

瘦 AP 升级排错指南

【翻译内容】

目录

介绍.....	3
先决条件.....	3
需求.....	3
使用设备.....	3
升级工具-基本操作	4
注意事项.....	5
证书类型.....	5
问题.....	7
征兆.....	7
解决方案.....	7
Cause 1	7
Cause 2.....	10
Cause 3.....	12
Cause 4.....	13
Cause 5.....	15
Cause 6.....	16
Cause 7.....	17
Cause 8.....	17
排错指南.....	17

介绍

本文档介绍在使用升级工具升级胖 AP 到瘦 AP 时可能遇到的问题，以及针对这些问题的解决方案。

先决条件

需求

在升级前，确保 AP 工作在 IOS 12.3(7)JA 或更新的版本。

WLC 运行最低版本为 3.1.

如果使用 WCS，最低运行在 3.1 版本。

升级工具必须运行在 Win2000 或者 WinXP 平台上。

使用设备

本文档适用于 WLC4400、2100、2006、WLCM、WiSM、3750G 控制器。

以下 AP 可适用该文档升级：

- A11 1121 无线接入点
- A11 1130AG 无线接入点
- A11 1240AG 无线接入点
- A11 1250 系列无线接入点
- 所有的基于 IOS 软件的 1200 系列模块化无线接入点 (1200/1220 Cisco IOS Software Upgrade, 1210 and 1230 AP)，无线射频模块支持：
 - 如果是 802.11G 模块，支持 MP21G 和 MP31G
 - 如果是 802.11A 模块，支持 RM21A and RM22A

1200 系列 AP 支持 802.11a、802.11g 或者 802.11a/g 混合模式升级到瘦 AP。如果 AP 包括两个射频模块，并且其中一个已经工作在瘦 AP

模式下，升级工具仍然可以执行升级。升级的时候会报错，提示哪个无线模块不能被支持做升级。

- All 1310 AG access points
- Cisco C3201 Wireless Mobile Interface Card (WMIC)
- 注意:第二代的 802.11a 无线模块包含 2 个 part number.

要执行 AP 升级, AP 必须运行 IOS 12.3(7)JA 或更新版本的软件.

对于 Cisco C3201WMIC, AP 升级前必须工作在 IOS 12.3(8)JK 以后的版本.

以下 WLC 支持将胖 ap 升级到瘦 ap:

- 2000 series controllers
- 2100 series controllers
- 4400 series controllers
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Controller Network Modules within the Cisco 28/37/38xx Series Integrated Services Routers
- Catalyst 3750G Integrated Wireless LAN Controller Switches

WLC 最低运行在 3.1 版本.

升级工具-基本操作

升级工具在胖 ap 到瘦 ap 的转换过程中，执行一些基本的任务，包括：

- 基本条件检测—检测 AP 硬件、射频模块以及软件版本是否支持
- AP 升级的准备工作：为 AP 加入 WLC 配置公开密钥体系（PKI），对于出厂没有安装证书的 AP，将产生自签名 SSC 证书。
- 下载胖 AP 升级到瘦 AP 的镜像文件，例如 12.3(11)JX1 或者 12.3(7)JX，以允许 AP 加入到 WLC，一旦下载完成，AP 将重新启动。
- 产生一个输出文件，包括 AP 的 MAC 地址、证书类型、离散密钥等。该文件可以导入 WCS 中，并通过 WCS 导入其他 WLC 中。

升级步骤请参考 [Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode](#)。

注意事项

使用升级工具前，需要注意以下事项：

- 通过升级工具升级无线接入点不适用于连接到 40xx, 41xx, or 3500 无线控制器.
- 802.11b-only 或者第一代 802.11a 射频模块不支持升级.
- 如果希望升级后保留静态 IP 地址、掩码、主机名、网关，ap 在升级前需要加载以下胖 ap 镜像版本：
 - 12.3(7) JA
 - 12.3(7) JA1
 - 12.3(7) JA2
 - 12.3(7) JA3
 - 12.3(7) JA4
 - 12.3(8) JA
 - 12.3(8) JA1
 - 12.3(8) JA2
 - 12.3(8) JEA
 - 12.3(8) JEA1
 - 12.3(8) JEA2
 - 12.3(8) JEB
 - 12.3(8) JEB1
 - 12.4(3g) JA
 - 12.4(3g) JA1
- Ap 升级前工作在以下镜像下，将无法保留静态 IP 地址、掩码、主机名、网关等信息
 - 12.3(11) JA
 - 12.3(11) JA1
 - 12.3(11) JA2
 - 12.3(11) JA3
- 升级完成后，升级工具不会释放操作系统的内存资源，除非关掉升级工具。如果批量升级 AP，需要每次升级完成后，重新启动升级工具以释放内存，否则会影响升级的速度.

证书类型

AP 有两种类型

- 出厂安装有证书 (MIC)

- AP 需要自签名认证 (SSC)

MIC 为 AP 出厂时安装的证书，2005 年 7 月 18 日之前出厂的思科 Aironet 接入点是没有预安装的 MIC，当升级到瘦 AP 模式时，这些 AP 会创建一个自签名认证。配置控制器接受自签名认证，以允许某些 AP 的加入。

升级工具日志显示 AP 是 MIC AP 还是 SSC AP, 如下所示:

```

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

```

以上粗体部分显示 AP 为 MIC AP。更多信息请参考 [Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode](#)

使用 SSC AP 时，WLC 不需要产生证书。升级工具向 WLC 的验证列表里增加 AP 的 MAC 地址和公共密钥，用于 WLC 验证 AP 自签名认证。

如果这些条目没有加入到 WLC，可以检查升级工具输出的 CSV 文件，里面应该包括每个 AP 的条目，并将其导入到 WLC 中。如果通过 WLC 命令 `config auth-list` 或者通过 web 页面导入，每次只能导入 1 个文件；通过 WCS 可以将整个 CSV 文件作为一个模版导入。

Note: 如果瘦 ap 希望使用胖 ap 的功能，需要加载胖 AP 的 IOS 镜像；相反，如果胖 ap 需要转换为瘦 ap，需要加载 LWAPP recovery 镜像。

可以通过 AP 上 MODE 按键或者命令 **archive download** 更改 AP 的镜像。关于使用 MODE 按键去重新加载 AP 到默认的镜像文件，请参考 [Troubleshooting](#)。

问题

征兆

AP 无法加入到 WLC。

解决方案.

Cause 1

AP 通过 LWAPP 协议无法找到 WLC，或者 AP 无法连到 WLC。

排错

使用以下步骤：

1. WLC 上使用命令 **debug lwapp events enable** .

查找 LWAPP discovery > discovery response > join request > join response sequence. 如果没有发现 LWAPP discovery request, 就意味着 AP 没有发现 WLC。

以下 **debug lwapp events enable** 输出为 WLC 成功的向 LAP 返回 JOIN REPLY 的信息：

```
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 和 WLC 的连通性。如果 AP 和 WLC 在同一子网，确保他们使用正确的连接；如果 AP 和 WLC 位于不同子网，确保两个子网之间使用路由器并启用路由
3. 确保正确配置了发现机制。

如果 WLC 的发现过程使用 DNS，确认 DNS Server 上配置 CISCO-LWAPP-CONTROLLER.local-domain 和 WLC IP 地址 的映射。所以，如果 AP 能够解析这个域名，它将会发一个 LWAPP Join 消息去解析出 WLC IP 地址。

如果使用 option 43，确保正确配置了 DHCP 服务器。

发现机制的更多信息请参考 [Register the LAP with the WLC](#)

Option43 的更多信息请参考 [DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example](#)

Note: 对配置了静态地址的胖 AP 升级，3 层发现机制只能使用 DNS。

在 AP 上输入 `debug lwapp client events` 和 `debug ip udp` 可以看到很多 UDP 包信息，包括：

- a. 从 AP 的 IP 到 WLC 管理接口地址作为源的包

- b. 从 WLC AP 的管理接口地址到 AP IP 的包.
- c. 一系列从 AP 的 IP 到 AP 管理接口地址的包

Note:以下为 debug ip udp 上的输出:

```
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
```

解答

执行以下步骤：

1. 查看手册。
2. 正确配置网络以支持 LWAPP 发现机制。
3. 将 AP 和 WLC 位于同一子网
4. 可以通过命令 `lwapp ap controller ip address A.B.C.D` 为 AP 人为的设置 WLC 地址：

A.B.C.D 为 WLC 管理接口的 IP 地址。

Note: 该命令用在那些从未注册到 WLC 上的 AP 上，或者那些通过 WLC 更改过默认密码的 AP 上。更多信息请参考 [Resetting the LWAPP Configuration on a Lightweight AP \(LAP\)](#) 。

Cause 2

WLC 时钟超过了证书的有效期限。

排错

执行以下步骤：

1. 输入 `debug lwapp errors enable` 和 `debug pm pki enable`。

该命令显示 AP 和 WLC 之间的认证信息，并可以清楚地显示证书过期。

以下为 WLC 上 `debug pm pki enable` 命令的输出部分：

```
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 verified using
>ciscoDefaultMfgCaCert<
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)

```

以上粗体部分明确地说明 **controller time is outside the certificate validity interval of the AP**. 因此, AP 无法注册到 WLC 上, WLC 的时钟应该设置在 AP 证书有效期之内。

2. 在 AP 上输入 `show crypto ca certificates` 核实证书的有效期间, 如下所示:

```

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
```

```
.....
.....
.....
```

注意粗体部分 **Associated Trustpoint: Cisco_IOS_MIC_cert**，与之关联的 AP 的名字(在这里, **Name: C1200-001563e50c7e**)。

3. WLC 上通过命令 **show time** 核实日期和时间是否在有效期范围内。

如果不在该范围内，需要做相应的更改。

解决方案

在 WLC 图形界面下选择 **Commands > Set Time**，或者使用命令 **config time** 更改 WLC 时间。

Cause 3

AP 自签名证书(SSC)的功能被关闭。

排错

这种情况下，WLC 会看到如下信息：

```
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
```

完成以下步骤：

执行以下任意步骤：

- WLC 上输入命令 `show auth-list` 以检查 WLC 是否接受 AP 的自签名证书。

以下为命令 `show auth-list` 的输出：

```
#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

- WLC 图形界面下选择 **Security > AP Policies**.
 - a. 检查选项 **Accept Self Signed Certificate** 是否被选中
 - b. 选择 **SSC** 作为证书类型.
 - c. 在授权列表里增加 AP 的 MAC 地址和密钥

密钥可以通过命令 `debug pm pki enable` 得到. 参考 Cause 4

Cause 4

自签名 (SSC) 公共密钥错误或者不匹配

排错

完成以下步骤：

1. 输入命令 `debug lwapp events enable`.

确认 AP 试图加入 WLC

2. 输入命令 `show auth-list`, 显示 WLC 存储的公共密钥
3. 输入命令 `debug pm pki enable`, 显示真实的公共密钥, 该密钥必须与 WLC 存储的密钥一致。如下所示：

(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
>cscscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscscoDefaultMfgCaCert<
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
bclacc13 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
280cbcd1 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
```

!-- 这是真实的 SSC 密钥值。

```
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
```

解决方案

完成以下步骤：

1. 使用命令 `debug pm pki enable` 输出的密钥值, 去替换授权列表里的值。
2. 输入命令 `config auth-list add ssc AP_MAC AP_key` 将 MAC 地址和密钥添加到授权列表里。如下所示：

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
```

!-- 以上命令要在同一行上输入

Cause 5

AP 上证书或密钥被破坏。

排错

完成以下步骤：

使用命令 `debug lwapp errors enable` 和 `debug pm pki enable` 可以看到证书或密钥被破坏。

解决方案

使用以下任意方式：

- 出厂自带证书的 AP-MIC AP—需要备件更换服务(RMA).
- 自签名证书的 AP-SSC AP—降低版本到 12.3(7)JA.

使用以下步骤降级版本：

1. 使用重起按键.
2. 清空 WLC 配置
3. 再次运行升级.

Cause 6

WLC 可能工作在 2 层模式下。

排错

完成以下步骤：

检查 WLC 工作的模式

需要升级的 AP 只支持 3 层发现机制，不支持 2 层发现机制。

解决方案

1. 将 WLC 配置为 3 层模式
2. 重起，将 AP 管理接口地址设置为与 WLC 管理接口地址同一网段。

如果存在服务接口，比如 WLC4402 或 4404，将其网段配置为独立于 AP 管理地址和 WLC 管理地址的网段。

Cause 7

升级过程中看到如下错误信息：

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

排错

1. 确保 TFTP 服务器配置正确

如果使用升级工具自带的 TFTP 服务器，防火墙可能禁止 TFTP 流量

2. 检查是否使用正确的镜像文件.

升级到瘦 AP 需要一个特殊的镜像，且不是一个可以正常工作的镜像。

Cause 8

AP 升级后收到以下错误信息：

```
*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 30 秒后重起，并重复这个操作。。

解决方案

该 AP 为自签名认证的 AP，升级完成后，将 SSC、MAC 地址加入到 WLC 的 AP 授权列表中。

排错指南

胖 AP 升级到瘦 AP 需要注意：

- Cisco 建议 AP 升级前使用以下步骤清空 NVRAM，否则会出现问题：
 - 图形界面下 **System Software > System Configuration > Reset to Defaults**, 或者 **Reset to Defaults Except IP**.
 - CLI 命令行下输入 **write erase** 和 **reload** , 不保存配置.
- Cisco 建议使用 TFTP32, 最新版本可通过该连接下载 <http://tftpd32.jounin.net/> .
- 如果使用升级工具自带的 TFTP, 确保防火墙关闭
- 再次检查用来升级的镜像, 该文件不同于正常的 IOS.

在文件夹选项中确保显示已知文件的扩展名。

- 使用最新的升级工具和 Upgrade Recovery Image..
- .tar 镜像无法引导 AP 启动, 该文件类似.zip 是个压缩文件, 在 AP 上通过 **archive download** 命令将该文件解压到 AP flash 中, 或者先将.tar 文件取出来, 然后把可以引导的镜像文件放到 AP 的 flash 中。

相关技术文档

- [Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode](#)
- [Resetting the LWAPP Configuration on a Lightweight AP \(LAP\)](#)
- [DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example](#)
- [Technical Support & Documentation - Cisco Systems](#)