以通过所有防火墙到达控制器在该 VLAN 上的动态地址。从 DHCP 服务器 ping 动态接口地址。Ping 源 IP 地址为动态接口的网关地址的 DHCP 服务器。
4. 确保 AP 的 VLAN 可以在交换机和路由器上使用，并且它们的端口配置为 Trunk 端口，以便带有 VLAN 标记的数据包（包括 DHCP）可以通过有线网络。
5. 确保 DHCP 服务器配置为可在 AP 的 VLAN 上分配 IP 地址。您也可以将 WLC 配置为 DHCP 服务器。有关如何在 WLC 上配置 DHCP 服务器的详细信息，请参阅 Cisco 无线局域网控制器配置指南 5.0 版的使用 GUI 配置 DHCP 部分。
6. 验证控制器在其动态接口上的 IP 地址是否将属于 DHCP 服务器上的一个 DHCP 范围。
7. 最后，确认您未使用不会响应单播 DHCP 请求（例如 PIX）的 DHCP 服务器。

如果您无法解决 DHCP 问题，可以尝试以下 2 个解决方案：

- 尝试使用内部 DHCP 服务器。将动态接口上的 DHCP 服务器地址配置为管理 IP 地址，然后使用 DHCP 获取内部池的地址。如果 DHCP 的范围是启用的，它应该会工作。
- 确认这些调试未在 CLI（控制台或 SSH）中通过发送输出对 DHCP 请求做出任何响应：0.
  debug mac addr <mac address>
  1. debug dhcp message enable
  2. debug dhcp packet enable 这将表明 DHCP 数据包已转发，但控制器没有收到响应。

最后，出于控制器安全方面的考虑，不建议将 VLAN 或子网放在同时还包含 LAP 的控制器上，除非 VLAN 或子网是管理接口子网。

注意： RADIUS 服务器或 DHCP 服务器不能存在于控制器的任何动态接口子网上。安全功能将阻止试图与控制器通信的返回数据包。

使用 Syslog 服务器对 LAP 加入过程进行故障排除

使用控制器软件 5.2 版，您可以配置 AP 以向 Syslog 服务器发送所有与 CAPWAP 相关的错误。由于在 Syslog 服务器自身上即可查看所有 CAPWAP 错误消息，因此无需在控制器上启用任何 debug 命令。有关此功能及用于启用此功能的命令的详细信息，请参阅 Cisco 无线局域网控制器配置指南 5.2 版的接入点加入过程故障排除部分。

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得到地址(请检查DHCP服务器租期APâ s MAC地址)。
- 尝试从控制器对 AP 执行 ping 操作。
- 检查交换机上的 STP 配置是否正常工作，以便发送给 VLAN 的数据包不会被阻止。
- 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AP重启，它启动WLC发现顺序并且设法找出AP。重新启动AP并且检查是否加入WLC。

下面列出了 LAP 未加入 WLC 的一些常见原因。

问题 1：控制器时间不在证书有效间隔内

要对此问题进行故障排除，请完成以下步骤：

1. 发出 **debug lwapp errors enable** 和 debug pm pki enable 命令。**debug lwapp event enable** 命令输出显示 AP 与 WLC 之间传递的证书消息的调试。输出清楚地表明证书被拒绝。**注意：** 确保考虑协调世界时 (UTC) 偏差。以下是 **debug lwapp events enable** 命令在控制器上的输出：**注意：** 由于空间有限，此输出的一些行被拆分为两行显示。
```
Thu Jan  1 00:09:46 1970: 00:0b:85:5b:fb:d0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Jan 1 00:09:46 1970: 00:0b:85:5b:fb:d0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:5b:fb:d0 on Port 2
Thu Jan  1 00:09:57 1970: 00:0b:85:5b:fb:d0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:5b:fb:d0 to 00:0b:85:33:52:81 on port '2'
Thu Jan  1 00:09:57 1970: 00:0b:85:5b:fb:d0 LWAPP Join-Request does not include valid
certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:5b:fb:d0. Thu Jan 1 00:09:57 1970:
00:0b:85:5b:fb:d0 Unable to free public key for AP 00:0B:85:5B:FB:D0 Thu Jan 1 00:09:57
1970: spamProcessJoinRequest : spamDecodeJoinReq failed
```
以下是 **debug pm pki enable** 命令在控制器上的输出。此输出遵循证书验证过程。**注意：** 由于空间有限，此输出的一些行被拆分为两行显示。
```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e, MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject
is 00:15:63:e5:0c:7e
```

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
 ......................
 ......................
 ......................
 ......................
 Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
 Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
>cscoDefaultMfgCaCert<
 Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
2005/04/15/07:55:03
 Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert validity
interval: make sure the controller time is set. Fri Apr 15 07:55:03 2005:
sshpmFreePublicKeyHandle: called with (nil)
```

此信息清楚地表明控制器时间不在 LAP 的证书有效间隔内。因此，LAP 无法注册到控制器。LAP 上安装的证书有预定义的有效间隔。应该设置控制器时间，在这种情况下在LAPâ s证书的证书有效性间隔内。

2. 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。
3. 在可以访问 CLI 的 LAP 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

```
：AP0015.63e5.0c7e#show crypto ca certificates .....................................
..................................................... ..........................................
..................................................... Certificate Status: Available Certificate
Serial Number: 4BC6DAB80000000517AF Certificate Usage: General Purpose Issuer: cn=Cisco
Manufacturing CA o=Cisco Systems Subject: Name: C1200-001563e50c7e ea=support@cisco.com
cn=C1200-001563e50c7e o=Cisco Systems l=San Jose st=California c=US CRL Distribution Point:
http://www.cisco.com/security/pki/crl/cmca.crl Validity Date: start date: 17:22:04 UTC Nov
30 2005 end date: 17:32:04 UTC Nov 30 2015 renew date: 00:00:00 UTC Jan 1 1970 Associated
Trustpoints: Cisco_IOS_MIC_cert ..............................
..................................... ..................................... 
```

由于可能有多个与此命令的输出相关的有效间隔，此处未列出完整输出。您只需要考虑由 Associated Trustpoint:Cisco_IOS_MIC_cert 以及名称字段中的相关 AP 名称指定的有效间隔。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。

问题 2：在管理域中不匹配

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

注意： 由于空间有限，此输出的一些行被拆分为两行显示。

```
Wed Oct 24 17:13:20 2007: 00:0b:85:91:c3:c0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:80 on port '2'
Wed Oct 24 17:13:20 2007: 00:0e:83:4e:67:00 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:91:c3:c0 on Port 2
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:91:c3:c0 to 00:0b:85:33:52:81 on  port '2'
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 AP ap:91:c3:c0:
txNonce  00:0B:85:33:52:80 rxNonce  00:0B:85:91:C3:C0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 LWAPP Join-Request MTU path
from AP 00:0b:85:91:c3:c0 is 1500, remote debug mode is 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully added NPU Entry
for AP 00:0b:85:91:c3:c0 (index 48)
Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 2, vlanId 0
AP IP: 10.77.246.18, AP Port: 7228, next hop MAC: 00:17:94:06:62:88
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Successfully transmission
of LWAPP Join-Reply to AP 00:0b:85:91:c3:c0
```

```
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:46 2007: 00:0b:85:91:c3:c0 Register LWAPP event
for AP 00:0b:85:91:c3:c0 slot 1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:91:c3:c0 to  00:0b:85:33:52:81
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP info for AP 00:0b:85:91:c3:c0 --
static 0, 10.77.246.18/255.255.255.224, gtw 10.77.246.1
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 Updating IP 10.77.246.18 ===> 10.77.246.18
for AP 00:0b:85:91:c3:c0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 0 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211a Regulatory Domain
(-N) does not match with country (US )  reg. domain -AB for the slot 0
Wed Oct 24 17:13:47 2007: spamVerifyRegDomain RegDomain set for
slot 1 code 21 regstring -N regDfromCb -AB
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: 80211bg Regulatory Domain (-N)
does not match with country (US ) reg. domain -AB for the slot 1 Wed Oct 24 17:13:47 2007:
spamVerifyRegDomain AP RegDomain check for the country US failed Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 AP 00:0b:85:91:c3:c0: Regulatory Domain check Completely FAILED The AP will
not be allowed to join Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0
Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0 apfSpamProcessStateChangeInSpamContext: Deregister
LWAPP event for AP 00:0b:85:91:c3:c0 slot 1 Wed Oct 24 17:13:47 2007: 00:0b:85:91:c3:c0
Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 0 Wed Oct 24 17:13:47 2007:
00:0b:85:91:c3:c0 Deregister LWAPP event for AP 00:0b:85:91:c3:c0 slot 1
```

此消息清楚地表明 LAP 与 WLC 的管理域不匹配。WLC 支持多个管理域，但是要从各管理域中加入 LAP，必须首先选择各域。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 和 WLC 时，请确保它们具有相同的管理域。只有这样 LAP 才能注册到 WLC。

注意： 对于单个 LAP 来说，802.1b/g 和 802.11a 无线电设备必须在同一管理域中。

问题 3：错误消息 AP cannot join because the maximum number of APs on interface 2 is reached

当 AP 试图加入控制器时，您就可能看到此错误消息：

```
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Fri May 19 16:18:06 2006  [ERROR] spam_lrad.c 4498: AP cannot join because the maximum number of
APs on interface 2 is reached.
```

默认情况下，4400 系列控制器能支持每端口最多 48 个 AP。当您试图在控制器上连接多于 48 个 AP 时，就会收到此错误消息。不过，您可以使用下列方法之一将 4400 系列控制器配置为在单个接口（每端口）上支持更多 AP：

- 链路聚合（用于工作在第 3 层模式下的控制器）
- 成倍增加 AP-manager 接口（用于工作在第 3 层模式下的控制器）
- 连接其他端口（用于工作在第 2 层模式下的控制器）

有关详细信息，请参阅配置 4400 系列控制器以支持多于 48 个接入点。

注意： Cisco 已面向企业用户推出具有其他能力的 5500 系列 WLC，对每个端口的 AP 数量没有限制。有关详细信息，请参阅 Cisco 无线局域网控制器配置指南 6.0 版的在链路聚合与成倍增加 AP-Manager 接口之间选择部分。

问题 4：对于 SSC AP，SSC AP 策略禁用

如果控制器上禁用 SSC 策略，您将在控制器上的 **debug lwapp events enable** 和 debug pm pki enable 的命令输出中看到此错误消息：

```
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 1553: spamProcessJoinRequest :
spamDecodeJoinReq failed
Wed Aug 9 17:20:21 2006 [ERROR] spam_crypto.c 1509: Unable to free public key for
AP 00:12:44:B3:E5:60
Wed Aug 9 17:20:21 2006 [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include valid
certificate in CERTIFICATE_PAYLOAD from AP 00:12:44:b3:e5:60. Wed Aug 9 17:20:21 2006 [CRITICAL]
sshpmPkiApi.c 1493: Not configured to accept Self-signed AP cert
```

要对此问题进行故障排除，请完成以下步骤：

执行以下两种操作之一：

- 在控制器的 CLI 中发出 **show auth-list** 命令，以查看控制器是否配置为可接受带有 SSC 的 AP。以下是输出示例：`#show auth-list Authorize APs against AAA ..... disabled Allow APs with Self-signed Certificate (SSC) .... enabled Mac Addr Cert Type Key Hash ----------------------- ---------- ---------------------------------------- 00:09:12:2a:2b:2c SSC 12345678901234567890123456789012345678901234567890`
- 在 GUI 中选择 **Security > AP Policies**。查看 **Accept Self Signed Certificate** 复选框是否被选中。如果未选中，请选中它。选择 **SSC** 作为证书类型。将 AP 连同 MAC 地址和密钥哈希添加到授权列表中。此密钥哈希可以从 **debug pm pki enable** 命令的输出中得到。有关如何获取密钥哈希值的信息，请参阅问题 6。

问题 5：在 WLC 上启用了 AP 授权列表；LAP 未在授权列表中列出

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

```
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 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
LWAPP 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
LWAPP 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 LWAPP 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 LWAPP 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 lwapp client error** 命令时将会看到此消息：

```
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.
```

这再次清楚地表明 LAP 未在控制器上的 AP 授权列表中列出。

可以使用以下命令查看 AP 授权列表的状态：

```
(Cisco Controller) >show auth-list Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

为将 LAP 添加到 AP 授权列表中，请使用 **config auth-list add mic <Ap MAC 地址>** 命令。关于如何

配置LAP授权的更多信息，参考在Cisco Unified无线网络配置示例的轻量级接入点(LAP)授权。

问题 6：SSC 公钥哈希错误或缺失

要对此问题进行故障排除，请完成以下步骤：

1. 发出 **debug lwapp events enable** 命令。此命令将验证 AP 是否试图加入。
2. 发出 **show auth-list** 命令。此命令将显示控制器中存储的公钥哈希。
3. 发出 **debug pm pki enable** 命令。此命令将显示实际公钥哈希。实际公钥哈希必须与控制器中存储的公钥哈希相匹配。两者不一致将引发问题。以下是此调试消息的示例输出：**注意：** 由于空间有限，此输出的一些行被拆分为两行显示。(Cisco Controller) > **debug pm pki enable**

```
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle... Mon
May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert bsnDefaultRootCaCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Mon May
22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert cscoDefaultMfgCaCert< Mon May 22
06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data Mon May 22
06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122 300d06092a864886 f70d0101 Mon May
22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f003082010a 02820101 Mon
May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7ad425fa7
face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3
9b87625143b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data
038181eb 058c782e56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key
Data f81fa6ce cd1f400bb5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles:
Key Data dde0648e c4d63259774ce74e 9e2fde19 Mon May 22 06:34:10 2006:
sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea65d8639b d63aa0e3 Mon May 22 06:34:10
2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e079cd31041 b0734a55 Mon May 22
06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502dc54e75f2 6d28fc6b Mon May
22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e3102d37140 7c9c865a Mon
May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb88053e8b
7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f
76cf78bcbc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data
031fb2a3 b5e572df2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key
Data fe64641f de2a6fe323311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles:
Key Data 1bfae1a8 eb076940280cbed1 49b2d50f Mon May 22 06:34:14 2006:
sshpmGetIssuerHandles: Key Data f7020301 0001 Mon May 22 06:34:14 2006:
sshpmGetIssuerHandles: SSC Key Hash is 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This
is the actual SSC key-hash value. Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path
from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14 2006:
spamRadiusProcessResponse: AP Authorization failure for 00:0e:84:32:04:f0
```

要解决此问题，请完成以下步骤：

1. 从 **debug pm pki enable** 命令的输出中复制公钥哈希，然后以此哈希值替换授权列表中的公钥哈希。
2. 发出 **config auth-list add ssc AP_MAC AP_key** 命令，以将 AP MAC 地址和密钥哈希添加到授权列表中。以下是此命令的示例：**注意：** 由于空间有限，此命令被拆分为两行显示。(Cisco Controller)>**config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9**

问题 7：AP 上存在证书或公钥损坏的情况

由于证书存在问题，LAP 不会加入控制器。

发出 **debug lwapp 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： 由于空间有限，此输出的一些行被拆分为两行显示。

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 LWAPP 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 APâ 请求返回材料授权(RMA)。
- SSC APâ 对Cisco IOS的降级？软件版本12.3(7)JA。如果是带有 SSC 的 AP，请使用 MODE 按钮将其转换回 IOS。然后再次使用 lwapp 升级工具将其转换回 LWAPP。执行此操作将会再次生成证书。

要进行降级，请完成以下步骤：

1. 使用 reset 按钮选项。
2. 清除控制器设置。
3. 再次运行升级。

有关对 LAP 进行降级的详细信息，请参阅将自治 Cisco Aironet 接入点升级到轻量模式。

如果您有 WCS，可以将 SSC 推送到新的 WLC。有关如何使用 WCS 配置 AP 的详细信息，请参阅 *Cisco Wireless Control System 配置指南 5.1 版* 的配置接入点部分。

问题 8：控制器可能在第 2 层模式下运行

要对此问题进行故障排除，请完成以下步骤：

检查控制器的操作模式。经过转换的 AP 仅支持第 3 层发现。经过转换的 AP 不支持第 2 层发现。

要解决此问题，请完成以下步骤：

1. 将 WLC 设置为使用第 3 层模式。
2. 重新启动并配置 AP-manager 接口。如果您有一个服务端口（例如 4402 或 4404 上的服务端口），您应使该端口与 AP-manager 和管理接口在不同的超网中。

问题 9：转换到 LWAPP 后在 AP 上收到这条错误消息

您将看到以下错误消息：

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs
no certs in the  SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

AP 将在 30 秒后重新加载，然后重新开始此过程。

要解决此问题，请完成以下步骤：

1. 您有一个 SSC AP。将其转换回自治 IOS 映像。
2. 发出 **write erase** 命令清除配置并重新加载。重新加载时不要保存配置。

问题 10：控制器在错误的 VLAN 上收到 AP 发现消息（您可以看到发现消息调试，但不是响应）

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

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!
此消息表明控制器通过源 IP 地址不在控制器上任何已配置子网中的广播 IP 地址收到了发现请求。这也意味着控制器将丢弃数据包。

问题在于 AP 不会向管理 IP 地址发送发现请求。控制器将报告来自控制器上未配置的 VLAN 的广播发现请求。这种情况通常在客户 trunk 允许 VLAN 而不限制它们通过无线 VLAN 时发生。

要解决此问题，请完成以下步骤：

1. 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 必须使用任一发现方法接收控制器 IP 地址。
2. 对交换机进行配置，使其允许一些不在控制器上的 VLAN。在 trunk 上限制允许的 VLAN。

问题 11：1250 LAP 无法加入 WLC

安装包含运行版本 4.1.185.0 的 2106 WLC。Cisco 1250 AP 无法加入控制器。

WLC 上的日志显示如下：

```
Mon Jun 2 21:19:37 2008AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2
21:19:37 2008 AP Associated. Base Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:26 2008 AP
Disassociated. Base Radio MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:20 2008 AP with MAC
f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x) is unknown. Mon Jun 2 21:19:20 2008 AP Associated. Base
Radio MAC: f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:09 2008 AP Disassociated. Base Radio
MAC:f0:2x:cf:2x:1d:3x Mon Jun 2 21:19:03 2008 AP with MAC f0:2x:cf:2x:1d:3x (APf02x.cf2x.1d3x)
is unknown.
```

解决方案：这是因为版本 4.1 不支持 Cisco 1250 系列 LAP。Cisco Aironet 1250 系列 AP 在 4.2.61 及更高版本的控制器中受支持。要解决此问题，请将控制器软件升级到 4.2.61.0 或更高版本。

问题 12：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，为使 LAP 能够加入控制器并与其进行通信，请确保在防火墙上启用了以下端口。

您必须启用以下端口：

- 为 LWAPP 流量启用如下 UDP 端口：数据 - 12222控制 - 12223
- 为移动性流量启用如下 UDP 端口：16666 - 1666616667 - 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]）

以下端口为可选端口（可根据自己的需要决定是否启用）：

- 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 13：网络中存在重复的 IP 地址

这是 AP 试图加入 WLC 时会遇到的另一个常见问题。当 AP 试图加入控制器时，您就可能看到此错误消息。

```
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 可以保持功率循环但无法加入控制器。

调试将表明，WLC 收到 AP 发出的 LWAPP 发现请求并将 LWAPP 发现响应传输给 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，请删除具有重复的 IP 地址的设备或更改设备的 IP 地址，以便网络中的设备具有唯一的 IP 地址。

然后，AP 就可以加入 WLC 了。

问题 14：如果网络 MTU 小于 1500 字节，LWAPP AP 将不会加入 WLC

原因是 Cisco bug ID **CSCsd94967**。LWAPP AP 可能无法加入 WLC。如果 LWAPP 加入请求大于 1500 字节，LWAPP 必须对 LWAPP 加入请求进行分段处理。针对所有 LWAPP AP 的逻辑是第一个分段的大小为 1500 字节（包括 IP 和 UDP 报头），第二个分段的大小为 54 字节（包括 IP 和 UDP 报头）。如果 LWAPP AP 与 WLC 之间的网络中有一个大小小于 1500 字节的 MTU（在使用隧道协议（如 IPSec VPN、GRE、MPLS 等）时，也可能会遇到这种情况），WLC 将无法处理 LWAPP 加入请求。

在下列条件下您将会遇到此问题：

- WLC 运行 3.2 版或更早版本的软件
- AP 与 WLC 之间的网络路径 MTU 小于 1500 字节

要解决此问题，请使用以下任一选项：

- 升级到 WLC 软件 4.0 版，前提是平台支持该版本。在 WLC 4.0 版中，通过允许 LWAPP 隧道重组最多 4 个分段解决了此问题。
- 将网络路径 MTU 增大到 1500 字节。
- 对可通过低 MTU 路径到达的位置使用 1030 REAP。我们已对到 1030 AP 的 REAP LWAPP 连接进行了修改，通过减小 REAP 模式所用的 MTU 解决了此问题。

问题 15：1142 系列 LAP 不会加入 WLC，WLC 上显示如下错误消息：lwapp_image_proc:unable to open tar file

仅支持 1142 系列 LAP 与 WLC 5.2 版及更高版本结合使用。如果您运行 WLC 5.2 版之前的版本，将无法向控制器注册 LAP，并且将会看到类似于如下所示的错误消息：

```
*Mar 27 15:04:38.596: %LWAPP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.597: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Mar 27 15:04:38.606: %LWAPP-3-CLIENTERRORLOG: not receive read response(3)
*Mar 27 15:04:38.609: lwapp_image_proc: unable to open tar fileMar 12 15:47:27.237
spam_lrad.c:8317 LWAPP-3-IMAGE_DOWNLOAD_ERR3:
Refusing image download request from AP 0X:2X:D0:FG:a7:XX - unable to open
image file /bsn/ap//c1140
```

为将 1140 LAP 注册到 WLC，请将 WLC 上的固件升级到 5.2 版或更高版本。

问题 16：1000 系列 LAP 无法加入无线局域网控制器，WLC 运行 5.0 版

原因是 WLC 软件 5.0.148.0 版或更高版本与 Cisco Aironet 1000 系列 AP 不兼容。如果有Cisco 1000系列LAP在网络，运行WLC版本5.0.48.0， 1000系列LAP不加入控制器，并且您看到在WLC的此陷阱消息。

```
"AP with MAC xx:xx:xx:xx:xx:xx is unkown"
```

问题 17：有不能Mesh的镜像的拉普加入WLC

轻量级接入点不向WLC登记。日志显示此错误消息

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

如果轻量级接入点装备mesh镜像并且在网桥模式，这能发生。如果LAP定购了与对此的mesh软件，您需要添加LAP对AP authorization list。选择**安全> AP策略**并且添加**AP**到Authorization list。AP应该然后加入，下载镜像从控制器，然后向WLC登记在网桥模式。然后您需要更改AP到本地传送方式。LAP下载镜像，重新启动并且注册回到在本地传送方式的控制器。

问题18 ：错误消息 - Dropping primary discovery request from AP XX: AA ：BB ：XX ： DD ：DD - maximum APs joined 6/6

WLC 可以支持的 LAP 数量有限。每个 WLC 都能支持一定数量的 LAP，具体取决于型号和平台。当 WLC 在达到最大 AP 容量后再收到发现请求时，您就会在其上看到此错误消息。

下面列出了不同 WLC 平台和型号上支持的 LAP 数量：

- 2100 系列控制器支持 6 个、12 个或 25 个 LAP。具体数量取决于 WLC 的型号。
- 4402 支持最多 50 个 LAP，而 4404 支持最多 100 个 LAP。使其非常适合于大型企业和高密度应用。
- Catalyst 6500 系列无线服务模块 (WiSM) 集成了 Catalyst 6500 交换机和两个 Cisco 4404 控制器，可支持最多 300 个 LAP。
- Cisco 7600 系列路由器 WiSM 集成了 Cisco 7600 路由器和两个 Cisco 4404 控制器，可支持最多 300 个 LAP。
- Cisco 28/37/38xx 系列集成多业务路由器集成了 28/37/38xx 路由器和 Cisco 控制器网络模块，支持最多 6 个、8 个、12 个或 25 个 LAP，具体取决于网络模块的版本。支持 8 个、12 个或 25 个 AP 的版本以及 NME-AIR-WLC6-K9 6 接入点版本较之 NM-AIR-WLC6-K9 6 接入点版本拥有更快的处理器和更大的板载内存。
- Catalyst 3750G 集成 WLC 交换机集成了 Catalyst 3750 交换机和 Cisco 4400 系列控制器，可支持最多 25 或 50 个 LAP。

相关信息

- Cisco 统一无线网络的轻量级接入点(LAP)授权配置示例
- 轻量 AP (LAP) 注册到无线 LAN 控制器 (WLC)
- Cisco 无线局域网控制器配置指南 4.1 版
- 技术支持和文档 - Cisco Systems