无线局域网控制器(WLC)错误和系统消息常见消息

目录

简介

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。

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

Q. 我们打算采用 Cisco 4404 WLC，将 200 多个接入点 (AP) 从 Cisco IOS® 软件转换为轻量接入点协议 (LWAPP)。完成 48 个 AP 的转换后，我们在 WLC 上收到如下消息：**[[ERROR] spam_lrad.c 4212:AP cannot join because the maximum number of APs on interface 1 is reached**为什么会出现此错误？

A. 您必须创建更多的 AP 管理器接口才能支持 48 个以上的 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* 创建第二个 AP 管理器接口才能转换更多的 AP。但是，请确保每个管理器的主端口和备份端口配置不重叠。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。

Q. 我有一个无线局域网控制器 (WLC) 4402，并使用 1240 轻量接入点 (LAP)。我正尝试在 WLC 上启用 128 位加密。当我在 WLC 上选择 128 位 WEP 加密时，收到一条错误消息，表示 1240 不支持 128 位：**[[ERROR] spam_lrad.c 12839:Not creating SSID mde on CISCO AP xx:xx xx xx xx xx because WEP128 bit is not supported**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，并不包括初始化矢量 (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。

Q. 为什么当我在 WLC 上配置 WEP 时，显示“WEP key size of 128 bits is not supported on 11xx, 12xx and 13xx model APs.Wlan will not be pushed to these Access Points.”错误消息？

A. 当您在无线局域网控制器上选择静态 WEP 作为第 2 层安全方法时，您可以选择如下 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，可选择 **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. 客户端无法向为 WPA2 配置的 WLAN 进行认证，且控制器显示“apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED:Could not process the RSN and WARP IE's.station not using RSN (WPA2) on WLAN requiring RSN.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. 发生此错误多半是由于客户端不兼容。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，请确保已安装了 Microsoft 提供的 WPA2 补丁 以支持 WPA2。
- 升级客户端的驱动程序和固件。
- 关闭 WLAN 上的 Aironet 扩展功能。

Q. 当我重启 WLC 时，收到“Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event found as violated by the radio 00:XX:XX:XX:XX and detected by the dot11 interface at slot 0 of AP 00:XX:XX:XX:XX in 300 seconds when observing Probe responses, Beacon Frames ”错误消息。为什么会发生此错误，我该如何消除它？

A. 当启用 MFP 的 LAP 检测到帧包含不正确的 MIC 值时，将显示此错误消息。有关 MFP 的详细信息，请参阅带 WLC 和 LAP 的基础架构管理帧保护 (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，请参阅无线局域网控制器 (WLC) 移动组常见问题解答。

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。

Q. 客户端 AIR-PI21AG-E-K9 已使用可扩展的认证协议，即通过安全隧道的灵活认证（EAP-FAST）与接入点（AP）顺利关联。然而，当关联的 AP 关闭时，客户端不漫游到另一个 AP。同时控制器消息日志中连续显示以下消息：""Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922:Unable to allow user into the system - perhaps the user is already logged onto the system?Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557:Unable to delete username for mobile 00:40:96:ad:75:f4"为什么？

A. 当客户端卡需要执行漫游时，会发送认证请求，但它并不会正确处理密钥（不通知 AP/控制器，也不回复重新认证)。

此错误记录在 Cisco Bug ID CSCsd02837 中（仅限注册用户）。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，由于以下任何原因，还会出现“Unable to delete username for mobile”消息：

- 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。

Q. 当我在 6509 交换机中安装新的无线服务模块 (WiSM) 刀片，并用 Microsoft IAS 服务器实现受保护的可扩展的认证协议 (PEAP) 时，收到以下错误消息：Mar 1 00:00:23.526:%LWAPP-5-CHANGED LWAPP changed state to 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 LWAPP changed state to DOWN *Mar 1 00:00:23.528:%LWAPP-5-CHANGED LWAPP changed state to DISCOVERY *Mar 1 00:00:23.557:LWAPP_CLIENT_ERROR_DEBUG:lwapp_crypto_init_ssc_keys_and_certs no certs in the SSC Private File *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 debug 显示 WLC 发送了接入请求，但 IAS 服务器无响应。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。

Q. 轻量接入点 (LAP) 不向控制器注册。可能存在什么问题？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:f0.Thu Feb 3 03:20:47 2028:Unable to free public key for AP 00:0B:85:68:F4:F0。

A. 当接入点 (AP) 向 WLC 发送轻量接入点协议 (LWAPP) 加入请求时，会在 LWAPP 消息中嵌入其 X.509 证书。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，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。它还会查看 AP 证书有效间隔的开始日期和时间，并与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。要设置 WLC 上的时钟，可发出 **show time** 和 **config time** 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) 日志中显示如下消息：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 与 WLC 之间的 LWAPP 隧道经过 MTU 在 1500 字节以下的网络路径，那么您会收到此错误消息。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 ID CSCsd39911（仅限注册用户）。

解决办法是将控制器固件升级到 4.0(155)。

Q. 我正尝试在非隔离区 (DMZ) 中在内部控制器与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 命令的输出显示了如下消息：**Security Policy Mismatch for WLAN <Wlan ID>.Anchor Export Request from Switch IP:**<controller Ip address> Ignored。问题出在哪里？

A. 访客隧道为访客用户访问公司无线网络提供了更安全的方式。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 **debug 命令输出**所示，问题可能是为内部控制器以及 DMZ 控制器中特定 WLAN 配置的任意安全策略不匹配。请检查安全策略以及其他设置（如会话超时设置）是否匹配。

出现此问题的另一常见原因是对于特定 WLAN，DMZ 控制器不能锚定到其自身。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。

Q. 我在 2006 无线局域网控制器 (WLC) 上看到许多“CPU Receive Multicast Queue is full on Controller”消息，但 4400 WLC 上没有。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. 由于控制器上已禁用了组播，因此引起此报警的消息也许是地址解析服务 (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。

Q. 我在一个控制器中看到“[SECURITY] apf_foreignap.c 763:**STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port.**”错误消息。此错误消息是什么意思，我应该采取什么措施来解决它？

A. 当控制器收到没有状态机的 MAC 地址的 DHCP 请求时，会显示此消息。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。以下措施有助于减少此消息，即对于在交换机上采用 **switchport vlan allow** 命令进入控制器的中继，在控制器上只允许使用 VLAN。

Q. 我为什么会在控制台中看到以下错误消息：Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc？

A. 这可能是由于高 CPU 负载所致。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。

此错误消息在 Cisco 无线局域网控制器和轻量接入点版本 3.2.116.21 发行版本注释的重负载控制器 CPU 部分中有记录。

Q. 我在无线控制系统 (WCS) 上收到如下 Wired Equivalent Privacy (WEP) 密钥错误消息：**The WEP Key configured at the station may be wrong.Station MAC Address is 'xx: xx xx xx xx xx', AP base radio MAC is 'xx: xx xx xx xx xx' and Slot ID is '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？**

A. 如果您所有安全相关配置均完善无缺，那么您现在收到的消息是由于 Bug 所致。控制器中存在某些已知 Bug。请参阅 Cisco Bug ID CSCse17260（仅限注册用户）和 CSCse11202（仅限注册用户），其中分别说明了“**WPA 和 TKIP 客户端**上在站点中配置的 WEP 密钥可能有问题”。实际上，**CSCse17260** 与 **CSCse11202** 是重复的。**CSCse11202** 在 WLC 版本 3.2.171.5 中已修复。

注意： 最新的 WLC 版本中已修复了以上 Bug。

Q. 我们使用外部 RADIUS 服务器通过控制器验证无线客户端。控制器定期发送以下错误消息：no radius servers are responding。我们为什么会看到此错误消息？

A. 当请求从 WLC 发出到达 RADIUS 服务器时，每个数据包都有一个 WLC 希望获得响应的序列号。如果无响应，则显示“radius-server not responding”消息。

WLC 收到 RADIUS 服务器响应的默认时间为 2 秒。此值在 WLC GUI 的 **Security > authentication-server** 下进行设置。最大值为 30 秒。因此，将此超时值设置为最大值或许有助于解决此问题。

有时，RADIUS 服务器会对来自 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，在此情况下，控制器会将 RADIUS 服务器标记为无响应。

为解决静默丢弃问题，可在 WLC 中禁用**主动故障切换功能**。

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 服务器标记为无响应。然而，这是不应该的，因为 AAA 服务器也许并不仅仅对该特定客户端做出响应（通过执行静默丢弃）。它可以对其他具有效证书的有效客户端进行响应。但是，WLC 仍可能将 AAA 服务器标记为无响应，并且无法正常工作。

为了克服这种情况，请禁用**主动故障切换功能**。发出**设置radius aggressive-failover disable命令**从控制器CLI为了执行此。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。

Q. 多个客户端无法关联到 LWAPP，且控制器日志中显示“IAPP-3-MSGTAG015:`iappSocketTask` iappRecvPkt returned error”错误消息。为什么会发生这种情况？

A. 这主要是由于支持 CCX v4 但客户端套件版本低于 10.5.1.0 的 Intel 适配器的问题所引起的。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 ID CSCsi91347（仅限注册用户）。

Q. 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 网络的失败次数超过预先配置的 EAP 尝试次数时，会发生此错误。如果用户认证失败，则控制器会排除该客户端，且客户端无法连接到网络，直到排除计时器到期或由管理员覆盖。

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。

Q. 我在无线局域网控制器 (WLC) 上看到以下错误消息：`An Alert of Category Switch is generated with severity 1 by Switch WLCSCH01/10.0.16.5 The message of the alert is Controller '10.0.16.5'.`RADIUS server(s) are not responding to authentication requests。问题是什么？

A. 此问题也许是由于 Cisco Bug ID CSCsc05495 导致的。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。

Q. 我在 Monitor > 802.11b/g Radios 情况下收到噪声配置文件故障消息。我想知道为什么会看到此 FAILED 消息？

A. 噪声配置文件 FAILED/PASSED 状态在 WLC 执行完测试结果之后进行设置，并与当前集合阈值进行比较。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参数，但建议您先了解清楚网络设计以及它是如何影响网络性能之后，再更改设置。

Radio Resource Management (RRM) PASSED/FAILED 阈值是在 **802.11a Global Parameters >**

Auto RF 和 802.11b/g Global Parameters > Auto RF 页面上为所有 AP 全局设置的。RRM PASSED/FAILED 阈值是在 802.11 AP Interfaces > Performance Profile 页面上为该 AP 单独设置的。

Q. 我无法将端口 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，每个端口上应当配置一个 AP 管理器（没有备份）。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。

Q. 我看到以下错误消息：**The AP '00:0b:85:67:6b:b0' received a WPA MIC error on protocol '1' from Station '00:13:02:8d:f6:41'.**Counter measures have been activated and traffic has been suspended for 60 seconds。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帧计数器。此错误意味网络中有人正试图重播原始客户端发送的消息，或者可能意味着该客户端发生故障。

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。如果随后的 MIC 失败发生在最近一次失败的 60 秒之内，则 IEEE 802.1X 实体作为请求方的 STA 将解除自身或所有 STA 对于安全关联的认证（如果其 IEEE 802.1X 实体作为认证程序）。

此外，设备在检测到第二次故障后至少 60 秒内，不接收或传输任何对等体发出的或发往对等体的任何 TKIP 加密的数据帧，以及任何未加密的数据帧（IEEE 802.1X 消息除外）。如果设备是 AP，则在此 60 秒内禁止与 TKIP 建立新的关联。60 秒结束时，AP 会恢复正常操作并允许 STA 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。该命令即 config 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。

Q. 我的控制器日志中显示以下错误消息：**[[ERROR] dhcp_support.c 357:dhcp_bind():servPort dhcpstate failed**为什么？

A. 发生以上错误最常见的原因，是由于控制器的服务端口已启用 DHCP 但未从 DHCP 服务器收到 IP 地址。

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。

Q. 我的无线客户端无法连接到无线局域网 (WLAN) 网络。与接入点 (AP) 相连的 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. 作为访问介质的一个条件，MAC 层会检查其网络分配矢量 (NAV) 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。站点首先根据帧的长度和数据速率计算发送帧所需的时间，然后再传送帧。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，这很可能是伪装（潜在实时攻击），您需要通过数据包捕获进行确认。

Q. 我们在配置控制器并重新启动它之后，无法以安全 Web (https) 模式访问控制器。当我们尝试以安全 Web 模式访问控制器时，收到以下错误消息：`Secure Web:`Web Authentication Certificate not found (error)。出现该问题的原因是什么？

A. 发生该问题可能有多种原因。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
```

在此命令输出中，您应该可以看到以下消息：Web Authentication certificate has been generated。

现在，您应该可以在重新启动控制器后，以安全 Web 模式访问控制器了。

Q. 如果在有效客户端中，攻击者的 MAC 地址是已加入控制器的接入点（AP）的地址，则该控制器有时会针对该客户端报告以下 IDS 取消关联洪水签名攻击警报消息：`IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'.The Signature description is 'Disassociation flood', with precedence 'x'.The attacker's mac address is 'hh:hh hh hh hh hh', channel number is 'x', and the number of detections is 'x'`为什么会发生这种情况？

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

如果攻击者的 MAC 地址是已加入控制器的 AP 的地址，那么该控制器有时会针对该有效客户端报告 IDS 取消关联洪水攻击。

如果客户端与 AP 关联，但由于卡拔下、漫游超出范围等原因与 AP 停止通信，AP 将等待直到空闲

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 Syslog 中收到以下错误消息：`[[WARNING] apf_80211.c 2408:Received a message with an invalid supported rate from station <xx:xx xx xx xx xx xx> [ERROR] apf_utils.c 198:Missing Supported Rate`为什么？

A. 实际上，Missing Supported Rate 消息表示在无线设置下为某些必需的数据速率配置了 WLC，但 NIC 卡中缺少必需的数据速率。

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。

Q. 我们的网络中广播了以下 Syslog 错误消息：AP:001f.ca26.bfb4:`%LWAPP-3-CLIENTERRORLOG Decode Msg:`could not match WLAN ID <id>。为什么会发生这种情况，该如何阻止？

A. 此消息是由 LAP 广播的。这被看到，当您配置WLAN WLAN的时覆盖功能，并且特定的WLAN没有通告。

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，以便消息广播到单独服务器。

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

A. 通常，此错误消息表明控制器宣布无线客户端的冲突(即分开的AP宣布他们有客户端)，并且控制器没有接收从一个AP的一移交到下。没有要保持的网络状态。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，可以有与移动性配置的一问题。否则，与一个特定客户端或情况涉及的它也许是异常情况。

Q. 我的控制器引发了以下警报消息：`'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)在特定的无线电的时， SNR阈值之下下跌此警报信息被上升。12是覆盖孔检测的默认SNR阈值。

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级别在一给的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配置文件值。

详细，客户端SNR阈值由每个AP的传输功率定义(代表在dbm)，减不变值17dBm，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访问这样：

1. 在WLC GUI中，请去无线主要标题并且选择选择WLAN标准的**Network选项**在左侧的(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。在此部分中，可以找到 Coverage 值（3 到 50 dbm）。此值是用户可配置覆盖配置文件值。
3. 可编辑此值以修改客户端 SNR 阈值。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. 我在使用 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并且报告此错误消息："*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. 有一验证涉及的Cisco Bug ID CSCsh62641 (仅限注册用户)在ACS 4.1，其中ACS给错误消息。

此 Bug 可能是个问题。有此bug的一补丁程序联机在应该解决问题的ACS 4.1下载(仅限注册用户)页。

Q. Cisco 4400 系列无线局域网控制器 (WLC) 不启动。此错误消息在控制器接收：**ide 0:4 fatload **(IRQ) dev 0 blk 0 status 0x51 Error reg:10 **0。为什么？

A. 出现此错误的原因也许是硬件问题。开TAC案例进一步排除故障此问题。为了开TAC案例，您需要有与思科的一个有效合同。参考的技术支持为了与Cisco TAC联系。

Q. 无线局域网控制器 (WLC) 遇到存储器缓冲区问题。一旦存储器缓冲区全双工，控制器失败并且需要重新启动联机它回到。消息日志中显示以下错误消息：Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506:9 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)。WLC 版本 4.1.185.0 中已解决此 Bug 问题。升级您的控制器对此软件版本或以后为了解决此消息。

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：May 03 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 (1)SPA 192.168.1.233/TPA 192.168.1.233。这些消息指示什么？

A. 当 WLAN 标记为必需的 DHCP 时，会发生这种情况。在这类情况下，通过DHCP收到IP地址仅的站点允许联合。静态客户端不允许关联到此 WLAN。WLC作为DHCP中继代理并且记录所有站点的IP地址。当WLC从一个站点的接收ARP请求在WLC前接收从站点的DHCP信息包并且记录了其IP地址时，此错误消息生成。

Q. 当您使用在以太网(柏吾)时的电源在思科2106无线局域网控制器，AP无线电没有启用。APRadio slot disabled.错误消息。我如何修复此错误？

A. 此错误消息出现，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。

思科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。

您必须启动对此错误消息被服从的**预标准**模式启动AP。这可以从控制器CLI执行用**设置ap电源预标准{enable (event)|disable} {all|Cisco_AP}** 命令完成。

如果升级到从前一版本的软件版本4.1此should命令已经配置，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

Q. 控制器生成`dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED Unable to add an ARP entry for xx:xx. - xxx.xentry does not exist.`类似于此。此 Syslog 消息是何含义？

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ARP应答转发对NPU，但是WLC软件不应该尝试添加此条目到网络处理器。如果它如此，这些消息生成。没有在WLC的功能影响由于此，但是WLC生成此系统消息。

Q. 我安装并配置了新的 Cisco 2106 WLC。WLC表明温度传感器失败。当您登录Web接口在“控制器摘要下时”，说“在内部温度旁边”。一切别的东西看上去通常作用。

A. 内部温度传感器失败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。这新建的传感器比4.2版本良好工作，但是不是与软件兼容后。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。

有与此问题CSCsk97299 (仅限注册用户)涉及的已知Cisco Bug ID。此bug在WLC版本4.2版本注释被提及。

Q. 对于所有 SSID，我都收到了“radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND:`WLAN <WLAN ID>RADIUS`-所有Ssid的”消息。此消息看上去为不使用AAA服务器的Ssid。

A. 此错误消息意味着控制器没有能联系默认RADIUS服务器或一个未定义。

此行为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。请将您的控制器升级到版本 4.2。

Q. “Message:`10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL Interface1MAC`错误消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CPU被发出的数据包时。

Q. 无线局域网控制器 (WLC) 上显示以下错误消息：

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

这些错误消息有何含义？

A. 这些消息是供参考消息并且是正常引导程序步骤的一部分。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，每进程的设置顺序派出此消息，例如， DHCP服务器设置，没有标记(RF ID)不配置，等等。这些是可能安全忽略的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. “The 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. 系统可能检测到 ARP 伪装或毒化。但是，此消息不一定暗示所有有恶意ARP伪装发生。当发生以下情况时，会显示此消息：

- WLAN配置与要求的DHCP，并且一个客户端设备，在关联在该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，当客户端保持从一个前期关联时的一有效DHCP租用。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`此情况效果是客户端无法发送或收到所有数据流，直到它DHCP通过WLC。参考Cisco无线LAN控制器系统信息指南的DTL Messages Section欲知更多信息。

Q. LAP 未使用以太网供电 (POE)。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，如果在以太网(柏吾)设置的电源没有正确地配置。当转换对轻量级模式，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)，亦称内嵌电源的电源。

参考配置在以太网的电源关于如何配置在以太网(柏吾)的电源的更多信息。

Q. 我在无线局域网控制器 (WLC) 上看到此消息：***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。发现和加入进程在轻量对无线局域网控制器(WLC)的AP(LAP)注册详细解释

此错误消息在WLC被看到，当收到发现请求时，在到达了其最大数量AP产能后。

如果LAP的主要控制器没有配置或，如果其新建的箱外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全双工AP产能的控制器， WLC获得请求并且意识到在其最大数量AP产能和不回答请求并且给此错误。

Q. 在哪里能找到关于LWAPP系统消息的更多信息？

A. 参考的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错误消息出现在无线局域网控制器(WLC)。这说明了什么？

A. WLC不能装载自定义Web验证/Passthrough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验证套件有文件名的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可能不显示所有已配置的AP组。问题是什么？

A. 丢失AP组能被看到是否使用CLI**显示WLAN AP组**发出命令。

尝试添加列表的一其他AP组。例如， 51 AP组部署和第51未命中(页3)。添加第52组，并且页3在Web GUI应该出版。

为了解决此问题，升级对WLC版本7.0.220.0。

相关信息

- **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**
- **技术支持和文档 - Cisco Systems**