WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例

目录

简介

本文档说明了如何使用外部 RADIUS 服务器针对可扩展的认证协议 (EAP) 身份验证配置无线 LAN 控制器 (WLC)。此配置示例使用思科安全访问控制服务器(ACS)，外部RADIUS服务器为了验证用户凭证。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 轻量级接入点(AP)和思科WLCs的配置的基础知识。
- 基本了解轻量 AP 协议 (LWAPP)。
- 知识如何配置一个外部RADIUS服务器类似Cisco Secure ACS。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Aironet 1232AG 系列轻量 AP
- 运行固件 5.1 的 Cisco 4400 系列 WLC
- 运行 4.1 版的 Cisco 安全 ACS
- Cisco Aironet 802.11 a/b/g 客户端适配器
- Cisco Aironet Desktop软件(ADU)该运行固件4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）查找有关本文档所使用命令的详细信息。

完成这些步骤可为 EAP 身份验证配置设备：

1. 配置 WLC 进行基本操作并将轻量 AP 注册到控制器。
2. 配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证。
3. 配置 WLAN 参数。
4. 将 Cisco Secure ACS 配置为外部 RADIUS 服务器并创建身份验证客户端的用户数据库。

网络图

在此设置中，Cisco 4400 WLC 和一个轻量 AP 通过集线器相连。一个外部 RADIUS 服务器（Cisco 安全 ACS）也连接到同一个集线器。所有设备都在同一个子网中。AP 首先注册到控制器。您必须配置WLC和AP轻量级扩展身份认证协议(LEAP)验证的。连接到 AP 的客户端使用 LEAP 身份验证与 AP 关联。使用 Cisco 安全 ACS 执行 RADIUS 身份验证。

配置 WLC 进行基本操作并将轻量 AP 注册到控制器

使用命令行界面 (CLI) 中的启动配置向导来配置 WLC，以便进行基本操作。此外，也可以使用 GUI 配置 WLC。本文档介绍用 CLI 中的启动配置向导对 WLC 进行的配置。

首次启动 WLC 之后，它将直接进入启动配置向导。使用配置向导配置基本设置。可以在 CLI 或 GUI 中运行该向导。以下输出展示 CLI 中启动配置向导的示例：

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.77.244.204 Management Interface Netmask: 255.255.255.224 Management Interface Default Router:
10.77.244.220 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 10.77.244.220 AP Manager Interface IP
Address: 10.77.244.205 AP-Manager is on Management subnet, using same values AP Manager
Interface DHCP Server (10.77.244.220): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group
```

```
Name: Test Network Name (SSID): Cisco123 Allow Static IP Addresses [YES][no]: yes Configure a
RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS
server. Please see documentation for more details. Enter Country Code (enter 'help' for a list
of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configuration saved!
Resetting system with new configuration..
```

这些参数为基本操作设置 WLC。在此配置示例中，WLC 使用 **10.77.244.204** 作为管理接口 IP 地址，使用 10.77.244.205 作为 AP 管理器接口 IP 地址。

轻量 AP 必须注册到 WLC，然后才能在 WLC 上配置任何其他功能。本文档假定轻量 AP 已注册到 WLC。如何的更多信息参考轻量AP (LAP)注册到无线局域网控制器(WLC)关于轻量AP向WLC登记。

配置 WLC 以便通过外部 RADIUS 服务器进行 RADIUS 身份验证

需要配置 WLC 以便将用户凭证转发到外部 RADIUS 服务器。外部RADIUS服务器然后验证用户凭证和提供访问对无线客户端。

完成以下这些步骤，为外部 RADIUS 服务器配置 WLC：

1. 从控制器的 GUI 中选择**安全性**和“RADIUS 身份验证”，以便显示“RADIUS 身份验证服务器”页。然后，单击**新建**定义 RADIUS 服务器。
2. 在 **RADIUS 身份验证服务器 > 新建**页中定义 RADIUS 服务器参数。这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。Network User 和 Management 复选框决定基于 RADIUS 的身份验证是否适用于 WLC 管理和网络用户。此示例使用Cisco Secure ACS作为IP地址为10.77.244.196的 RADIUS服务器。
3. WLC 现在可使用 RADIUS 服务器进行身份验证。如果选择 **Security > Radius > Authentication**，则可以发现列出了 RADIUS 服务器。支持RFC 3576在Cisco CNS接入登记程序(CAR) RADIUS服务器，但是不Cisco Secure ACS服务器版本4.0和前。还可以使用本地 RADIUS 服务器功能验证用户的身份。随 4.1.171.0 版代码引入了本地 RADIUS 服务器。运行以前版本的 WLC 没有本地 RADIUS 功能。本地 EAP 是允许用户和无线客户端在本地进行身份验证的身份验证方法。当后端系统中断或外部身份验证服务器停机时，它用于要与无线客户端保持连接的远程办事处。本地 EAP 从本地用户数据库或 LDAP 后端数据库检索用户凭证，以便对用户进行身份验证。本地 EAP 支持在控制器与无线客户端之间进行 LEAP、具有 PAC 的 EAP-FAST、具有证书的 EAP-FAST 和 EAP-TLS 身份验证。本地 EAP 旨在作为备用身份验证系统。如果在控制器上配置任何 RADIUS 服务器，则控制器将首先尝试用 RADIUS 服务器对无线客户端进行身份验证。只有在因 RADIUS 服务器超时或未配置任何 RADIUS 服务器而找不到任何 RADIUS 服务器时才尝试本地 EAP。有关如何在无线 LAN 控制器上配置本地 EAP 的详细信息，请参阅无线 LAN 控制器上的 EAP-FAST 本地 EAP 身份验证以及 LDAP 服务器配置示例。

配置 WLAN 参数

下一步，配置客户端连接无线网络所使用的 WLAN。在配置 WLC 的基本参数时，也配置了 WLAN 的 SSID。可以对 WLAN 使用此 SSID 或创建新的 SSID。在本例中，您创建新的 SSID。

注意： 在控制器上最多可以配置十六个 WLAN。Cisco WLAN 解决方案对轻量 AP 最多可以控制十六个 WLAN。可以向每个 WLAN 都分配唯一的安全策略。轻量 AP 广播所有活动的 Cisco WLAN 解决方案 WLAN SSID，并实施为每个 WLAN 定义的策略。

完成以下这些步骤以配置新 WLAN 及其相关参数：

1. 从控制器的 GUI 中单击 **WLAN** 以显示“WLAN”页。此页列出控制器上存在的 WLAN。
2. 选择**新建**创建新的 WLAN。输入 WLAN 的 Profile Name 和 WLAN SSID，然后单击 **Apply**。本例使用 Cisco 作为 SSID。
3. 创建新 WLAN 后，就会显示新 WLAN 的 WLAN > Edit 页。在此页中，可以定义此 WLAN 特有的各种参数，其中包括常规策略、安全策略、QoS 策略和其他高级参数。从下拉菜单中选择相应的接口。可以根据 WLAN 网络的需要修改其他参数。选中常规策略下的 **Status** 框以启用 WLAN。
4. 单击 **Security** 选项卡，然后选择 Layer 2 Security。从 Layer 2 Security 下拉菜单中选择 **802.1x**。在 802.1x 参数中，选择 WEP 密钥大小。本例使用 128 位 WEP 密钥，它是 104 位 WEP 密钥加上 24 位初始化矢量。
5. 选择 **AAA Servers** 选项卡。从 Authentication Servers (RADIUS) 下拉菜单中选择相应的 RADIUS 服务器。此服务器用于对无线客户端进行身份验证。
6. 单击 **Apply** 保存配置。

将 Cisco 安全 ACS 配置为外部 RADIUS 服务器并创建身份验证客户端的用户数据库

完成以下这些步骤，在 Cisco 安全 ACS 上创建用户数据库并启用 EAP 身份验证：

1. 从 ACS GUI 中选择 **User Setup**，输入用户名，然后单击 Add/Edit。本例中用户为 **ABC**。
2. User Setup 页出现后，定义该用户特有的所有参数。本例中配置用户名、密码和 Supplementary User Information，因为对于 EAP 身份验证只需要此参数。单击 **Submit**，并重复同一过程以向数据库添加更多用户。默认情况下，所有用户都被分在默认组下，并向这些用户分配为该组定义的同一个策略。如果要将特定用户分配给不同组，请参阅适用于 Windows 服务器的 Cisco 安全 ACS 3.2 用户指南的用户组管理部分获取详细信息。
3. 定义控制器作为 ACS 服务器上的 AAA 客户端。从 ACS GUI 中单击 **Network Configuration**。出现 Network Configuration 页时，定义 WLC 的名称、IP 地址、共享密钥和身份验证方法 (RADIUS Cisco Airespace)。有关其他非 ACS 身份验证服务器的信息，请参阅制造商提供的文档。**注意：** 在 WLC 和 ACS 服务器上配置的共享密钥必须匹配。共享密钥区分大小写。
4. 单击 **System Configuration** 和 Global Authentication Setup 以确保将身份验证服务器配置为执行期望的 EAP 身份验证方法。在 EAP 配置设置下，选择相应的 EAP 方法。本例使用 LEAP 身份验证。完成后，单击 **Submit**。

配置客户端

还应针对相应的 EAP 类型配置客户端。在 EAP 协商过程中，客户端向服务器提议采用 EAP 类型。如果服务器支持该 EAP 类型，则其确认 EAP 类型。如果不支持 EAP 类型，则服务器发送一个否定确认，而客户端下次将用不同的 EAP 方法进行协商。直到用支持的 EAP 类型协商时，此过程才会继续。本例使用 LEAP 作为 EAP 类型。

完成以下这些步骤以便用 Aironet Desktop Utility 配置客户端上的 LEAP。

1. 双击 **Aironet Utility** 图标将其打开。
2. 单击 **Profile Management** 选项卡。
3. 单击某个配置文件，然后选择 **Modify**。
4. 在 General 选项卡下选择 *Profile Name*。输入 WLAN 的 **SSID**。**注意：** SSID 区分大小写，并且需要与在 WLC 上配置的 SSID 完全匹配。
5. 在 **Security** 选项卡下选择 *802.1x*。选择 EAP 类型作为 **LEAP**，然后单击 Configure。
6. 选择 **Use Temporary Username and Password**，它将在每次重新启动计算机时提示您输入用

户凭据。选中此处给出的三个选项之一。本例使用 **Automatically Prompt for Username and Password**，它要求您在登录 Windows 之前除了输入 Windows 用户名和密码，还要输入 *LEAP* 用户凭据。如果希望在客户端适配器漫游和重新关联到网络时 LEAP 请求方始终尝试恢复上次会话，而无须提示重新输入凭据，则选中窗口顶部的 **Always Resume the Secure Session** 复选框。**注意：** 有关其他选项的详细信息，请参阅 Cisco Aironet 802.11a/b/g 无线局域网客户端适配器（CB21AG 和 PI21AG）安装和配置指南的配置客户端适配器部分。

7. 在 **Advanced** 选项卡下，可以配置 Preamble、Aironet extension 和其他 802.11 选项，如 Power、Frequency 等等。
8. 单击 **Ok**。客户端现在尝试与所配置的参数关联。

验证

使用本部分可确认配置能否正常运行。

尝试使用 LEAP 身份验证将无线客户端与轻量 AP 关联，以验证配置是否按预期工作。

注意： 本文档假定为 LEAP 身份验证配置了客户端配置文件。有关如何为 LEAP 身份验证配置 802.11 a/b/g 无线客户端适配器的详细信息，请参阅使用 EAP 身份验证。

激活无线客户端的配置文件后，即要求用户提供 LEAP 身份验证的用户名/密码。示例如下：

轻量 AP 和 WLC 先后将用户凭据传递给外部 RADIUS 服务器（Cisco 安全 ACS）以验证凭据。RADIUS 服务器将数据与用户数据库进行比较，并在用户凭据有效时提供对无线客户端的访问以验证用户凭据。ACS 服务器的 Passed Authentication 报告表示客户端已通过 RADIUS 身份验证。示例如下：

RADIUS 身份验证成功后，无线客户端即与轻量 AP 关联。

在 WLC GUI 的 **Monitor** 选项卡下也可以检查此情况。选择 **Monitor > Clients**，然后检查客户端的 MAC 地址。

故障排除

完成以下这些步骤以排除配置的故障：

1. 使用 **debug lwapp events enable** 命令检查 AP 是否注册到 WLC。
2. 检查 RADIUS 服务器是否从无线客户端接收并验证身份验证请求。检查 NAS-IP-Address、Date 和 Time 以验证 WLC 是否能访问 RADIUS 服务器。检查 ACS 服务器上的 Passed Authentications 和 Failed Attempts 报告以完成此操作。在ACS服务器上的报表和活动下可获得这些报表。下面是 RADIUS 服务器身份验证失败时的一个示例：**注意：** 有关如何对 Cisco 安全 ACS 上的调试信息进行故障排除和获取这些信息，请参阅获取适用于 Windows 的 Cisco 安全 ACS 的版本和 AAA 调试信息。
3. 还可以使用这些 **debug** 命令排除 AAA 身份验证的故障：**debug aaa all enable** — 配置所有 AAA 消息的调试。**debug dot1x packet enable** — 启用对所有 dot1x 数据包的调试。这是从 **enable命令调试的802.1x aaa的**一输出示例：：`(Cisco Controller) >debug dot1x aaa enable`

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23
15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23
15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23
15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.793:
00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.793:
```

00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11 *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8, id=2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43 .....ABC *Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] **Sending auth request to 'RADIUS' (proto 0x140001)** *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1, length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f ....B:...$.. *Sep 23 15:15:43.799: 00000010: 41 42 43 ABC *Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=35, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed ...#......[2.e.. *Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13 ..O...5..k..WP.. *Sep 23 15:15:43.904: 00000020: 41 42 43 ABC *Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response' *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 **AAA Message 'Interim Response' received for mobile 00:40:96:ac:dd:05** *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=3, dot1xcb->id = 3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.907: 00000000: 03 03 00 04 .... *Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=1 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8 *Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12 *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.. !!!! *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1, length=19, id=3) for mobile 00:40:96:ac:dd:05 *Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae ....)#...l.. *Sep 23 15:15:43.915: 00000010: 41 42 43 ABC *Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (proto 0x140001) *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **AAA response 'Success'** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] **Returning AAA response** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 **AAA Message 'Success' received for mobile 00:40:96:ac:dd:05** *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing

```
avps[0]: attribute 8, vendorId 0, valueLen 4 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05
processing avps[1]: attribute 79, vendorId 0, valueLen 35 *Sep 23 15:15:43.918:
00:40:96:ac:dd:05 Received EAP Attribute (code=2, length=35,id=3) for mobile
00:40:96:ac:dd:05 *Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6
c3 4c ...#.....f,j...L *Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6
92 ce 60 a6 ..i.....).V...`. *Sep 23 15:15:43.918: 00000020: 41 42 43 ABC *Sep 23
15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1, vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25, vendorId 0,
valueLen 21 *Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
vendorId 0, valueLen 16
```

注意： 某些线路在debug输出中包裹的归结于空间限制条件。

4. 监视 WLC 上的日志，以检查 RADIUS 服务器是否接收用户凭据。单击 **Monitor** 从 WLC GUI 中检查这些日志。从左侧的菜单中单击 **Statistics**，然后从选项的列表中单击 RADIUS 服务器。这非常重要，因为在某些情况下如果 WLC 上的 RADIUS 服务器配置错误，则 RADIUS 服务器将永不接收用户凭据。下面是当 RADIUS 参数配置错误时 WLC 上显示日志的方式：可以使用 **show wlan summary** 命令的组合以识别您的哪些 WLAN 使用 RADIUS 服务器身份验证。然后，可以查看 **show client summary** 命令以了解哪些 MAC 地址（客户端）在 RADIUS WLAN 上成功地通过了身份验证。也可以将此与 Cisco 安全 ACS 的 passed attempts 或 failed attempts 日志关联。

故障排除提示

- 确认控制器上 RADIUS 服务器处于 active 状态而非 standby 或 disabled。
- 使用 **ping** 命令检查是否可从 WLC 访问 RADIUS 服务器。
- 检查 RADIUS 服务器是否为从 WLAN (SSID) 的下拉菜单中选择的。
- 如果使用 WPA，则必须安装适用于 Windows XP SP2 的最新 Microsft WPA 修补程序。此外，应将客户端请求方的驱动程序升级到最新。
- 如果采用 PEAP，例如 XP SP2 的证书，其中由 Microsoft wireless-0 实用程序管理卡，则需要从 Microsoft 获得 KB885453 修补程序。如果使用 Windows Zero Config/客户端请求方，则禁用 **Enable Fast Reconnect**。如果选择 **Wireless Network Connection Properties > Wireless Networks > Preferred networks**，则可以这样做。然后选择 **SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect**。然后，可以在窗口末尾找到启用或禁用的选项。
- 如果使用 Intel 2200 或 2915 卡，请参阅 Intel 网站上有关其卡已知问题的声明：Intel® PRO/Wireless 2200BG 网络连接Intel® PRO/Wireless 2915ABG 网络连接下载最新的 Intel 驱动程序以避免出现任何问题。可以从 http://downloadcenter.intel.com/ 下载 Intel 驱动程序
- 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。但是，不应这样做，因为如果采用安静丢弃，则 AAA 服务器可能仅对该特定客户端不响应。它可以是对其他具有有效证书的有效客户端的响应。但是，WLC 仍可将 AAA 服务器标记为 not responding，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。从控制器 GUI 中发出 **config radius aggressive-failover disable** 命令执行此功能。如果禁用了此操作，则当连续三个客户端都未能从 RADIUS 服务器收到响应时，控制器将只会故障切换到下一个 AAA 服务器。

操作的EAP计时器

在802.1x验证时，用户也许发现`DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE MAX EAPOL-Key M1 retransmissions reached for mobile xx:xx xx xx xx`错误消息。

此错误消息表明客户端没有响应及时到控制器在WPA (802.1x)密钥协商时。控制器在关键协商时设置答复的一个计时器。一般，当您看到此消息时，它归结于与请求方的一个问题。确保您运行客户

端驱动程序和固件最新的版本。在WLC，有您能操作帮助与客户端验证的一些个EAP计时器。这些EAP计时器包括：

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

在您能调整这些值前，您需要知道什么他们执行，并且更改他们如何将影响网络：

- **EAP标识请求超时**：此计时器影响您多久等待在EAP标识请求之间。默认情况下，这是一秒钟(4.1和降低)和30秒(4.2和更加极大)。此更改的原因是，因为一些客户端、手helds、电话，扫描仪等，有困难时期响应足够快速。设备类似膝上型计算机，通常不要求这些值的处理。可用的值是从1到120。因此，当此属性设置为值为30时，什么发生？当客户端首先连接时，它发送EAPOL开始对网络，并且WLC发送在EAP数据包下，请求用户或计算机的标识。如果WLC不收到标识答复，发送另一标识请求在第一以后的30秒。这在初始连接发生，并且，当客户端漫游。当我们增加此计时器，什么发生？如果一切是好，没有影响。然而，如果有在网络的一个问题(包括客户端问题、AP问题或者RF问题)，它能的网络连通性导致延迟。例如，如果设置计时器为最大值120秒， WLC等在标识请求之间的2分钟。如果客户端漫游，并且答复没有由WLC接收，则我们创建，最少，此客户端的一两分钟中断。此计时器的建议是*5*。此时，没有理由放置此计时器在其最大值。
- **EAP标识请求最大重试次数**：最大重试次数值是WLC将发送标识请求给客户端的次数，在删除其条目前从MSCB。一旦最大重试次数被到达， WLC发送解除验证帧给客户端，迫使他们重新启动EAP进程。可用的值是1到20。其次，我们将较详细地查看此。最大重试次数与标识超时一起使用。如果安排您的标识超时设置到120，并且您的最大重试次数到20多久执行它采取2400(或120 * 20)。这意味着将需要客户端的40分钟能将删除和开始EAP进程再。如果设置标识超时到5，与最大重试次数值为12，则它将采取60 (或5 * 12)。与前一个示例对比，有一分钟，直到客户端删除并且必须开始EAP。最大重试次数的建议是*12*。
- **关键超时**：对于EAPOL-Key超时值，默认是1秒或1000毫秒。这意味着，当EAPOL密钥被交换在AP和客户端之间时默认情况下， AP将发送密钥和等待至1秒客户端的能响应。在等待定义的时间时间值以后， AP再将重新传输密钥。您能使用**设置提前的eap EAPOL KEY超时***<time>*命令为了修改此设置。在6.0的可用的值是在200和5000毫秒之间，而在6.0之前的代码允许在1和5秒范围的值。记住，如果有不响应对一关键尝试的一个客户端，扩大计时器能提供他们有点更多时刻响应。然而，为WLC/AP采取对解除验证客户端为了整个802.1x进程能重新开始的这可能也延长时间。
- **EAPOL-Key最大重试次数**：对于EAPOL-Key最大重试次数值，默认是2。这意味着我们两次将再试原始关键尝试给客户端。使用**设置提前的eap EAPOL KEY重试次数***<retries>*命令，此设置可以被修改。可用的值在0和4重试次数之间。使用关键超时的(即1秒)默认值和EAPOL-Key重试次数的(2)默认值进程去如下，如果客户端不响应对最初的关键尝试：AP发送一关键尝试给客户端。它为回复等一秒钟。如果没有回复，则第一EAPOL-Key重试次数发送。它为回复等一秒钟。如果没有回复，则第二EAPOL-Key重试次数发送。如果仍有从客户端的无响应，并且重试值满足，则客户端deauthenticated。再次，如同关键超时，扩大EAPOL-Key重试值能，在某些情况下，是有利的。然而，因为解除验证消息将被延长，设置它对最大数量可能再是有害。

从 ACS RADIUS 服务器提取包文件用于故障排除

如果使用 ACS 作为外部 RADIUS 服务器，则此部分可用于排除配置的故障。package.cab 是一个包含高效排除 ACS 故障所需的所有必要文件的 Zip 文件。可以使用 CSSupport.exe 实用程序创建 package.cab，也可以手动收集文件。

参考创建ObtainingVersion*和AAA调试信息*package.cab文件部分*Cisco Secure ACS for Windows的关于*如何创建和抽出从WCS的包文件的更多信息。

相关信息

- 对轻量接入点进行 WLAN 控制器故障切换配置示例
- 无线 LAN 控制器 (WLC) 软件升级
- Cisco 无线 LAN 控制器命令参考
- 技术支持和文档 - Cisco Systems