查看无线局域网控制器(WLC)错误和系统消息常见问题

目录

简介

本文档介绍有关思科无线局域网(WLAN)控制器(WLC)的错误消息和系统消息的常见问题(FAQ)。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

错误消息常见问题解答

问：开始使用Cisco 4404 WLC将200多个接入点(AP)从Cisco IOS®软件转换为轻量AP协议(LWAPP)。48个AP的转换已完成，WLC上收到的消息显示：`[] spam_lrad.c 42121APAP。` 为什么会出现此错误？

A.您必须创建其他AP管理器接口才能支持超过48个AP。否则，您将收到如下错误消息：

```
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，并配置其他 AP 管理器接口未使用的主/备份端口。您必须创建另一个AP管理器接口以启动其他AP。但是，请确保每个管理器的主端口和备份端口配置不会重叠。换句话说，如果 AP 管理器 1 使用端口 1 作为主端口，端口 2 作为备份端口，则 AP 管理器 2 必须使用端口 3 作为主端口，端口 4 作为备份端口。

问：我有一台无线局域网控制器(WLC)4402，我使用1240个轻量接入点(LAP)。我在WLC上启用了128位加密。当我在WLC上选择128位WEP加密时，我收到一个错误消息，指出1240s不支持128位：`[ERROR] spam_lrad.c 12839WEP128CISCO AP xx:xx:xx:xx:xx:xx:xx:xx:xxSSID`型。为什么我会收到此错误消息？

A.WLC上显示的密钥长度实际上是共享密钥中的位数，不包括初始化向量(IV)的24位。包括 Aironet 产品在内的许多产品都称它为 128 位 WEP 密钥。实际上它包括 104 位密钥及 24 位 IV。因此，在 WLC 上采用 128 位 WEP 加密时，必须启用的是 104 位密钥大小。

如果您在 WLC 上选择 128 位密钥大小，它实际上是 152 位 (128 + 24 IV) WEP 密钥加密。仅 Cisco 1000 系列 LAP（AP1010、AP1020、AP1030）支持使用 WLC 128 位 WEP 密钥设置。

问：为什么11xx、`12xx13xxAP128WEPWLAN`当我尝试在WLC上配置WEP时，会出现什么错误消息？

答：在无线LAN控制器上，当您选择静态WEP作为第2层安全方法时，您有以下选项或WEP密钥大小。

- 未设置
- 40 位
- 104 位
- 128 位

这些密钥大小值不包括与 WEP 密钥连接在一起的 24 位初始化矢量 (IV)。因此，对于64位 WEP，您需要选择**40位**作为WEP密钥大小。控制器会将 24 位 IV 添加到其上，以构成 64 位 WEP 密钥。同样，对于128位WEP密钥，请选择**104位**。

控制器也支持 152 位 WEP 密钥（128 位 + 24 位 IV）。11xx、12xx 和 13xx 型号 AP 不支持此配置。因此，当您尝试用 144 位配置 WEP 时，控制器会显示消息，表示 11xx、12xx 和 13xx 型号 AP 不支持此 WEP 配置。

Q.客户端无法验证配置为WPA2的WLAN，并且控制器显示`apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILEDRSNWARP IERSNWLANRSN(WPA2)MobileStation:00:0c:f1:0c:51:22, SSID:<`错误消息。为什么我会收到此错误消息？

A.这主要是客户端不兼容造成的。请尝试采用以下步骤来修复此问题：

- 检查客户端对于 WPA2 是否经过 Wi-Fi 认证，并检查客户端的 WPA2 配置。
- 检查数据表以查看客户端实用程序是否支持 WPA2。安装供应商发布的所有补丁程序以支持 WPA2。如果使用Windows实用程序，请确保已安装Microsoft的WPA2补丁以支持WPA2。有关详细信息，请参阅Microsoft支持。
- 升级客户端驱动程序和固件。
- 关闭 WLAN 上的 Aironet 扩展功能。

问：重新启动WLC后，我收到`Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event(s)s found is violated by the radio 00:XX:XX:XX:XXand detet11 interface at slot 0 of AP 00:XX:XX:XX300`为什么会发生此错误，我该如何消除它？

A.当启用MFP的LAP检测到具有错误MIC值的帧时，将显示此错误消息。有关MFP的详细信息，请参阅具有WLC和LAP的基础设施管理帧保护(MFP)配置示例。执行以下四个步骤之一：

1. 检查并删除网络中将产生无效帧的所有恶意或无效的 AP 或客户端。
2. 禁用基础架构 MFP，如果不启用 MFP，移动组中的其他成员（如 LAP）可从未启用 MFP 的组中其他 WLC 的 LAP 获得管理帧。有关移动组的详细信息，请参阅无线LAN控制器(WLC)移动组常见问题。
3. WLC 版本 4.2.112.0 和 5.0.148.2 中已修复此错误。将 WLC 升级到以上版本之一。
4. 最后，可尝试重新载入生成此错误消息的 LAP。

问：客户端AIR-PI21AG-E-K9已成功与采用可扩展身份验证协议 — 通过安全隧道的灵活身份验证(EAP-FAST)的接入点(AP)关联。然而，当关联的 AP 关闭时，客户端不漫游到另一个 AP。此消息持续显示在控制器消息日志中："`Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922 — 200662 14:48:49 [] apf_ms.c 255700:40:96:ad:75:f4`"。为什么？

A.当客户端卡需要漫游时，它会发送身份验证请求，但无法正确处理密钥（不会通知AP/控制器，不会应答重新身份验证）。

Cisco bug IDCSCsd02837中记录了此错误。此 Bug 已采用 Cisco Aironet 802.11a/b/g 客户端适配器安装向导 3.5 修复。

通常，由于也会出现Unable to delete username for mobilemessage:

- 多个客户端设备使用了同一个用户名。
- 用于该 WLAN 的认证方法具有外部匿名身份。例如，在 PEAP-GTC 或 EAP-FAST 中，可以将一个通用用户名定义为外部（可视）身份，而将真正的用户名隐藏在客户端与 RADIUS 服务器之间的 TLS 隧道中，因此控制器既看不到也无法使用它。此时，会出现此消息。这个问题在某些第三方客户端和某些老的固件客户端中更常见。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：当我在6509交换机中安装新的无线服务模块(WiSM)刀片并通过Microsoft IAS服务器实施受保护的可扩展身份验证协议(PEAP)时，我收到以下错误： **`*Mar 1 00:00:23.526: %LWAPP-5-CHANGED: LWAPP DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT .Reload Reason: FAILED CRYPTO INIT. *Mar 1 00:00:23.700: %LWAPP-5-CHANGED: LWAPPDOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED: LWAPPDISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:lwapp_cryinit keys_and_certsSSC*Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG:*Mar 1 00:00:23.557: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT .`** **为什么？**

A.RADIUS和dot1x调试显示WLC发送访问请求，但是没有来自IAS服务器的响应。完成以下步骤以解决该问题：

1. 检查并验证 IAS 服务器配置。
2. 检查日志文件。
3. 安装能提供认证详细信息的软件（如 Ethereal）。
4. 终止然后启动 IAS 服务。

问：轻量接入点(LAP)未注册到控制器。可能是什么问题？我在控制器上看到以下错误消息： **`Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0Thu Feb 3 03:20:47 2028AP 00:0B:85:68:F4:F0。`**

A.接入点(AP)向WLC发送轻量接入点协议(LWAPP)加入请求时，会将其X.509证书嵌入到LWAPP消息中。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，它将使用AP公钥验证X.509证书的签名，并检查证书是否由受信任的证书颁发机构颁发。它还查看AP证书有效间隔的开始日期和时间，并将该日期和时间与其自己的日期和时间进行比较。

此问题可能是由于 WLC 上时钟设置不正确引起的。要在WLC上设置时钟，请发出 show time 和 config time 命令。

问.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)日志显示类似以下内容的消息： **`LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01。`** **为什么？**

A.如果AP和WLC之间的LWAPP隧道经过MTU小于1500字节的网络路径，您可能会收到此错误消息。这会导致 LWAPP 数据包的分段。这是控制器中的一个已知 Bug。请参阅Cisco bug IDCSCsd39911。

解决办法是将控制器固件升级到 4.0(155)。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我想在内部控制器与非军事区(DMZ)上的虚拟锚点控制器之间建立访客隧道。然而，当用户试

图与访客 SSID 关联时，用户无法如预期的那样从 DMZ 接收 IP 地址。所以，用户流量没有通过隧道传输给 DMZ 中的控制器。debug mobile handoff命令的输出显示如下消息：`WLAN <Wlan ID>IP<Ip>`。问题出在哪里？

A.访客隧道为访客用户访问企业无线网络提供额外的安全性。这有助于确保访客用户首先必须通过公司防火墙才能访问公司网络。当用户与指定为访客 WLAN 的 WLAN 关联时，用户流量通过隧道传输到位于公司防火墙之外的 DMZ 中的 WLAN 控制器。

在此情况中，该访客隧道未能如预期那样正常工作的原因可能有几个。如debugcommand输出所示，问题可能在于内部和DMZ控制器中为该特定WLAN配置的任何安全策略不匹配。请检查安全策略以及其他设置（如会话超时设置）是否匹配。

此问题的另一个常见原因是，对于该特定WLAN，DMZ控制器未锚定到其自身。为使访客隧道正常工作，且 DMZ 能管理属于访客 WLAN 的用户的 IP 地址，必须对该特定 WLAN 执行正确锚定。

问：我在2006无线局域网控制器(WLC)上看到许多"控制器上的CPU接收组播队列已满"消息，但在4400 WLC上看不到这些消息。为什么？我已经在控制器上禁用了组播。2006 与 4400 WLC 平台的组播队列限制有何区别？

A.因为控制器上禁用了组播，导致此警报的消息可以是地址解析协议(ARP)消息。2000 WLC 与 4400 WLC 在队列深度（512 数据包）上没有区别。不同之处在于 4400 NPU 过滤 ARP 数据包，而 2006 在软件中完成所有操作。这解释为什么在 2006 WLC 中看到以上消息，但 4400 WLC 中没有。44xx WLC 通过硬件（通过 CPU）处理组播数据包。2000 WLC 通过软件处理组播数据包。CPU 处理比软件处理效率更高。所以，4400 的队列清除速度更快，而 2006 WLC 在收到很多以上消息时需要花更多时间来处理。

问：我看到"`[SECURITY] apf_foreignap.c 763: STA [00:0A:E4:36:1F:9B]1AP`"息。此错误意味着什么？我需要采取什么步骤来解决它？

A.当控制器收到MAC地址的DHCP请求时，如果控制器没有状态机，则会看到此消息。在网桥或运行虚拟机（如 VMWare）的系统中，经常会出现此消息。控制器听取 DHCP 请求，因为执行 DHCP 监听，因此知道哪些地址与附加到其接入点 (AP) 的客户端关联。无线客户端的所有流量都通过控制器。当数据包的目的地是无线客户端时，它会去往控制器，然后通过轻量接入点协议 (LWAPP) 隧道，从 AP 到达客户端。为了缓解此消息，可以做的一件事是只允许控制器上使用的 VLAN连接到中继上，该中继在交换机上使用**switchport vlan** allowcommand连接到控制器。

问：为什么在控制台上看到此错误消息：`Msg 'Set Default Gateway' of System Table failed Id = 0x0050b986 error value = 0xfffffffc`?

A.这可能是由于CPU负载过高。当控制器 CPU 负载很重时，例如当它执行文件复制或其他任务时，没有时间处理 NPU 为响应配置消息而发送的所有 ACK。此时，CPU 会生成错误消息。不过，此错误消息不会影响服务或功能。

有关详细信息，请参阅思科无线LAN控制器。

问：我在无线控制系统(WCS)上收到以下有线等效保密(WEP)密钥错误消息：在站点配置的WEP密钥`MAC"xx:xx:xx:xx:xx:xx"APMAC"xx:xx:xx:xx:xx:xx"ID"1"`。然而，我的网络中并未使用 WEP 作为安全参数，只使用了 Wi-Fi Protected Access (WPA)。为什么我会收到这些 WEP 错误消息？

答：如果您的所有安全相关配置都非常完美，那么您现在收到的消息就是由于漏洞所致。控制器中存在某些已知 Bug。请参阅Cisco bug IDCSCse17260和Cisco，但ID为CSCse11202，其中说明"在站点配置的WEP密钥可能分别与WPA和TKIP客户端错误"。实际上，Cisco Bug ID **CSCse17260**是Cisco Bug ID **CSCse11202的副本**。WLC版本3.2.171.5**已提**供适用于思科但ID为CSCse11202的修

补程序。

注意：最新的WLC版本已针对这些漏洞进行了修复。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我使用外部RADIUS服务器通过控制器验证无线客户端。控制器定期发送此错误消息：无RADIUS。为什么会看到这些错误消息？

A.当请求从WLC发送到RADIUS服务器时，每个数据包都有一个序列号，WLC期望收到响应。如果没有响应，则显示一条消息`show radius-server not responding`。

WLC 收到 RADIUS 服务器响应的默认时间为 2 秒。这是在WLC GUI的**Security > authentication-server**下设置的。最大值为 30 秒。因此，将此超时值设置为最大值会非常有用，这样可以解决此问题。

有时，RADIUS服务器**对来自WLC的**请求数据包执行“静默丢弃”。RADIUS 服务器可以因证书不匹配以及其他几个原因而拒绝这些数据包。这是服务器执行的有效操作。此外，在这种情况下，控制器可以将RADIUS服务器标记为不响应

为了克服静默放弃问题，请在WLC中禁用**主动**故障切换功能。

如果在WLC中启用了**主动**故障切换功能，则WLC过于主动，无法将AAA服务器标记为不响应。但是，不能执行此操作，因为AAA服务器无法仅响应该特定客户端（它执行静默丢弃）。它可以对其他具有效证书的有效客户端进行响应。但是，WLC仍然可以将AAA服务器标记为不响应且无法正常工作。

要克服此问题，请禁用**主动**故障切换功能。从控制器CLI发出**config radius aggressive-failover disable**command以执行此操作。如果禁用了此功能，则当连续三个客户端都未能从 RADIUS 服务器收到响应时，控制器只会将故障切换到下一个 AAA 服务器。

问：多个客户端无法关联到LWAPP，并且控制器记录`IAPP-3-MSGTAG015: iappSocketTask: iappRecvPkt returned error`消息。为什么会发生这种情况？

答：这主要是因为支持CCX v4但运行早于10.5.1.0的客户端捆绑版本的英特尔适配器出现问题。要修复此问题，可将软件升级到 10.5.1.0 或更高版本。有关此错误消息的详细信息，请参阅Cisco bug IDCSCsi91347。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我在无线局域网控制器(WLC)上看到以下错误消息：`Reached Max EAP-Identity Request retries(21) for STA 00:05:4e:42:ad:c5`。为什么？

A.当用户尝试连接到EAP保护的WLAN网络并且未通过预配置的EAP尝试次数时，会出现此错误消息。当用户无法进行身份验证时，控制器会排除客户端，并且客户端无法连接到网络，直到排除计时器过期或被管理员手动覆盖。

排除会检测单个设备执行的认证尝试。当该设备达到最大失败次数时，将不再允许该 MAC 地址进行关联。

以下情况下将发生排除：

- 共享认证连续 5 次认证失败后（不提供第 6 次尝试）
- MAC 认证连续 5 次关联失败后（不提供第 6 次尝试）
- 连续 3 次 EAP/802.1X 认证失败后（不提供第 4 次尝试）
- 任何外部策略服务器故障 (NAC)
- 任何 IP 地址复制实例
- 连续 3 次 Web 认证失败后（不提供第 4 次尝试）

表示客户端排除时间长短的计时器是可以配置的，并且可以在控制器或 WLAN 级别启用或禁用排除。

问：我在无线局域网控制器(WLC)上看到此错误消息：交换机WLCSCH01/10.0.16.5生成严重级别为1的类别交换机警"10.0.16.5"RADIUS server(s) are not responding to authentication requests。问题是什么？

A.这可能是由于Cisco Bug ID CSCsc05495。由于此 Bug 的存在，控制器会定期将不正确的 AV 对（属性 24，“state”）插入认证请求消息中，这违反了 RADIUS RFP 并会造成某些认证服务器出现问题。此 Bug 在 3.2.179.6 中已修复。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我收到“Noise Profile failure（噪音配置文件故障）”消息，位于“Monitor（监控）”>“802.11b/g Radios（802.11b/g无线电）”下。我想知道为什么会看到此 FAILED 消息？

A.在WLC完成测试结果之后，并与当前设置的阈值比较，设置Noise Profile FAILED/PASSED状态。默认情况下，噪声值设置为 -70。FAILED 状态表明已超出该特定参数或接入点 (AP) 的阈值。您可以调整配置文件中的参数，但建议您在清楚地了解网络设计及其如何影响网络性能之后更改设置。

在**802.11a Global Parameters > Auto** RFand **802.11b/g Global Parameters > Auto RFpages上为所有AP全局设置**Radio Resource Management(RRM)PASSED/FAILED阈值。在**802.11 AP Interfaces > Performance** Profilepage上为此AP**单独设置**RRM PASSED/**FAILED阈**值。

问：我不能将端口2设置为AP管理器接口的备份端口。返回的错误消息如下：Could not set port configuration。我可以将端口 2 设置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管理器没有备份端口。较早版本中支持该设置。自版本 4.0 起，不再支持 AP 管理器接口的备份端口。通常，必须在每个端口上配置一个AP管理器（无备份）。如果使用链路聚合 (LAG)，则只有一个 AP 管理器。

必须为系统端口 1 分配静态（或永久）AP 管理器接口，且该接口必须具有唯一 IP 地址。它不能映射到备份端口。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。

问：我看到以下错误消息：AP '00:0b:85:67:6b:b0''00:13:02:8d:f6:41''1'WPA MICCounter measures have been activated and traffic has been suspended for 60 seconds。为什么？

A.消息完整性检查(MIC)包含在Wi-Fi保护访问(WPA)中，可防止中间人攻击的帧计数器。此错误表示网络中的某个人想要重播原始客户端发送的消息，或者可能表示客户端出现故障。

如果客户端的 MIC 检查反复失败，控制器会对检测到错误 60 秒的 AP 接口禁用 WLAN。将记录第

一次 MIC 失败，并启动计时器以强制实施应对措施。如果在最近一次故障发生后的60秒内发生后续MIC故障，则其IEEE 802.1X实体充当请求方的STA如果其IEEE 802.1X实体充当验证方，则该STA应使自身无效或使所有具有安全关联的STA失效。*

此外，设备在检测到第二个故障后的至少60秒内不接收或传输任何TKIP加密数据帧，也不接收或传输任何对等体发送或传输任何除IEEE 802.1X消息以外的未加密数据帧。如果设备是AP，则在此60秒时间段内不允许与TKIP进行新的关联；在60秒时间段结束时，AP将恢复正常操作并允许STA进行（重新）关联。

这样可防止对加密方案的可能攻击。在低于 4.1 的 WLC 版本中，这些 MIC 错误无法关闭。在无线局域网控制器版本 4.1 及更高版本中，有一个命令可更改 MIC 错误的扫描时间。命令**isconfig wlan security tkip hold-down <0-60 seconds> <wlan id>**。使用值 0 可为应对措施禁用 MIC 故障检测。

*Invalidate：结束身份验证。

问：此错误消息出现在我的控制器日志中：`[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed`。为什么？

A.当控制器的服务端口启用了DHCP但未从DHCP服务器接收IP地址时，最容易看到这些错误消息。

默认情况下，物理服务端口接口安装有 DHCP 客户端并通过 DHCP 寻找地址。WLC 尝试为该服务端口请求 DHCP 地址。如果 DHCP 服务器不可用，则服务端口的 DHCP 请求失败。因而会产生此错误消息。

应急方案是为该服务端口配置一个静态 IP 地址（即使该服务端口已断开），或者让可用的 DHCP 服务器为该服务端口分配一个 IP 地址。然后，如有必要，重新载入控制器。

该服务端口实际上是为发生网络故障时的控制器带外管理和系统恢复而预留的。它也是当控制器处于启动模式时唯一的活动端口。该服务端口不能传输 802.1Q 标记。所以，它必须连接到相邻交换机的接入端口。是否使用该服务端口是可选的。

该服务端口接口控制通过的通信，并由系统静态映射到服务端口。在不同管理子网、AP 管理器和任意动态接口上，它必须具有 IP 地址。此外，它不能映射到备份端口。服务端口可以使用 DHCP 获取 IP 地址，或为其分配一个静态 IP 地址，但不能将默认网关分配给该服务端口接口。可通过控制器定义静态路由，以对服务端口进行远程网络访问。

问：我的无线客户端无法连接到无线局域网(WLAN)网络。接入点(AP)所连接的WiSM报告以下消息：`Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00`。这是什么意思？

A.作为访问介质的条件，MAC层会检查其网络分配矢量(NAV)的值。NAV 是驻留在每个站点上的计数器，用于表示上一帧发送其帧所需的时间。在站点可以尝试发送帧之前，NAV 值必须为零。在传输帧之前，站点根据帧长度和数据速率计算发送帧所需的时间量。站点在帧报头的持续时间字段中放入一个表示该时间的值。当其他站点收到帧时，会检查此持续时间字段值并以此为基础设置相应的 NAV。此过程保留发送站的介质。

高 NAV 意味着 NAV 值过大（802.11 的虚拟载波侦听机制）。如果报告的MAC地址为00:00:00:00:00:00，则它可能是伪装的（可能是真实攻击），您需要通过数据包捕获确认这一点。

问：我配置控制器并重新启动它后，无法在安全Web(https)模式下访问控制器。当我尝试访问控制器安全Web模式时收到此错误消息：`Secure Web: Web Authentication Certificate not found(error)`。出现该问题的原因是什么？

答：有几个原因与此问题相关。一个常见的原因是控制器的虚拟接口配置导致的。为解决该问题，可删除该虚拟接口，然后用以下命令重新生成接口：

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

然后，请重新启动控制器。控制器重新启动后，在控制器上采用以下命令重新生成本地 Webauth 证书：

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

在此命令的输出中，您可以看到以下消息：`Web Authentication certificate has been generated`。

现在，您可以在重新启动后访问控制器的安全Web模式。

Q.控制器有时会报告针对有效客户端的此IDS取消关联泛洪签名攻击警报消息，其中攻击者MAC地址是加入该控制器的接入点(AP)的地址：警"x.x.x.x"AP"<AP>""802.11b/g"IDS""The Signature description is 'Disassociation flood', with precedence 'x'.MAC'hh:hh:hh:hh:hh''x''x'。为什么会发生这种情况？

A.这是由于Cisco bug IDCSCsg81953（仅限注册用户）导致的。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

有时会报告针对有效客户端的IDS解除关联泛洪攻击，其中攻击者MAC地址是加入该控制器的AP的MAC地址。

当客户端与AP关联但由于移除卡而停止通信时，它会漫游到覆盖范围之外，以此类推，到AP，AP会一直等待，直到空闲超时。一旦达到空闲超时，AP 向该客户端发送取消关联帧。如果客户端不确认取消关联帧，则 AP 会多次重复发送该帧（大约 60 次）。控制器的 IDS 子系统收到这些重复发送的帧，并通过此消息提出警报。

此 Bug 在版本 4.0.217.0 中已解决。为消除针对有效客户端和 AP 的此警报消息，可将您的控制器升级到该版本。

Q.我在控制器的系统日志中收到以下错误消息：[] apf_80211.c 2408<xx:xx:xx:xx:xx:xx:xx:xx> [] apf_utils.c 198。为什么？

A.实际上，`Missing Supported Rate`消息表明WLC在无线设置下配置为某些所需的数据速率，但NIC卡缺少所需速率。

如果您在控制器上设置了必需的数据速率（如 1 和 2M），但 NIC 卡未对这些数据速率进行通信，那么您会收到此类消息。这属于 NIC 卡的错误行为。另一方面，如果您的控制器启用了 802.11g，且客户端只有 802.11b 卡，那么这是一个合法消息。如果此消息不引起任何问题，并且卡仍然可以连接，则此消息可以忽略。如果此消息是针对某个卡的，那么请确保卡的驱动程序是最新的。

问：此系统日志AP:001f.ca26.bfb4: %LWAPP-3-CLIENTRORLOG: Decode Msg: could not match WLAN ID <id>播。为什么会发生这种情况，该如何阻止？

A.此消息由LAP广播。当您为WLAN配置了WLAN覆盖功能并且未通告该特定WLAN时，就会看到这

种情况。

`ap syslog host global 0.0.0.0`以将其停止，或者您可以放置特定IP地址（如果您有syslog服务器），以便只将消息广播到服务器。

问：我在无线局域网控制器(WLC)上收到以下错误消息：`[]apf_mm.c 581 00:90:7a:05:56:8a`。为什么？

答：通常，此错误消息表示控制器已通告无线客户端的冲突（即，各个AP通告它们拥有该客户端），并且控制器未收到从一个AP到另一个AP的切换操作。没有要保持的网络状态。删除无线客户端，然后让客户端重试。如果此问题频繁发生，则可能是移动配置有问题。否则，它可能是与特定客户端或条件相关的异常。

问：我的控制器发出此警报消息：`"12"`。此错误是什么？如何解决此问题？

A.当客户端信噪比(SNR)降至低于特定无线电的SNR阈值的值时，会发出此警报消息。12是覆盖空洞检测的默认SNR阈值。

当客户端的SNR水平小于给定的SNR阈值时，覆盖空洞检测与校正算法确定是否存在覆盖空洞。此SNR阈值取决于两个值：AP发射功率和控制器覆盖范围配置文件值。

具体而言，客户端SNR阈值由每个AP的发射功率（以dBm表示）减去常量值17dBm，再减去用户可配置的覆盖配置文件值来定义（此值默认为12 dB）。

- **客户端SNR截止值(|dB|)= [AP发射功率(dBm) — 常量(17 dBm) — 覆盖配置文件(dB)]**

可通过以下方式访问此用户可配置的覆盖配置文件值：

1. 在WLC GUI中，转至无线的主标题，并为左侧选择的WLAN标准（802.11a或802.11b/g）选择**Network**选项。然后，在窗口右上角选择**Auto RF**。
2. 在Auto RF Global parameters页中，找到Profile Thresholds部分。在此部分中，可以找到Coverage 值（3 到 50 dbm）。该值是用户可配置的覆盖配置文件值。
3. 可编辑此值以修改客户端 SNR 阈值。影响此SNR阈值的另一种方法是增加发射功率和补偿覆盖空洞检测。

问：我使用ACS v 4.1和4402无线局域网控制器(WLC)。当WLC尝试对ACS 4.1的无线客户端进行MAC身份验证时，ACS无法响应ACS并报告以下错误消息："*Internal error has occurred*"。我所有的配置都正确。为什么会发生此内部错误？

答：ACS 4.1中存在与身份验证相关的Cisco bug IDCSCsh62641，其中ACS显示`Internal error has occurr`error消息。

此Bug可能是问题。在ACS 4.1下载站点上有一个针对此Bug的修补程序，可以修复此问题。

> **注意**：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：Cisco 4400系列无线局域网控制器(WLC)无法启动。控制器上收到此错误消息：`** Unable to use ide 0:4 for fatload ** Error(no IRQ)dev 0 blk 0: status 0x51 Error reg: 10 ** Cannot read from device 0`。为什么？

答：此错误的原因可能是硬件问题。打开TAC案例以进一步解决此问题。要创建TAC案例，您需要与思科签订有效的合同。如需联系Cisco TAC，请参阅技术支持。

问：无线LAN控制器(WLC)遇到内存缓冲区问题。一旦内存缓冲区已满，控制器就会崩溃，需要重新启动才能使其重新联机。以下错误消息显示在消息日志中：Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Out of System buffers Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537MbufMon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGetMbufs。为什么？

A.这是由Cisco Bug IDCSCsh93980引起的。WLC 版本 4.1.185.0 中已解决此 Bug 问题。将控制器升级到此软件版本或更高版本，以克服此消息。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我执行无线局域网控制器(WLC)4400到4.1代码的升级，我们的系统日志被以下消息淹没：May03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP(op 1)SPA 192.168.1.233/TPA 192.168.1.233。这些消息表示什么？

A.当WLAN标记为需要DHCP时，可能会出现这种情况。在这种情况下，只允许通过DHCP接收IP地址的工作站进行关联。静态客户端不允许关联到此 WLAN。WLC充当DHCP中继代理并记录所有站点的IP地址。当WLC收到来自站点的ARP请求时，在WLC收到来自站点的DHCP数据包并记录其IP地址之前，生成此错误消息。

问：在Cisco 2106无线局域网控制器上使用以太网供电(PoE)时，AP无线电设备未启用。AP。显示错误消息。我如何修复此错误？

A.当为接入点供电的交换机是预标准交换机，但AP不支持预标准输入电源模式时，会出现此错误消息。

Cisco试行标准交换机不支持智能电源管理(IPM)，但是对于标准接入点有足够的功率。

您必须在**出现此**错误消息的AP上启用Pre-Standard电源模式。这可以通过控制器CLI执行，**config ap power pre-standard {enable |禁用} {all | Cisco_AP}命**令。

如果从以前版本升级到软件版本4.1，则必须已经配置此命令（如果需要）。但是，可能需要为新安装输入此命令，或者如果您将AP重置为出厂默认设置。

您可以使用以下 Cisco 试行标准 15 W 交换机：

- 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

问：控制器生成dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILEDxx:xx.-xxx.xARPsyslog似。此系统日志消息意味着什么？

答：当某些无线客户端发送ARP应答时，网络处理器单元(NPU)需要知道该应答。因此，ARP应答会转发到NPU，但WLC软件不得尝试将此条目添加到网络处理器。如果是，则生成这些消息。因此，WLC不会受到功能影响，但WLC会生成此系统日志消息。

问：我安装并配置了一个新的Cisco 2106 WLC。WLC指示温度传感器发生故障。当您登录Web界面中的"控制器摘要"时，内部温度旁示"传感器故障"。其他一切似乎都运转正常。

答：内部温度传感器故障是表面故障，可通过升级到WLC版本4.2.61.0来解决。

WLC 2106和WLC 526构建于**07/01/2007之上或之**后，**可**使用其他供应商提供的温度传感器芯片。此新传感器工作正常，但与4.2版之后的软件不兼容。因此，早期的软件无法读取温度并显示此错误。所有其他控制器功能不受此缺陷的影响。

存在与此问题相关的已知Cisco Bug IDCSCsk97299。WLC版本4.2的版本说明中提到了此Bug。

注意：只有注册的思科用户才能访问内部思科漏洞信息和工具。

问：我收到radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Could not find appropriate RADIUS server for WLAN <WLAN ID> - unable to find a default server"消息。即使对于不使用AAA服务器的SSID，也会出现此消息。

A.此错误消息表示控制器无法联系默认RADIUS服务器，或者未定义该服务器。

此行为的一个可能原因是已在版本4.2中解决的Cisco bug IDCSCsk08181。请将您的控制器升级到版本 4.2。

问：Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL1MAC(WLC)上。这说明了什么？

A.这意味着控制器在发送来自CPU的数据包时出错。

问：无线局域网控制器(WLC)上会显示以下错误消息：

- 71014:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL"cliWebInitParms.cfg"
- 71014:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL"rfidInitParms.cfg"
- 71014:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL"dhcpParms.cfg"
- 71014:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL"bcastInitParms.cfg"
- 31816:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILEDsshpmInitParms.cfg-Process: Name:fp_main_task Id:11ca7618
- 31816:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILEDbcastInitParms.cfg-Process: Name:fp_main_task Id:11ca7618

问： 这些错误消息有何含义？

A.这些消息是信息性消息，是正常启动过程的一部分。由于读取或删除多个不同配置文件失败，这些消息出现。当找不到特定的配置文件或无法读取配置文件时，每个进程的配置序列都会发出此消息，例如no DHCP server config、no tags(RF ID)config等等。这些是可以安全忽略的低严重性消息。这些消息不会中断控制器的操作。

Q. HE6-WLC01,local0,alert2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN:Unable to keep rogue 00:14:XX:02:XX:XX – AP息。这说明了什么？

A.这意味着执行恶意遏制功能的AP不再可用，并且控制器找不到任何合适的AP来执行恶意遏制。

问：DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP(op 1)received with invalid SPA 192.168.1.152/TPA 192.168.0.206 system消息出现在无线LAN控制器上。此消息意味着什么？

A.系统可能检测到ARP欺骗或中毒。但是，此消息并不一定意味着发生了任何恶意ARP欺骗。当发生以下情况时，会显示此消息：

- WLAN配置了“需要DHCP”，客户端设备在与WLAN关联后，无需首先完成DHCP即可传输ARP消息。这可能是正常行为；例如，当客户端静态寻址时，或当客户端持有先前关联的有效DHCP租用时。错误消息可能看起来如下例所示：

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA
192.168.1.152/TPA 192.168.0.206
```

此情况的作用是客户端无法发送或接收任何数据流量，直到它通过WLC建立DHCP。

有关详细信息，请参阅Cisco无线LAN控制器系统消息指南的DTL消息部分。

问：LAP不使用以太网供电(POE)进行通电。我看到无线局域网控制器上的日志：

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

问： 问题是什么？

答：如果以太网供电(POE)设置配置不正确，则可能会发生这种情况。当已转换为轻量模式的接入点（例如AP1131或AP1242）或1250系列接入点由连接到思科预智能电源管理(pre-IPM)交换机的馈电器供电时，您需要配置以太网供电(PoE)，也称为内联电源。

有关详细信息，请参阅配置以太网供电、以太网支持。

问：您会在无线局域网控制器(WLC)上看到以下消息：

```
*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
```

这说明什么？

A.轻量接入点跟踪特定算法以查找控制器。轻量AP(LAP)注册到无线LAN控制器(WLC)中详细介绍了发现和加入过程。

当WLC在达到最大AP容量后收到发现请求时，会看到此错误消息。

如果LAP的主控制器未配置，或者如果它是新的开箱即用的LAP，它会向所有可到达控制器发送LWAPP发现请求。如果发现请求到达运行在其全部AP容量的控制器，WLC将获取请求，并意识到它已达到最大AP容量，且不响应请求并出现此错误。

问：在哪里可以找到有关LWAPP系统消息的更多信息？

答：有关LWAPP系统消息的详细信息，请参阅Cisco无线LAN控制器系统消息指南，4.2（已停用）。

问：无线局域网控制器(WLC)上显示`Error extracting webauth files`错误消息。这说明了什么？

如果任何捆绑文件文件名超过30个字符（包括文件扩展名），A.WLC无法加载自定义Web身份验证/传递捆绑包。自定义Web身份验证捆绑包的文件名限制为30个字符。确保捆绑包内的文件名不超过30个字符。

问：无线LAN控制器(WLC)运行带有大量AP组的5.2或6.0代码，Web GUI不显示所有已配置的AP组。问题是什么？

A.如果使用CLI，可以看到缺失的AP组 `show wlan ap-groups` 命令。

尝试向列表中添加一个附加的AP组。例如，部署了51个AP组，第51个组丢失（第3页）。添加第52组，第3页必须显示在Web GUI中。

要解决此问题，请升级到WLC版本7.0.220.0。

相关信息

- WiSM 故障排除常见问题
- 无线支持页
- 思科技术支持和下载

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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