Cisco无线网络中针对客户端的排错

【翻译内容】

目录

介绍

好的无线网络需要考虑很多因素，本文档介绍客户端在接入 Cisco 无线网络环境时会遇到的问题，并对这些问题提供相应的解决方案。

前提

需求

Cisco 建议您具有以下知识点:

- Cisco 无线方案的基本概念
- 熟悉通过 WLC 图形界面的基本配置

设备要求

本文档使用所有要加入 Cisco 无线网络的客户端，没有硬件及软件版本的特定要求。

背景资料

WLC 是 Cisco 无线环境的核心部分，用于管理整个无线网络，并响应瘦 ap 的注册，并将完整的配置文件下载到瘦 AP 上。首先要确保 AP 成功注册到 WLC 上，可以通过在 WLC 图形界面下 wireless 菜单察看是否有 AP 在列表下。

配置错误

以下为 WLC 上一些常见的错误配置:

SSID 不匹配

客户端使用 SSID 关联无线网络，所以要确保 WLC 和客户端 SSID 一致，通过在 WLC 图形界面下进入 WLAN 页面去验证。

Note: SSID 大小写敏感，更改或者重新创建 SSID，可使客户端重新建立连接。

安全设置不匹配

WLC 和客户端的安全配置要匹配。例如，如果使用封装类型 Static WEP、802.1x 或者 WPA,要确保客户端和 WLC 设置一致。关于 WLC 和客户端安全配置的更多信息，请参考 Authentication on Wireless LAN Controllers Configuration Examples.

Note: 二层安全方案（例如 WPA 或者 802.1X）不能用于三层安全方案（例如 web 认证或 Passthrough）。更多信息请参考 Wireless LAN Controller Layer 2 and Layer 3 Security Compatibility Matrix.

WLAN 未启动

WLC 的无线功能默认为禁用，当配置无线网络时，需要将其启用，通过在图形界面下，点击 WLAN 菜单，选择客户要连接 SSID 的 WLAN，选择 WLAN 〉Edit 启用。

数据速率不支持

WLC 配置中，需要将 802.11a/b/g 某些速率设置为 mandatory，而将其他速率关掉或者设置为 supported，客户端为了能够关联 WLC，必须能够支持 WLC 上设置的强制速率。通过 WLC 图形配置界面菜单 Wireless 进行配置，进入 802.11b/g/n > Network or 802.11a/n > Network 选项。

Note: 为了更好的连接性，将最低速率设置为 mandatory ，而将其他速率设置为 supported.

客户端被屏蔽

WLC 配置中，可以屏蔽可疑行为的客户端，该特性用来禁止非法客户端访问网络，检查 WLC 关联的客户端 MAC 是否出现在 WLC 的客户端屏蔽列表中，在 Security 菜单下点击 Disabled Clients 选项查看。

Note:更多信息请参考 Configuring Client Exclusion Policies

Radio 前导（Preamble）

Radio 前导（或称作 header）是数据报头的一部分数据，包括无线设备何时收发数据等信息。

有些客户端不支持短前导（short preamble），以至于无法连接短前导设置的网络。由于短前导可以改善数据吞吐量的特性，从而在 WLC 上被设置为默认打开。在 WLC 图形界面中通过 Wireless 菜单下， 802.11b/g > network 将该特性关闭。

Cisco 专有特性造成第三方客户端连接故障

如果第三方客户端无法连接，需要将一些 Cisco 私有特性关闭。以下为 Cisco 私有特性：

- Aironet IE: 该特性包括 AP 的名字、负载、关联客户端的数量等信息。CCX 客户端使用这些信息选择最佳 AP 进行关联。
- MFP: 管理帧保护（Management Frame Protection）用来确保管理帧的完整性，避免在传输过程中被篡改、破坏。

  WLC 中，该特性默认情况下打开。在 WLC 图形界面下选择 WLANs 菜单，进入相应的 WLAN 中，点击 Advanced Tab of WLANs > Edit page, 取消选项 Aironet IE and MFP，从而关闭该特性。

IP 地址故障

无线客户端需要 IP 地址与网络通信，如果客户端无法从 WLC 获取地址，请执行以下操作：

1. 如果使用例如 802.1x 或 WPA 的 2 层验证方式,必须正确配置客户端认证以获取有效的 IP。

   Note: 如果客户端配置 3 层认证方式，例如 web authentication, 或者 web passthrough ，客户端将在认证前获取 IP 地址。

2. WLC 上定义的无线网络要与一个动态接口映射，并被配置为相应的 VLAN 及对立的网络。关联到该无线网络的客户端通过该 VLAN 的子网获取相应的 IP 地址。该网段可用地址、网关等信息通过 DHCP 服务器获取。

   Note: 清确保 DHCP 可达，并运行正常。

3. 确保为 WLC 接口 VLAN 配置的 DHCP 服务器 IP 地址正确。通过以下方式检测，进入 **Controller** 菜单，点击 **Interfaces** 菜单， **DHCP** server 选项，确保相关的物理接口正常运行. 通过命令 **debug dhcp packet enable 和 debug dhcp message enable** 查看 WLC 关于 DHCP 的相关信息。

   Note: WLC 可以配置作为 DHCP 服务器，可以参考如下文档 Cisco Wireless LAN Controller Configuration Guide, Release 5.0.

4. WLC 通常使用交换机连接网络，检查连接 WLC 的交换机端口是否配置为 Trunk，是否允许相应的 VLAN 通过。更多信息请参考 Configure the Layer 2 Switch Port that Connects to the WLC as Trunk Port section of the document Guest WLAN and Internal WLAN using WLCs Configuration Example.
5. 如果 WLC 启用了 **DHCP Addr. Assignment field**，客户端只能通过 DHCP 服务器连接网络而不能通过静态设置 IP 地址连入无线网络。通过进入 WLAN 菜单，选中相应的无线网络，进入 **Advanced** 菜单，察看 **DHCP Address Assignment** 的状态.
6. 有些 DHCP 服务器，例如 Cisco PIX 防火墙不支持 DHCP Relay，即只支持基于广播的 DHCP 数据包，而不支持基于单播的 DHCP 数据包。请确保客户端连接的端口上启动了 DHCP server 功能。

   Note: DHCP Relay 的支持特性请参考相关产品手册。

客户端故障

客户端一侧的操作检查同样重要！客户端执行以下步骤：

1. 有时，无线网卡无法被识别，请尝试更换插槽或者计算机测试。更新信息请参考 Troubleshooting section of the document Cisco Aironet 340,

350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.

Note: 确保操作系统能够支持无线网卡

2. 通过设备管理器确保驱动正确安装。如果显示“该设备工作正常”则表明驱动安装正确，否则请尝试卸载并重新安装。更多信息请参考 Installing the Client Adapter section of the document Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.

   Note:如果使用 ACU 配置无线网卡，请确保射频功能打开，另外在网络连接中检查无线网络是否被启用。

3. 确保客户端 SSID、安全等配置与 WLC 的配置相匹配，如果使用 Cisco 客户端软件，请参考 Using the Profile Manager section of the document Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.
4. 如果可以连接到无线网络，但是无法传输数据，请尝试关闭其他连接，包括 VPN、有线连接等。如果有多个无线网卡，请将其关闭，以免冲突.
5. 如果某个客户端有问题，请尝试更新其驱动；如果有大量客户端出现问题，请升级 WLC。
6. 确保使用 WIFI 认证的无线设备，以避免兼容性问题
7. 如果使用微软系统和软件，请确保安装最新的补丁
8. 有些客户端反映 EAP 验证速度过慢，导致关联 WLC 超时，WLC 上收到以下提示：

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

WLC 上使用以下命令增加 EAP 的验证时间，防止超时

config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries <1-20>

config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>

```
config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>
```

射频故障

射频干扰会降低连接性能。射频干扰主要来自附近的 802.11 设备，或者其他的干扰源如微波、无绳电话。来自附近的 802.11 设备的干扰有两种类型：

- **共信道干扰 Co-channel interference**：多个 AP 的覆盖范围重叠，使用相同的信道或者频谱重叠造成共信道干扰。确保使用非重叠的信道，例如 802.11 使用信道 1/6/11
- **邻近信道干扰 Adjacent Channel interference**：AP 之间距离太近，即使他们工作在非重叠的信道，如果使用较强的功率也会造成干扰。可以通过降低 AP 的发射功率解决。

使用频谱分析仪定位使用 2.4G 频段的微波、无绳电话、或者 5G 频段的干扰源。另一个影响无线通信的因素是信号强度，障碍物例如墙、金属可以吸收无线信号而从降低信号的强度。可以通过增加功率或者使用高增益天线来解决该故障。

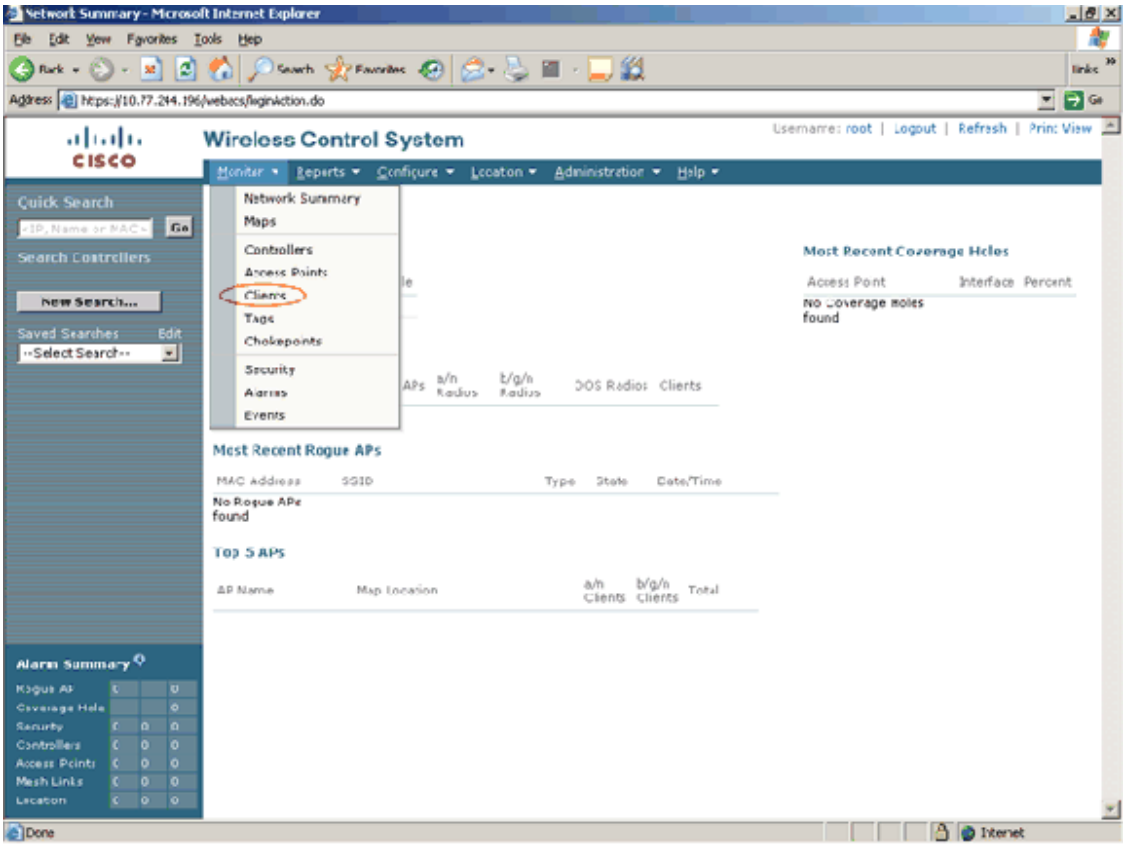
Note：信噪比不同于信号强度和噪音，是影响链路质量和通信速度的主要因素。低的信噪比会降低通信的性能以及造成连接中断。现场分析工具可以显示某个位置的信噪比以及吞吐性能。

射频资源管理（RRM）是 WLC 中集成的软件特性，可以适时的提供射频信号管理，更多信息请参考 Configuring Radio Resource Management section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.0.

使用 WCS 排错客户端故障

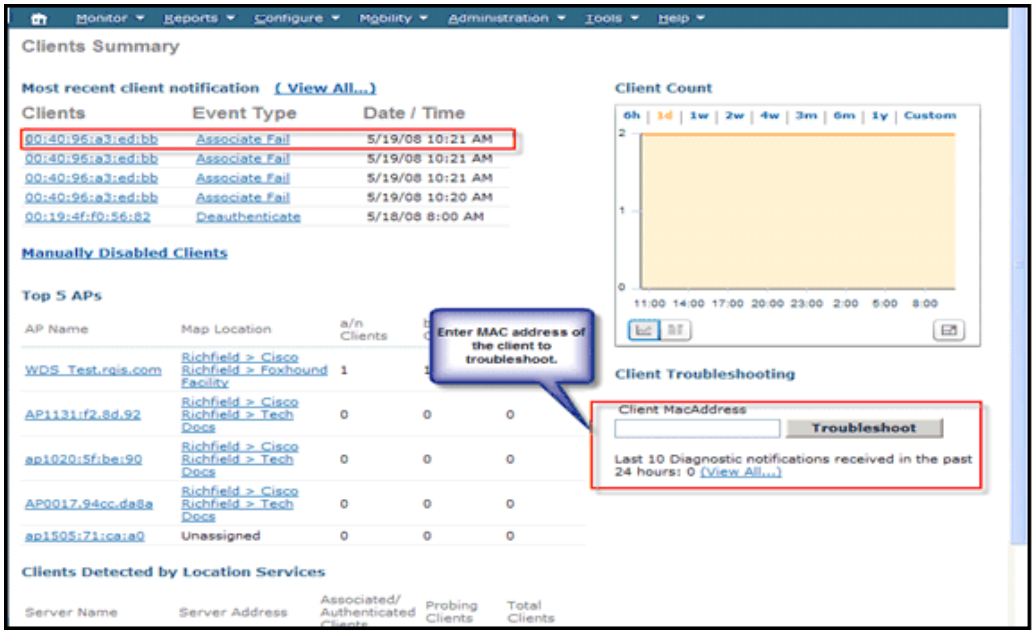
WCS 的排错软件可以使用如下步骤排错与客户端有关的故障：

1. 点击 **Monitor** 菜单，选择 **Clients**.



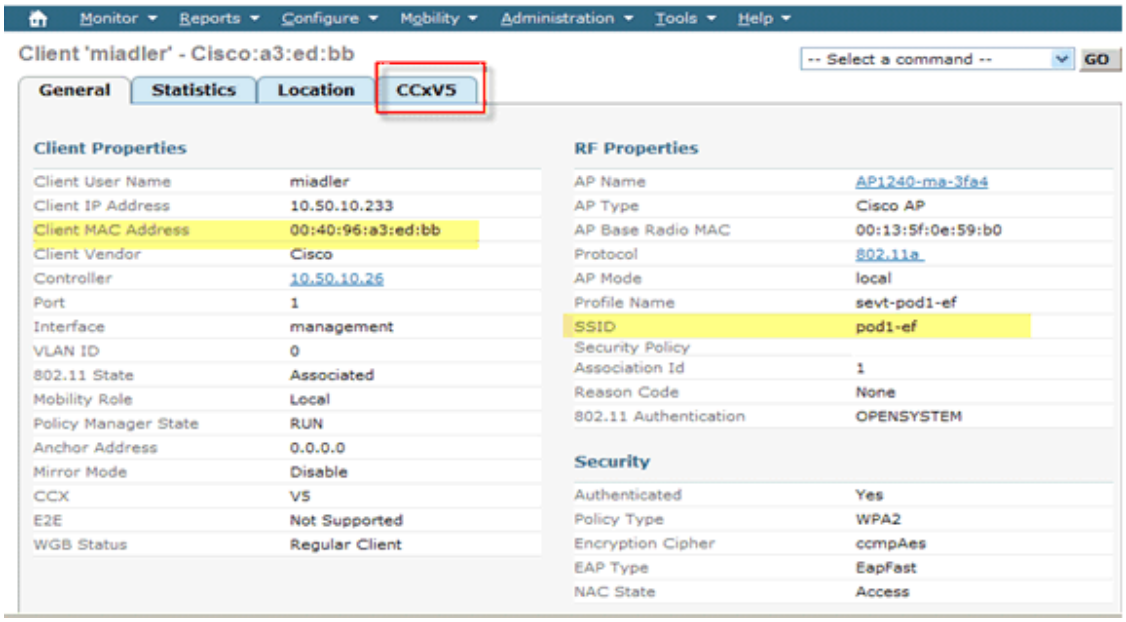
2. 弹出客户端信息页面，如 Figure 1,

Figure 1



3. 选中其中一个客户端可以看到 SSID 等信息，如 Figure 2 。Figure 1 右下角 Troubleshoot 中可以输入需要排错的 MAC 地址. 弹出的新页面如 Figure 3.

Figure 2



WEP 排错

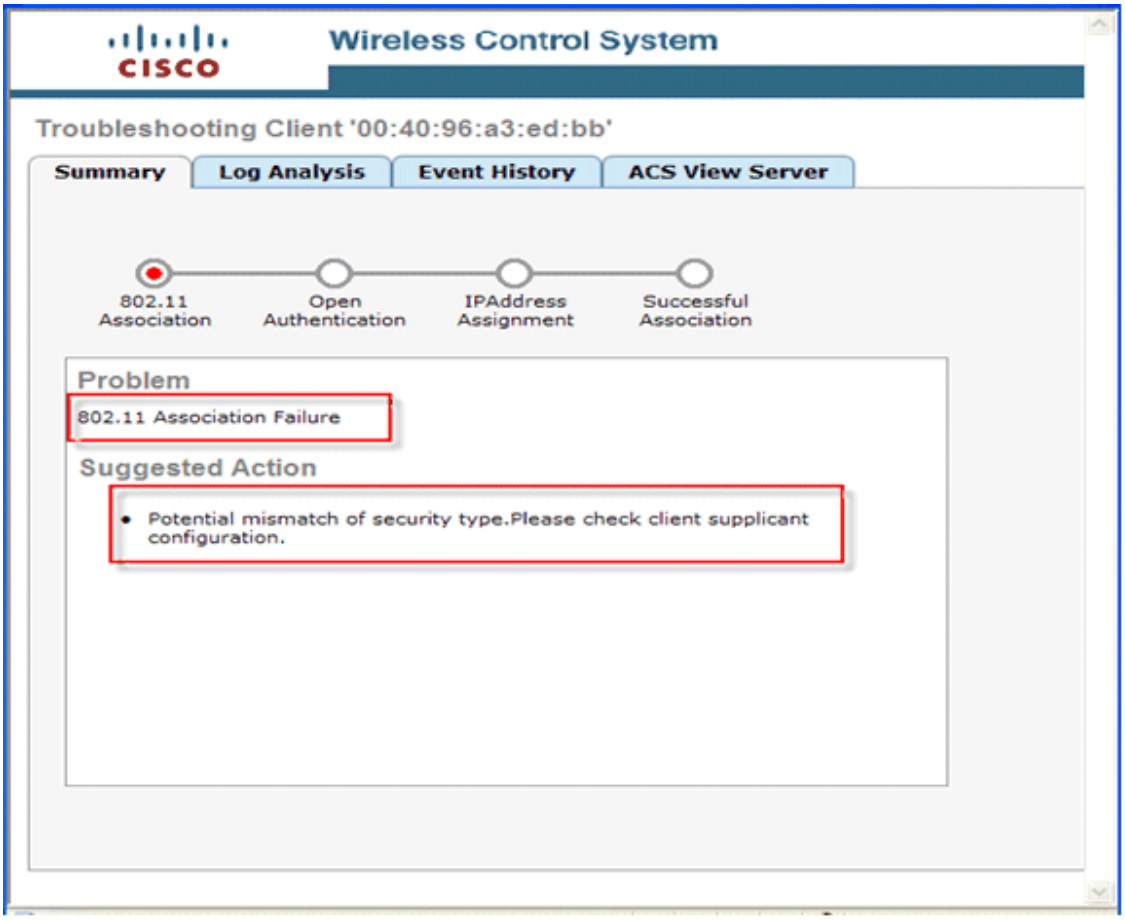
传统的无线客户端使用的 WEP 安全机制排错较难。在客户端和 AP 上检查以下选项：

- WEP 密钥长度(密钥不匹配)
- WEP 密钥索引(配置不匹配)
- 验证方式(open versus shared key)

验证方式不匹配

WCS 客户端排错工具可以方便快捷的帮助找出问题的存在。Figure 2 所示为 **WCS 排错工具**.

Figure 3



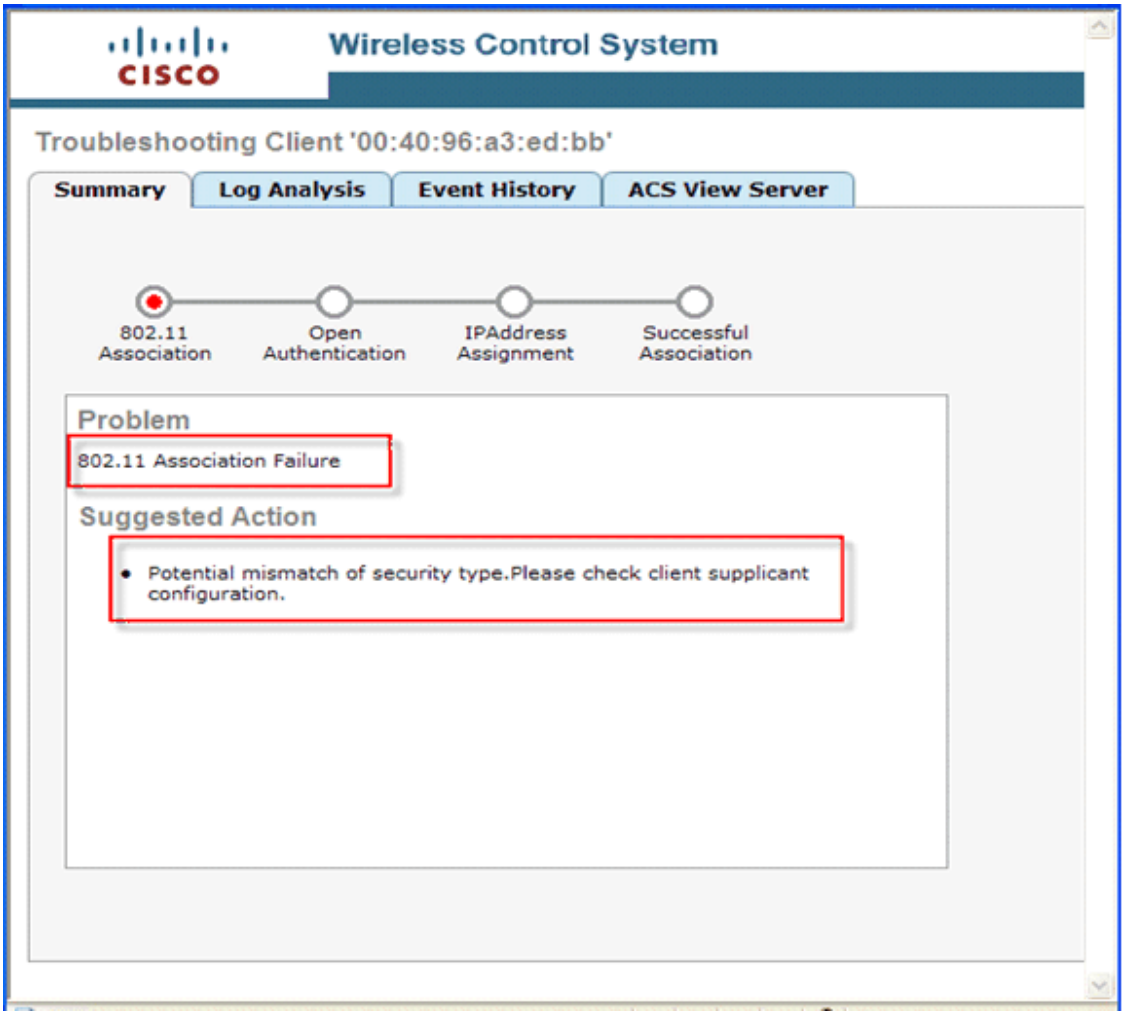
WEP 密钥索引不匹配

通常，客户端和 AP 上可以配置多大 4 个 WEP 密钥。其中 1 个作为传输密钥，该密钥在客户端和 AP 上必须匹配。例如，如果 AP 使用密钥 2 作为传输密钥，客户端也必须使用密钥 2。另一个需要注意的是，有些厂商将的密钥索引为 0 到 3，而有些为 1-4，这会导致索引双方不匹配，而造成连接失败，所以，需要观察报文中“Key ID”字段。

WPA-PSK 排错

WPA-PSK 的排错在很多情况下类似 WEP，很多错误是由于密钥不匹配。通过 WCS 客户端排错工具，管理员可以收集 WPA 传输的日志信息。以下 log 粗体部分显示可能存在的问题（客户端错误的配置了 pre-shared key）。无线网络使用 WPA-PSK 作为 2 层加密策略，而客户端错误的配置了 PSK。如下所示：

<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.

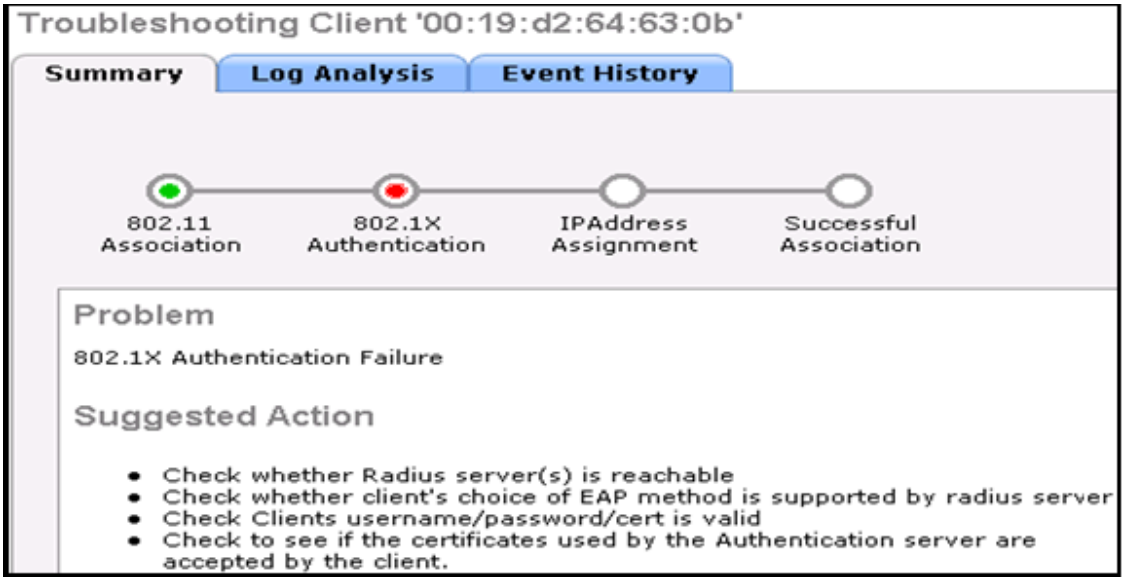


802.1X 排错

随着 WLAN 的普及，传统的客户端逐步被淘汰；部署 802.1x 是一个新的趋势。 但会造成一些列不匹配的故障(client <> AP <> WLC <> L2/L3 network <> AAA server)． 客户端和 AAA 服务器之间的不匹配有以下几种：

- 错误的 EAP 类型
- 错误的证书或证书过期
- 错误的 EAP 内部方法

例如在客户端错误的输入了密码，通过 WCS 排错工具可以清晰的指出问题的所在：



点击 Log Analysis 可以看到认证没有成功的信息

<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 排错

一个好的排错过程需要包括客户端的“Policy Manager State”，如以下所示，出现问题的客户端停留在 WEBAUTH_REQD 状态。这意味着 802.11 过程成功的完成了，可能发生了以下错误：

- 错误的用户名/密码
- 错误的访问控制列表（访问外部 Web 验证服务器）
- DNS 没有正确配置等

Note: 更多关于 web 认证的排错，请参考 Controller Web Authentication Configuration Example.

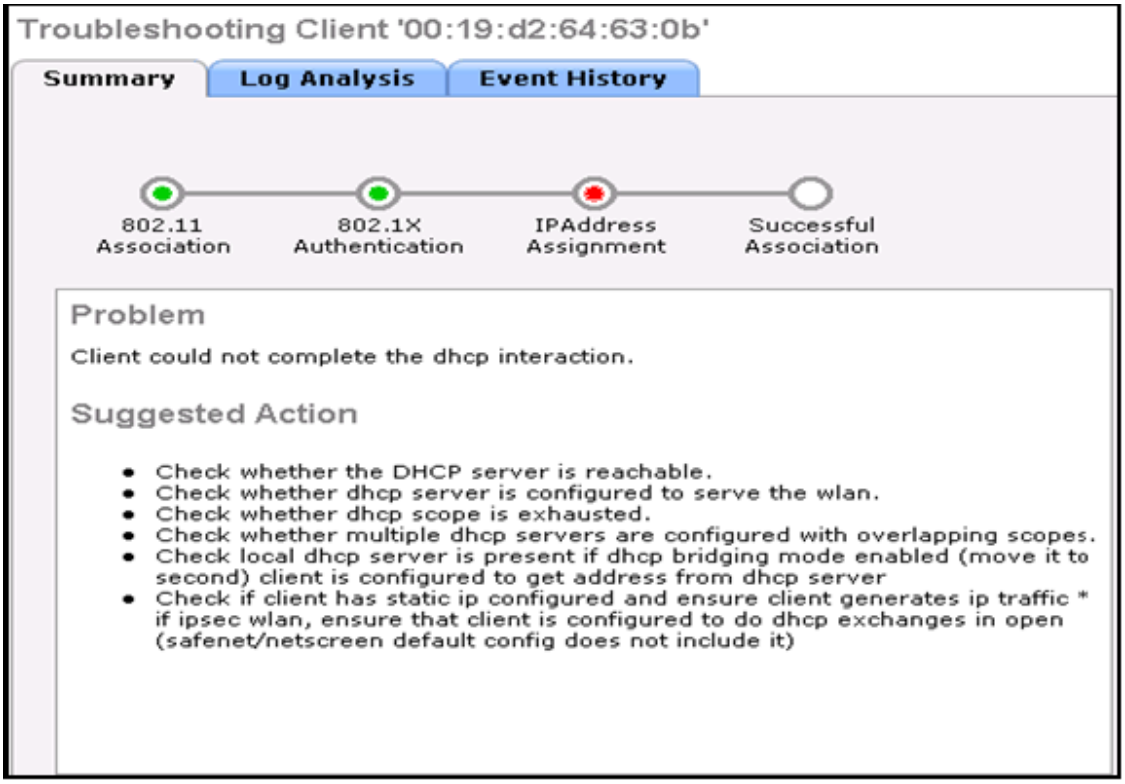
日志信息显示 web 认证没有成功。在实验环境中，可以通过以下方式模拟，如使 web 认证安全特性，但是输入错误的用户登陆信息。通过 WCS 客户端排错工具可以看到如下信息

<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 and IP Addressing 排错

通常，客户端使用多个无线网络，比如员工在家使用静态地址，但是在公司也错误的使用了静态地址，便导致了连接错误。这可以通过 WCS 客户端排错工具（如下所示）找到问题的原因。该工具同样可以找出一些隐性问题，如地址空间不足、错误的地址范围等。


Troubleshooting Client '00:19:d2:64:63:0b'
Summary
Log Analysis
Event History
802.11 Association
802.1X Authentication
IPAddress Assignment
Successful Association
Problem
Client could not complete the dhcp interaction.
Suggested Action
Check whether the DHCP server is reachable.
Check whether dhcp server is configured to serve the wlan.
Check whether dhcp scope is exhausted.
Check whether multiple dhcp servers are configured with overlapping scopes.
Check local dhcp server is present if dhcp bridging mode enabled (move it to second) client is configured to get address from dhcp server
Check if client has static ip configured and ensure client generates ip traffic * if ipsec wlan, ensure that client is configured to do dhcp exchanges in open (safenet/netscreen default config does not include it)