# 统一无线网络：排除客户端问题

## 目录



## 简介

无线电频率(RF)环境复杂和动态。创建良好的无线环境需要考虑多种因素。本文档介绍了在 Cisco 统一无线环境中连接无线客户端时可能会遇到的各种问题，以及排除和解决这些问题所要采取的步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco 统一无线解决方案
- Cisco无线LAN控制器(WLC) GUI基本配置

## 使用的组件

本文档适用于参与到 Cisco 统一环境中的所有设备，不局限于特定软件和硬件版本。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 背景信息

在 Cisco 统一环境中，WLC 发挥着中心作用。它管理着整个无线网络。轻量级接入点(拉普)，服务无线客户端，注册对WLC并且下载从WLC的整个配置。要采取的初始步骤是检查 LAP 是否已注册到 WLC。单击 WLC GUI 中的 Wireless 菜单，检查 LAP 是否已列在页面中。

# 配置问题

对于成功的无线连接而言，正确完成 WLC 上的配置非常重要。本部分将介绍一些最常见的配置问题。

## SSID 不匹配

客户端使用其 SSID 识别和关联到无线网络，所以请确保 WLC 和客户端上配置的 SSID 相同。要检查 WLC 上配置的 SSID，请单击 **WLANs** 页。单击相应的 *WLAN*，在 General 选项卡下检查配置的 SSID。

**注意：** *SSID* 区分大小写。如果删除并重新创建 WLAN，SSID 可帮助无线客户端与 WLAN 进行关联。

## 安全性不匹配

WLC 和客户端上的安全配置必须匹配。如果身份验证类型是静态 WEP，请检查 WLC 上相应的加密密钥/密钥索引是否与客户端上的匹配。如果身份验证类型是 802.1x 或 WPA，请确保客户端和 WLC 之间的身份验证类型/加密密钥大小相匹配。有关如何针对各种安全解决方案配置 WLC 和客户端的详细信息，请参阅无线 LAN 控制器上的身份验证配置示例。

**注意：** 第 2 层安全解决方案（如 WPA 或 802.1x）不能用于配置为使用第 3 层安全解决方案（如 Web 身份验证或 Web 穿透）的 WLAN。有关兼容的安全解决方案的详细信息，请参阅无线 LAN 控制器第 2 层和第 3 层安全兼容性列表。

## WLAN 被禁用

对于成功的无线连接而言，相应的 WLAN 在 WLC 上必须处于活动状态。在 WLC 上，默认情况下 WLAN 处于未启用状态。要激活 WLAN，请单击 WLC 中的 **WLANs** 菜单。此时将显示 WLC 上配置的 WLAN 的列表。单击配置了客户端要与之关联的 SSID 的 WLAN。在 **WLAN > Edit** 页的 General 选项卡下，选中状态框。

## 数据速率不受支持

对于特定的标准（802.11b/g 或 802.11a），您可以在 WLC 上选择将某些数据速率设置为必需数据速率，而将其他数据速率设置为支持的或禁用的数据速率。对于成功的关联而言，无线客户端必须支持 WLC 上配置的必需数据速率。要检查 WLC 上配置的数据速率，请单击 WLC GUI 中的 **Wireless** 菜单，在页面左侧显示的 802.11b/g/n > Network 或 802.11a/n > Network 选项下检查配置的数据速率。请查阅客户端供应商的支持页，以对此进行确认。如果升级客户端驱动程序，则其可以帮助客户端支持所需的数据速率。

**注意：** 为了实现更好的连接，请在 WLC 上将最低数据速率设置为 **mandatory**，将其他数据速率设置为 supported。

## 客户端被禁用

在 WLC 上，有一个选项可用于手动禁用客户端。此功能有助于防止恶意客户端尝试访问网络。检查无法关联的客户端的 MAC 地址是否出现在 Disabled Clients 列表中，如果在，请将其删除。单击 GUI 中 Security 菜单下的 **Disabled Clients** 选项，您可以找到禁用的客户端列表。

**注意：** 如果客户端不遵守 WLC 上配置的默认客户端排除策略，则会被拒绝关联到网络。有关客户端排除策略的详细信息，请参阅 Cisco 无线 LAN 控制器配置指南 4.2 版的配置客户端排除策略部分。

## 无线电报头

无线电报头（有时称为标头）是数据包头部数据中的一部分，它包含了无线设备发送和接收数据包时所需的信息。

一些客户端不支持**短报头**，所以无法连接到启用了短报头的 WLAN。短报头可以提高吞吐量性能，因此 WLC 上默认启用了短报头。要禁用短报头，请单击 WLC GUI 的 **Wireless** 菜单。然后，单击左侧的 **802.11b/g > network** 菜单。*取消选中* **short preamble** 复选框。

## Cisco 专有功能 - 第三方客户端的问题

如果无法连接到网络的客户端设备是非 Cisco 设备，禁用一些 Cisco 专有功能可以使连接成功。有关客户端支持的功能的列表，请联系第三方客户端设备的供应商。

以下是一些重要的专有功能：

- Aironet IE - Aironet IE 包含接入点在 WLAN 的信标和探测响应中发出的接入点名称、负载、相关客户端数等信息。CCX 客户端使用这些信息选择与之关联的最佳接入点。
- **MFP** —管理帧保护是介绍的功能保证管理帧的完整性，例如解除验证、分离、信标和探测器，接入点保护传输的管理帧，当添加一消息完整性检查信息元素(MIC IE)时到每帧。入侵者作出的对帧进行复制、修改或重播的任何尝试都将使 MIC 无效，这会导致（配置为对 MFP 帧进行检测的）任何接收接入点都报告出现不一致情况。默认情况下，对 WLC 上创建的任何 WLAN 都启用这些功能。要禁用这些功能，请在 WLC 中单击 WLAN 菜单。此时将显示 WLC 上配置的 WLAN 的列表。单击客户端要与之关联的 WLAN。在 Advanced Tab of WLANs > Edit 页下，取消选中与 Aironet IE 和 MFP 对应的框。
- **无线电报头 -** 无线电报头（有时称为标头）是数据包头部数据中的一部分，它包含了无线设备和客户端设备发送和接收数据包时所需的信息。您可以根据无线客户端上支持的设置，将无线电报头设为长报头或短报头。

- **以太网封装转换 -** 当无线设备接收的数据包不是 802.3 数据包时，无线设备必须使用封装转换方法将数据包格式设置为 802.3。以下是两种转换方法：802.1H：此方法可以为 Cisco Aironet 无线产品提供最佳性能。802.1H 是默认设置。RFC1042：可使用该设置确保与非 Cisco Aironet 无线设备之间的互操作性。RFC1042 不能提供 802.1H 所提供的互操作性优势，但其被其他无线设备制造商所使用。
- **wpa 握手超时 -** 某些供应商需要更长的 wpa 握手超时时间。您可以使用 **dot11 wpa handshake timeout** 命令更改 wpa 握手超时。
- **ssid -** 某些供应商要求广播 ssid。要广播 ssid，请在 ssid 配置下启用*访客模式*。

## IP 地址问题

无线客户端需要有效的 IP 地址才能与网络的其他部分进行通信。

控制器类似一个具有 IP 帮助地址的路由器。也就是说，它填充网关 IP 地址并通过在其上安装了客户端的动态接口将该地址单播到 DHCP 服务器。因此请注意，在默认情况下，交换机上的 DHCP 监听将阻止不受信任的端口上的这些 DHCP 数据包。

当 DHCP 所提供的信息回到控制器时，会将 DHCP 服务器 IP 地址更改为它的虚拟 IP 地址。这样做的原因是，当 Windows 在 AP 之间漫游时，其所做的第一件事就是尝试联系 DHCP 服务器并更新它的地址。

通过 DHCP 服务器地址 1.1.1.1（这是控制器上的典型虚拟 IP 地址），控制器可以拦截该数据包并欺骗 Windows。这也是为什么所有控制器上的虚拟 IP 地址都相同的原因。如果 Windows 便携式计算机漫游到另一控制器上的 AP，它将尝试联系该控制器上的虚拟接口。由于移动性事件和上下文传输的原因，Windows 客户端漫游到的新控制器已拥有再次欺骗 Windows 所需的所有信息。

如果要使用内部 DHCP 服务器，您所要做的只是将管理 IP 地址作为 DHCP 服务器放在为子网创建的动态接口上。然后将该接口分配给 WLAN。控制器在每个子网上都需要一个 IP 地址的原因是，这样它才能在 DHCP 请求中填充 DHCP 网关地址。

我们看到了很多 DHCP/IP 地址问题。以下是这些问题的原因以及解决问题的步骤：

1. 如果配置的身份验证类型是第 2 层安全解决方案之一（如 802.1x 或 WPA），客户端必须成功进行身份验证之后才能获取有效的 IP 地址。首先检查客户端是否成功进行了身份验证。**注意：** 一种例外情况是，如果为客户端配置的是第 3 层安全解决方案（如 Web 验证或 Web 穿透），则客户端会在身份验证前分配到 IP 地址。
2. WLC 上定义的每个 WLAN 都映射到 WLC 的一个动态接口上，该动态接口配置有属于唯一子网的 VLAN。与该 WLAN 关联的客户端将分配有来自相应 VLAN 的接口子网的 IP 地址。检查是否已在 DHCP 服务器上定义了该 WLAN 的 IP 子网和网关，以便客户端在该子网上获取 IP 地址。请参阅相应供应商的文档，配置 DHCP 服务器。**注意：** 作为前提条件，请检查是否可以从 WLC 访问 DHCP 服务器，以及 DHCP 服务是否已打开。
3. 确保在映射到 WLAN 的 WLC 接口中正确定义了 DHCP 服务器的 IP 地址。要对此进行检查，请单击 GUI 中的 **Controller** 菜单。单击左侧的 **Interfaces** 菜单，检查 DHCP 服务器字段。在同一页中，检查接口是否已映射到开启并处于活动状态的*物理端口*。要排除 DHCP 相关问题，请在 WLC 上使用 **debug dhcp packet enable** 和 debug dhcp message enable 命令。**注意：** 您也可以将 WLC 配置为 DHCP 服务器。有关在 WLC 上如何配置 DHCP 服务器的详细信息，请参阅文档 Cisco 无线 LAN 控制器配置指南 5.0 版的使用 GUI 配置 DHCP 部分。
4. WLC 上默认启用 DHCP 代理。WLC 会将数据包单播到 WLAN 接口上配置的 DHCP 服务器或单播到 WLAN 本身。如果 DHCP 服务器不支持 Cisco DHCP 代理行为，请在 WLC 上禁用

DHCP 代理。有关如何在 WLC 上禁用 DHCP 代理的详细信息，请参阅 Cisco 无线 LAN 控制器配置指南 5.2 版的配置 DHCP 代理部分。

5. WLC 通常通过交换机连接到有线网络。检查连接到 WLC 和 DHCP 服务器的交换机端口是否已配置为中继端口，以及这些端口上是否允许相应的 VLAN。有关如何配置 Cisco 交换机的详细信息，请参阅文档使用 WLC 的访客 WLAN 和内部 WLAN 配置示例的将连接到 WLC 的第 2 层交换机端口配置为中继端口部分。
6. 如果为 WLAN 启用了 **DHCP Addr.Assignment** 字段，则不允许静态客户端与 WLAN 相关联。此选项要求与该 WLAN 关联的所有客户端必须通过 DHCP 获取 IP 地址。要检查该选项是否已启用，请单击 WLC GUI 中的 WLANs 菜单。此时将显示 WLC 上配置的 WLAN 的列表。单击相应的 WLAN。转到 **Advanced** 选项卡，找到 DHCP Address Assignment 字段。
7. 某些 DHCP 服务器（如 Cisco PIX 防火墙）不支持 DHCP 中继服务。它们仅接受广播 DHCP 数据包，而不接受来自 DHCP 中继代理的任何单播数据包，所以此情况下请确保 DHCP 客户端直接连接到启用了服务器的接口。**注意：** 请查阅相应的供应商文档，获取 DHCP 中继支持信息。

## 客户端问题

同样重要的是，客户端上的所有配置也必须正确。在客户端上执行以下检查：

1. 有时，计算机无法识别客户端卡。这种情况下，请尝试在另一插槽中使用该卡。如果无效，请尝试在另一计算机中使用该卡。有关安装过程中的问题的详细信息，请参阅文档适用于 Windows 的 Cisco Aironet 340、350 和 CB20A 无线 LAN 客户端适配器安装和配置指南的故障排除部分。**注意：** 确保无线卡与计算机上安装的操作系统兼容。这可以通过客户端卡的数据表进行检查。
2. 检查客户端是否已在计算机上正确安装。客户端卡的状态可以通过 **Windows Device Manager** 屏幕进行检查。查找内容为*"This device is working properly"*的消息。如果消息内容不是如此，则表明驱动程序未正确安装。请尝试卸载驱动程序，然后在计算机上重新安装该驱动程序。要卸载驱动程序，请在 Device Manager 屏幕中右键单击无线适配器，然后单击 **Uninstall**。有关如何重新安装客户端适配器的详细信息，请参阅文档适用于 Windows 的 Cisco Aironet 340、350 和 CB20A 无线 LAN 客户端适配器安装和配置指南的安装客户端适配器部分。**注意：** 如果使用 ACU 配置客户端卡，请确保 ACU 上未禁用无线电。此外，在 Windows 控制面板的**网络连接**下检查卡是否处于已启用状态。**注意：** 请只对无线卡使用一个客户端软件。始终建议对无线卡使用供应商提供的客户端软件。作为第二选择，您也可以使用 PC 供应商提供的客户端软件或 Windows 提供的 WZC。**注意：** 完成这些步骤为了调试WZC ：请使用**enabled命令netsh ras设置的跟踪***为了打开WZC调试。请使用**netsh ras设置的跟踪*已禁用**命令为了关闭WZC调试。日志写入对*C:\Windows\tracing*。*eapol.log*、*rastls.log*和*wzctrace.log*是最重要的日志。**注意：** 参考的无线诊断和故障排除 欲知更多信息。
3. 客户端上的配置必须与 WLC 上的配置匹配。这主要是指客户端上的 SSID 和安全配置。如果使用 Cisco 实用程序配置客户端，请参阅文档适用于 Windows 的 Cisco Aironet 340、350 和 CB20A 无线 LAN 客户端适配器安装和配置指南的使用配置文件管理器部分。
4. 如果无法传输数据（即使成功进行了无线关联之后也无法传输），请尝试禁用其他所有适配器，包括 VPN 适配器和有线适配器。如果计算机中有不止一个无线适配器，请禁用其他适配器以防止适配器之间发生冲突。
5. 如果只有单个客户端有连接问题，请尝试升级该客户端的驱动程序和固件。如果大多数客户端都有连接问题，并且已排除了其他问题，则请选择升级 WLC。
6. 确保设备（即客户端和 WLC）通过了 Wi-Fi 认证，以避免发生任何与安全和操作相关的互操作性问题。

7. 如果使用的是 Windows 计算机，请确保安装了 Microsoft 提供的所有最新安全补丁程序或修补程序。如果使用的是 Windows 客户端实用程序，请确保您已安装了 Microsoft 提供的最新补丁程序。
8. 某些客户端响应 EAP 身份验证时较缓慢。这会导致在 WLC 上发生超时，您可能会在 WLC 上收到以下错误消息：

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station <Mac address of the
client>
```

要回应此消息，请增加 WLC 上的 EAP 超时值，以便为客户端身份验证提供充足的时间。使用以下命令调整 WLC 上的 EAP 计时器：

```
config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to send an
EAP identity request to wireless clients. config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of t imes the WLC attempts to send EAP
request to the Radius Server . config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to negotiate
the encryption key.
```

## RF 问题

RF 干扰是连接不良的一个主要原因。干扰可能由邻近的 802.11 网络或其他干扰源（如使用相同频率的微波炉或无绳电话）引起。由邻近的 802.11 网络引起的干扰有两种类型：

- **同信道干扰：**当覆盖区域重叠的接入点配置在同一个信道中或配置在有重叠频率的多个信道中时，会导致重叠覆盖区域中的客户端产生连接问题。要避免此问题，请将信道号更改为非重叠信道，或将接入点远移，使它们的覆盖区域不再相互重叠。例如，在 802.11b/g 中，网络信道 1、6 和 11 是非重叠信道。
- **相邻信道干扰：**当接入点之间的距离太近或接入点使用高输出功率水平时，即使接入点配置在非重叠信道上，也会产生干扰。可降低接入点的功率以解决此问题。**注意：** 非重叠信道也称为相邻信道，这就是*相邻信道干扰*这一名称的由来。

使用频谱分析仪确定干扰源（例如在 2.4 GHz 频率范围工作的微波炉或无绳电话，或在 5 GHz 频率范围工作的设备）。一旦识别了干扰源，请将其消除。此外，您也可以更改无线网络的工作标准，例如，从 802.11b/g 更改到 802.11a，以避免干扰。

有效的 RF 通信的另一个重要方面是信号强度。弱信号强度会导致连接断断续续。墙壁、金属等障碍物会吸收和反射 RF 能量，从而降低信号强度。在接入点上将功率增加到必需的水平可以提供足够的覆盖范围。您也可以使用高增益天线提高覆盖范围和信号强度，但请确保该天线经过了 FCC 批准，可与设备一起使用。

**注意：** 信噪比 (SNR) 是衡量链路质量的关键因素，它是指信号强度和 RF 噪声（来自其他与无线网络处于相同频率的源的 RF 信号或能量）之间的比。较高的 SNR 表示链路质量较好，这样可以更快地传输数据。较低的 SNR 值表示链路质量不佳，会导致连接断断续续或性能较差。无线数据包分析程序/现场勘测软件可以显示特定位置的 SNR 和吞吐量。

在Cisco Unified环境，有呼叫在WLCs实现的高级无线电资源管理(RRM)的概念。RPM 是一款嵌入控制器的软件，它就像一位内置的 RF 工程师，可以连续提供实时的无线网络 RF 管理。它会自动处理以上提及的所有 RF 问题。有关 RRM 的详细信息，请参阅文档 Cisco 无线 LAN 控制器配置指南 5.0 版的配置无线电资源管理部分。

# 错误消息

在客户端连接过程中，在 WLC 和客户端两方可能都会收到多种错误消息。

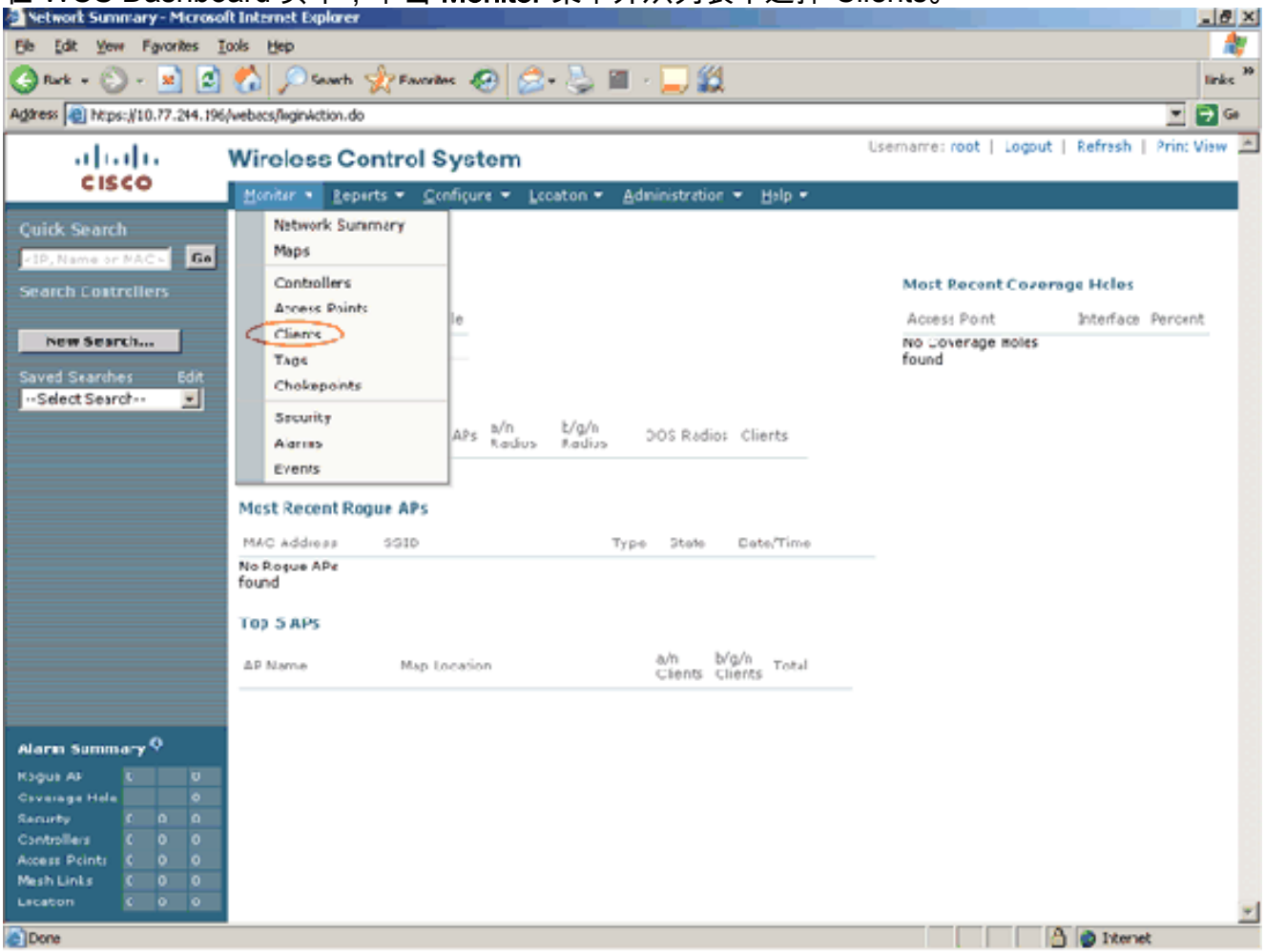
- **客户端无法通过 DHCP 获取 IP 地址或在通过 DHCP 获取 IP 地址的过程中遇到延迟。控制器上的 debug dhcp 显示以下消息：**

  `Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK` *DHCP NAK* 通常由 DHCP 服务器发送，用于表明客户端试图从其自身不从属的子网中获取 IP 地址。这一情况通常会在客户端从一个 WLC 漫游到另一个 WLC 时发生，在另一个 WLC 中，为同一 WLAN 分配了不同的 VLAN。在 WLC 上配置 DHCP 代理可以解决该问题。

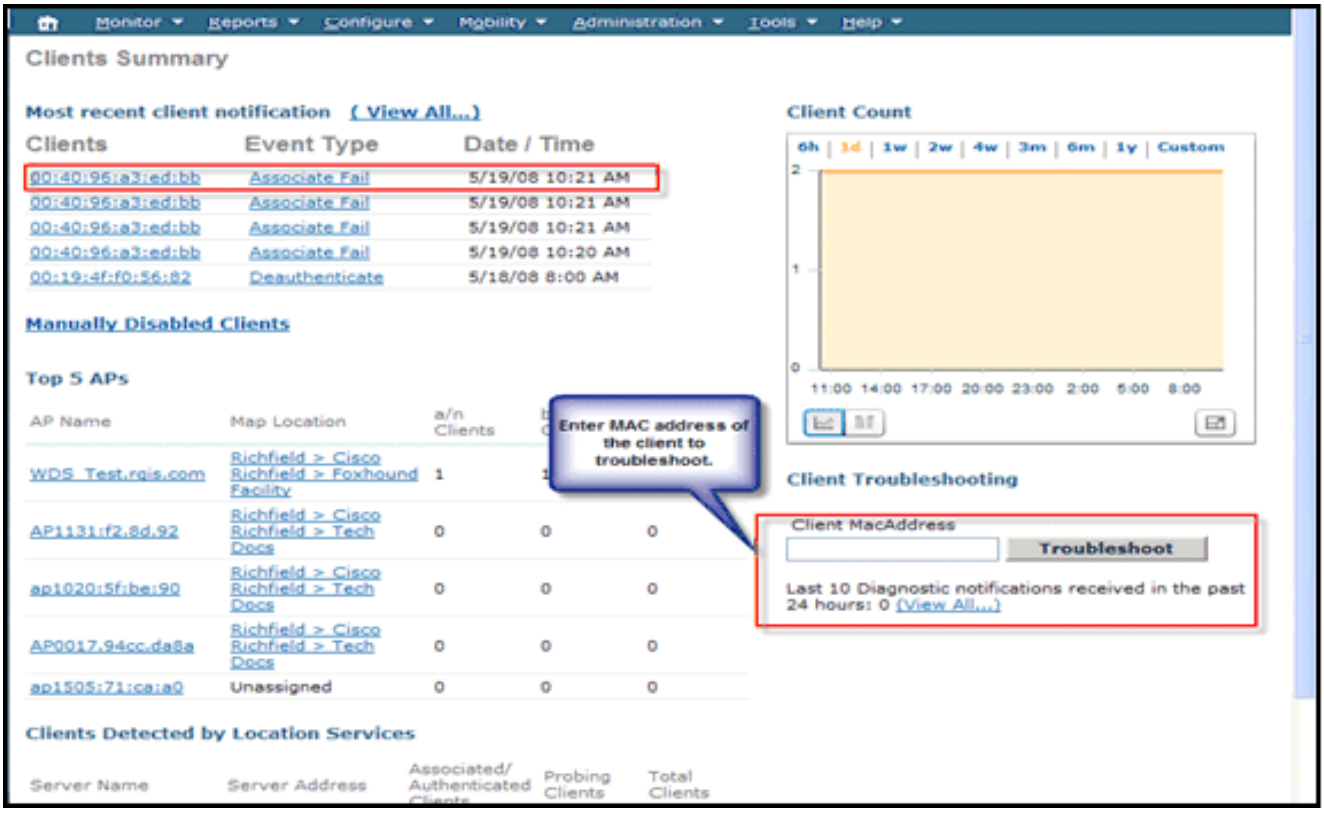
# 使用 WCS 排除客户端问题

WCS 可用于在无线环境中排除客户端相关问题。进行故障排除时，WCS 将借助于自身中内置的故障排除工具。要通过 WCS 对客户端进行故障排除，用户需要执行以下步骤

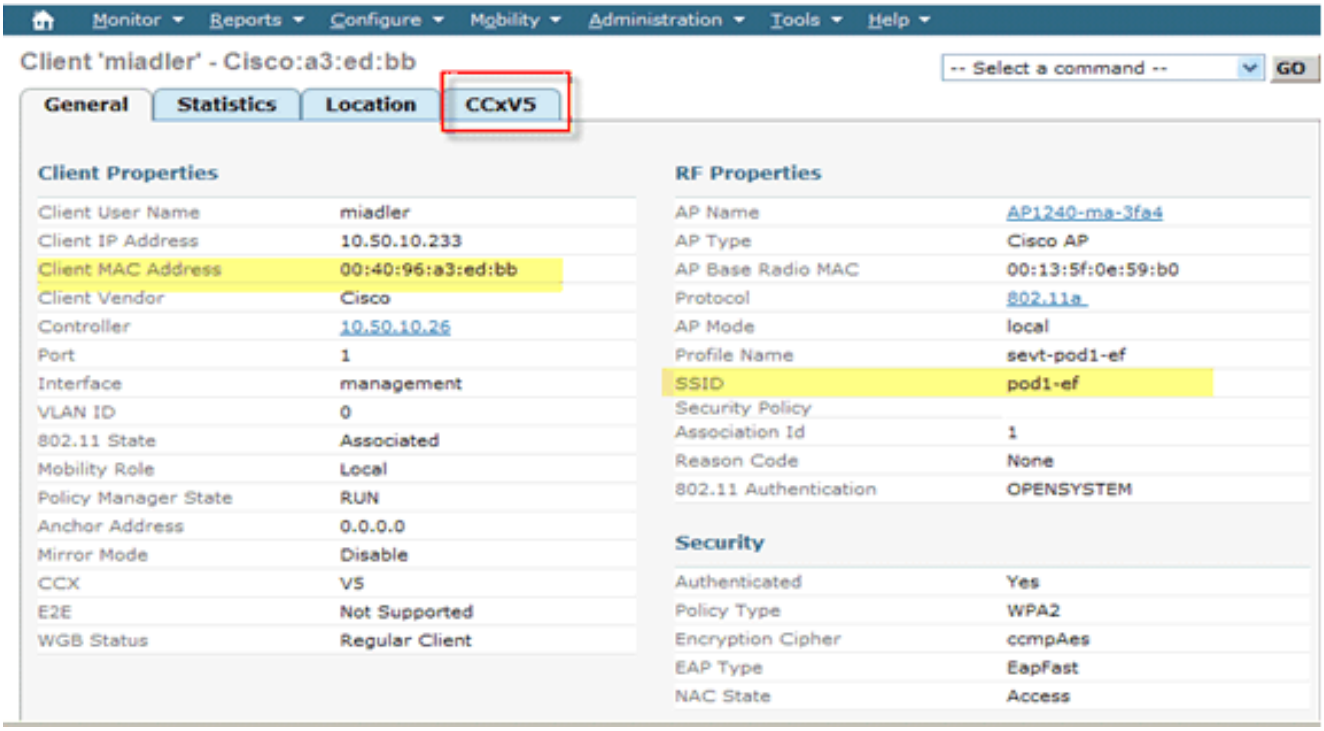
1. 在 WCS Dashboard 页中，单击 **Monitor** 菜单并从列表中选择 Clients。




2. 此时会打开如图 1 所示的 Client Summary 页，该页将显示无线网络中的客户端的列表。**图 1**




3. 单击客户端可获得特定客户端的详细信息，如 SSID 或身份验证方法。图 2 显示了这方面的一个示例。在图 1 所示的 Client Summary 页右下方的 **Troubleshoot** 对话框中，用户可以输入要进行故障排除的设备的 MAC 地址。该操作可以打开如图 3 所示的 Troubleshooting Tool 页。识别并选择了要进行故障排除的设备后，用户将看到 Client Details 页：**图 2**




## WEP 故障排除

仍使用 WEP 安全机制的旧版无线客户端通常较难进行故障排除。在客户端和 AP 上执行以下检查：

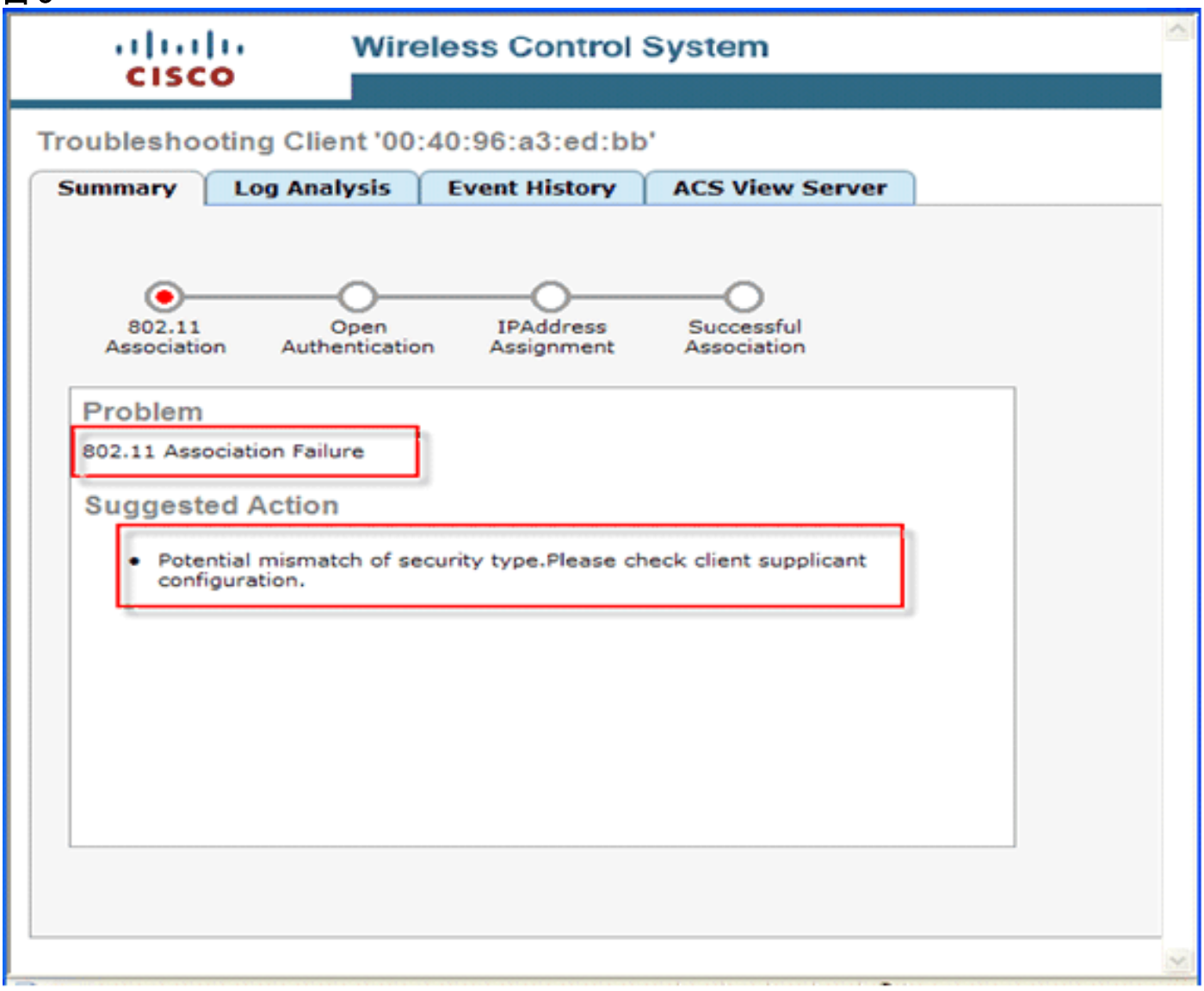
- WEP 密钥长度（以及密钥不匹配）

- WEP 密钥索引（以及配置不匹配）
- 配置的身份验证方法（开放与共享密钥）

## 身份验证不匹配

虽然数据包捕获是一个繁琐的过程，但 WCS 客户端故障排除工具可以轻松帮助指出问题所在。通常，就是该工具提供的这种小“提示”减少了故障排除的时间。图 2 显示了 **WCS 故障排除工具**。如图中所示，问题阶段被确定并以直观方式显示出来，这就为进行详细分析做好了准备。

**图 3**



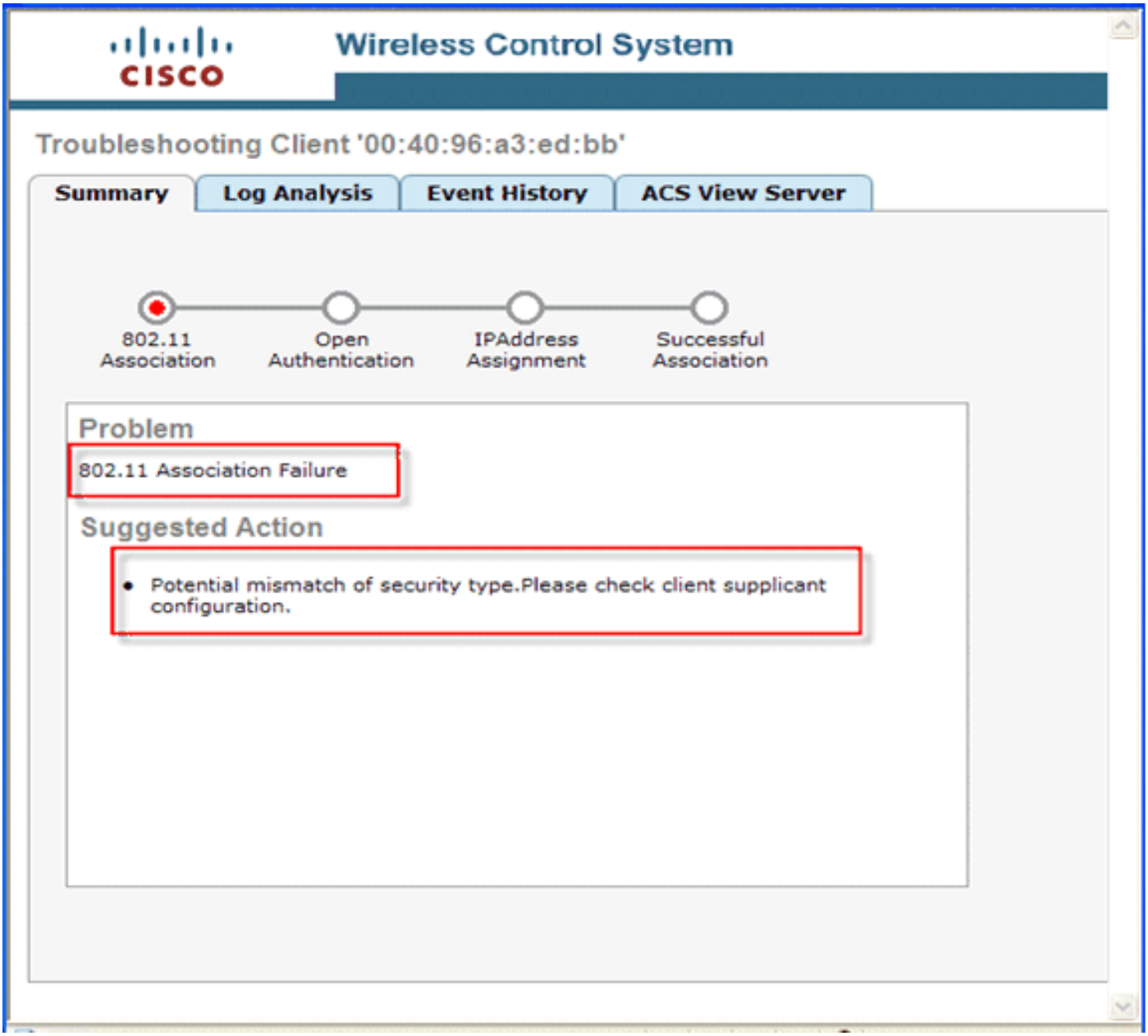

## WEP 密钥索引不匹配

一般而言，您可以在客户端和 AP 上最多配置 4 个 WEP 密钥。其中一个密钥将被选作传输密钥。客户端和 AP 之间的传输密钥必须匹配。例如，密钥 2 被选作了客户端上的传输密钥，则该密钥必须与 AP 上的密钥 2 匹配，但 AP 可以有与传输密钥不同的密钥。另一问题通常是这样：客户端和基础设施供应商对规范的理解不同，这就导致了产品中的具体实施不同。一个常见的示例是，有些供应商使用 0 到 3 的密钥索引，而有些使用 1 到 4 的密钥索引。这会导致配置不匹配和连接尝试失败。发生这种情况时，请密切注意数据包解码中记录的“Key ID”字段，从中可以知道这是否是引起问题的根本原因。

## WPA-PSK 故障排除

WPA-PSK 故障排除在许多方面类似于 WEP 故障排除。大多数失败的尝试都是因为密钥的错误配置而引起的。通过 WCS 客户端故障排除工具，管理员可以收集 WPA 事务日志。这些日志（如以下突出显示内容所示）可以显示潜在问题可能出现在哪里*（此特定示例中的问题为客户端上的预共享密钥配置错误）*，这些日志源自 WCS 客户端故障排除工具中的 Log Analysis 选项卡。将 WLAN 设置为使用 WPA-PSK 作为第 2 层安全策略，并为客户端配置错误的 PSK。以下为事件中 PSK 密钥配置错误时的日志：

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Client 802.1x authentication failure exceeded the limit. <TIMESTAMP> ERROR 10.10.10.2 EAPOL-
key has possible incorrect psk configuration.
```

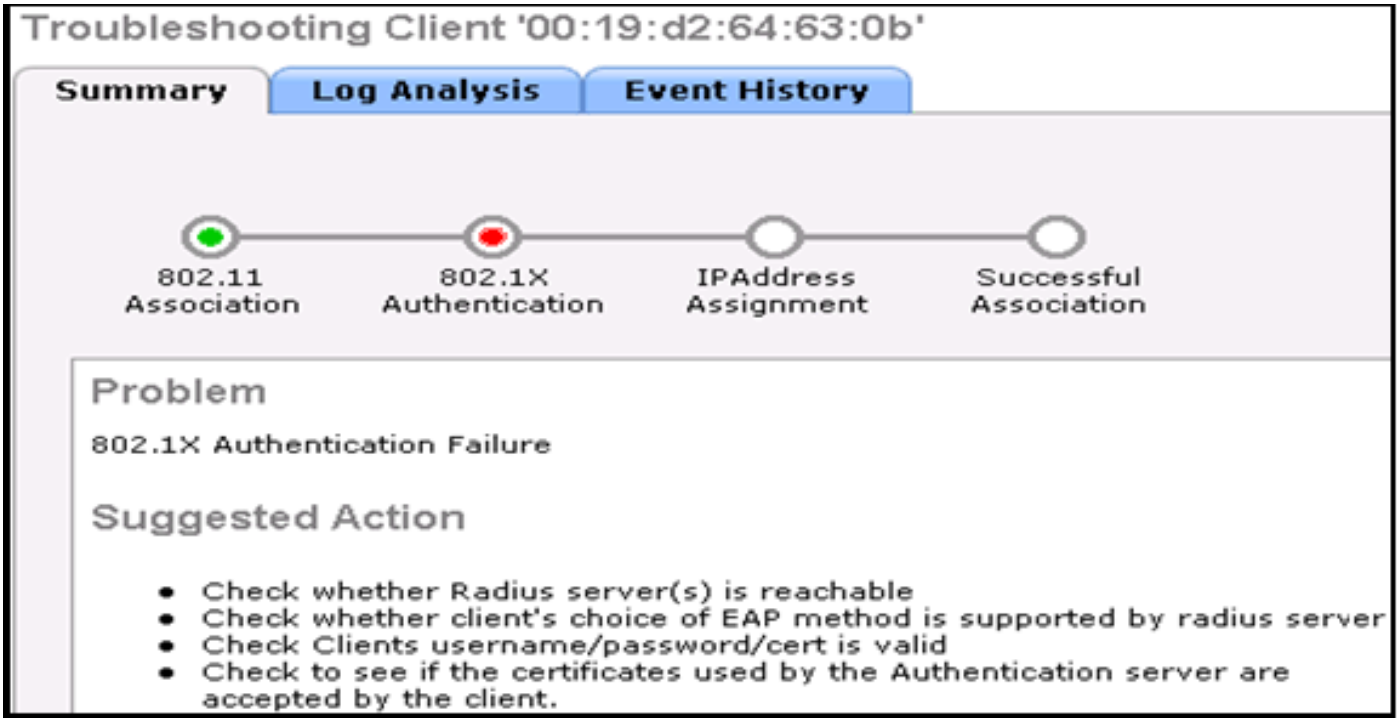



## 802.1X 故障排除

现在采用 WLAN 的情况日益普遍，旧版客户端正逐步淘汰；802.1x 是将来大多数部署的方向。在这条链（客户端 <> AP <> WLC <> L2/L3 网络 <> AAA 服务器）中会出现多种与配置错误相关的问题。此处假设 WLC 和 AAA 服务器之间的所有配置都正确。请求方（客户端）与 AAA 服务器之间发生的问题通常有以下几个：

- EAP 类型错误
- 凭证错误/证书过期
- EAP 内部方法错误

在客户端上，在安全设置下修改用户凭证；例如，输入错误的口令，然后再次运行相同的测试。故障排除工具会准确指出问题所在，并提供建议操作。




单击以上所示图片中的 **Log Analysis** 选项卡，检查日志，查找任何指示 802.1x 身份验证失败的日志内容。

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2 Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2 Received eap failurefrom the client.
```

## Web-Auth 故障排除

一般而言，良好的故障排除做法必须包括对问题客户端的“Policy Manager State”的检查。如以下 WCS 屏幕截图中所确认的，该问题客户端在 *WEBAUTH_REQD* 状态下出现了问题。这意味着 802.11 过程的完成没有任何错误，但可能发生以下问题：

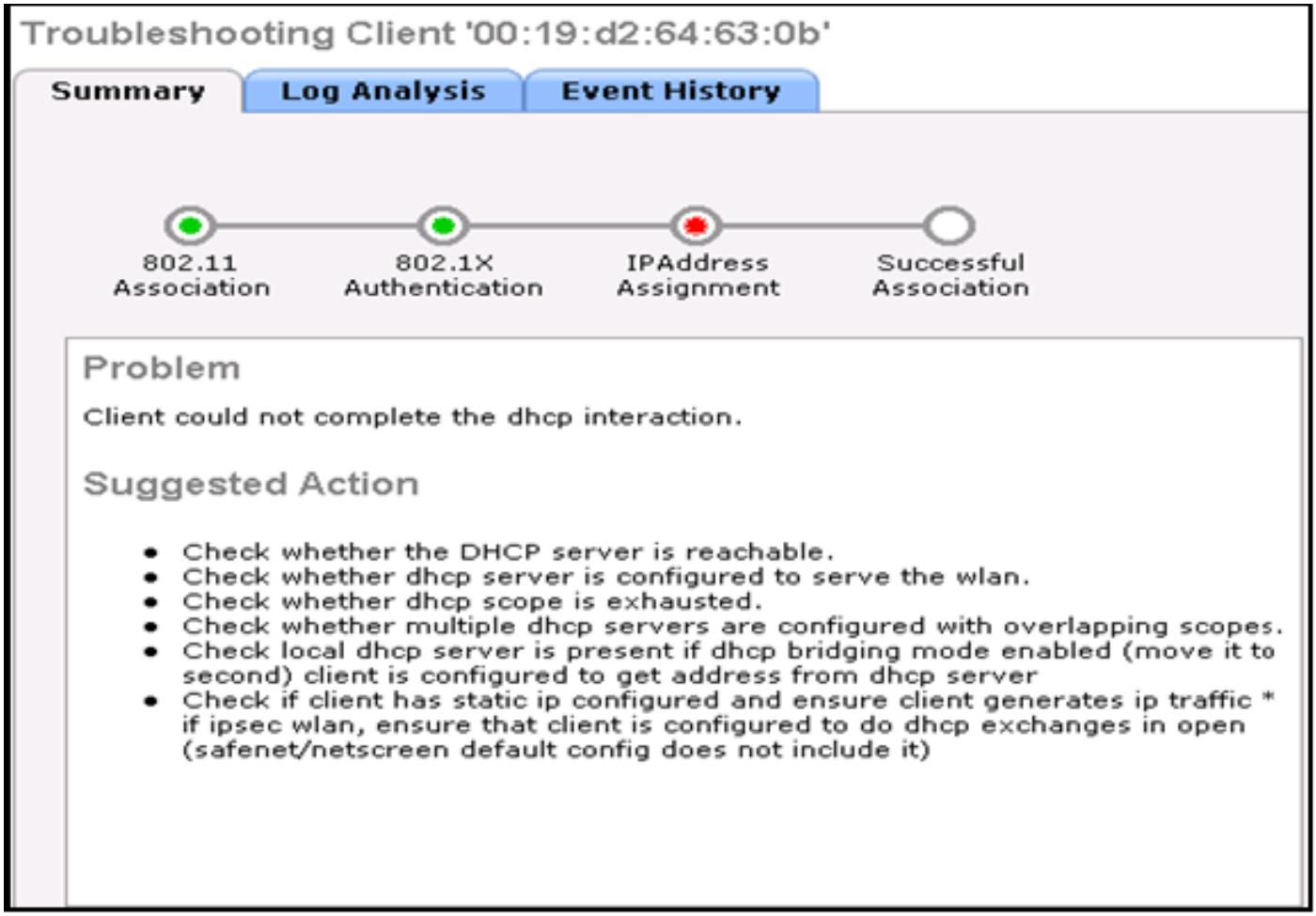
- 用户名/口令错误
- ACL 实施错误（无法访问外部 web-auth 服务器（如果有的话））
- DNS 配置不正确，以及其他问题**注意：** 有关对 Web 身份验证进行故障排除的详细信息，请参阅文档控制器 Web 身份验证配置示例。


从 WCS 收集的日志显示 web-auth 过程未成功。可以在实验室中模拟此种情况，做法是将 WLAN 第 3 层策略设置为 web-auth，然后不去完成 web-auth 过程或输入错误的/不存在的登录凭证。检查客户端故障排除工具的概要部分，了解问题出现在哪里。您将在 WCS 上看到以下日志：

```
 <TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required <TIMESTAMP> INFO 10.10.10.2 Client moved to associated
state successfully <TIMESTAMP> INFO 10.10.10.2 Controller association request message received
```

## DHCP 和 IP 编址故障排除

通常，客户端设备会在不止一个无线网络中使用。例如，员工会在家庭网络或公共网络中使用公司设备。员工在家庭网络中可能分配有一个静态 IP 地址。他/她会在不知情的情况下使用先前分配的静态 IP 地址连接到公司网络。这就会导致连接问题，而通过 WCS 客户端故障排除套件的帮助可以很轻松地指出该问题（如下所示）。这方面的大多数问题都出在无线客户端上，但也可能指向有线基础架构上的潜在问题（例如，范围用尽、范围错误等）。请通过在客户端上分配错误的静态 IP 地址或在交换机上更改 DHCP 范围参数，尝试创建这样一个情景。




## 相关信息

- Cisco 无线 LAN 控制器配置指南 5.1 版
- 统一无线网络中的无线电资源管理
- 技术支持和文档 - Cisco Systems