H-REAP 操作模式配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[优于 REAP 的 H-REAP](#)
[配置](#)
[网络图](#)
[配置](#)
[为 AP 事先指导控制器并配置 H-REAP](#)
[H-REAP 的工作原理](#)
[H-REAP 交换状态](#)
[集中身份验证、集中交换](#)
[验证集中身份验证、集中交换](#)
[身份验证关闭、交换关闭](#)
[集中身份验证、本地交换](#)
[验证集中身份验证、本地交换](#)
[身份验证关闭、本地交换](#)
[本地身份验证、本地交换](#)
[验证本地身份验证、本地交换](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍混合远程边缘接入点 (H-REAP) 的概念并通过配置示例解释其不同的操作模式。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解无线LAN控制器(WLC)以及如何配置WLC基本参数
- 了解 REAP

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 7.0.116.0 版本的 Cisco 4400 系列 WLC
- 思科1131AG轻量接入点(LAP)
- 运行版本 12.4(11)T 的 Cisco 2800 系列路由器
- 运行固件版本4.0的思科Aironet 802.11a/b/g客户端适配器
- Cisco Aironet Desktop Utility 版本 4.0
- 运行 4.0 版的 Cisco 安全 ACS

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。

背景信息

H-REAP 是适合分支机构和远程办公室部署的一种无线解决方案。H-REAP使客户能够通过WAN链路在分支机构或远程办公室中配置和控制接入点(AP)，而无需在每个办公室部署控制器。

当与控制器的连接丢失时，H-REAP 可以在本地交换客户端数据流并在本地进行客户端身份验证。当连接到控制器后，H-REAP 也能通过隧道使数据流返回到控制器。在连接模式下，混合REAP AP也可以执行本地身份验证。

H-REAP仅在以下位置受支持：

- 1130AG、1140、1240、1250、1260、AP801、AP 802、1040和AP3550 AP
- Cisco 5500、4400、2100、2500和Flex 7500系列控制器
- Catalyst 3750G 集成控制器交换机
- Catalyst 6500 系列无线服务模块 (WiSM)
- 用于集成多业务路由器(ISR)的无线局域网控制器模块(WLCM)

H-REAP 上的客户端数据流可以在 AP 上本地交换，也可以通过隧道返回到控制器。这取决于每个 WLAN 的配置。此外，H-REAP 上本地交换的客户端数据流可以带有 802.1Q 标记以提供有线端分离。在广域网中断期间，所有本地交换、本地身份验证的 WLAN 上的服务仍然持续。

注意：如果AP处于H-REAP模式并在远程站点本地交换，则不支持根据RADIUS服务器配置将用户动态分配到特定VLAN。但是，您应该能够根据在AP本地完成的静态VLAN到服务集标识符(SSID)映射，将用户分配到特定VLAN。因此，可以将属于特定 SSID 的用户分配到特定的 VLAN（SSID 在 AP 本地映射到该 VLAN）。

注意： 如果WLAN语音很重要，则AP应在本地模式下运行，以便获得CCKM和连接准入控制(CAC)支持，H-REAP模式不支持这些支持。

优于 REAP 的 H-REAP

有关帮助了解REAP的详细信息，请参阅带轻量AP和无线LAN控制器(WLC)的远程边缘AP(REAP)配置示例。

引入 H-REAP 是因为 REAP 有以下缺点：

- REAP 没有有线端分离。这是因为缺少 802.1Q 支持。来自各个 WLAN 的数据都到达同一个有线子网。
- 在广域网发生故障时，REAP AP 除了在控制器中指定的第一个 WLAN 上提供服务外，会停止在所有其他 WLAN 上提供服务。

以下是 H-REAP 克服这两个缺点的方法：

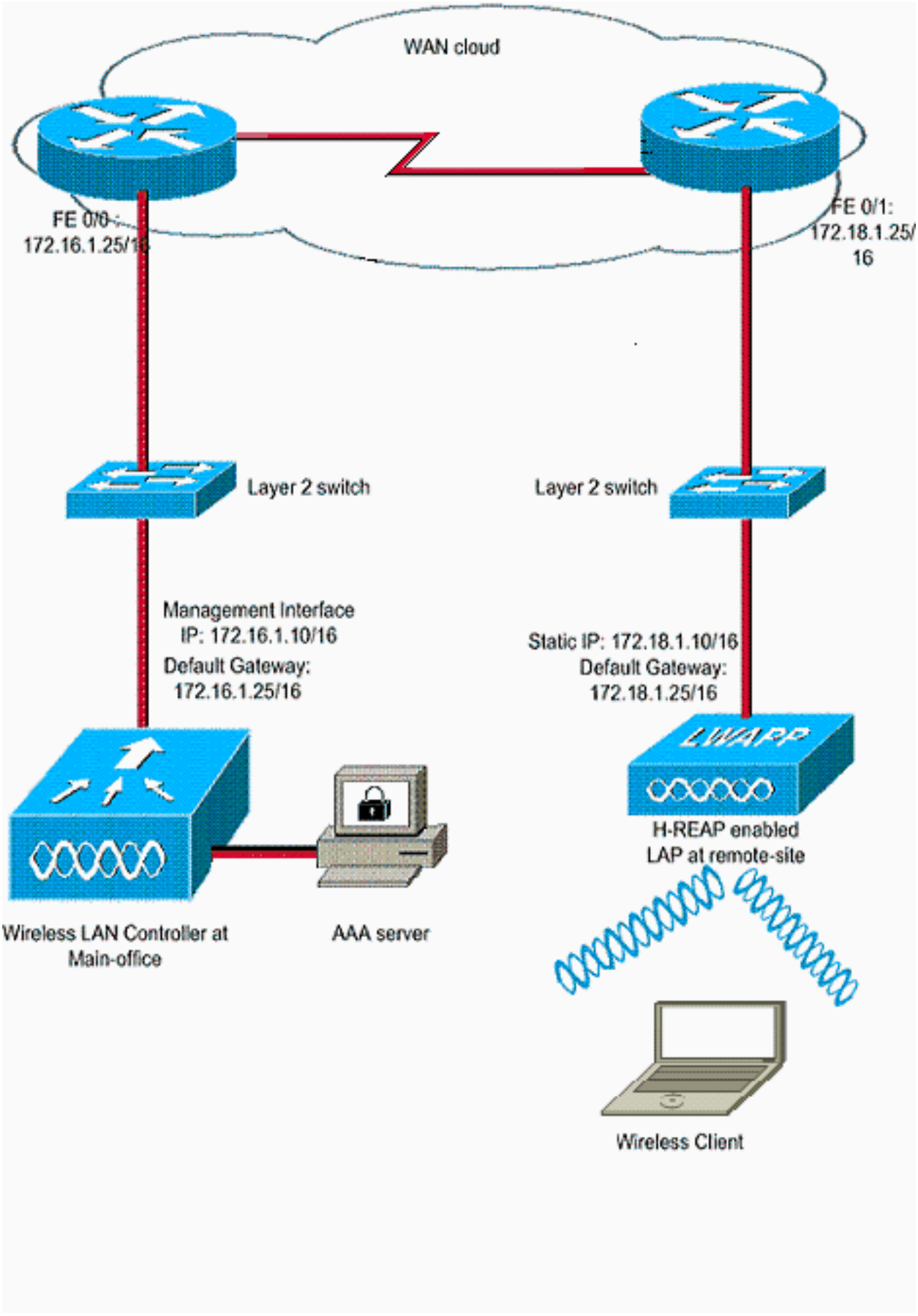
- 提供对 dot1Q 的支持和 VLAN 到 SSID 的映射。VLAN 到 SSID 映射需要在 H-REAP 上完成。当您执行此操作时，请确保正确地允许配置的 VLAN 通过中间交换机和路由器的端口。
- 为所有配置为本地交换的 WLAN 提供持续的服务。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



配置

本示例假定已用基本配置对控制器进行了配置。控制器使用以下配置：

- 管理接口 IP 地址 - 172.16.1.10/16

- AP 管理器接口 IP 地址 - 172.16.1.11/16
- 默认网关路由器 IP 地址 - 172.16.1.25/16
- 虚拟网关 IP 地址 - 1.1.1.1

注意：本文档不显示H-REAP和控制器之间可用的WAN配置和路由器和交换机的配置。本文假定您了解使用的广域网封装和路由协议。此外，本文档假定您了解如何配置它们，以便通过WAN链路在H-REAP和控制器之间保持连接。在本例中，在广域网链路上使用 HDLC 封装。

为 AP 事先指导控制器并配置 H-REAP

如果希望AP从CAPWAP发现机制不可用的远程网络发现控制器，可以使用启动。此方法使您能够指定 AP 应该连接的控制器。

为了事先指导支持 H-REAP 的 AP，请将 AP 连接到总部的有线网络。在其启动期间，支持 H-REAP 的 AP 首先为自身查找一个 IP 地址。在它通过 DHCP 服务器获取一个 IP 地址后，即会启动并且查找控制器以执行注册过程。

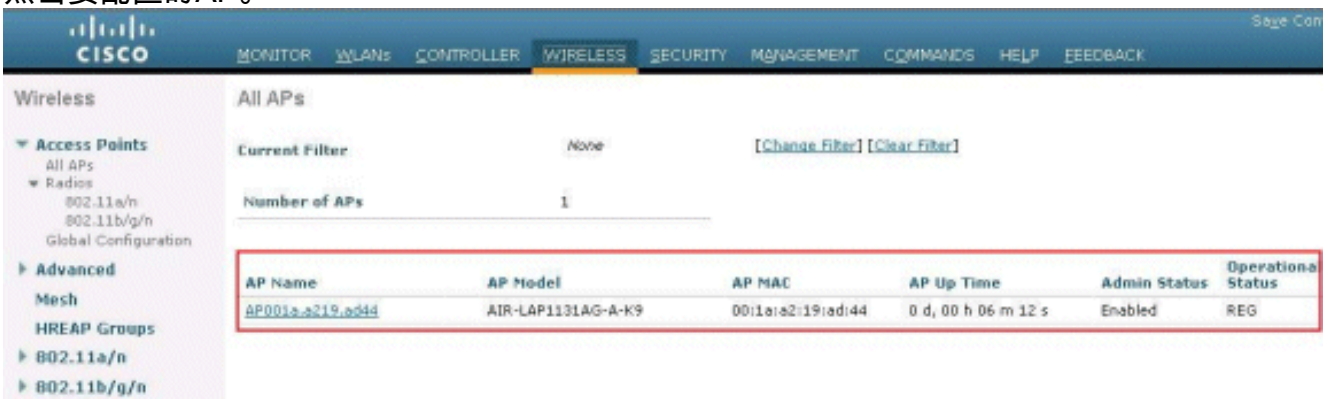
H-REAP AP可以通过轻量AP(LAP)注册到无线LAN控制器(WLC)中介绍的任何方式获取控制器IP地址。

注意：您还可以在AP上配置LAP，以通过CLI命令发现控制器。有关更多信息，请参阅使用 CLI 命令发现 H-REAP 控制器。

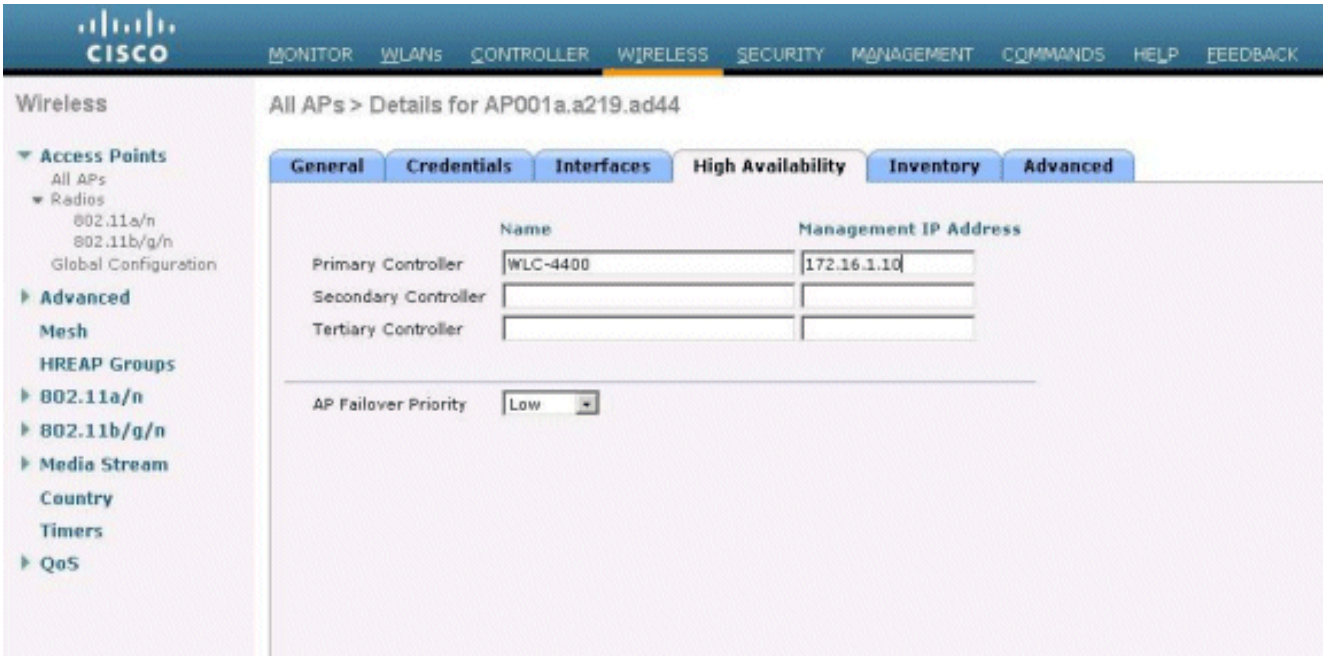
本文档中的示例对 H-REAP 使用 DHCP 选项 43 过程来获知控制器 IP 地址。然后它加入控制器，从控制器下载最新的软件镜像和配置，并初始化无线链路。它将下载的配置保存在非易失性存储器中以便在独立模式下使用。

在向控制器注册该 LAP 后，请完成以下步骤：

1. 在控制器 GUI 中，选择 **Wireless>Access Points**。此操作将显示向此控制器注册的 LAP。
2. 点击要配置的AP。

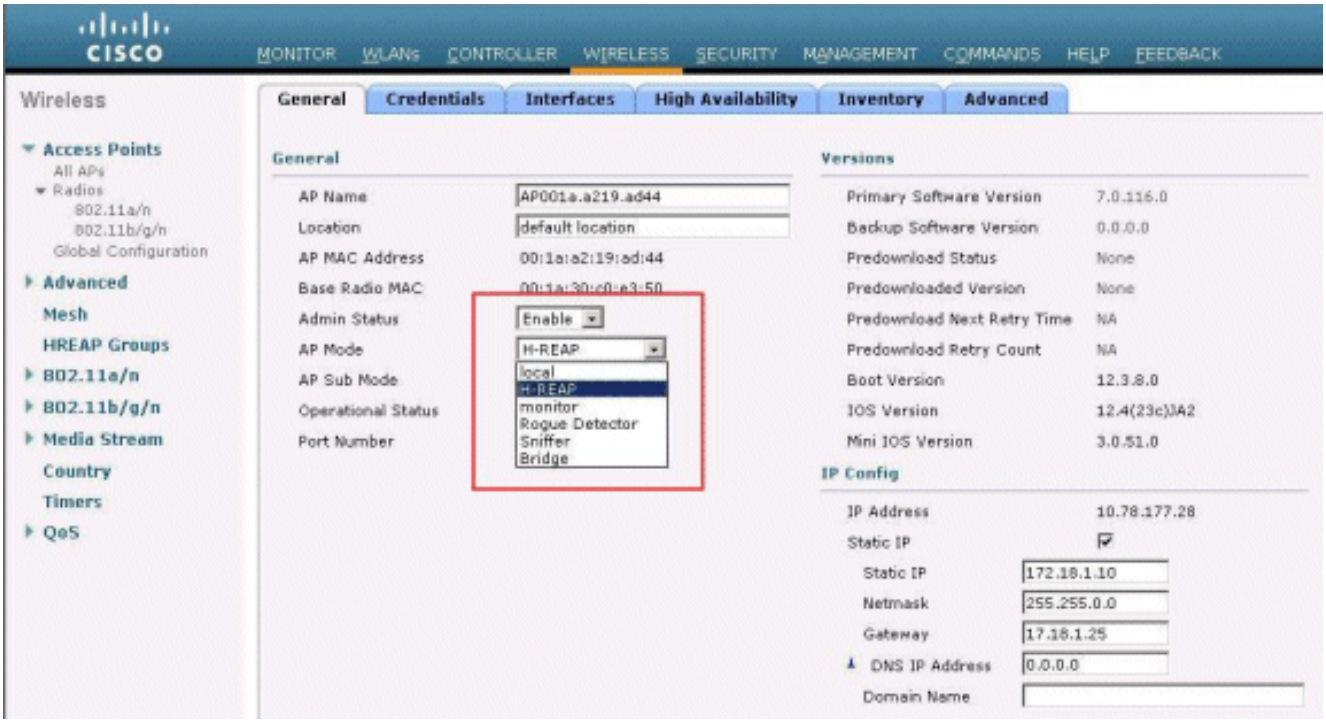


3. 在“AP”>“详细信息”窗口中，单击“高可用性”选项卡，定义AP将用于注册的控制器名称，然后单击“**应用**”。



您最多可以定义三个控制器名称(主控制器、辅助控制器和第三控制器)。 AP 将按照您在此窗口中提供的顺序搜索控制器。因为本示例只使用一个控制器，所以示例将该控制器定义为主控制器。

4. 配置 H-REAP 的 LAP。要将LAP配置为在H-REAP模式下运行，请在APs>Details窗口的General选项卡下，从相应的下拉菜单中选择**AP**模式作为H-REAP。这样即将 LAP 配置为在 H-REAP 模式下运行。



注意：在本例中，您可以看到AP的IP地址已更改为静态模式，且静态IP地址172.18.1.10已分配。这样分配是因为它是将在远程办公室中使用的子网。因此，您仅在首次通过注册阶段使用DHCP服务器的IP地址。在 AP 注册到控制器后，将地址更改为静态 IP 地址。

现在已经为 LAP 事先指导了控制器并将 LAP 配置为了 H-REAP 模式，下一步是在控制器端配置 H-REAP 并讨论 H-REAP 交换状态。

H-REAP 的工作原理

支持 H-REAP 的 LAP 在以下两种不同的模式下运行：

- **连接模式**：当H-REAP与WLC的CAPWAP控制平面链路处于启用状态且运行正常时，该H-REAP即处于连接模式。这意味着 LAP 与 WLC 之间的广域网链路未断开。
- **独立模式**：当 H-REAP 到 WLC 的广域网链路断开时，称 H-REAP 处于独立模式。例如，当此 H-REAP 不再通过广域网链路与 WLC 连接时。

用于对客户端进行身份验证的身份验证机制可以定义为**集中或本地。**

- **集中身份验证 - 指涉及远程站点 WLC 过程的身份验证类型。**
- **本地身份验证 - 指不涉及任何 WLC 过程进行身份验证的身份验证类型。**

注意：所有802.11身份验证和关联处理都发生在H-REAP上，无论LAP处于哪种模式。当处于连接模式时，H-REAP 则将这些关联和身份验证代理到 WLC。在独立模式下，LAP 无法向 WLC 通知此类事件。

当客户端连接到 H-REAP AP 时，AP 将所有身份验证消息转发给控制器。在成功进行身份验证之后，其数据包在本地进行交换或通过隧道返回到控制器。具体操作取决于所连接的 WLAN 的配置。

使用 H-REAP，在控制器上配置的 WLAN 可以在以下两种不同的模式下运行：

- **集中交换**：如果将 H-REAP 上的 WLAN 的数据流配置为通过隧道传输到 WLC，则称该 WLAN 在集中交换模式下运行。
- **本地交换**：如果 H-REAP 上的 WLAN 的数据流在 LAP 自身的有线接口本地终止，无需通过隧道传输到 WLC，则称该 WLAN 在本地交换模式下运行。**注意**：只能为H-REAP本地交换配置 WLAN 1到8，因为只有这些WLAN可应用于支持H-REAP功能的1130、1240和1250系列AP。

H-REAP 交换状态

与前一部分中提及的身份验证模式和交换模式相结合，H-REAP 可以在以下任何一种状态下运行：

- 集中身份验证、集中交换
- 身份验证关闭、交换关闭
- 集中身份验证、本地交换
- 身份验证关闭、本地交换
- 本地身份验证、本地交换

集中身份验证、集中交换

在此状态下，对于给定的 WLAN，AP 将所有客户端身份验证请求转发给控制器，并将所有客户端数据通过隧道传给 WLC。只有当 H-REAP 处于连接模式时，此状态才有效。不管使用何种身份验证方法，在广域网断开期间，配置为在此模式下运行的任何 WLAN 都将中断。

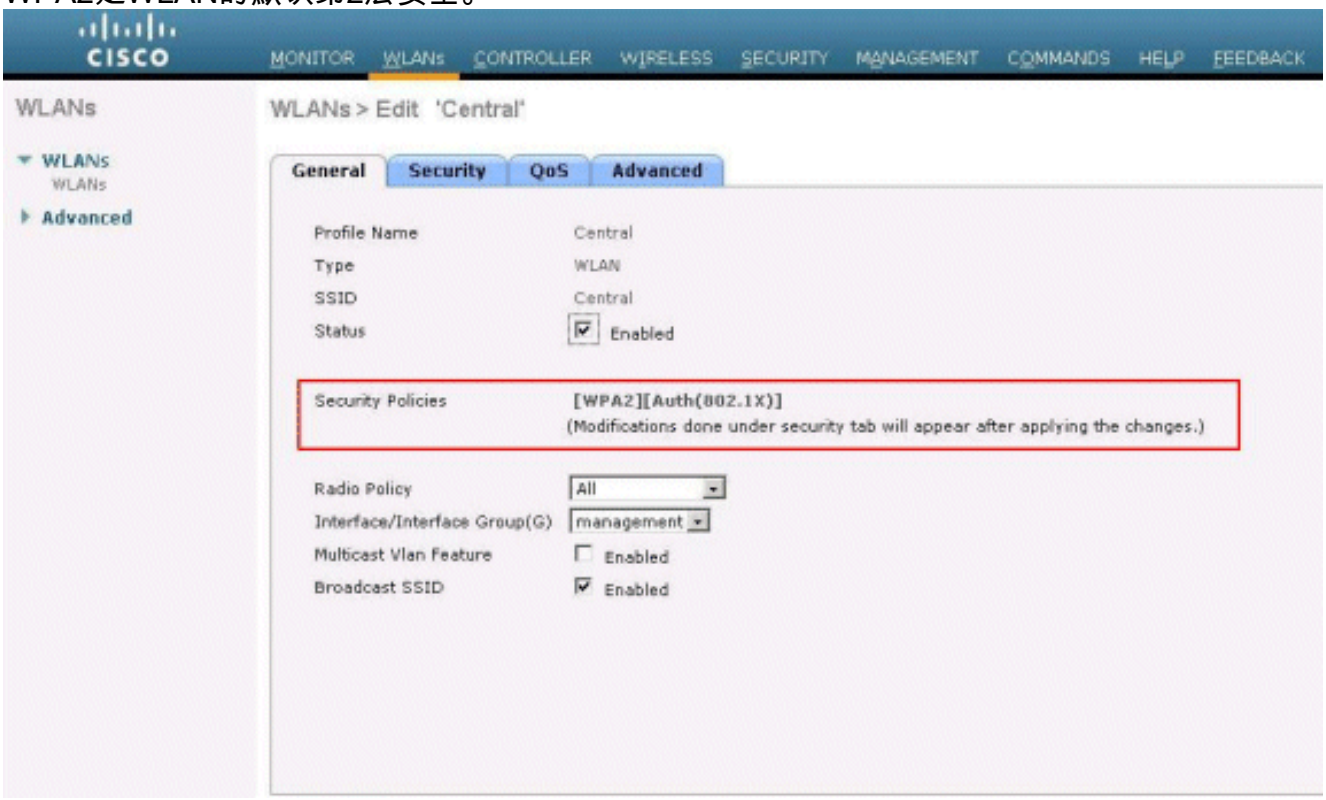
本示例使用以下配置设置：

- WLAN/SSID 名称：**中心**
- 第 2 层安全：**WPA2**
- H-REAP 本地交换：**禁用**

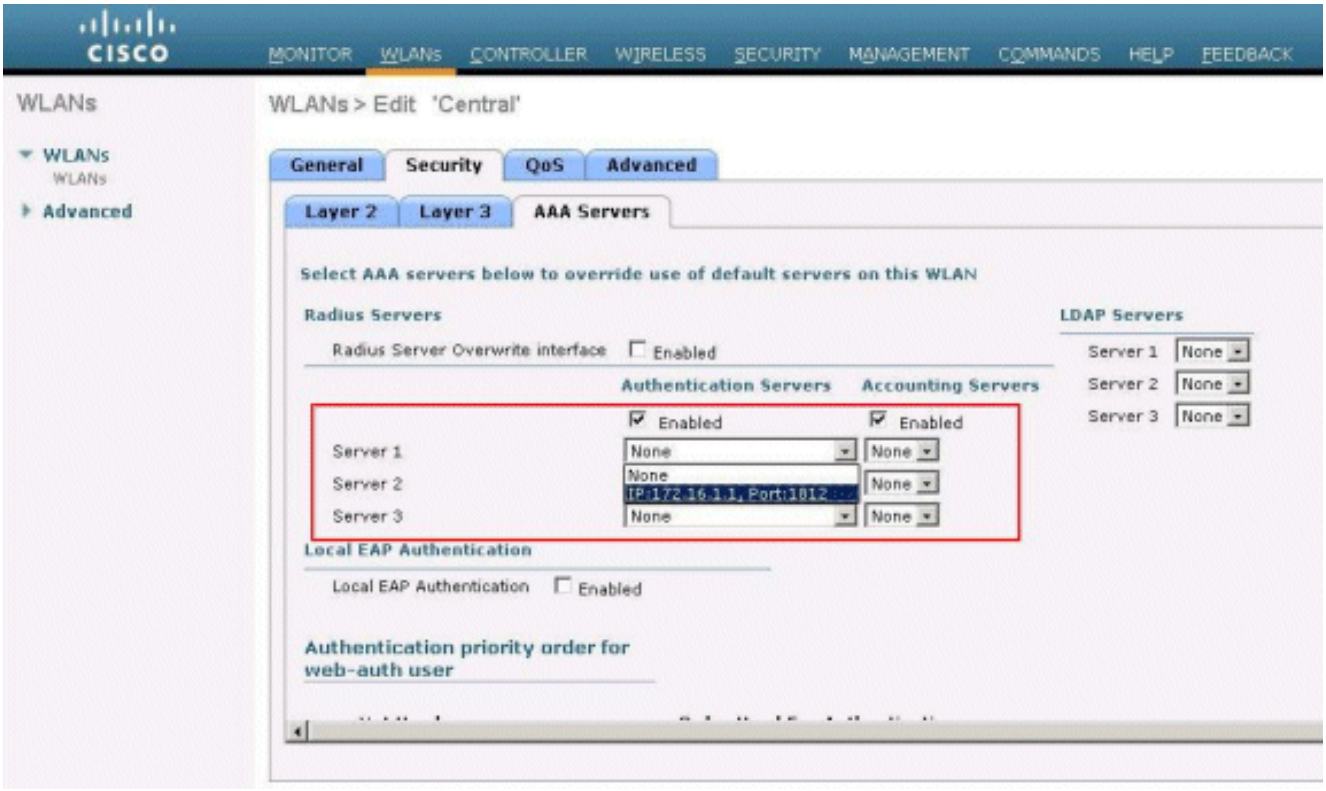
要配置 WLC 进行集中身份验证、集中交换，请使用 GUI 完成以下步骤：

1. 单击 **WLANs 以创建一个名为 central 的新 WLAN，然后单击 Apply。**

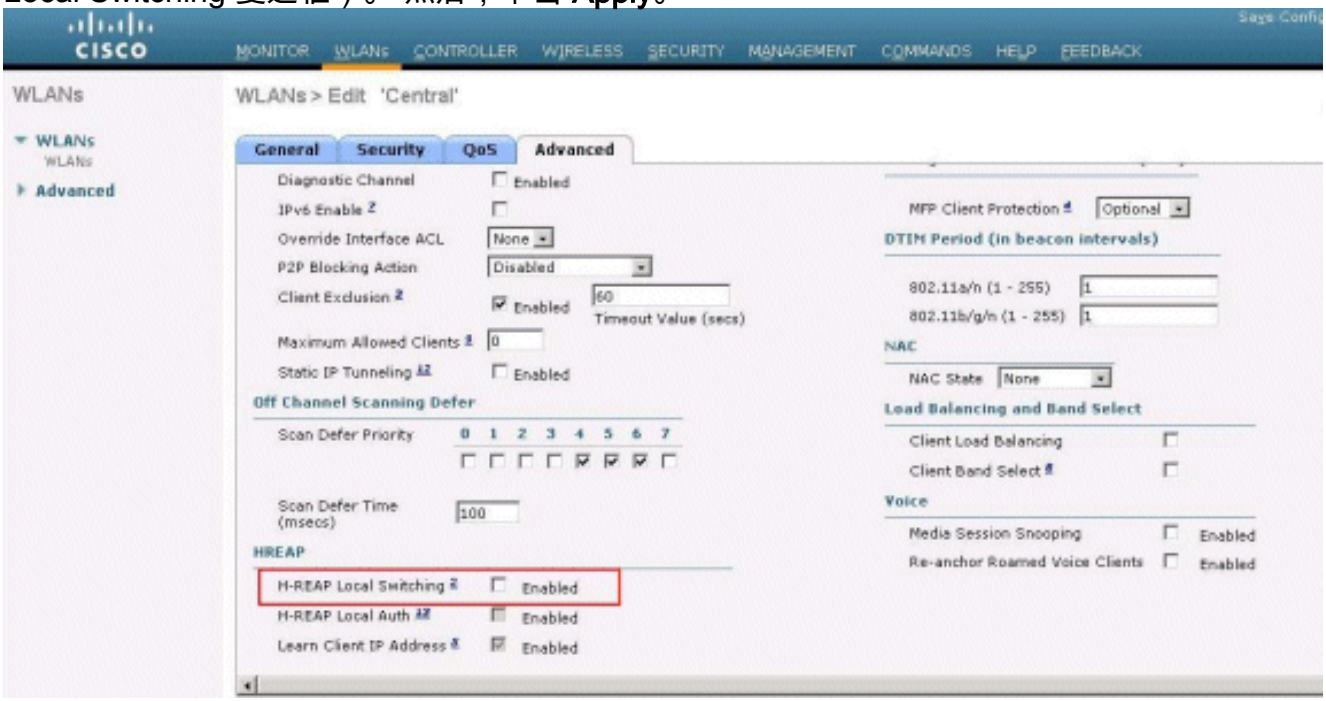
2. 由于此WLAN使用集中身份验证，因此我们在Layer 2 Security字段中使用WPA2身份验证。WPA2是WLAN的默认第2层安全。



3. 选择AAA Servers选项卡，然后选择为身份验证配置的适当服务器。



4. 因为此 WLAN 使用集中交换，所以要确保禁用 H-REAP Local Switching 复选框（即未选中 Local Switching 复选框）。 然后，单击 **Apply**。

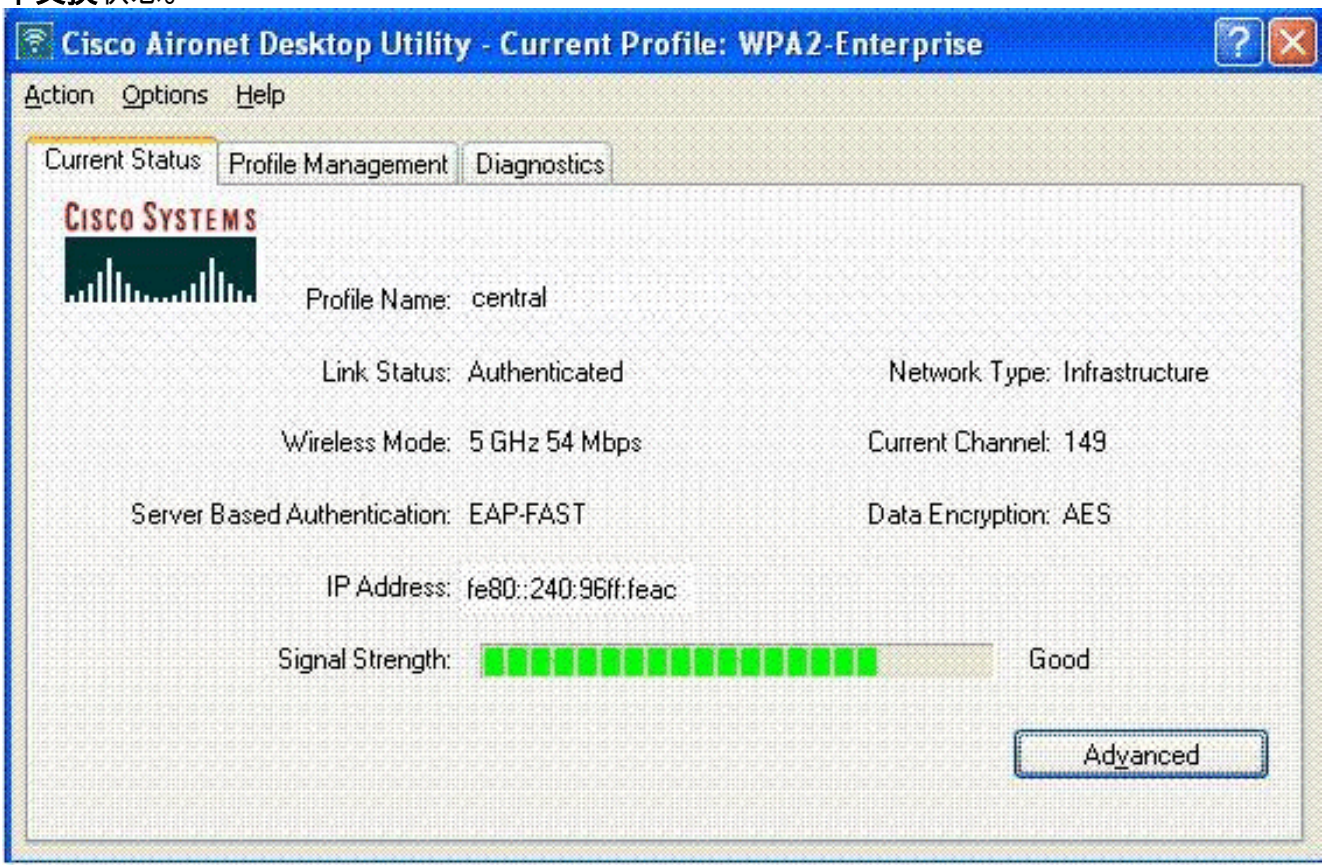


验证集中身份验证、集中交换

请完成以下步骤：

1. 用相同的 SSID 和安全配置对无线客户端进行配置。在本例中，SSID是*Central*，安全方法是*WPA2*。
2. 输入在 RADIUS server>User Setup 中配置的用户名和口令，以在客户端中激活该 central SSID。本示例使*用User1*作为用户名和密码。

客户端由 RADIUS 服务器集中身份验证并且与 H-REAP AP 关联。H-REAP 此时处于**集中身份验证、集中交换**状态。



身份验证关闭、交换关闭

使用集中身份验证、集中交换部分中说明的配置，禁用连接控制器的广域网链路。现在，控制器等待来自 AP 的检测信号应答。检测信号应答类似于保活消息。控制器尝试发出五个连续的检测信号，每一秒钟发出一个。

因为它没有收到来自 H-REAP 的检测信号应答，所以 WLC 撤销 LAP 的注册。

从WLC的CLI发出**debug capwap events enable**命令以验证注销过程。以下是该 **debug 命令的输出示例：**

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

H-REAP 进入独立模式。

因为该 WLAN 以前集中身份验证并集中交换，所以控制流和数据流都通过隧道传回到控制器。因此，如果没有控制器，则客户端将无法保持与 H-REAP 的联系而断开。H-REAP 客户端关联和身份验证均关闭的状态称为身份验证关闭、交换关闭。

集中身份验证、本地交换

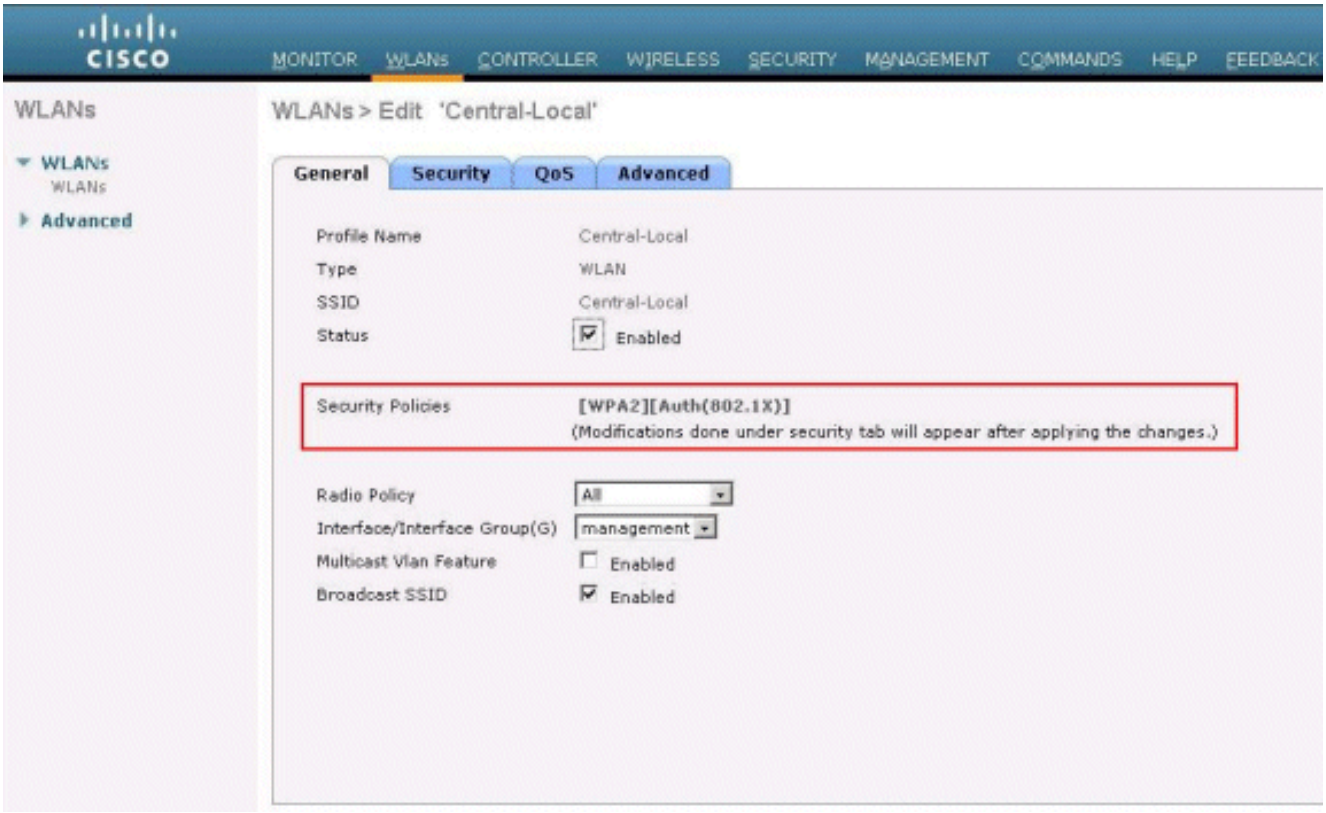
在此状态下，对于给定的 WLAN，WLC 处理所有的客户端身份验证，H-REAP LAP 在本地交换数据包。客户端成功进行身份验证后，控制器会向H-REAP发送capwap控制命令，并指示LAP在本地交换给定客户端的数据包。在成功进行身份验证之后，会逐个客户端发送此消息。此状态仅在连接模式下适用。

本示例使用以下配置设置：

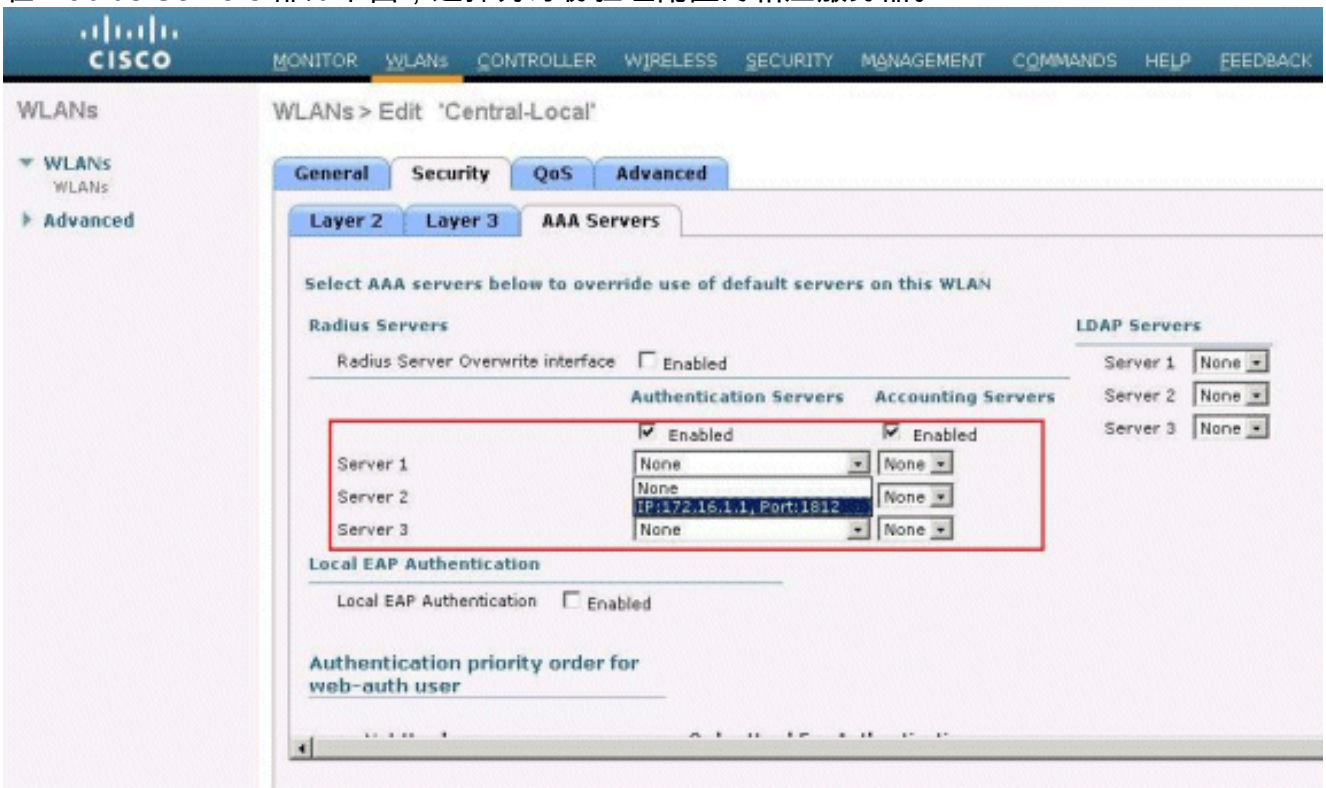
- WLAN/SSID 名称：**central-local**
- 第 2 层安全：**WPA2**。
- H-REAP 本地交换：**启用**

在控制器的 GUI 中，完成以下步骤：

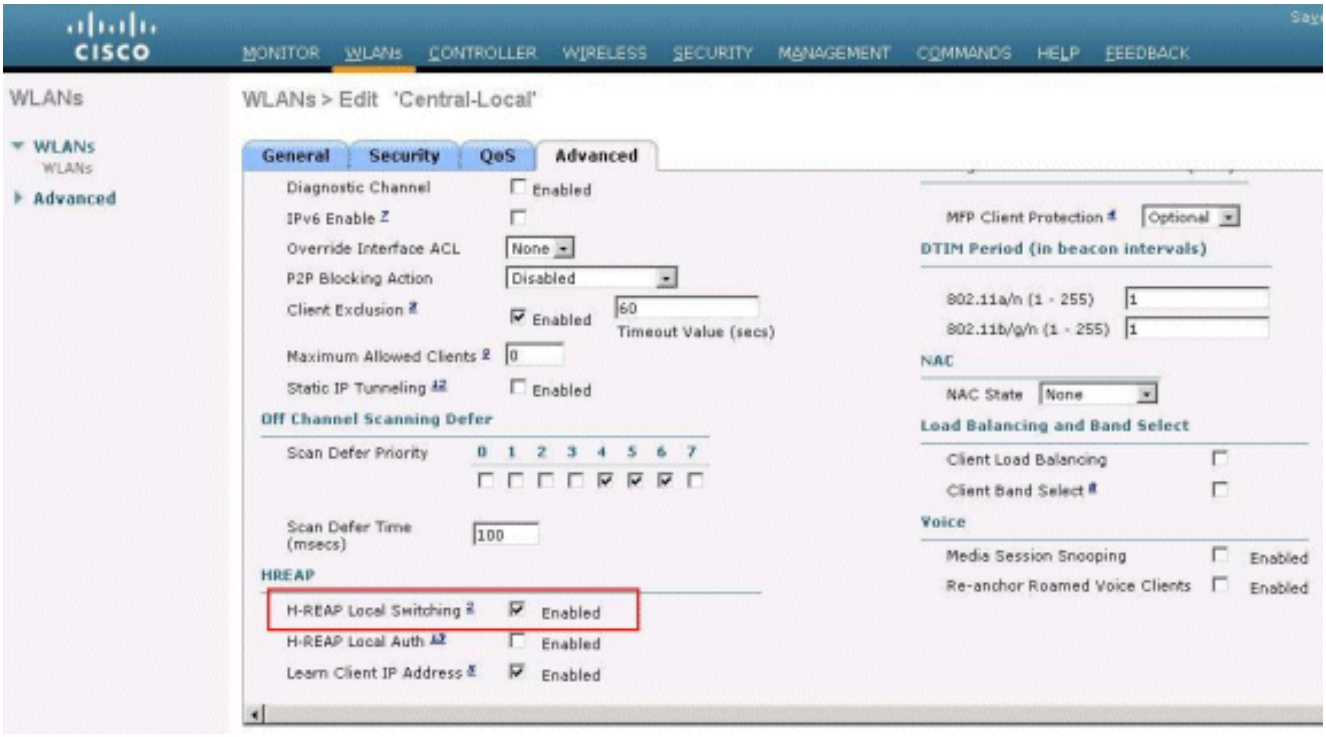
1. 单击 **WLANs 以创建一个名为 central-local 的新 WLAN，请然后单击 Apply。**
2. 由于此WLAN使用集中身份验证，因此请在**Layer 2 Security字**段中选择WPA2身份验证。



3. 在 Radius Servers 部分下面，选择为身份验证配置的相应服务器。



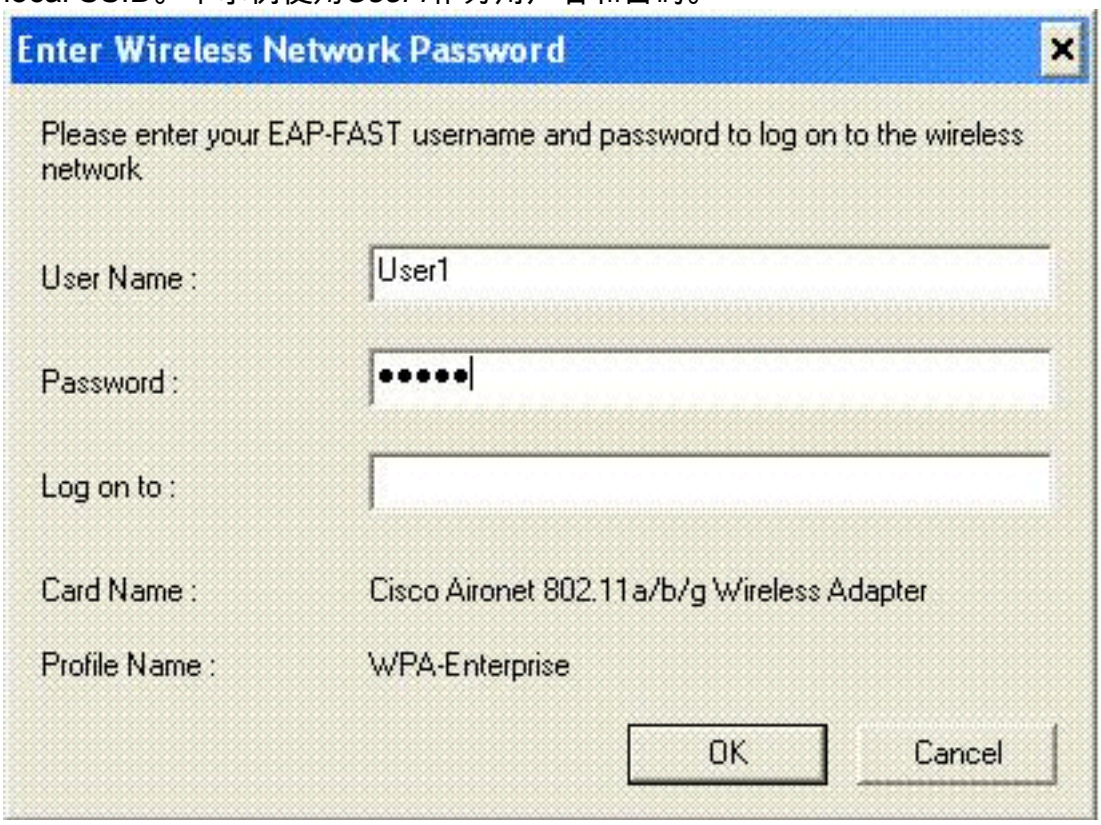
4. 选中 **H-REAP Local Switching 复选框以便在 H-REAP 上本地交换属于此 WLAN 的客户端数据流。**



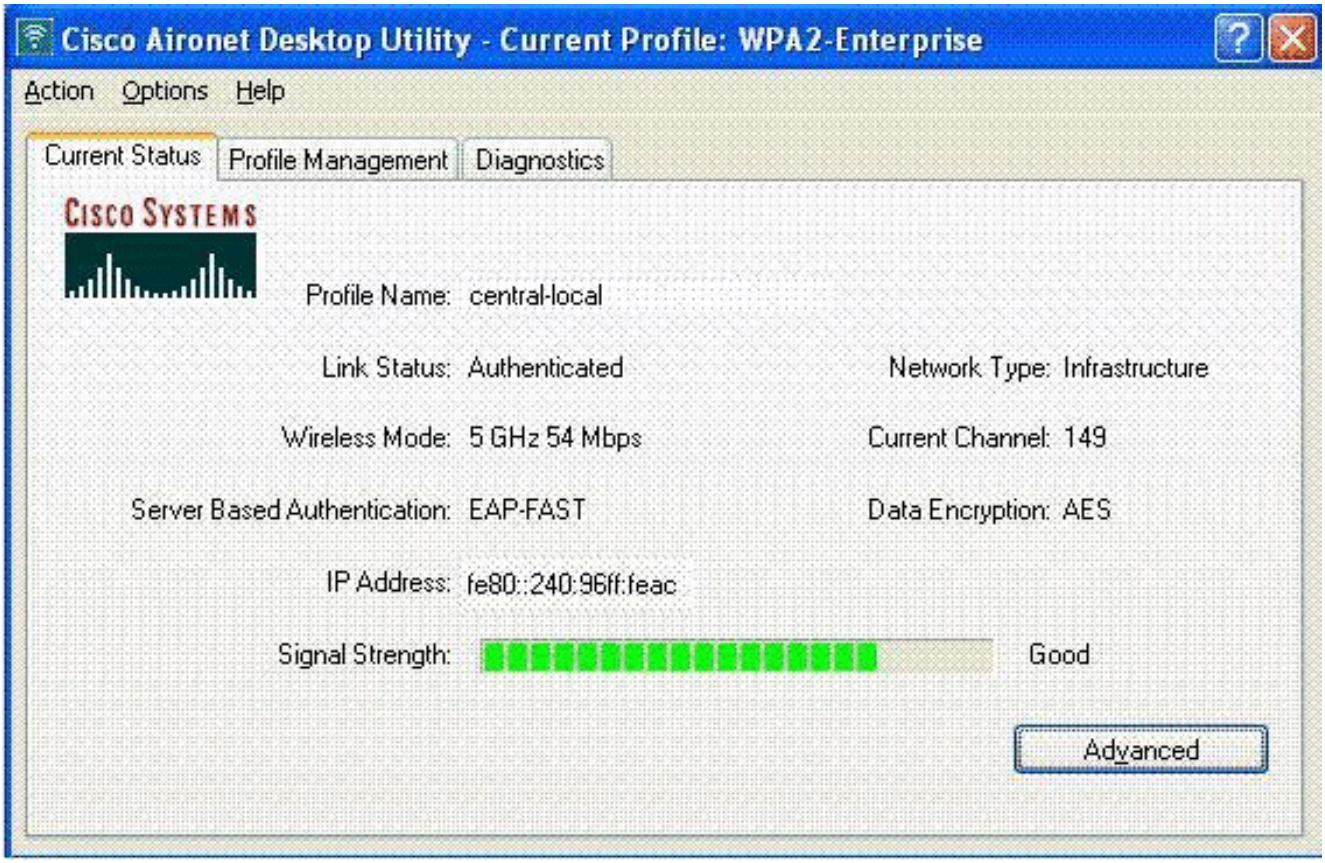
验证集中身份验证、本地交换

请完成以下步骤：

1. 用相同的 SSID 和安全配置对无线客户端进行配置。在本例中，SSID为*Central-Local*，安全方法为*WPA2*。
2. 输入在 RADIUS server>User Setup 中配置的用户名和口令，以在客户端中激活该 central-local SSID。本示例使*用User1*作为用户名和密码。



3. Click **OK**.客户端由 RADIUS 服务器集中身份验证并且与 H-REAP AP 关联。H-REAP 此时处于**集中身份验证、本地交换**状态。



身份验证关闭、本地交换

如果一个本地交换的 WLAN 配置为要求在 WLC 上处理任何验证类型（例如 EAP 身份验证 [动态 WEP/WPA/WPA2/802.11i]、WebAuth 或 NAC），则一旦广域网发生故障，它将进入**身份验证关闭、本地交换状态。**在此状态下，对于给定的 WLAN，H-REAP 拒绝尝试进行身份验证的任何新增客户端。但会继续发送信标并探测响应，以保持现有的客户端保持正常连接。此状态仅在独立模式下有效。

为了验证此状态，请使用集中身份验证、本地交换部分中说明的配置。

如果连接 WLC 的广域网链路断开，则 WLC 将完成撤销注册 H-REAP 的过程。

撤销注册后，H-REAP 即会进入独立模式。

通过此 WLAN 关联的客户端仍然保持其连通性。然而，因为控制器、验证程序不可用，H-REAP 不允许任何来自此 WLAN 的新连接。

这可以通过激活同一 WLAN 中的另一个无线客户端来验证。您会发现此客户端的身份验证将失败，并且不允许关联该客户端。

注意：当WLAN客户端计数等于零时，H-REAP将停止所有关联的802.11功能，不再为给定SSID信标。这将使 WLAN 转入下一个 H-REAP 状态：**身份验证关闭、交换关闭。**

本地身份验证、本地交换

在此状态下，H-REAP LAP 处理客户端身份验证并在本地交换客户端数据包。此状态仅在独立模式下有效，仅适用于可在 AP 本地处理并且不涉及控制器处理的身份验证类型

如果配置的身份验证类型可以在 AP 本地处理，则先前处于**集中身份验证、本地交换状态的 H-**

REAP 将转入此状态。如果配置的身份验证无法在本地处理（例如 802.1x 身份验证），则在独立模式下，H-REAP 进入**身份验证关闭、本地交换模式。**

以下是独立模式下可以在 AP 本地处理的常用身份验证机制：

- Open（未解决）
- 共享
- WPA-PSK
- WPA2-PSK

注意：当AP处于连接模式时，所有身份验证过程都由WLC处理。当 H-REAP 处于独立模式时，开放、共享和 WPA/WPA2-PSK 身份验证移交给执行所有客户端身份验证的 LAP。

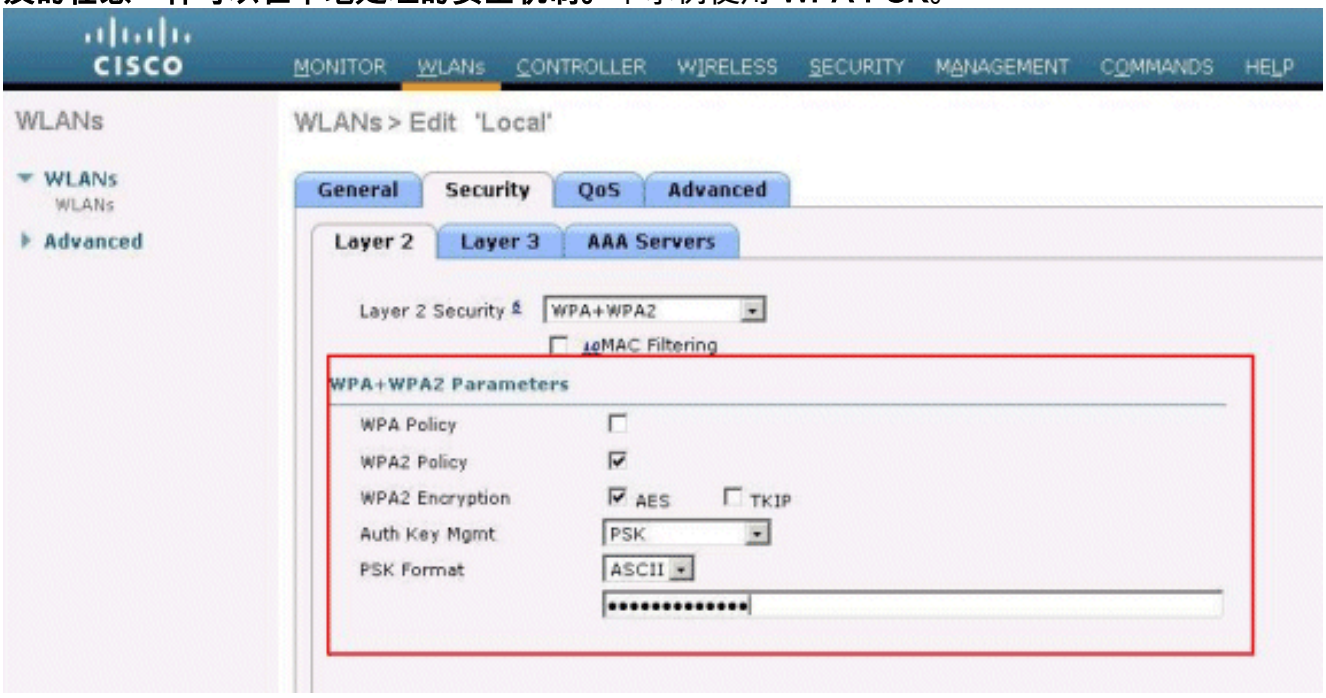
注意：当在WLAN上启用本地交换的情况下使用混合REAP时，不支持外部Web身份验证。

本示例使用以下配置设置：

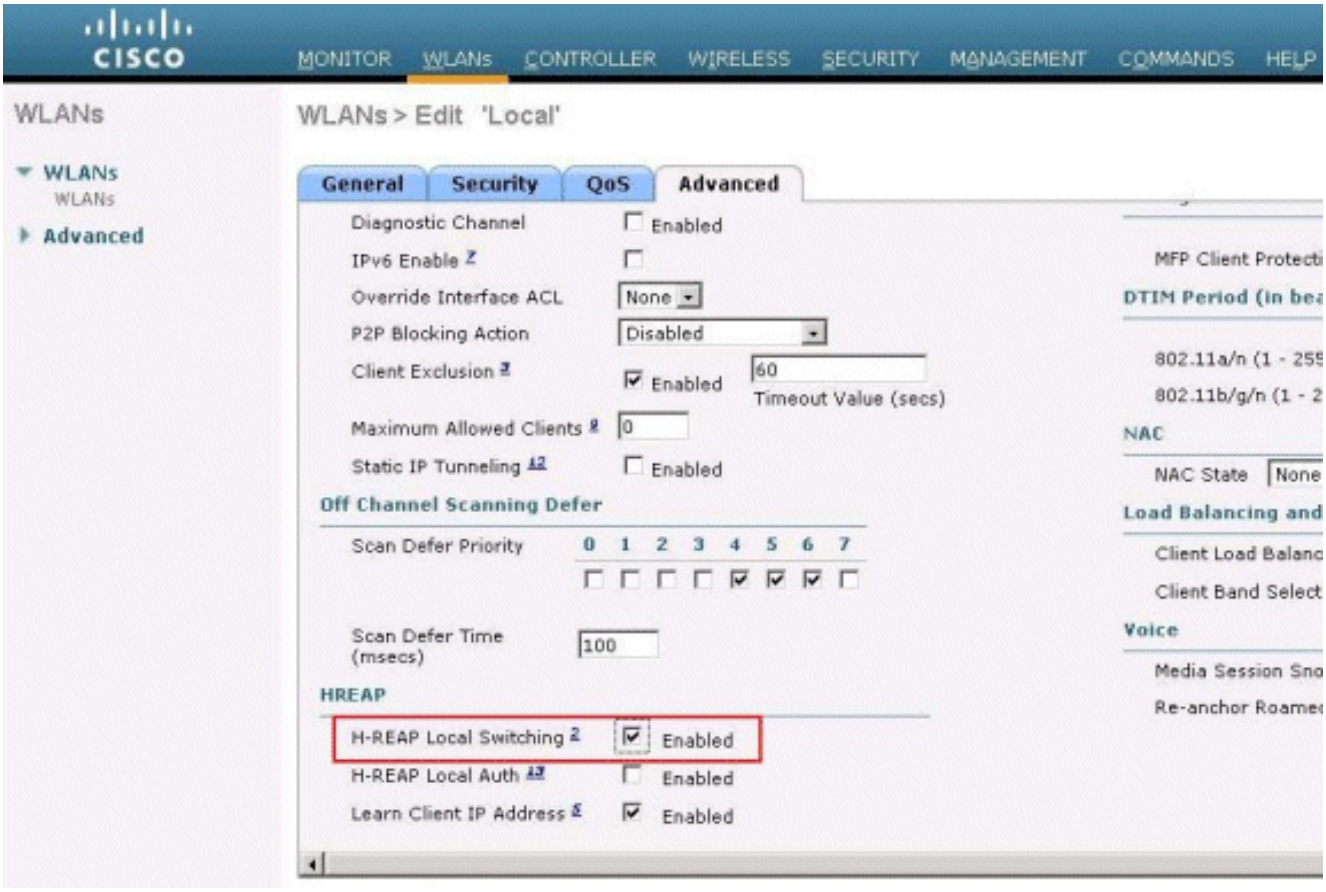
- WLAN/SSID 名称：**本地**
- 第 2 层安全：**WPA-PSK**
- H-REAP 本地交换：**启用**

在控制器的 GUI 中，完成以下步骤：

1. 单**击WLAN**以创建名为Local的新WLAN，然后单击**Apply**。
2. 因为此 WLAN 使用本地身份验证，所以请在 Layer 2 Security 字段中选择 **WPA-PSK 或所提及的任意一种可以在本地处理的安全机制。**本示例使用 **WPA-PSK**。



3. 选择后，您需要配置所要使用的预共享密钥/密码短语。要成功地进行身份验证，预共享密钥/密码短语必须与客户端使用的相同。
4. 选中 **H-REAP Local Switching 复选框以便在 H-REAP 上本地交换属于此 WLAN 的客户端数据流。**



验证本地身份验证、本地交换

请完成以下步骤：

1. 用相同的 SSID 和安全配置对客户端进行配置。这里，SSID是*Local*，安全方法是*WPA-PSK*。
2. 在客户端中激活本地SSID。客户端将在控制器上进行集中身份验证并且与 H-REAP 关联。客户端数据流配置为在本地交换。此时，H-REAP 处于集中身份验证、本地交换状态。
3. 禁用连接到控制器的广域网链路。控制器照例完成撤销注册进程。H-REAP 从控制器撤销注册。撤销注册后，H-REAP 即会进入独立模式。但是，属于此 WLAN 的客户端仍然保持与 H-REAP 的关联。此外，因为此处的身份验证类型可以在 AP 本地处理而无需控制器，所以 H-REAP 允许任何新增无线客户端通过此 WLAN 进行关联。
4. 要验证这一点，请激活同一 WLAN 上的其他无线客户端。您会看到可以成功地对客户端进行身份验证和关联。

故障排除

- 要进一步排除H-REAP的控制台端口上的客户端连接问题，请输入以下命令：
  `AP_CLI#show capwap reap association`
- 要进一步排除控制器上的客户端连接问题并限制进一步调试的输出，请使用以下命令：
  `AP_CLI#debug mac addr`
- 要调试客户端的802.11连接问题，请使用以下命令：
  `AP_CLI#debug dot11 state enable`
- 使用以下命令调试客户端的802.1X身份验证过程和失败：
  `AP_CLI#debug dot1x events enable`

- 可以使用以下命令调试后端控制器/RADIUS消息：
  ```
  AP_CLI#debug aaa events enable
  ```

- 或者，要启用一整套客户端debug命令，请使用以下命令：
  ```
  AP_CLI#debug client
  ```

相关信息

- 无线 LAN 控制器和轻量接入点基本配置示例
- 无线局域网控制器上的 VLAN 配置示例
- Cisco 无线 LAN 控制器配置指南 7.0 版
- 混合 REAP 设计和部署指南
- 混合远程边缘接入点 (H-REAP) 基本故障排除
- 对轻量接入点进行 WLAN 控制器故障切换配置示例
- 无线产品支持
- 技术支持和文档 - Cisco Systems