LWAPP升级工具故障排除提示

目录

简介

本文档讨论了使用升级工具将自治接入点 (AP) 升级为轻量模式时可能发生的一些重要问题。本文档还提供了有关如何纠正这些问题的信息。

先决条件

要求

执行升级之前，AP 必须运行 Cisco IOS® 软件版本 12.3(7)JA 或更高版本。

Cisco 控制器至少必须运行软件版本 3.1。

Cisco Wireless Control System (WCS)（如果使用）至少必须运行版本 3.1。

Windows 2000 和 Windows XP 平台支持升级实用程序。必须使用这两个 Windows 操作系统版本之一。

使用的组件

本文档中的信息基于以下接入点和无线局域网控制器。

支持此迁移的 AP 包括：

- 所有1121G接入点
- 所有 1130AG 接入点
- 所有 1240AG 接入点
- 所有 1250 系列接入点
- 对于所有基于 IOS 的 1200 系列模块化接入点（1200/1220 Cisco IOS 软件升级版、1210 和 1230 AP）平台来说，能否支持此迁移取决于无线电：如果支持 802.11G、MP21G 和 MP31G如果支持 802.11A、RM21A 和 RM22A可以升级使用以下支持的任意无线电组合的 1200 系列接入点：仅限 G、仅限 A 或 G 和 A。对于包含双重无线电的接入点，如果其中一个无线电支持 LWAPP，升级工具仍会执行升级。此工具将在详细日志中添加一条警告消息，指示不支持的无线电。
- 所有 1310 AG 接入点
- Cisco C3201 无线移动接口卡 (WMIC)**注意：** 第二代 802.11a 无线电包含两个部件号。

执行升级之前，接入点必须运行 Cisco IOS 版本 12.3(7)JA 或更高版本。

对于 Cisco C3201WMIC，执行升级之前，接入点必须运行 Cisco IOS 版本 12.3(8)JK 或更高版本。

下列 Cisco 无线局域网控制器支持已升级为轻量模式的自治接入点：

- 2000 系列控制器
- 2100 系列控制器
- 4400 系列控制器
- 适用于 Cisco Catalyst 6500 系列交换机的 Cisco 无线服务模块 (WiSM)
- Cisco 28/37/38xx 系列集成多业务路由器中的控制器网络模块
- Catalyst 3750G 集成无线局域网控制器交换机

Cisco 控制器至少必须运行软件版本 3.1。

Cisco Wireless Control System (WCS) 至少必须运行版本 3.1。Windows 2000 和 Windows XP 平台支持升级实用程序。

您可以从 Cisco 软件下载页面下载最新版本的升级实用程序。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

升级过程 - 概述

用户运行可接受带有接入点及其凭证列表的输入文件的升级实用程序。该实用程序使用一系列 Cisco IOS 命令远程登录到输入文件中的接入点，并使接入点做好升级准备，这些命令包括创建自

签名证书的命令。并且，该实用程序远程登录到控制器以便对该设备进行编程，从而向特定自签名证书接入点授权。然后，该实用程序在接入点上加载 Cisco IOS 软件版本 12.3(11)JX1，使其能够加入控制器。接入点在加入控制器之后会从控制器下载完整的 Cisco IOS 版本。升级实用程序生成含有接入点和相应自签名证书密钥哈希值列表的输出文件，可将该输出文件导入到 WCS 管理软件。然后，WCS 可向网络上的其他控制器发送此信息。

有关详细信息，请参阅将自治 Cisco Aironet 接入点升级为轻量模式的升级过程部分。

升级工具 - 基本操作

上述升级工具用于将自治 AP 升级为轻量模式（条件是该 AP 与此升级兼容）。升级工具执行从自治模式升级为轻量模式所必需执行的基本任务。这些任务包括：

- 基本情况检查 - 验证 AP 是否受支持、是否运行最低软件版本，以及是否支持无线电类型。
- 确保AP配置作为根。
- 准备自治 AP 以便进行转换 - 添加 Public Key Infrastructure (PKI) 配置和证书层次结构，以便可以在 Cisco 控制器上对 AP 进行身份验证，并且可为 AP 生成自签名证书 (SSC)。如果 AP 提供有厂商预装证书 (MIC)，则不会使用 SSC。
- 下载自治到轻量模式的升级映像，例如，12.3(11)JX1 或 12.3(7)JX，以便允许 AP 加入控制器。成功下载之后，此操作将重新引导 AP。
- 生成包括 AP MAC 地址、证书类型和安全密钥哈希的输出文件，并自动更新控制器。可将此输出文件导入到 WCS 并导出到其他控制器。

重要说明

在使用此实用程序之前，请考虑以下重要说明：

- 使用此工具转换的接入点无法连接到 40xx、41xx 或者 3500 控制器。
- 无法升级仅采用 802.11b 或第一代 802.11a 无线电的接入点。
- 如果要在转换和重新引导之后保留接入点的静态 IP 地址、网络掩码、主机名和默认网关，在将接入点转换为 LWAPP 之前，必须在接入点上加载以下自治映像之一：12.3(7)JA12.3(7)JA112.3(7)JA212.3(7)JA312.3(7)JA412.3(8)JA12.3(8)JA112.3(8)JA212.3(8)JEA12.3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g) JA12.4(3g) JA1
- 如果从以下自治映像之一将接入点升级为 LWAPP，转换后的接入点则不会保留其静态 IP 地址、网络掩码、主机名和默认网关：12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- 完成升级过程之后，LWAPP 升级工具不会释放 Windows 操作系统内存资源。仅当退出升级工具之后，才会释放内存资源。如果要升级多批接入点，必须在两次批处理之间退出此工具，以便释放内存资源。如果未在两次批处理之间退出此工具，升级工作站的性能会因内存消耗过度而迅速降低。

证书类型

有两种不同的 AP：

- 具有 MIC 的 AP
- 必须具备 SSC 的 AP

出厂安装的证书可以通过术语“MIC”来标识，它是厂商预装证书 (Manufacturing Installed Certificate) 的首字母缩写词。2005 年 7 月 18 日之前出厂的 Cisco Aironet 接入点没有 MIC，因此在升级这些

接入点以便在轻量模式下运行时会创建自签名证书。将对控制器进行编程，以便接受自签名证书，从而对特定接入点进行身份验证。

必须处理使用轻量接入点协议 (LWAPP) 的 Cisco Aironet MIC AP（如 Aironet 1000 AP），并排除相应故障。换句话说，请检查 IP 连接，调试 LWAPP 状态机，然后检查加密。

升级工具日志显示 AP 是 MIC AP 还是 SSC AP。下面是此升级工具生成的详细日志的示例：

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO 172.16.1.60 MIC is already configured in the AP 2006/08/21 16:59:07
INFO 172.16.1.60 Hardware is PowerPC405GP Ethernet, address is 0015.63e5.0c7e (bia
0015.63e5.0c7e) 2006/08/21 16:59:08 INFO 172.16.1.60 Inside Shutdown function 2006/08/21
16:59:10 INFO 172.16.1.60 Shutdown the Dot11Radio1 2006/08/21 16:59:11 INFO 172.16.1.60 Shutdown
the Dot11Radio0 2006/08/21 16:59:12 INFO 172.16.1.60 Updating the AP with Current System Time
2006/08/21 16:59:13 INFO 172.16.1.60 Saving the configuration into memory 2006/08/21 16:59:13
INFO 172.16.1.60 Getting AP Name 2006/08/21 16:59:58 INFO 172.16.1.60 Successfully Loaded the
LWAPP Recovery Image on to the AP 2006/08/21 16:59:58 INFO 172.16.1.60 Executing Write Erase
Command 2006/08/21 17:00:04 INFO 172.16.1.60 Flash contents are logged 2006/08/21 17:00:06 INFO
172.16.1.60 Environmental Variables are logged 2006/08/21 17:00:06 INFO 172.16.1.60 Reloading
the AP 2006/08/21 17:00:08 INFO 172.16.1.60 Successfully executed the Reload command
```

在此日志中，突出显示的行指定该 AP 安装有 MIC。有关证书和升级过程的详细信息，请参阅将自治 Cisco Aironet 接入点升级为轻量模式的升级过程概述部分。

对于 SSC AP，不会在控制器上创建任何证书。升级工具会让 AP 生成 Rivest、Shamir 和 Adelman (RSA) 密钥对，以便用于对自生成证书（即 SSC）签名。升级工具在控制器身份验证列表中添加一个条目，并添加该 AP 的 MAC 地址和公钥哈希。控制器需要公钥哈希才能验证 SSC 签名。

如果未向控制器添加此条目，请检查输出 CSV 文件。每个 AP 都应当对应有相应条目。如果找到该条目，请将该文件导入到控制器。如果使用控制器命令行界面 (CLI)（通过使用 **config auth-list** 命令）或交换机 Web 服务，一次只能导入一个文件。如果使用 WCS，则可以将整个 CSV 文件作为模板导入。

此外，请检查管理域。

注意：如果您具有 LAP AP，但希望使用 Cisco IOS 功能，则需要在该 AP 上加载自治 Cisco IOS 映像。相反，如果您具有自治 AP，并且希望将其转换为 LWAPP，则可以在自治 IOS 上安装 LWAPP 恢复映像。

可以完成相应步骤，以便使用“MODE”按钮或 **archive download** 命令更改 AP 映像。有关如何使用“MODE”按钮映像重新加载功能（适用于自治 IOS 或根据 AP 模型默认文件名命名的恢复映像）的详细信息，请参阅故障排除。

下一部分讨论了升级操作中的一些常见问题及其解决步骤。

问题

症状

AP 未加入控制器。本文档的解决方案部分按可能性高低顺序提供了此问题的原因。

解决方案

请使用本部分解决此问题。

原因 1

AP 无法通过 LWAPP 发现找到控制器，或者 AP 无法访问控制器。

故障排除

完成这些步骤：

1. 在控制器 CLI 中发出 **debug lwapp events enable** 命令。依次查找“LWAPP discovery”>“discovery response”>“join request”>“join response sequence”。如果未看到 LWAPP 发现请求，则表示 AP 无法找到或找不到控制器。以下是无线局域网控制器 (WLC) 向转换后的轻量 AP (LAP) 发送的成功加入回应的示例。以下是 **debug lwapp events enable** 命令的输出：
```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1' Thu May 25 06:53:54 2006: Successful
transmission of LWAPP Discovery-Response to AP 00:15:63:e5:0c:7e on Port 1 Thu May 25
06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e to
00:0b:85:33:84:a0 on port '1' Thu May 25 06:53:54 2006: Successful transmission of LWAPP
Discovery-Response to AP 00:15:63:e5:0c:7e on Port 1 Thu May 25 06:53:54 2006: Received
LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e to ff:ff:ff:ff:ff:ff on port '1' Thu May
25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
00:15:63:e5:0c:7e on Port 1 Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP
00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1' Thu May 25 06:54:05 2006: LWAPP Join-
Request MTU path from AP 00:15:63:e5:0c:7e is 1500, remote debug mode is 0 Thu May 25
06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e (index 51)Switch IP:
172.16.1.11, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679,
next hop MAC: 00:15:63:e5:0c:7e Thu May 25 06:54:05 2006: Successfully transmission of
LWAPP Join-Reply to AP 00:15:63:e5:0c:7e ..........................................
.............................................
..................................... // the debug output continues for full
registration process.
```
2. 检查 AP 网络和控制器之间的 IP 连接。如果控制器和 AP 位于同一子网，请确保它们已正确互联。如果位于不同子网，请确保在二者之间使用路由器，并且已在两个子网之间正确启用路由。
3. 验证是否已正确配置发现机制。如果使用“Domain Name System (DNS)”选项发现 WLC，请确保正确配置 DNS 服务器以便映射具有 WLC IP 地址的 CISCO-LWAPP-CONTROLLER.local-domain。因此，如果 AP 可以解析名称，则会向解析的 IP 地址发出一条 LWAPP 加入消息。如果使用选项 43 作为发现选项，请保证在 DHCP 服务器上进行适当配置。有关发现过程和序列的详细信息，请参阅将 LAP 注册到 WLC。有关如何配置 DHCP 选项 43 的详细信息，请参阅轻量 Cisco Aironet 接入点的 DHCP OPTION 43 配置示例。**注意：** 请记住，当转换静态寻址 AP 时，DNS 是唯一行之有效的第 3 层发现机制，这是因为将在升级过程中保留静态地址。您可以在 AP 上发出 **debug lwapp client events** 命令和 debug ip udp 命令，以便获取充足的信息来确定确切状况。您应当看到如下用户数据报协议 (UDP) 数据包序列：源自 AP IP 和控制器管理接口 IP。从控制器 AP 管理器 IP 到 AP IP。源自从 AP IP 到 AP 管理器 IP 的系列数据包。**注意：** 在某些情况下，可以存在多个控制器，并且 AP 可能尝试根据 LWAPP 发现状态机和算法加入不同控制器。出现此状况的原因可能在于控制器执行的默认动态 AP 负载均衡。需对此状况进行检查。**注意：** 以下是 **debug ip udp** 命令的示例输出：
```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222),
                     length=78
```

```
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223), length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679), length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=89
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679), length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223), length=222
```

解决方法

完成这些步骤：

1. 查看手册。
2. 修复基础架构，以便为 LWAPP 发现提供正确支持。
3. 将 AP 移至控制器所在的子网中，以便为 AP 提供事先指导。
4. 如果需要，发出 **lwapp ap controller ip address A.B.C.D** 命令，以便在 AP CLI 中手动设置控制器 IP：此命令的 *A.B.C.D* 部分即为 WLC 的管理接口 IP 地址。**注意：** 此 CLI 命令可在从未注册到控制器的 AP 上使用，也可以在加入以前的控制器时更改了默认启用口令的 AP 上使用。有关详细信息，请参阅重置轻量 AP (LAP) 上的 LWAPP 配置。

原因 2

控制器时间不在证书有效间隔内。

故障排除

完成这些步骤：

1. 发出 **debug lwapp errors enable** 和 debug pm pki enable 命令。上述 **debug** 命令显示 AP 与 WLC 之间传递的证书消息的调试。这些命令清楚地表明证书因不在有效间隔内而被拒绝的消息。**注意：** 确保考虑协调世界时 (UTC) 偏差。以下是 **debug pm pki enable** 命令在控制器上的输出：

```
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)
```

在此输出中，请注意突出显示的信息。此信息清楚地表明**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。应将控制器时间设置为在 AP 的证书有效间隔内。

2. 从 AP CLI 中发出 **show crypto ca certificates** 命令，以便验证在 AP 中设置的证书有效间隔。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（在本示例中为 Name:**C1200-001563e50c7e**）指定的有效间隔，如以上输出示例中的突出显示内容。**这是要考虑的实际证书有效间隔。**

3. 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证书有效间隔内，请更改控制器时间使其处于此间隔内。

解决方法

完成以下步骤：

在控制器 GUI 模式下选择**“Commands”>“Set Time”**或在控制器 CLI 中发出 config time 命令，以便设置控制器时间。

原因 3

对于 SSC AP，禁用 SSC AP 策略。

故障排除

在这些情况下，控制器上应显示以下错误消息：

```
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

完成这些步骤：

执行以下两种操作之一：

- 在控制器 CLI 中发出 **show auth-list** 命令，以查看控制器是否已配置为接受带有 SSC 的 AP。以下是 **show auth-list** 命令的示例输出：`#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 1234567890123456789012345678901234567890`
- 在 GUI 中选择 **Security > AP Policies**。

1. 查看 **Accept Self Signed Certificate** 复选框是否被选中。如果未选中，请选中它。
2. 选择 **SSC** 作为证书类型。
3. 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，请参阅原因 4。

原因 4

SSC 公钥哈希错误或丢失。

故障排除

完成这些步骤：

1. 发出 **debug lwapp events enable** 命令。验证 AP 是否尝试加入。
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：`(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 300d0609 2a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f00 3082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0 cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7 ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b876251 43b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb 058c782e 56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce cd1f400b b5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e c4d63259 774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea 65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e07 9cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502d c54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e31 02d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f 7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb 88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles:`

```
Key Data ca364f6f 76cf78bc bc1acc13 0d334aa6 Mon May 22 06:34:14 2006:
sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df 2c831e7e f765b7e5 Mon May 22 06:34:14
2006: sshpmGetIssuerHandles: Key Data fe64641f de2a6fe3 23311756 8302b8b8 Mon May 22
06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8 eb076940 280cbed1 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
```

解决方法

完成这些步骤：

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：`(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

原因 5

AP 上存在证书或公钥损坏的情况。

故障排除

完成以下步骤：

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。

解决方法

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)。
- SSC AP - 降级到 Cisco IOS 软件版本 12.3(7)JA。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。

原因 6

控制器可能正在第 2 层模式下运行。

故障排除

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。

解决方法

完成这些步骤：

1. 将 WLC 设置为使用第 3 层模式。
2. 重新引导 AP 管理器，并为 AP 管理器接口指定一个与管理接口处于同一子网中的 IP 地址。如果您具有服务端口（如 4402 或 4404 上的服务端口），则应将该端口和 AP 管理器及管理接口放置在不同超网中。

原因 7

升级期间显示以下错误：

```
FAILED   Unable to Load  the LWAPP Recovery Image on to the AP
```

故障排除

当显示此错误时，请完成以下步骤：

1. 验证 TFTP 服务器配置是否正确。如果使用 TFTP 服务器内嵌的升级工具，常见问题根源为个人防火墙软件，该软件会阻止传入 TFTP。
2. 检查升级使用的映像是否正确。升级为轻量模式需要特殊映像，而普通升级映像并不能发挥作用。

原因 8

转换之后，AP 上收到以下错误消息：

```
*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。

解决方法

完成以下步骤：

您有一个 SSC AP。转换为 LWAPP AP 之后，请在控制器的 AP 身份验证列表下添加 SSC 及其 MAC 地址。

故障排除提示

当从自治模式升级为 LWAPP 模式时，可使用以下提示：

- 当控制器尝试在转换后写入到 NVRAM 时，如果未清除 NVRAM，则会发生问题。Cisco 建议在将 AP 转换为 LWAPP 之前清除配置。要清除配置，请执行以下操作：从 IOS GUI 中 - 转至 **“System Software”>“System Configuration”>“Reset to Defaults”**或“Reset to Defaults Except IP”。从 CLI 中 - 在 CLI 中发出 **write erase** 和 reload 命令，当系统提示时，不要保存配置。由于条目变为 <ip 地址>,Cisco,Cisco,Cisco，这会导致更容易创建升级工具转换的 AP 的文本文件。
- Cisco 建议您使用 tftp32。可从 http://tftpd32.jounin.net/下载最新的 TFTPD 服务器。
- 如果在升级过程中启用了防火墙或访问控制列表，升级工具则无法将包含环境变量的文件从工作站复制到 AP。如果防火墙或访问控制列表阻止复制操作，并且选择了“Use Upgrade Tool TFTP Server”选项，此工具则无法更新环境变量，因此无法继续进行升级，并且上载到 AP 的映像将失败。
- 再次检查您尝试升级到的映像。从 IOS 到 LWAPP 映像的升级不同于普通 IOS 映像的升级。在“我的文档”/“我的电脑”-->工具-->“文件夹选项”下，确保取消选中“**隐藏已知文件类型的扩展名**”复选框。
- 始终确保使用提供的最新升级工具和升级恢复映像。这些最新版本可从无线软件中心获取。
- AP 无法引导 **.tar** 映像文件。该文件是类似于 zip 文件的归档文件。您需要使用 archive download 命令将 **.tar** 文件解包到 AP 闪存，或者首先从 tar 文件中提取可引导映像，然后将可引导映像放置到 AP 闪存中。

相关信息

- 将自治 Cisco Aironet 接入点升级为轻量模式
- 重置轻量 AP (LAP) 上的 LWAPP 配置
- 轻量 Cisco Aironet 接入点配置的 DHCP OPTION 43 示例
- 如何恢复哈希密钥接入点和导入它在控制器上
- 可能Cisco Aironet自治接入点转换到轻量级接入点协议(LWAPP)使用CLI，
- 技术支持和文档 - Cisco Systems