无线局域网控制器(WLC)错误和系统消息常见消息

Contents

[Introduction](#)
[错误信息FAQ](#)
[Related Information](#)

Introduction

本文档提供了有关 Cisco 无线局域网 (WLAN) 控制器 (WLC) 的错误消息和系统消息的最常见问题解答 (FAQ) 信息。

Refer to Cisco Technical Tips Conventions for more information on document conventions.

错误信息FAQ

Q. 我们从Cisco 4404 WLC开始了转换超过200接入点(APs)从Cisco IOS软件到轻量级AP协议(LWAPP)。我们完成了转换48 APs，并且我们收到陈述在WLC的一个消息：**[ERROR] spam_lrad.c 4212 1AP AP**错误出现？

A. 您必须创建另外的AP管理器接口为了支持超过48 APs。否则，您收到如下所示:的错误

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

配置多个AP管理器接口并且配置其他AP管理器接口不使用的主要的/备份端口。您*必须*创建第二个AP管理器接口为了提出另外的APs。但是，请切记您的每个管理器的主端口和备份端口配置不交迭。换句话说，如果AP管理器1使用端口1作为主要的和端口2作为备份， AP管理器2必须使用端口3作为主要的和端口4作为备份。

Q. 我有无线局域网控制器(WLC) 4402，并且我使用1240轻量级接入点(膝部)。我尝试对enable (event) 128-bit在WLC的加密。当我选择在WLC时的128-bit WEP加密，我收到说的一个错误1240s不支持128-bit ：**[ERROR] spam_lrad.c 12839 CISCO AP xxSSID mde xx xx xx xx xxWEP128**收到此错误？

A. 在WLCs显示的密钥长度实际上是在共有的秘密，并且不包括初始化矢量(iv)的24 BITS位的数量。许多产品，包括Aironet产品，称它128-bit WEP密钥。实际上它是有24位IV的一个104-bit键。104-bit的密钥大小是什么您必须在WLC的enable (event) 128-bit WEP加密的。

如果选择在WLC的128-bit密钥大小，它实际上是152-bit (128 + 24 IV) WEP密钥加密。仅Cisco 1000系列膝部(AP1010、AP1020， AP1030)支持使用WLC 128位WEP密钥设置。

Q. 我为什么获得11xx12xx13xxAPs128WEPWLAN错误信息，当我设法配置在WLC的WEP ？

A. 在无线局域网控制器上，当您选择静态WEP作为第2层安全方法时，您有这些选项或WEP密钥大小。

- 没有请设置
- 40位
- 104位
- 128位

这些密钥大小值不包括24位初始化矢量(iv)，用WEP密钥连接。因此，对于64位WEP，您需要选择**40位**作为WEP密钥大小。控制器添加24位IV到此为了做一把64位WEP密钥。同样地，对于一把128位WEP密钥，请选择**104位**。

控制器也支持152把位WEP密钥(128位+ 24位IV)。11xx、12xx和13xx式样APs不支持此配置。因此，当您设法用144位时配置WEP，控制器给予一个消息此WEP配置没有被推进对11xx、12xx和13xx式样APs。

Q. 客户端不能验证到为WPA2被配置，并且控制器显示apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILEDWLAN RSNIERSN (WPA2)RSN.MobileStation:00:0c:f1:0c:51:22WLAN SSID <>错误信息。为什么收到此错误？

A. 这主要发生由于在客户端的不兼容。设法这些步骤为了调整此问题：

- 检查客户端是否为WPA2是Wi-Fi认证的并且检查客户端的配置WPA2。
- 检查数据表或宣传单页为了发现客户端工具是否支持WPA2。安装供应商发布的所有补丁程序支持WPA2。如果使用Windows工具，请切记您从Microsoft安装 WPA2补丁程序为了支持WPA2。
- 升级客户端驱动程序和固件。
- 关闭在WLAN的Aironet扩展。

Q. 一旦我重新启动WLC，我300获得Mon Jul 17 15:23:28 2006MFP-00:XX:XX:XX:XX3023MICdot11 slot AP 00:XX:XX:XX:XX 0错误信息时。此错误为什么出现，并且如何摆脱它？

A. 当MFP被启用的膝部时，发现与不正确MIC值的帧此错误信息被看到。参考基础设施管理帧保护(MFP)与WLC和LAP配置示例关于MFP的更多信息。完成这四个步骤之一：

1. 检查并且去除所有恶意或无效APs或客户端您的网络的，产生无效帧。
2. 禁用基础设施MFP，如果MFP在移动组的其他成员没有允许和膝部能听到从没有被启用的MFP的膝部的管理帧在组的其他WLCs。参考无线局域网控制器(WLC)移动组FAQ关于移动组的更多信息。
3. 此错误信息的修正是可用的在WLC版本4.2.112.0和5.0.148.2。升级WLCs到这些版本之一。
4. 作为最后一个选项，请设法重新载入生成此错误信息的LAP。

Q. 客户端AIR-PI21AG-E-K9与接入点(AP)顺利地产生关联使用可扩充验证灵活协议认证通过获取建立隧道(EAP-FAST)。然而，当关联AP关闭时，客户端不漫游对另一个AP。此消息不断地出现于控制器消息日志："Fri Jun 2 14:48:49 2006[SECURITY] 1x_auth_pae.c 1922 -Fri Jun 2 14:48:49 2006[SECURITY] apf_ms.c 2557 00:40:96:ad:75:f4"为什么？

A. 当客户端卡需要执行漫游时，发送认证请求，但是不正确地处理键(不通知AP/controller，不回答再验证)。

这在Cisco Bug ID CSCsd02837 (仅限注册用户)描述。此Bug用Cisco Aironet 802.11a/b/g客户端适配器Install向导3.5修复了。

一般来说，消息的也发生由于任何这些原因：

- 特定的用户名在超过一个客户端设备使用。
- 用于该WLAN的认证方法有一个外部匿名身份。例如，在PEAP-GTC或在EAP-FAST，定义通用的用户名成外部(可视)是可能的身份，并且实际用户名被隐藏在TLS里面建立隧道在客户端和RADIUS服务器之间，因此控制器看不到它和使用它。在这类情况下，此消息能出现。此问题在某些第三方和某些老固件客户端通常看到。

Q. 当我在6509交换机上安装新的无线服务模块(WiSM)时前端并且实现Protected Extensible Authentication Protocol (PEAP)用Microsoft IAS服务器，我收到此错误：***Mar 1 00:00:23.526 %LWAPP-5-CHANGED LWAPP*Mar1 00:00:23.700 %SYS-5-RELOAD LWAPP CLIENT.Reload CRYPTO INIT*Mar 1 00:00:23.700 %LWAPP-5-CHANGED LWAPPDOWN *Mar1 00:00:23.528 %LWAPP-5-CHANGED LWAPP*Mar1 00:00:23.557 LWAPP_CLIENT_ERROR_DEBUG lwapp_crypto_init_ssc_keys_and_certsSSC*Mar certs 1 00:00:23.557 LWAPP_CLIENT_ERROR_DEBUG *Mar 1 00:00:23.557 lwapp_crypto_init PKI_StartSession*Mar 1 00:00:23.706 %SYS-5-RELOAD LWAPP。** 为什么？

A. RADIUS和dot1x调试表示， WLC发送一个访问请求，但是没有自IAS服务器的无响应。完成这些步骤为了排除问题故障：

1. 检查并且验证IAS服务器配置。
2. 检查日志文件。
3. 安装软件，例如Ethereal，能给予您认证详细资料。
4. 终止并且开始IAS服务。

Q. 轻量级接入点(膝部)不向控制器登记。什么也许是问题？我看到在控制器的这些错误信息：**Thu Feb 3 03:20:47 2028LWAPPAP 00:0b:85:68:f4:f0CERTIFICATE_PAYLOADThu Feb 3 03:20:47 2028AP00:0B:85:68:F4:F0。**

A. 当接入点(AP)发送轻量级接入点协议时(LWAPP)请加入请求对WLC，它嵌入其X.509证书在LWAPP消息。它也生成在LWAPP包括加入请求的随机的会话ID。当WLC接受时LWAPP加入请求，验证X.509证书的签名使用APs公共密钥并且检查委托的认证机关发行认证。它也查看起始日期和时刻的AP证书有效性间隔，并且与其自己的日期和时间比较该日期和时间。

此问题能发生由于在WLC的一个不正确时钟设置。为了设置在WLC的时钟，请发出**show time**，并且**设置计时**命令。

Q. 轻量接入点协议(LWAPP) AP无法加入其控制器。无线局域网控制器(WLC)日志显示消息类似于此：**LWAPPAP 00:0b:85:68:ab:01CERTIFICATE_PAYLOAD。** 为什么？

A. 如果在AP和WLC之间的LWAPP隧道横贯有MTU的一个网络路径在1500个字节以下，您能收到此错误信息。这导致LWAPP信息包的分段。这是在控制器的一个已知Bug。参考Cisco Bug ID CSCsd39911 (仅限注册用户)。

解决方案将升级控制器固件到4.0(155)。

Q. 我设法设立在我的内部控制器和虚拟锚点控制器之间的客户隧道在非敏感区域(DMZ)。然而，当用户尝试与客户SSID时产生关联，用户无法从DMZ收到IP地址，正如所料。所以，用户数据流没有被以隧道传输到在DMZ的控制器。调试便携移交命令的输出显示消息类似于此：`Wlan <wlan id>ExportIP <controller IP>`。问题出在哪里？

A. 客户隧道提供附加安全性进入对公司无线网络的客户用户入口。这帮助保证客人身份的用户无法访问公司网络，无需首先穿过公司防火墙。当指定客户WLAN的用户与WLAN时产生关联，用户数据流被以隧道传输到位于DMZ在公司防火墙外面的WLAN控制器。

现在，考虑到此方案，可以有建立隧道此的客户的几个原因不作用正如所料。因为debug命令输出暗示，问题也许是在为该特定的WLAN配置的不匹配任何安全策略在内部以及在DMZ控制器。证实安全策略以及其他设置，例如会话时间设置，是否被匹配。

此问题的另一常见原因是DMZ控制器不停住对本身为该特定的WLAN。对于建立隧道的客户适当地工作和为了DMZ能管理属于客户WLAN)用户(用户的IP地址，重要的是适当停住为该特定的WLAN完成。

Q. 我看到很多"CPU"消息在2006年无线局域网控制器(WLC)，但是不在4400 WLCs。为什么？我禁用在控制器的组播。什么是在组播队列限制上的区别在2006年和4400 WLC平台之间？

A. 由于组播在控制器被禁用，引起此警报的消息也许是地址解析服务(ARP)消息。没有区别队列深度(512个信息包)在2000年WLCs和4400 WLCs之间。区别是4400个NPU过滤器ARP信息包，而一切在2006年的软件执行。这解释2006年WLC为什么看到消息，但是不是4400 WLC。44xx WLC通过硬件处理组播信息包(通过CPU)。2000年WLC通过软件处理组播信息包。CPU处理比软件效率更高。所以，快速地清除4400's队列，而2006年WLC奋斗得有点，当看到很多这些消息时。

Q. 我看到"`[SECURITY] apf_foreignap.c 763 STA [00:0A:E4:36:1F:9B]AP1`"错误信息在我的一个控制器中。此错误是什么意思，并且应该采取什么步骤解决它？

A. 此消息被看到，当控制器收到DHCP请求没有一台状态机的MAC地址时。这从网桥或运行一台虚拟机类似VMWare的系统经常被看到。控制器听DHCP请求，因为执行监听的DHCP，因此知道哪些地址与连接其接入点的客户端产生关联(APs)。无线客户端的所有数据流穿过控制器。当信息包的目的地是无线客户端时，去控制器然后穿过轻量级接入点协议(LWAPP)隧道对AP和给客户端。可以做帮助缓和此消息的一件事是只允许在Trunk上的控制器使用去有连接孔VLAN的控制器的VLAN提供on命令交换机。

Q. 我为什么看到在控制台的此错误信息：`'' Id= 0x0050b986value= 0xffffffc` ？

A. 这可以归结于高CPU负荷。当控制器CPU大量负载例如时，当它执行文件副本或其他任务时，没有时间处理NPU发送以回应配置消息的所有ACKs。当这发生时， CPU生成错误信息。然而，错误信息不影响服务或功能。

这在版本注释的大量地控制装载装置CPU部分描述Cisco无线LAN控制器和轻量级接入点的版本的3.2.116.21。

Q. 我收到在我的无线控制system(WCS)的这些有线等效保密(WEP)键错误信息：`WEP MAC'xx xx xx xx xx xx' APMAC'xx xx xx xx xx xx'Slot ID'1'`。然而，我不使用WEP作为安全参数在我的网络。我只使用Wi-Fi保护访问(WPA)。为什么收到这些WEP错误信息？

A. 如果所有您与安全相关的配置完善，您收到现在的消息是由于Bug。有在控制器的一些已知Bug。参考Cisco Bug ID CSCse17260 (仅限注册用户)，并且CSCse11202 (仅限注册用户)，陈述“WEP密钥被配置在位置可能是错误的在**各自WPA和TKIP客户端**”。实际上， **CSCse17260**是**CSCse11202**重复项。**CSCse11202的**修正已经是可用的与WLC版本3.2.171.5。

Note: 最新的WLC版本有这些Bug的一个修正。

Q. 我们使用外部RADIUS服务器通过控制器验证无线客户端。控制器有规律地发此错误信息：`RADIUS`。为什么看到这些错误信息？

A. 当请求从WLC出去到RADIUS服务器时，每个信息包有WLC预计一种回应的一个序号。如果没有无响应，有显示`RADIUS`消息。

WLC的默认时间听到从RADIUS服务器是2秒。这从在**安全>认证服务器下的**WLC GUI设置。最大数量是30秒。所以，设置这次重视对其最大为了解决此问题也许是有用的。

有时， RADIUS服务器执行‘**静音丢弃**来自WLC的’请求信息包。RADIUS服务器能拒绝这些信息包由于认证不匹配和几个其他原因。这是一个有效动作由服务器。并且，在这些情况下，控制器将指示RADIUS服务器如不回应。

为了解决无声丢弃发出，禁用在WLC的**积极的故障切换功能**。

如果在 WLC 中启用主动故障切换功能，则 WLC 会过于主动，以至于无法将 AAA 服务器标记为 not responding。然而，不应该执行这，因为AAA服务器也许不是仅响应能力的对该特定的客户端(通过执行静音丢弃)。它可以是对其他有效客户端的一种回应(与有效证书)。然而， WLC也许仍然指示AAA服务器如不回应和不功能。

为了解决此，请禁用**积极的故障切换功能**。发出**设置半径aggressive-failover disable命令**从控制器CLI为了执行此。如果这是失效的，则控制器只失效对下个AAA服务器，如果有不能从RADIUS服务器收到答复的3个连续的客户端。

Q. 几个客户端无法联合到LWAPP，并且控制器记录`IAPP-3-MSGTAG015 iappSocketTask iappRecvPkt`错误信息。为什么会发生这种情况？

A. 这主要发生由于支持CCX v4，但是早于10.5.1.0请运行客户端套件版本的Intel适配器的一个问题。如果升级软件到10.5.1.0或以上，这调整此问题。参考Cisco Bug ID CSCsi91347 (仅限注册用户)关于此错误信息的更多信息。

Q. 我看到在无线局域网控制器(WLC)的此错误信息：`EAP(21) STA00:05:4e:42:ad:c5`。为什么？

A. 此错误信息出现，当用户设法连接到EAP保护的WLAN网络时和发生了故障EAP尝试的预先配置的数量。当用户不能验证时，控制器排除客户端，并且客户端不能连接到网络，直到排除计时器由管理员到期或手工改写。

排除发现单个设备做的认证尝试。当该设备超出故障时的最大数量，该MAC地址没有允许其中任一长期联合。

排除发生：

- 在共有的认证的5连续的认证失败以后(第6个尝试被排除)

- 在MAC验证的5个连续的关联故障以后(第6个尝试被排除)
- 在3连续的EAP/802.1X认证失败以后(第4个尝试被排除)
- 任何外部策略服务器故障(NAC)
- 任何IP地址复制实例
- 在3连续的Web认证失败以后(第4个尝试被排除)

可以配置计时器客户端多久被排除和排除可以启用或禁用的在控制器或WLAN级别。

Q. 我看到在无线局域网控制器(WLC)的此错误信息：1'10.0.16.5'WLCSCH01/10.0.16.5RADIUS。问题是什么？

A. 这也许是由于Cisco Bug ID CSCsc05495。因此请烦扰，控制器周期地注入不正确AV对(属性24， “状态”)违犯RADIUS RFP并且引起一些认证服务器的问题的认证请求消息。此Bug在3.2.179.6被修复。

Q. 我收到噪声配置文件故障消息在监控程序> 802.11b/g无线电下。我要知道我为什么看到此失败消息？

A. 噪声配置文件FAILED/PASSED状态在测试结果以后设置完成由WLC和与当前集阈值比较。默认情况下，噪声值设置到-70。故障状态表明该特定的参数或接入点(AP)的门限值超过了。您能调整在配置文件的参数，但是推荐更改设置，在您清楚了解网络设计后，并且如何将影响网络的性能。

高级无线电资源管理(RRM) PASSED/FAILED阈值全局为在**802.11a全局参数的**所有APs设置**>自动RF**和**802.11b/g全局参数>自动RF**页。RRM PASSED/FAILED阈值为在**802.11 AP接口>性能配置文件**页的此AP单个设置。

Q. 我不能set port 2作为AP管理器接口的备份端口。返回的错误信息是不set port。我能对set port 2作为管理接口的备份端口。两个接口的当前活动端口是端口1。为什么？

A. AP管理器没有一个备份端口。曾经更早版本支持它。从版本4.0和以上，不支持AP管理器接口的备份端口。通常，单个AP管理器在每个端口(没有备份)应该被配置。如果使用链路聚合(滞后)，只有一个AP管理器。

必须分配静态(或永久性) AP管理器接口到分布式系统端口1并且必须有唯一IP地址。它不可能被映射到备份端口。通常是在与管理接口相同的 VLAN 或 IP 子网上配置这一点，但这并非一项要求。

Q. 我看到此错误信息：AP '00:0b:85:67:6b:b0'00:13:02:8d:f6:41'1'WPA MIC60。为什么？

A. 在Wi-Fi保护访问(WPA)合并的Message Integrity Check (MIC)包括防止一次中间人攻击的一个帧计数器。此错误意味某人网络的设法重赛原始客户端传送的信息，或者也许意味着客户端是有故障的。

如果客户端重复失败MIC检查，控制器禁用在错误被发现在60秒的AP接口的WLAN。第一个MIC故障被记录，并且计时器是对抗措施的被起动的为了enable (event)实施。如果一个随后的MIC故障发生在最近早先故障的60秒以内，则IEEE 802.1X实体作为请求方的STA将deauthenticate或deauthenticate与安全关联的所有STAs，如果其IEEE 802.1X实体作为证明人。

此外，至少60秒，在发现第二个故障后，除IEEE 802.1X消息之外，设备不接收也不传输任何Tkip被加密的数据帧和不接收也传输任何末加密的数据帧，到/从任何对等体周期。如果设备是AP，在此60第二个周期，禁止与TKIP的新的关联;在60第二个周期结束时， AP恢复正常运行并且

允许STAs给(关于)关联。

这防止对加密机制的一次可能的攻击。这些MIC错误在WLC版本不可能被关闭在4.1之前。使用无线局域网控制器版本4.1和以上，有命令更改MIC错误的扫描时期。命令是**设置WLAN安全tkip抑制<0-60 seconds> <wlan id>**。请使用值0为了禁用MIC对抗措施的故障检测。

Q. 此错误信息在我的控制器日志被看到：**[ERROR] dhcp_support.c 357 dhcp_bind() servPort dhcpstate**为什么？

A. 这些错误信息主要被看到，当控制器的服务端口有启用DHCP时，但是从DHCP服务器不收到IP地址。

默认情况下，有一DHCP客户端安装的实际服务端口接口并且通过DHCP寻找地址。WLC尝试为服务端口请求DHCP地址。如果DHCP服务器不是可用的，则DHCP请求服务端口发生故障。所以，这生成错误信息。

解决方法是配置静态IP地址对服务端口(即使服务端口是断开的)或有可用的DHCP服务器分配IP地址到服务端口。若需要然后，请重新载入控制器。

服务端口为控制器的带外管理实际上是后备的和系统恢复和维护在网络故障情形下。它也是活跃的唯一的端口，当控制器在boot模式时。服务端口不能运载802.1Q标记。所以，必须连接它到邻居交换机的一个接入端口。使用服务端口是可选的。

通过服务端口接口控制通信和由对服务端口的系统静态映射。它必须有在一个不同的子网的一个IP地址从管理、AP管理器和所有动态接口。并且，它不可能被映射到备份端口。服务端口能使用DHCP为了获得IP地址，或者它可以分配静态IP地址，但是默认网关不可能分配到服务端口接口。静态路由可以通过远程网络访问的控制器被定义对服务端口。

Q. 我的无线客户端不能连接到无线局域网(WLAN)网络。WiSM接入点(AP)被连接对报告此消息：**APNAV DOSMAC 00:0g:23:05:7d:d0 Slot ID 0MAC 00:00:00:00:00:00**。这是什么意思？

A. 作为访问媒体的情况， MAC控制层检查其网络分配向量(NAV)的值。NAV是计数器居民在表示时间早先帧需要发送其帧的每个位置。在位置能尝试发送帧前， NAV一定零。在帧的发射前，位置计算必要的时间发送根据帧长度和数据速率的帧。位置放置表示在期限字段的这次在帧的报头的值。当位置接收帧时，他们检查此期限字段值并且使用它作为基本类型设置他们对应的NAVs。此进程为发送站保留媒体。

高NAV指示膨胀的NAV值(802.11的虚拟载波侦听机制的)出现。如果报告的MAC地址是00:00:00:00:00:00，很可能被伪装(潜在一次实际攻击)，并且您需要确认此与信息包获取。

Q. 在我们配置控制器并且重新启动它后，我们不能访问控制器在安全的Web (https)模式下。此错误信息收到，当设法访问控制器安全的Web模式时：**Web Web()**。什么是此问题的原因？

A. 可以有与此问题产生关联的几个原因。一常见原因能与控制器的虚拟接口配置有关。为了解决此问题，请去除虚拟接口然后重新生成它用此命令：

```
WLC>config interface address virtual 1.1.1.1
```

然后，请重新启动控制器。在重新启动后控制器，请重新生成webauth认证本地在控制器用此命令：

```
WLC>config certificate generate webauth
```

在此命令中的输出，您应该看到此消息：Web。

现在，您应该能访问控制器的安全的Web模式在重新启动。

Q. 控制器有时报告此IDS分离溢出签名攻击警报消息攻击者的MAC地址是那接入点(AP)被加入对该控制器的有效客户端：IDS 'Disassoc'AP ''x.x.x.x' <AP name>''802.11b/g'' 'x'MAC'hh hh hh hh hh hh''x''x'这发生？

A. 这是由于Cisco Bug ID CSCsg81953 (仅限注册用户)。

IDS分离对有效客户端的溢出攻击有时报告攻击者的MAC地址是那AP被加入对该控制器的地方。

当客户端被关联对AP，但是停止沟通由于卡删除，漫游在范围等等外面对AP， AP将等待直到空闲超时。一旦空闲超时被到达， AP发送该客户端一个分离帧。当客户端不承认分离帧时， AP重新传输帧许多时代(大约60个帧)。控制器的IDS子系统听到这些重新传输和与此消息的戒备。

此Bug在版本4.0.217.0被解决。升级您的控制器版本到此版本为了解决此警报消息有效客户端和APs。

Q. 我收到在控制器的Syslog的此错误信息：[WARNING] apf_80211.c 2408 <xxxx xx xx xx xx xx> [ERROR] apf_utils.c 198 为什么？

A. 实际上，消息表明WLC为在无线设置下的某些所需的数据数据传输比被配置，但是NIC卡错过必需的费率。

如果有数据速率，例如1和2M，必需的集在控制器，但是NIC卡在这些数据速率不连通，您能接受这一种消息。这是NIC卡行为不端。另一方面，如果您的控制器是802.11g是启用的，并且客户端是802.11b(only)卡，这是一个合法消息。如果这些消息不引起任何问题，并且卡能仍然连接，这些消息可以被忽略。如果消息是卡片细节的，则请确定此卡的驱动程序最新。

Q. 此Syslog AP:001f.ca26.bfb4 %LWAPP-3-CLIENTERRORLOG WLAN ID <id>错误信息是在我们的网络的广播。这为什么发生，并且如何终止它？

WLC>config certificate generate webauth

A. 此消息是广播由膝部。这被看到，当您配置了WLAN WLAN的时覆盖功能，并且特定的WLAN没有做通告。

配置ap0.0.0.0为了终止它或您能放置一个特定IP地址，如果有一个系统日志服务器，以便消息是广播到单独服务器。

Q. 我收到在我的无线局域网控制器(WLC)的此错误信息：[ERROR]apf_mm.c 581 00:90:7a:05:56:8a为什么？

A. 通常，此错误信息表明控制器宣布了无线客户端的冲突(即分开的APs宣布他们有客户端)，并且控制器从一个AP没有接受一移交到下。没有维护的网络状况。删除无线客户端并且再有客户端尝试。如果此问题频繁地发生，可以有移动性配置的一个问题。否则，与一个特定客户端或情况有关的它也许是异常情况。

Q. 我的控制器培养此告警消息：'12'。它如何是什么此错误和可以是解决的？

A. 当客户端信噪比(SNR)在特定的无线电时的SNR门限值之下下跌此告警消息被上升。12是覆盖孔检测的默认SNR门限值。

覆盖孔检测与纠正算法确定覆盖孔是否存在，当客户端的SNR级别在一被测量的SNR阈值之下通过。此 SNR 阈值根据两个值变化：AP传输功率和控制器覆盖描出值。

详细，客户端SNR阈值由每个AP的传输功率定义(表示在dbm)，减17dBm的恒定的值，减用户可配置覆盖配置文件值(此值被默认为12 dB)。

- **客户端SNR截止值(|dB|) = [AP 发射功率 (dBm) - 常数 (17 dBm) - 覆盖范围 (dB)]**

此用户可配置覆盖配置文件值可以被获取这样：

1. 在WLC GUI中，请去无线主标题并且为选择WLAN标准在左侧的选择**Network选项**(802.11a或802.11b/g)。然后，请选择在右上方的**自动RF**窗口。
2. 在自动RF全局参数页，请查找配置文件阈值部分。在此部分，您能找到覆盖(3到50 dbm)值。此值是用户可配置覆盖配置文件值。
3. 此值可以被编辑影响客户端SNR门限值。另一个方式影响此SNR阈值将增加传输功率和补偿覆盖孔检测。

Q. 我使用ACS v 4.1和4402无线局域网控制器(WLC)。当WLC尝试MAC验证无线客户端到ACS 4.1时，ACS不能回应ACS并且报告此错误信息：“*内部错误出现*”。我有正确所有我的配置。此内部错误为什么出现？

A. 有一认证涉及的Cisco Bug ID CSCsh62641 (仅限注册用户)在ACS 4.1，其中ACS产生错误信息。

此Bug也许是问题。有补丁程序可用为在应该解决问题的ACS 4.1下载(仅限注册用户)页的此Bug。

Q. Cisco 4400系列无线局域网控制器(WLC)不会引导。此错误信息在控制器收到：**ide 0:4 fatload **(IRQ) dev 0 blk 0 0x51reg 10 **0。为什么？

A. 此错误的原因也许是硬件问题。开TAC案例进一步排除此问题故障。为了开TAC案例，您需要有与Cisco的一个有效合同。参考技术支持为了与Cisco TAC联系。

Q. 无线局域网控制器(WLC)遇到存储器缓冲区问题。一旦存储器缓冲区是充分的，控制器失败并且需要重新启动忆起它联机。这些错误信息在消息日志被看到：Mon Apr 9 10:41:03 2007[ERROR] dtl_net.c 506 Mon Apr 9 10:41:032007[ERROR] sysapi_if_net.c 537 MbufMon Apr 9 10:41:03 2007[ERROR] sysapi_if_net.c 219 MbufGet Mbufs

A. 这归结于Cisco Bug ID CSCsh93980 (仅限注册用户)。此Bug在WLC版本4.1.185.0被解决了。升级您的控制器到为了此软件版本或以上解决此消息。

Q. 我们执行了升级我们的无线局域网控制器(WLC) 4400s对4.1代码，并且我们的Syslog由消息炮击，例如此：`dtl_net.c:1191 50303:55:49.591 DTL-1-ARP_POISON_DETECTED STA [00:17:f2:43:26:93 0.0.0.0] ARP (1)SPA 192.168.1.233/TPA 192.168.1.233`。这些消息指示什么？

A. 当WLAN被标记作为需要时的DHCP这能发生。在这类情况下，通过DHCP收到一个IP地址仅的位置允许联合。静态客户端不允许联合到此WLAN。WLC作为DHCP中继代理并且记录所有位置的IP地址。此错误信息生成，当WLC从位置时收到ARP请求，在WLC从位置收到了DHCP信息包并且记录了其IP地址前。

Q. 当您使用在以太网(PoE)时的功率在Cisco 2106无线局域网控制器， AP无线电不是启用的。`APslot`错误消息。我怎样能修理这个?

A. 此错误信息出现，当交换机，加电接入点，是预标准交换机，但是AP不支持输入电源预标准模式。

Cisco预标准交换机是不支持智能电源管理的一个(IPM)，但是有标准访问访问接入点的足够的功率。

您必须enable (event)对此错误信息被服从功率的**预标准**模式在AP的。这可以从控制器CLI执行用**设置ap功率预标准{enable (event)|功能失效} {全部|Cisco_AP}**命令。

如果升级到从前一版本的软件版本4.1已经配置此should命令，如果必须。但是，很可能，您需要输入新的安装的此命令，或者，如果重置AP对工厂默认值。

这些Cisco预标准15瓦特交换机是可用的：

- AIR-WLC2106-K9
- WS-C3550， WS-C3560， WS-C3750
- C1880
- 2600， 2610， 2611， 2621， 2650， 2651
- 2610XM， 2611XM， 2621XM， 2650XM， 2651XM， 2691
- 2811， 2821， 2851
- 3631 telco， 3620， 3640， 3660
- 3725， 3745
- 3825， 3845

Q. 控制器生成`dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED ARPxx xx. -xxx.x`类似于此。什么此系统消息意味着？

A. 当某些无线客户端发送ARP应答时，网络处理器单元(NPU)需要认识该回复。因此转发ARP应答对NPU，但是WLC软件不应该设法添加此条目到网络处理器。如果它如此，这些消息生成。没有对WLC的功能影响由于此，但是WLC生成此系统消息。

Q. 我安装了并且配置了新的Cisco 2106 WLC。WLC表明温度传感器出故障。当您记录到Web接口在“控制器汇总下时”，说“在内部温度旁边”。一切别的东西看上去通常作用。

A. 内部温度传感器故障是一装饰性一个并且可以用对WLC版本4.2.61.0的升级解决。

在07/01/2007以后526被构件的在或WLC 2106和WLC能使用从另一个供应商的温度传感器芯片。此新的传感器晚于4.2版本良好工作，但是不是与软件兼容。因此，更旧的软件不能读温度并且显示此错误。其他控制器功能没有影响的是受此缺陷的。

有已知Cisco Bug ID CSCsk97299 (仅限注册用户)与此问题有关。此Bug在WLC版本4.2版本注释被提及。

Q. 我获得radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND WLAN <WLAN ID>RADIUS-所有Ssid的"消息。此消息甚而为不使用AAA服务器的Ssid出现。

A. 此错误信息意味着控制器没有能联系默认RADIUS服务器或一个未被定义。

此工作情况的一个可能的来源是Cisco Bug ID CSCsk08181 (仅限注册用户)，在版本4.2被解决了。升级您的控制器到版本4.2。

Q. Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL 1MAC错误信息出现在无线局域网控制器(WLC)。这说明了什么?

A. 这意味着控制器有一个错误，当发送了一个CPU被发出的信息包时。

Q. 这些错误信息出现在无线局域网控制器(WLC) ：

- Jul 10 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL 'cliWebInitParms.cfg'
- Jul 10 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL 'rfidInitParms.cfg'
- Jul 10 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL 'dhcpParms.cfg'
- Jul 10 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL 'bcastInitParms.cfg'
- Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED sshpmInitParms.cfg-fp_main_task Id:11ca7618
- Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED bcastInitParms.cfg-fp_main_task Id:11ca7618

这些错误信息指示什么？

A. 这些消息是供参考消息并且是正常引导程序程序的一部分。这些消息出现由于疏忽读或删除几个不同的配置文件。当没找到时特定配置文件或，如果配置文件不可能读，每个进程的，例如，设置顺序派出此消息没有DHCP服务器设置，没有标记(RF ID)设置，等等。这些是可能安全被忽略的LOW严重性消息。这些消息不中断控制器的操作。

Q. HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN 00:14:XX:02:XX:XXAP错误消息。这说明了什么?

A. 这意味着执行恶意遏制功能的AP不再是可用的，并且控制器找不到所有适当的AP执行恶意遏制。

Q. DTL-1-ARP_POISON_DETECTED STA [00:01:02:0e:54:c4 0.0.0.0] ARP (1)SPA 192.168.1.152/TPA 192.168.0.206系统消息出现在无线局域网控制器。此消息暗示什么？

A. 很可能，系统发现ARP伪装或毒害。但是，此消息不一定暗示所有有恶意ARP伪装发生了。当这些情况是真的，消息出现：

- WLAN配置有需要的DHCP，并且一个客户端设备，在联合在该WLAN以后，传送ARP消息，不用第一个完成的DHCP。这可以是正常行为;例如，它能发生，当客户端静态对演讲时，或者，当客户端拿着从一个前期关联时的一个有效DHCP租约。错误信息能看起来象此示例：

```
WLC>config certificate generate webauth
```

此情况效果是客户端无法发送或收到所有数据流量，直到它DHCPs通过WLC。请参见Cisco无线LAN控制器系统信息指南的DTL Messages Section欲知更多信息。

Q. 膝部不使用在以太网(POE)的功率启动。我看到注册无线局域网控制器：

```
AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power
```

问题是什么？

A. 这能发生，如果没有正确地配置在以太网(POE)设置的功率。当被转换了成轻量级模式，例如，AP1131或AP1242或者一1250系列接入点时的接入点由被连接到Cisco PRE智能电源管理的馈电器供给动力(PRE IPM)交换机，您需要配置在以太网(PoE)，亦称内嵌电源的功率。

参考配置在以太网的功率关于如何配置在以太网(POE)的功率的更多信息。

Q. 您看到在无线局域网控制器(WLC)的此消息：

```
*Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6
```

这说明了什么?

A. 轻量级接入点跟随某一算法查找控制器。发现和在轻量AP (LAP)注册加入进程详细解释到无线局域网控制器(WLC)

此错误信息在WLC被看到，当收到发现请求时，在到达了其最大数量AP容量后。

如果没有配置LAP的主要控制器或，如果其新的箱外LAP，派出LWAPP发现请求到所有可及的控制器。如果发现请求到达运行在其充分的AP容量的控制器， WLC获得请求并且意识到在其最大数量AP容量和不回答请求并且产生此错误。

Q. 在哪里能找到关于LWAPP系统消息的更多信息？

A. 参考Cisco无线LAN控制器系统信息指南， 4.2关于LWAPP系统消息的更多信息。

Q. webauth错误信息的出现在无线局域网控制器(WLC)。这说明了什么?

A. WLC不能装载一个自定义Web认证/转接套件，如果任何一个被捆绑的文件有非常地比30个字符在文件名，包括文件扩展。定制的Web auth套件有文件名的30个字符限制。保证在套件内的文件名比30个字符不极大。

Q. 无线局域网控制器(WLCs)，运行5.2或6.0代码以很大数量的AP组， Web GUI可能不显示所有被配置的AP组。问题是什么？

A. 缺少AP组能被看到是否使用CLI显示WLAN AP组发出命令。

设法添加一个另外的AP组到列表。例如， 51个AP组配置的和第51失踪(第3)页。添加第52个组，并

且第3页应该出版于Web GUI。

为了解决此问题，升级到WLC版本7.0.220.0。

Related Information

- Cisco 无线 LAN 控制器配置指南 4.0 版
- WiSM 故障排除常见问题
- 无线 LAN 控制器 (WLC) 故障排除常见问题
- 无线支持页
- Technical Support & Documentation - Cisco Systems