H-REAP操作模式配置示例

目錄

簡介

本檔案介紹混合遠端邊緣存取點(H-REAP)的概念，並舉例說明其不同的運作模式。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 無線區域網路控制器(WLC)知識以及如何設定WLC基本引數
- REAP知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 4400系列WLC（執行韌體版本7.0.116.0）
- Cisco 1131AG輕量型存取點(LAP)
- 執行12.4(11)T版的Cisco 2800系列路由器。
- 運行韌體版本4.0的Cisco Aironet 802.11a/b/g客戶端介面卡
- Cisco Aironet案頭實用程式版本4.0
- 執行4.0版的Cisco Secure ACS

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

H-REAP是用於分支機構和遠端辦公室部署的無線解決方案。H-REAP使客戶能夠通過WAN鏈路從公司辦公室配置和控制分支或遠端辦公室的接入點(AP)，而無需在每個辦公室部署控制器。

H-REAP可以在本地交換客戶端資料流量，並在與控制器的連線斷開時本地執行客戶端身份驗證。連線到控制器時，H-REAP還可以將流量通道傳回控制器。在連線模式下，混合REAP AP還可以執行本地身份驗證。

H-REAP僅在以下位置受支援：

- 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整合式控制器交換器
- Catalyst 6500系列無線服務模組(WiSM)
- 適用於整合式服務路由器(ISR)的無線LAN控制器模組(WLCM)

H-REAP上的客戶端流量可以在AP本地交換，也可以通過隧道傳回控制器。這取決於每個WLAN的配置。此外，H-REAP上的本地交換客戶端流量可以進行802.1Q標籤，以提供有線端分離。在WAN中斷期間，所有本地交換且經過本地身份驗證的WLAN上的服務都會繼續存在。

注意：如果AP處於H-REAP模式並在遠端站點進行本地交換，則不支援基於RADIUS伺服器配置將使用者動態分配到特定VLAN。但是，您應該能夠根據在AP本地完成的靜態VLAN到服務集識別符號(SSID)對映為使用者分配特定VLAN。因此，可以將屬於特定SSID的使用者分配給在AP本地對映SSID的特定VLAN。

附註： 如果WLAN語音非常重要，則應在本地模式下運行AP，以獲得H-REAP模式不支援的CCKM和連線准入控制(CAC)支援。

H-REAP OVER REAP

如需更多資訊，請參閱使用輕量AP和無線LAN控制器(WLC)的遠端邊緣AP(REAP)組態範例，以協助瞭解REAP。

H-REAP的引入是因為REAP的這些缺點：

- REAP沒有有線端分離。這是因為缺少802.1Q支援。來自WLAN的資料位於同一個有線子網上。
- 在WAN發生故障時，REAP AP會停止在所有WLAN上提供的服務（控制器中指定的第一個服務除外）。

H-REAP就是這樣克服這兩個缺點的：

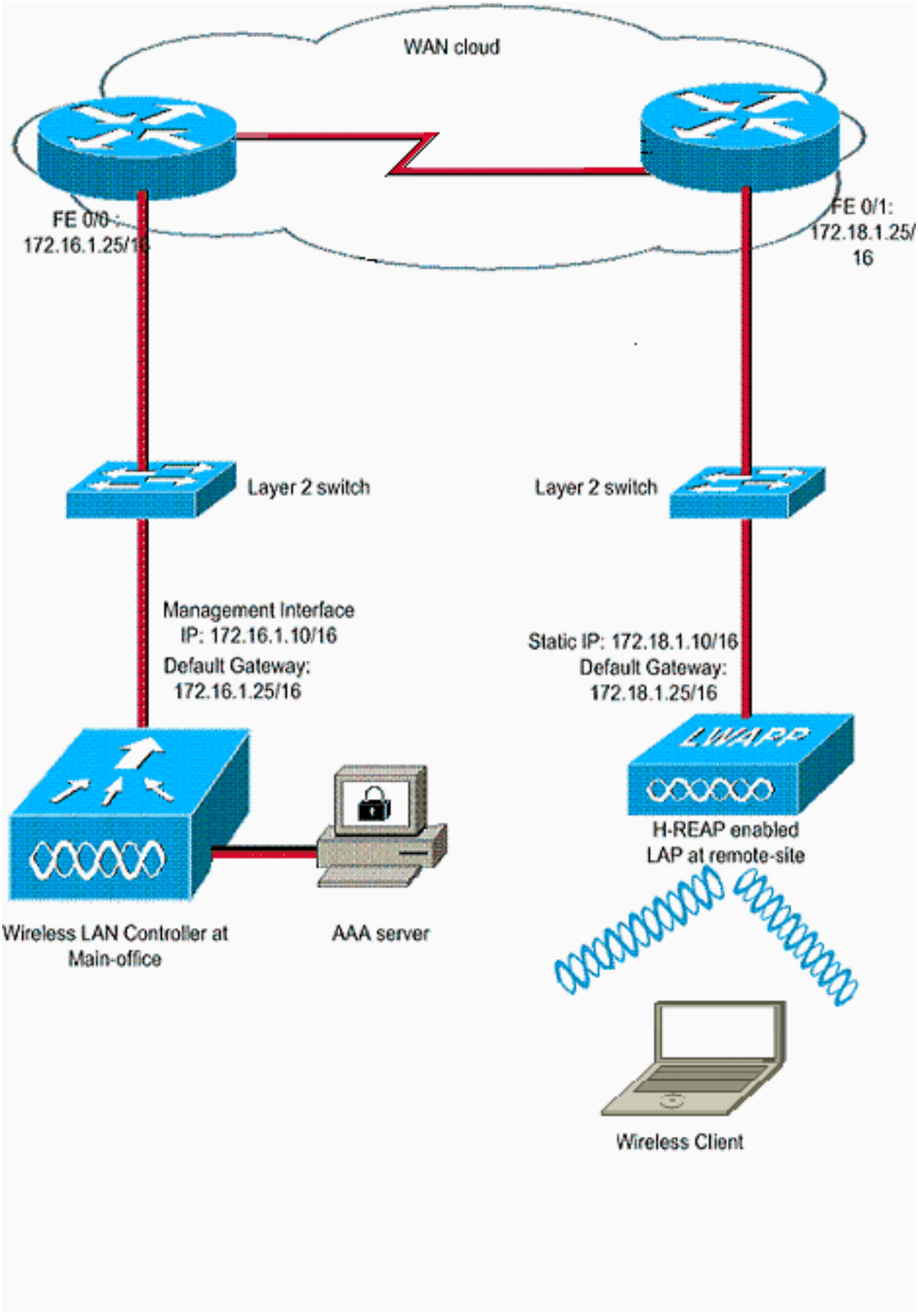
- 提供dot1Q支援和VLAN到SSID對映。此VLAN到SSID的對映需要在H-REAP中完成。執行此作業時，請確保已設定的VLAN正確允許通過中間交換機和路由器中的連線埠。
- 向為本地交換配置的所有WLAN提供持續服務。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



組態

此範例假設控制器已設定基本設定。控制器使用以下設定：

- 管理介面IP地址 — 172.16.1.10/16

- AP-Manager介面IP地址 — 172.16.1.11/16
- 預設網關路由器IP地址 — 172.16.1.25/16
- 虛擬網關IP地址 — 1.1.1.1

注意：本文檔未顯示H-REAP和控制器之間可用路由器和交換機的WAN配置和配置。假設您已瞭解使用的WAN封裝和路由協定。此外，本文檔還假設您瞭解如何配置這些裝置，以便通過WAN鏈路保持H-REAP和控制器之間的連線。在本示例中，WAN鏈路上使用HDLC封裝。

使用控制器為AP啟動並配置H-REAP

如果您希望AP從遠端網路發現控制器，而遠端網路沒有CAPWAP發現機制，您可以使用啟動功能。使用此方法可以指定AP應連線的控制器。

為了啟動支援H-REAP的AP，請將AP連線到總部有線網路。在啟動過程中，支援H-REAP的AP首先為自己查詢IP地址。一旦通過DHCP伺服器獲取IP地址，就會啟動並查詢控制器以執行註冊過程。

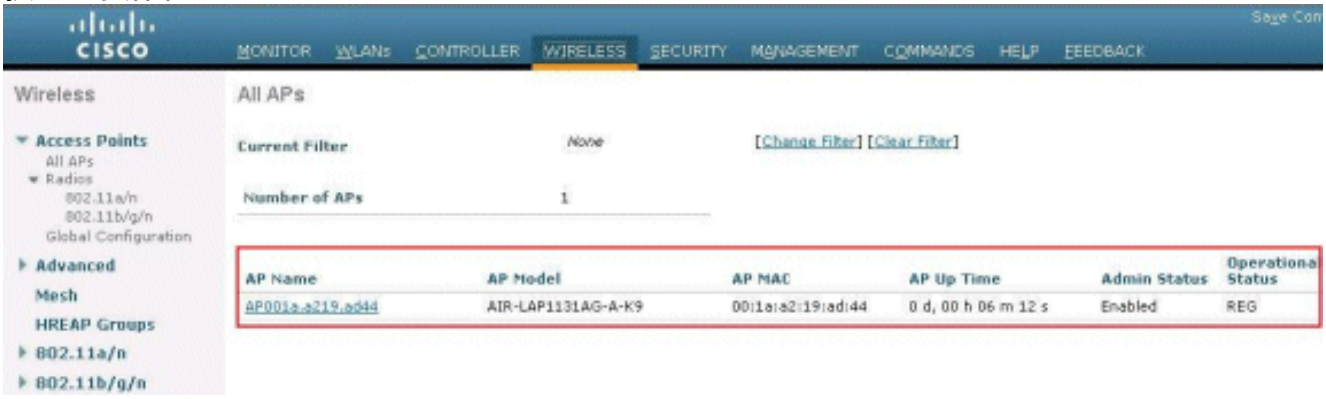
H-REAP AP可以使用向無線LAN控制器(WLC)註冊輕量AP(LAP)中說明的任何方法獲知控制器IP地址。

注意：您還可以配置LAP，以便通過AP上的CLI命令發現控制器。有關詳細資訊，請參閱使用CLI命令發現H-REAP控制器。

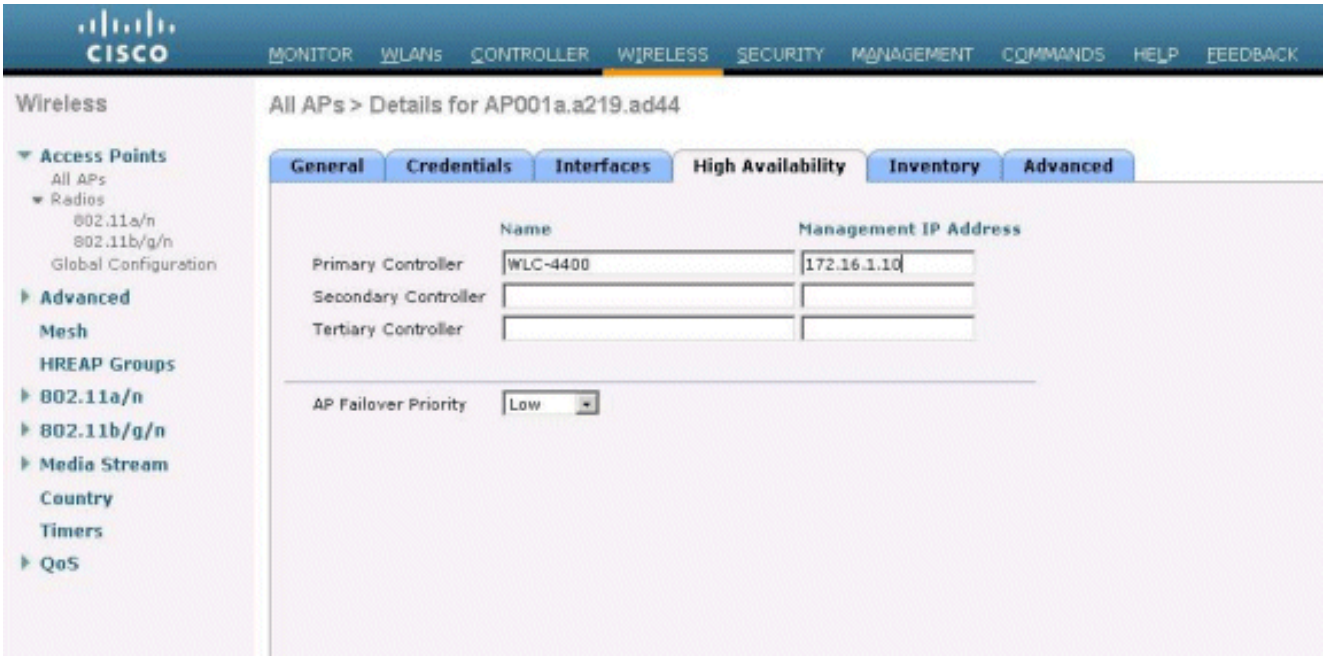
本文檔中的示例使用H-REAP的DHCP選項43過程來學習控制器IP地址。接著它加入控制器，從控制器下載最新的軟體映像和組態，並初始化無線電連結。它會將下載的配置儲存在非易失性記憶體中，以在獨立模式下使用。

在控制器上註冊LAP後，請完成以下步驟：

1. 在控制器GUI中，選擇**Wireless>Access Points**。這將顯示註冊到此控制器的LAP。
2. 按一下要配置的AP。

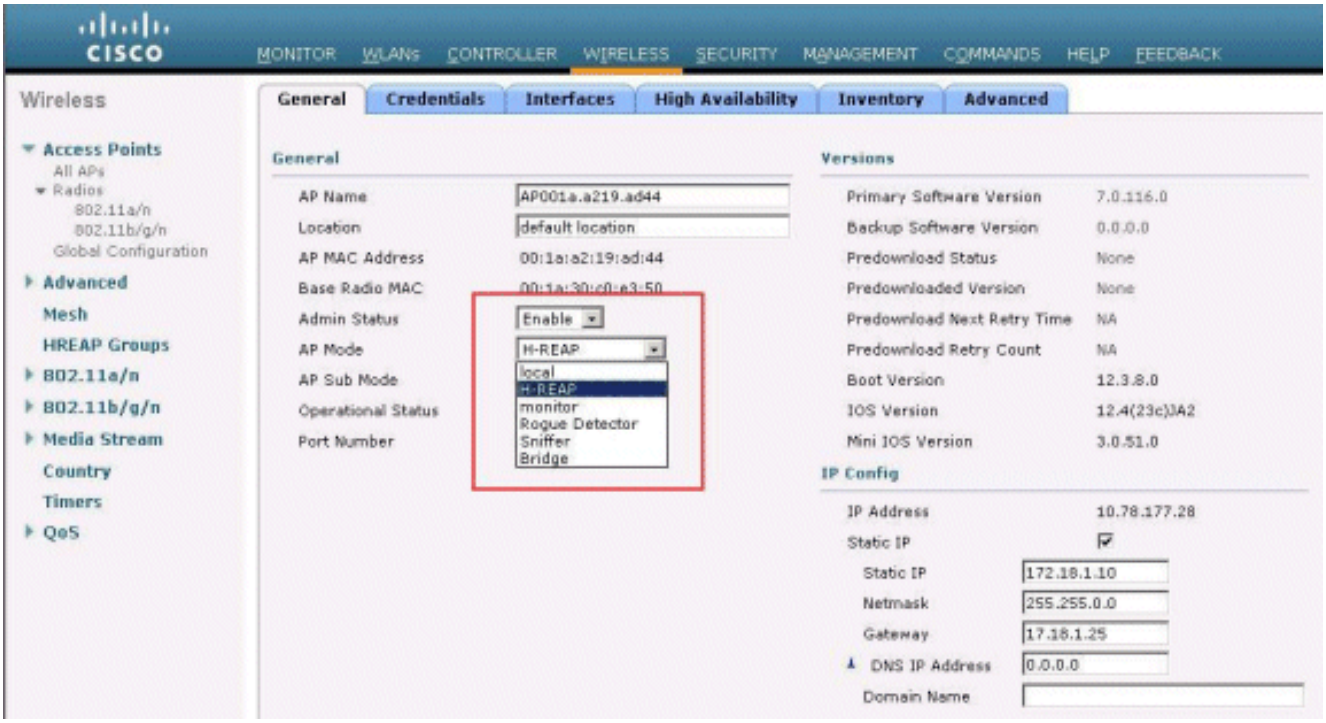


3. 在「APs>Details（APs>詳細資訊）」視窗中，按一下「High Availability（高可用性）」頁籤，定義AP用於註冊的控制器名稱，然後按一下**Apply**。



最多可以定義三個控制器名稱（主、次和第三控制器）。 AP按您在此視窗中提供的順序搜尋控制器。由於此範例僅使用一個控制器，因此範例將控制器定義為主要控制器。

4. 為H-REAP配置LAP。要將LAP配置為在H-REAP模式下運行，請在AP>Details視窗中，在General頁籤下，從相應的下拉選單中選擇**AP mode**作為H-REAP。這會將LAP配置為在H-REAP模式下運行。



注意：在本示例中，您可以看到AP的IP地址已更改為靜態模式，並且已分配靜態IP地址172.18.1.10。進行此分配是因為這是遠端辦公室要使用的子網。因此，您使用來自DHCP伺服器的IP地址，但僅在註冊階段第一次使用。將AP註冊到控制器後，您將地址更改為靜態IP地址。

現在您的LAP已準備好控制器並配置為H-REAP模式，下一步是在控制器端配置H-REAP並討論H-REAP交換狀態。

H-REAP運行理論

支援H-REAP的LAP在以下兩種不同模式下運行：

- **連線**模式：當H-REAP與WLC的CAPWAP控制平面鏈路啟動並正常運行時，H-REAP稱為連線模式。這表示LAP和WLC之間的WAN鏈路沒有關閉。
- **獨立**模式：當H-REAP與WLC的WAN鏈路斷開時，該H-REAP稱為獨立模式。例如，當此H-REAP不再連線到通過WAN鏈路連線的WLC時。

用於驗證客戶端的驗證機制可定義為**Central**或**Local**。

- Central Authentication — 指涉及遠端站點WLC進程的身份驗證型別。
- Local Authentication — 指不涉及來自WLC的任何身份驗證處理的身份驗證型別。

注意：所有802.11身份驗證和關聯處理均在H-REAP處進行，無論LAP處於哪種模式。在連線模式下，H-REAP會將這些關聯和驗證代理到WLC。在獨立模式下，LAP無法向WLC通知此類事件。

當客戶端連線到H-REAP AP時，AP會將所有身份驗證消息轉發到控制器。驗證成功後，其封包會進行本地交換或透過通道傳回控制器。這取決於其所連線的WLAN的配置。

透過H-REAP，控制器上設定的WLAN可以在兩種不同模式下運作：

- **中央交換**：如果H-REAP上的WLAN的資料流量配置為通過隧道連線到WLC，則該WLAN會以中央交換模式運行。
- **本地交換**：如果H-REAP上的WLAN的資料流量在LAP本身的有線介面本地終止，而沒有隧道連線到WLC，則稱該WLAN在本地交換模式下運行。**注意**：只能為H-REAP本地交換配置WLAN 1至8，因為只有這些WLAN可應用於支援H-REAP功能的1130、1240和1250系列AP。

H-REAP交換狀態

結合上一節中提到的身份驗證和交換模式，H-REAP可以在以下任一狀態下運行：

- 集中身份驗證、集中交換
- 身份驗證關閉，交換關閉
- 集中身份驗證、本地交換
- 身份驗證關閉，本地交換
- 本地身份驗證、本地交換

集中身份驗證、集中交換

在此狀態下，對於給定的WLAN，AP將所有客戶端身份驗證請求轉發到控制器，並將所有客戶端資料隧道連線到WLC。此狀態僅在H-REAP處於連線模式時有效。無論採用何種身份驗證方法，配置為在此模式下運行的任何WLAN都會在WAN中斷期間丟失。

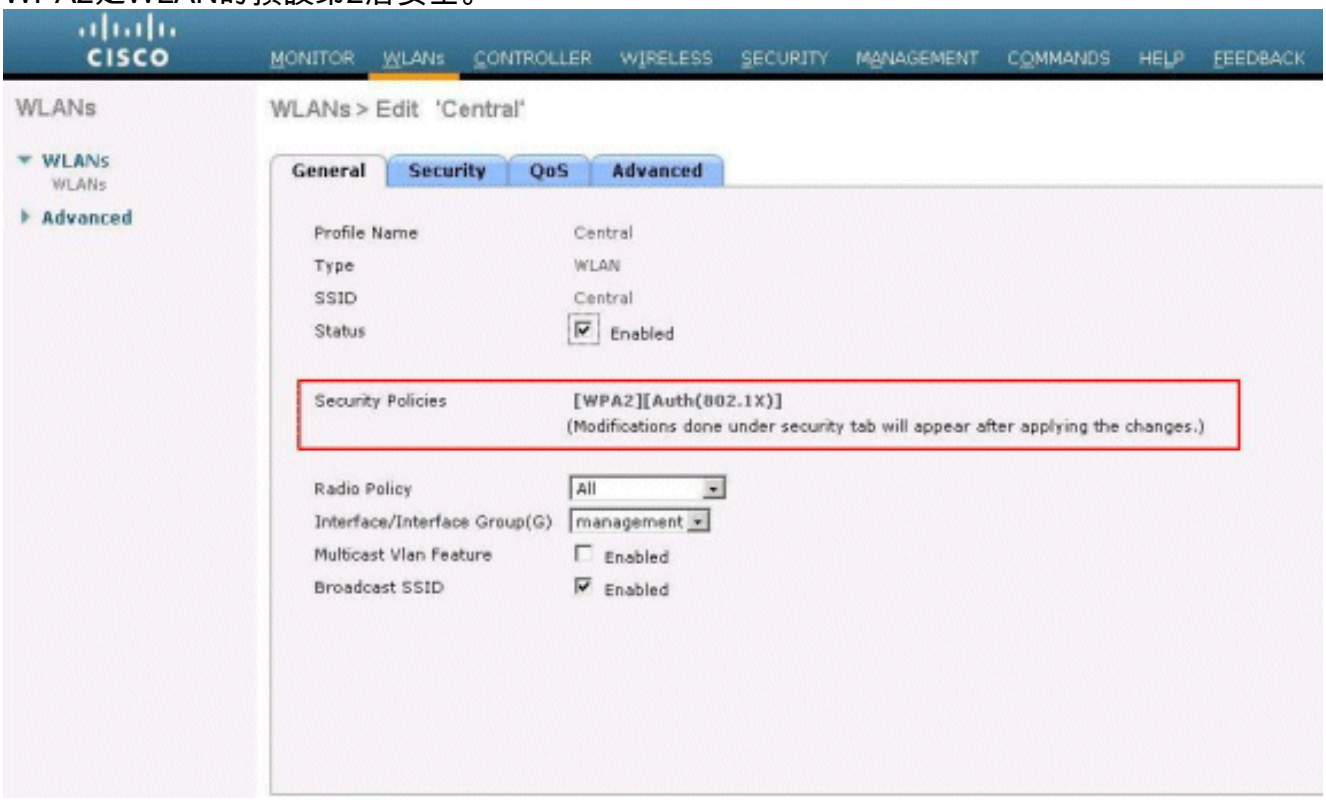
此示例使用以下配置設定：

- WLAN/SSID名稱：**中央**
- 第2層安全：**WPA2**
- H-REAP本地交換：**已禁用**

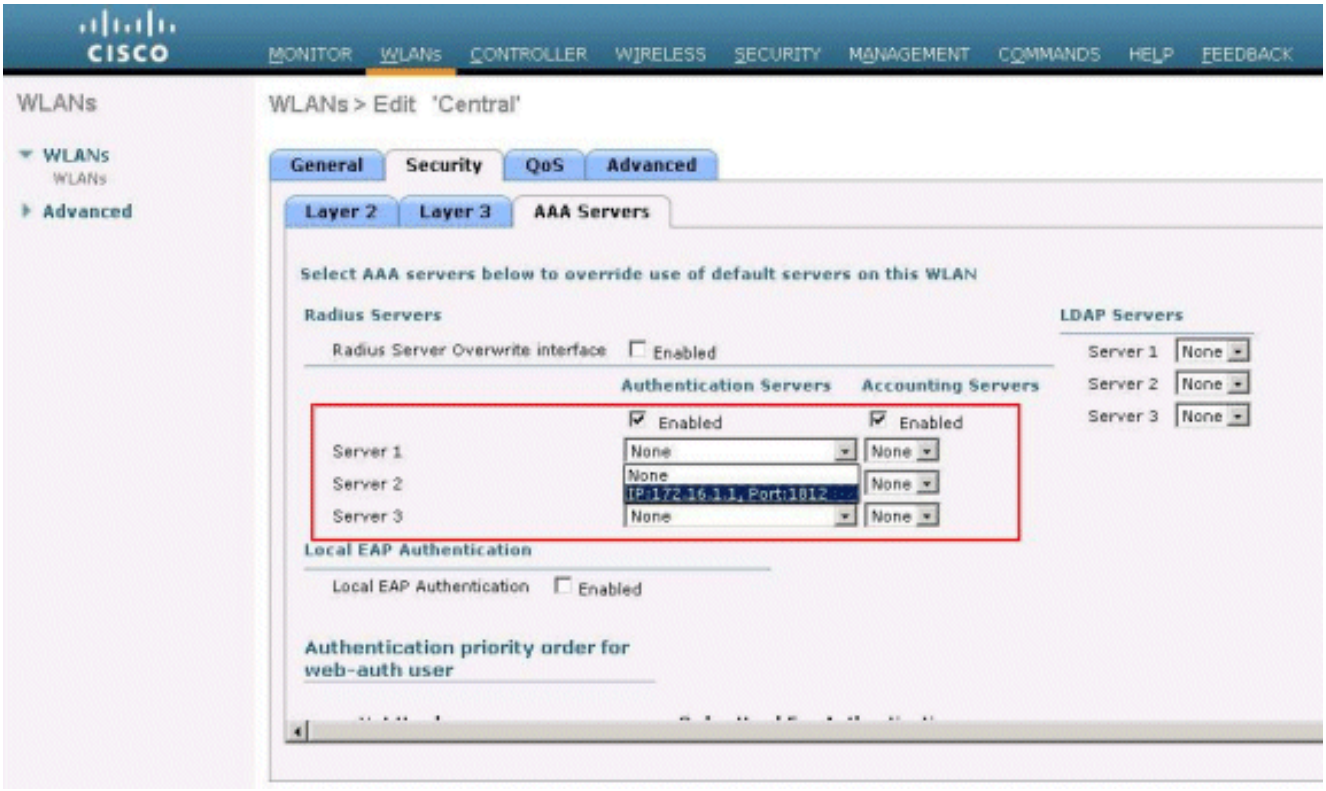
完成以下步驟，以便使用GUI將WLC設定為中央驗證、中央交換：

1. 按一下「**WLANs**」以建立一個名為「**Central**」的新WLAN，然後按一下「**Apply**」。

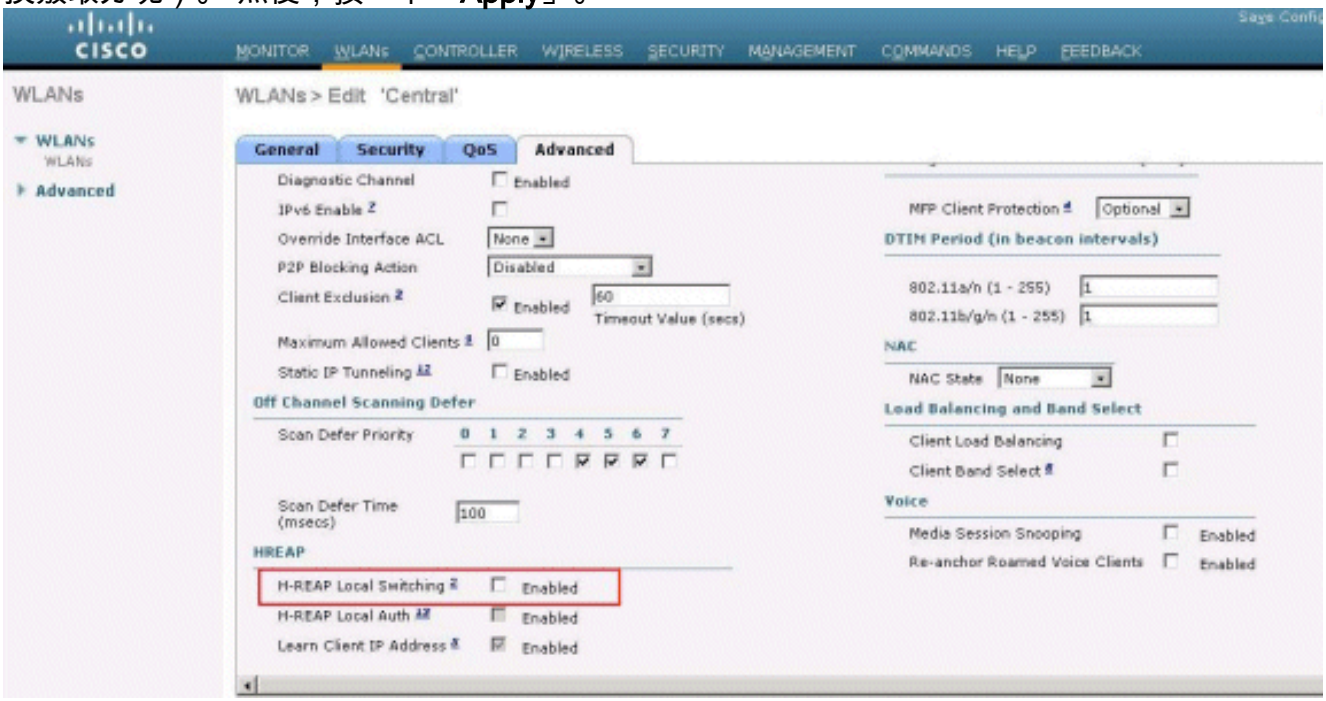
2. 由於此WLAN使用中央身份驗證，因此我們在Layer 2 Security欄位中使用WPA2身份驗證。WPA2是WLAN的預設第2層安全。



3. 選擇AAA Servers頁籤，然後選擇為身份驗證配置的相應伺服器。



4. 由於此WLAN使用中央交換，您需要確保H-REAP本地交換覈取方塊已禁用（即未選中本地交換覈取方塊）。 然後，按一下「Apply」。

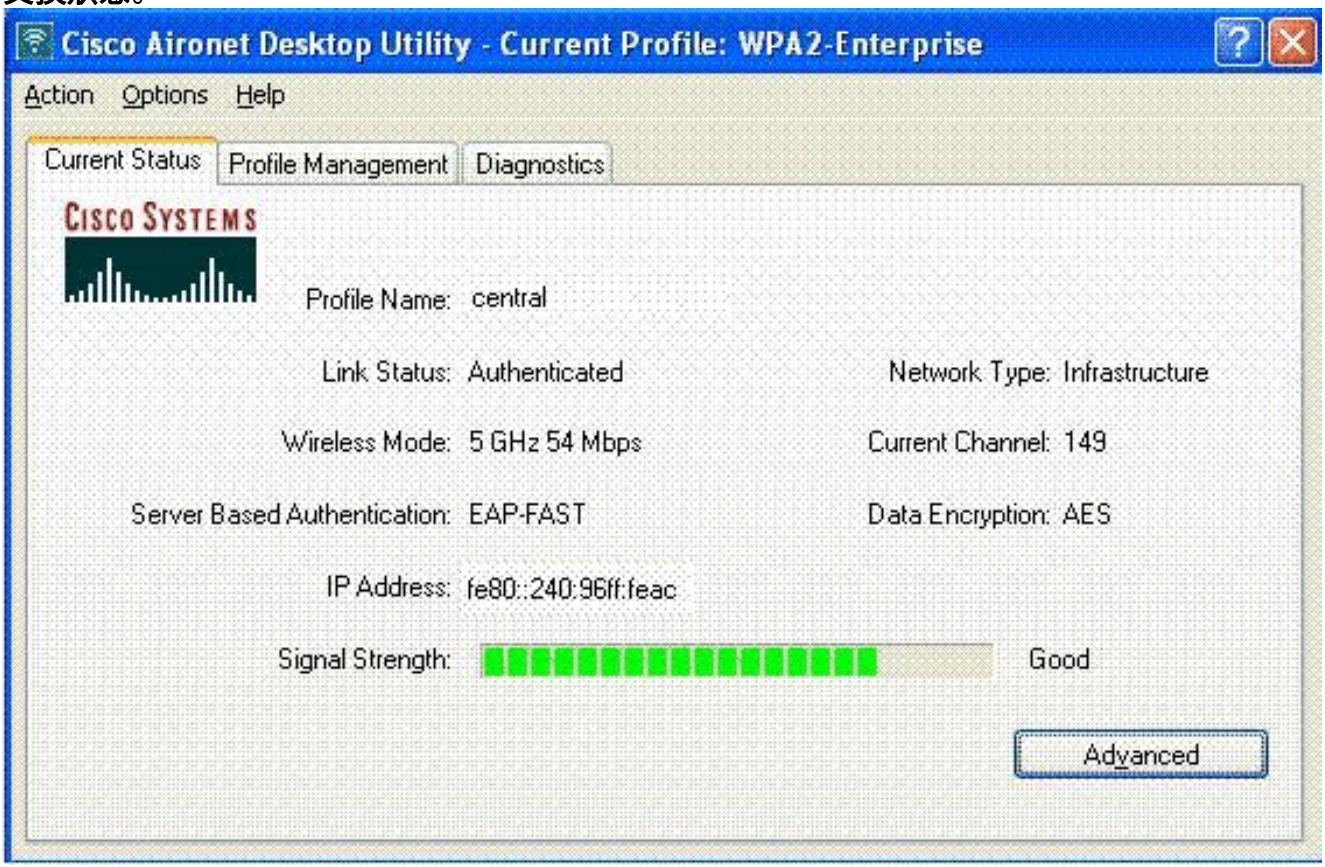


驗證集中身份驗證、集中交換

請完成以下步驟：

1. 使用相同的SSID和安全配置配置無線客戶端。在本示例中，SSID為*Central*，安全方法為*WPA2*。
2. 輸入在RADIUS伺服器>使用者設定中配置的使用者名稱和密碼，以啟用客戶端中的中央SSID。此示例使用*User1*作為使用者名稱和密碼。

使用者端會由RADIUS伺服器進行集中驗證，且與H-REAP AP關聯。H-REAP現在處於集中身份**驗證、集中交換狀態**。



身份驗證關閉，交換關閉

使用Central Authentication， Central Switching一節中介紹的相同配置，禁用連線控制器的WAN鏈路。現在，控制器等待來自AP的心跳應答。心跳應答類似於keepalive消息。控制器會嘗試連續五個心跳，每個心跳每秒一次。

由於未收到來自H-REAP的心跳應答，因此WLC會註銷LAP。

從WLC的CLI發出**debug capwap events enable**命令以驗證註銷程式。以下是**debug**指令的範例輸出：

```
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進入獨立模式。

由於此WLAN先前已經過中央驗證和中央交換，因此控制流量和資料流量都通過隧道傳回控制器。因此，如果沒有控制器，客戶端將無法保持與H-REAP的關聯且已斷開連線。客戶端關聯和身份驗證都關閉的H-REAP狀態稱為身份驗證關閉、交換關閉。

集中身份驗證、本地交換

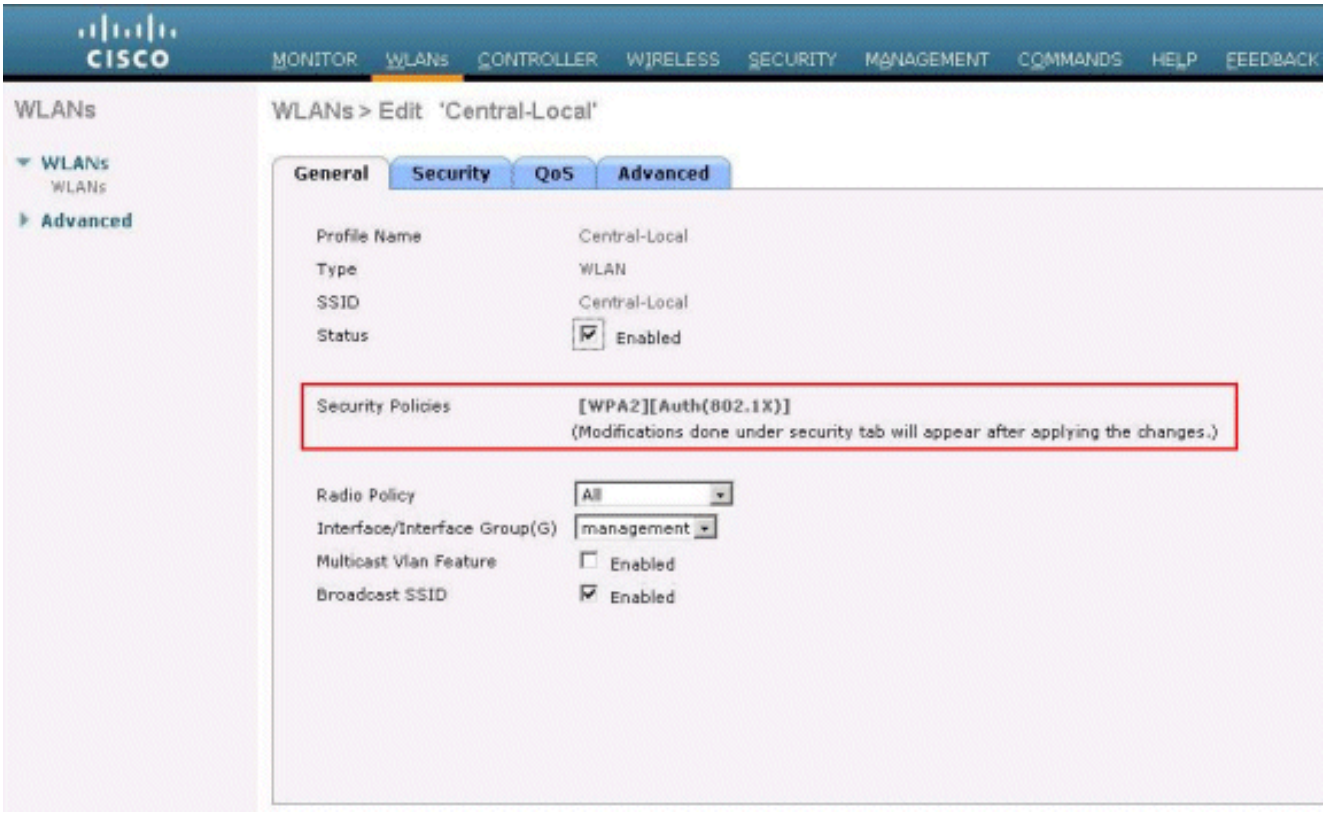
在此狀態下，對於給定的WLAN，WLC處理所有客戶端身份驗證，H-REAP LAP在本地交換資料包。在客戶端成功進行身份驗證後，控制器向H-REAP傳送capwap控制命令，並指示LAP在本地交換給定客戶端的資料包。成功身份驗證後，每個客戶端傳送此消息。此狀態僅適用於連線模式。

此示例使用以下配置設定：

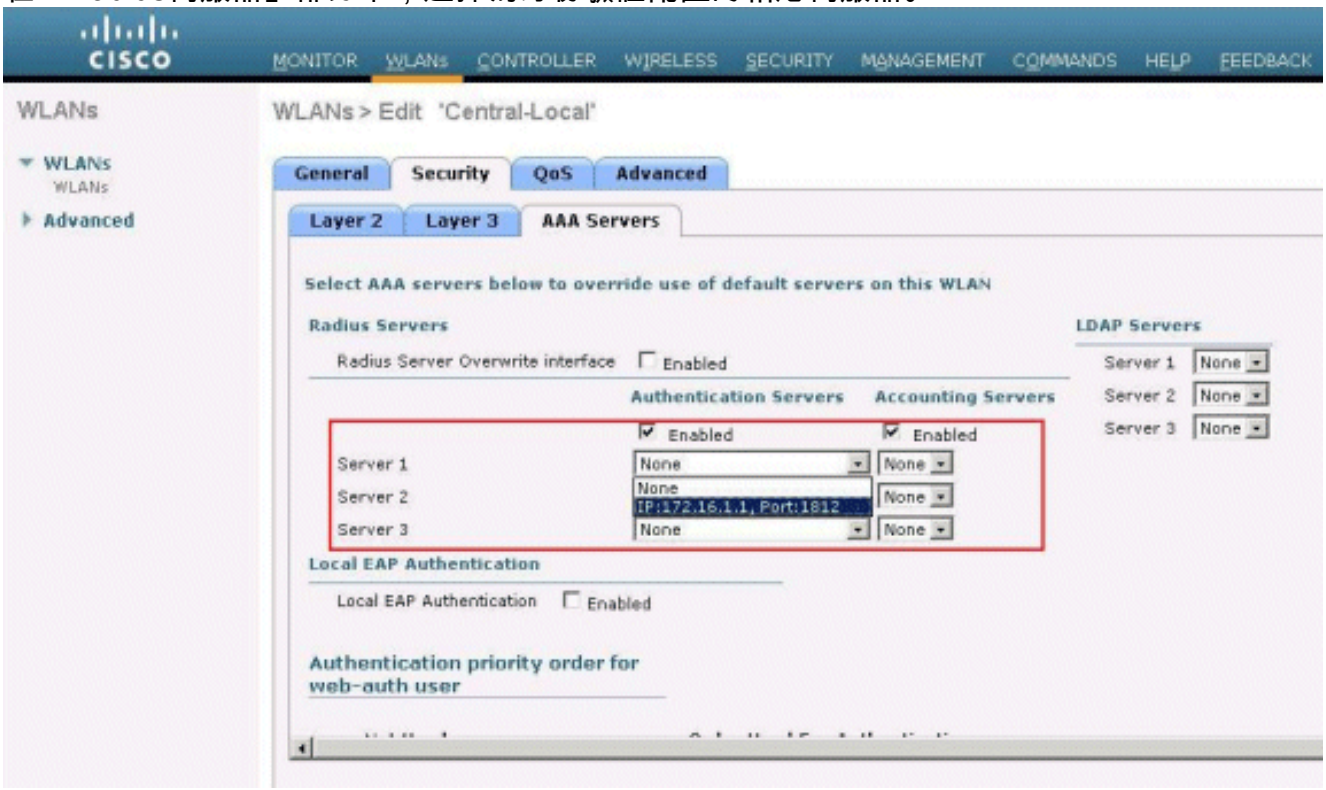
- WLAN/SSID名稱：**中央 — 本地**
- 第2層安全：**WPA2**。
- H-REAP本地交換：**已啟用**

在控制器GUI上，完成以下步驟：

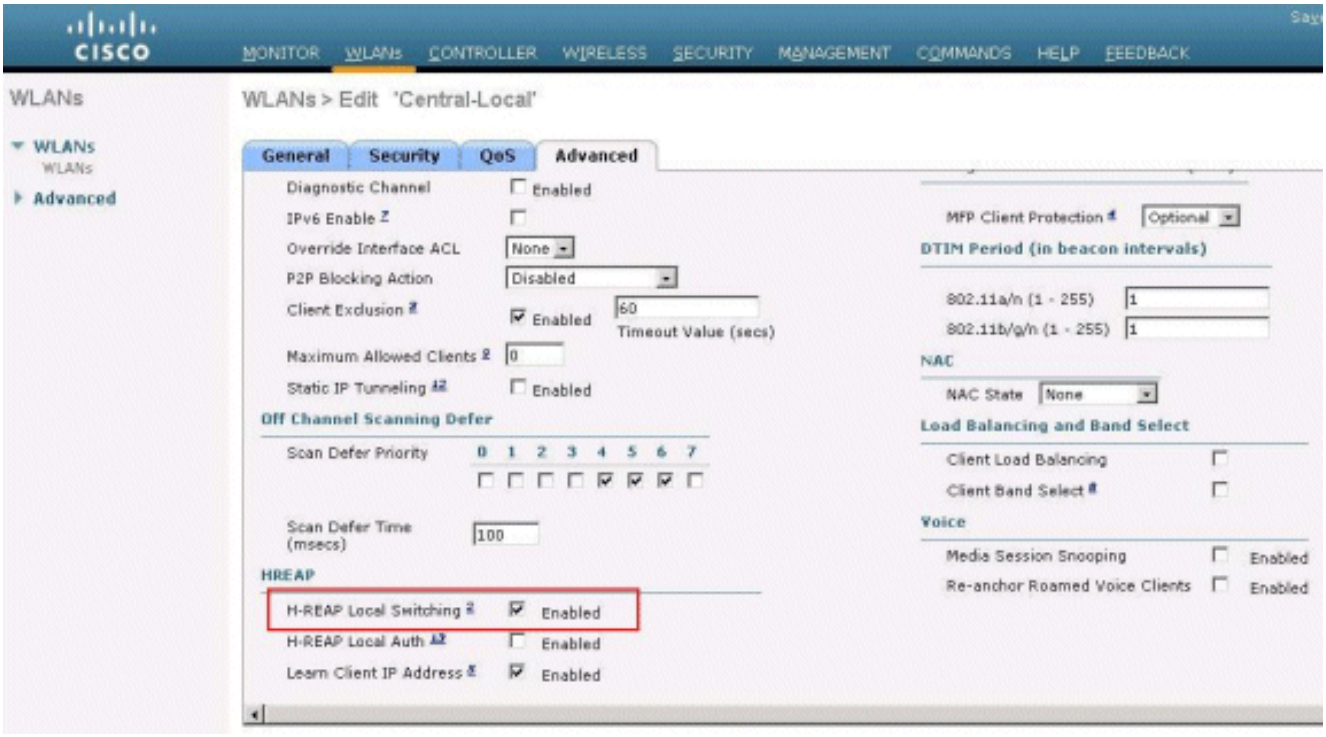
1. 按一下「**WLANs**」以建立一個名為「Central-Local」的新WLAN，然後按一下「**Apply**」。
2. 由於此WLAN使用中央身份驗證，請在Layer 2 Security欄位中選擇**WPA2身份驗證。**



3. 在「Radius伺服器」部分下，選擇為身份驗證配置的相應伺服器。



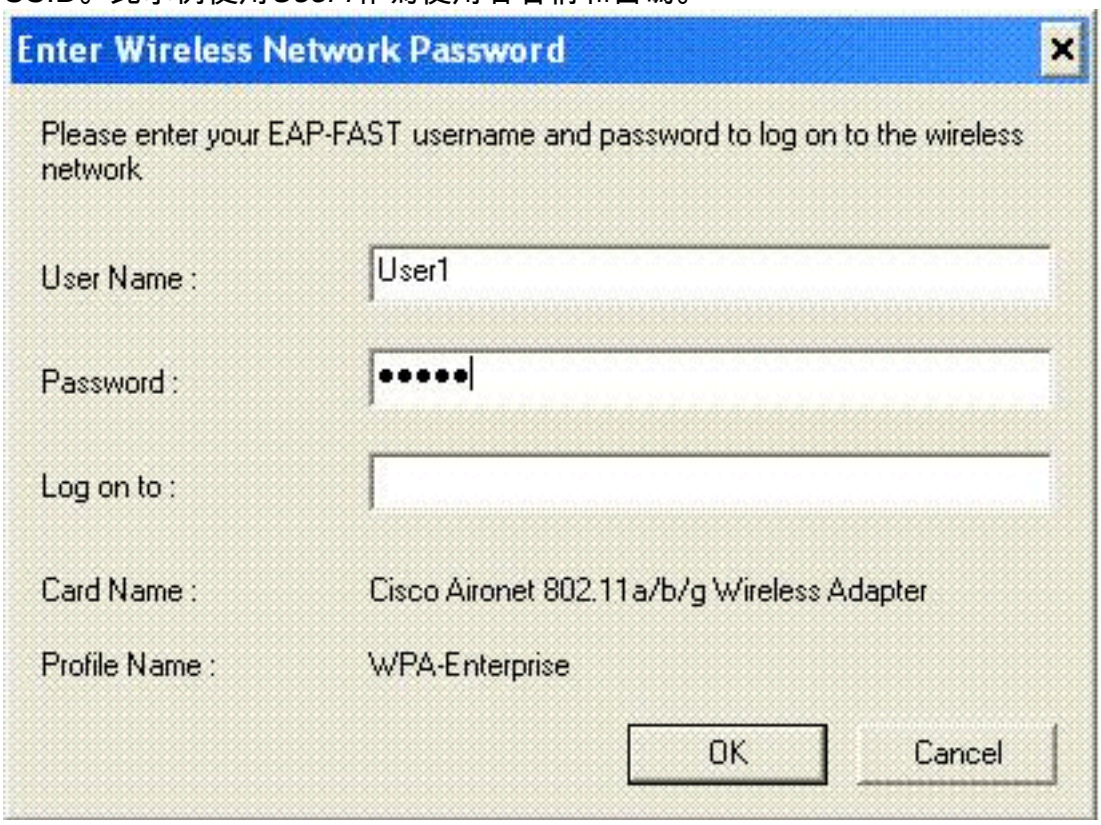
4. 勾選「**H-REAP Local Switching**」覈取方塊，以便在H-REAP本地交換屬於此WLAN的客戶端流量。



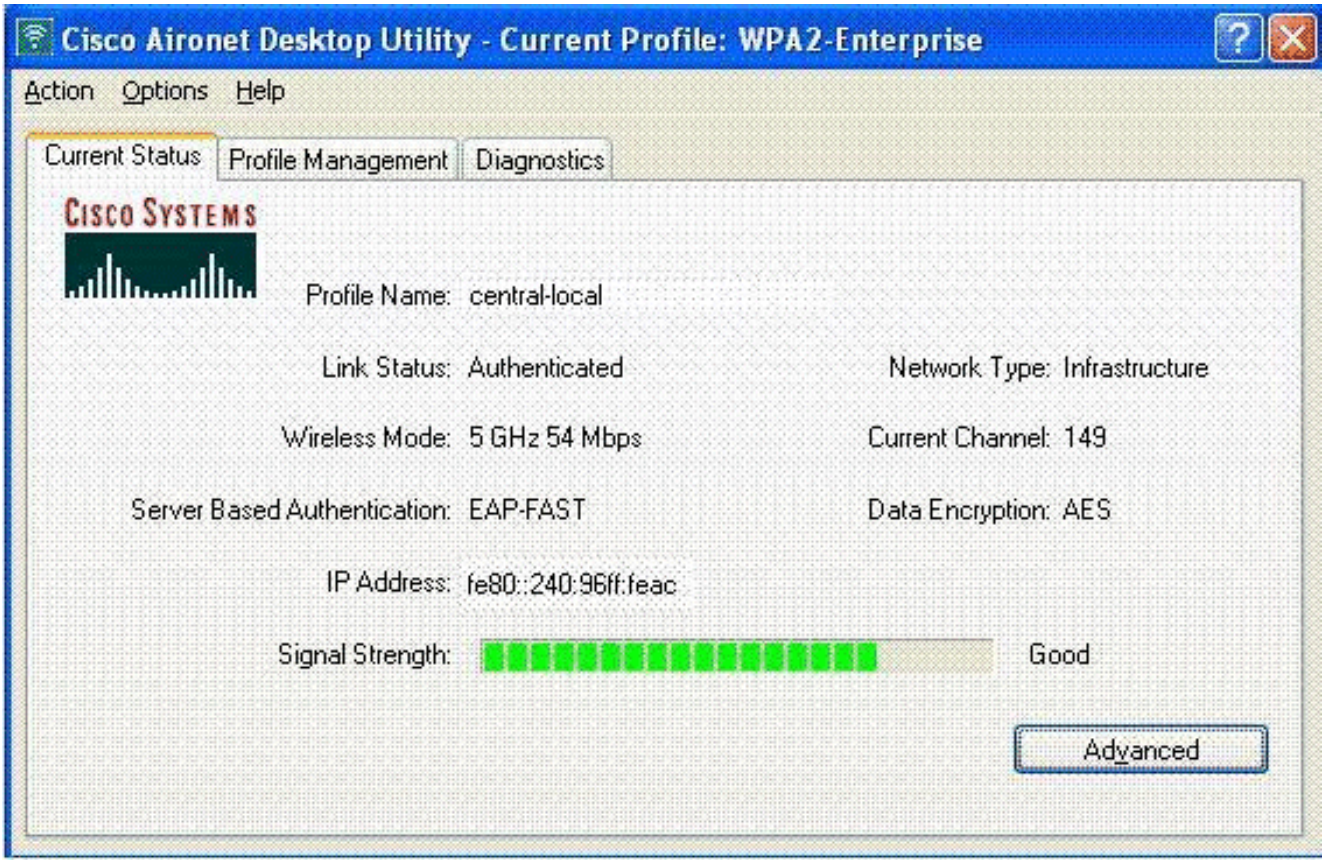
驗證集中身份驗證、本地交換

請完成以下步驟：

1. 使用相同的SSID和安全配置配置無線客戶端。在本示例中，SSID是*Central-Local*，安全方法是*WPA2*。
2. 輸入在RADIUS伺服器>使用者設定中配置的使用者名稱和密碼，以啟用客戶端中的中央本地SSID。此示例使用*User1*作為使用者名稱和密碼。



3. 按一下「**OK**」（確定）。使用者端會由RADIUS伺服器進行集中驗證，且與H-REAP AP相關聯。H-REAP現在處於集中身份**驗證、本地交換狀態**。



身份驗證關閉，本地交換

如果本地交換的WLAN設定為需要在WLC上處理的任何驗證型別（例如EAP驗證[動態WEP/WPA/WPA2/802.11i]、WebAuth或NAC），則在WAN發生故障時，WLAN會進入驗證關閉、本地交換狀態。在此狀態下，對於給定的WLAN，H-REAP拒絕任何嘗試進行身份驗證的新客戶端。但是，它會繼續傳送信標並探測響應，以使現有客戶端保持正確連線。此狀態僅在獨立模式下有效。

若要驗證此狀態，請使用在Central Authentication， Local Switching一節中說明的相同配置。

如果連線WLC的WAN鏈路斷開，則WLC將經歷註銷H-REAP的過程。

註銷後，H-REAP進入獨立模式。

透過此WLAN相關聯的使用者端仍可保持其連線。但是，由於控制器（身份驗證器）不可用，因此H-REAP不允許來自此WLAN的任何新連線。

這可以通過啟用同一WLAN中的另一個無線客戶端來驗證。您會發現該客戶端的身份驗證失敗，並且不允許該客戶端關聯。

注意：當WLAN客戶端計數等於零時，H-REAP將停止所有關聯的802.11功能，不再使用給定SSID的信標。這會將WLAN移至下一個H-REAP狀態：身份**驗證關閉，交換關閉**。

本地身份驗證、本地交換

在此狀態下，H-REAP LAP處理客戶端身份驗證並在本地交換客戶端資料包。此狀態僅在獨立模式下有效，並且僅適用於可以在AP本地處理且不涉及控制器處理的身份驗證型別

如果配置的身份驗證型別可在AP本地處理，則先前處於**中央身份驗證、本地交換狀態的**H-REAP會

進入此狀態。如果配置的身份驗證無法在本地處理（例如802.1x身份驗證），則在獨立模式下，H-REAP將進入身份驗證關閉、本地交換模式。

以下是一些可在獨立模式下在AP本地處理的常見驗證機制：

- 未解決
- 已共用
- WPA-PSK
- WPA2-PSK

注意：當AP處於連線模式時，WLC會處理所有身份驗證過程。當H-REAP處於獨立模式時，開放、共用和WPA/WPA2-PSK身份驗證將傳輸到所有客戶端身份驗證發生處的LAP。

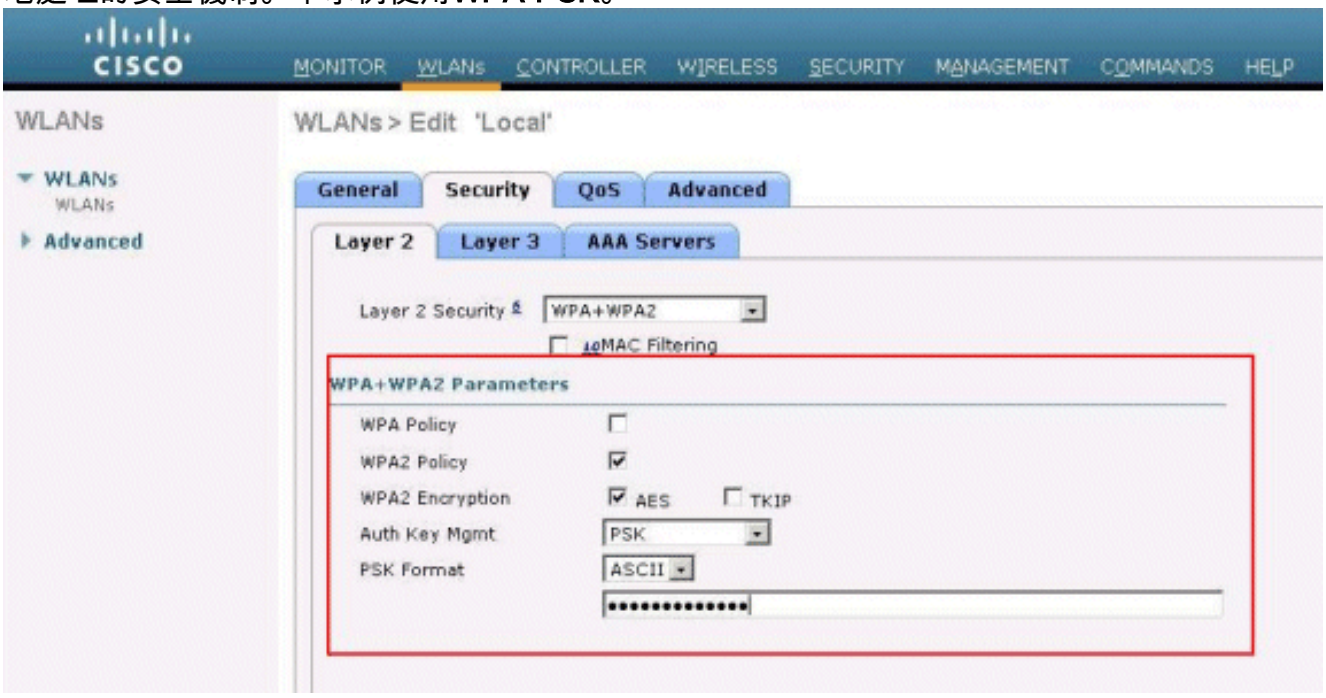
注意：在WLAN上啟用本地交換的情況下使用混合REAP時，不支援外部Web驗證。

此示例使用以下配置設定：

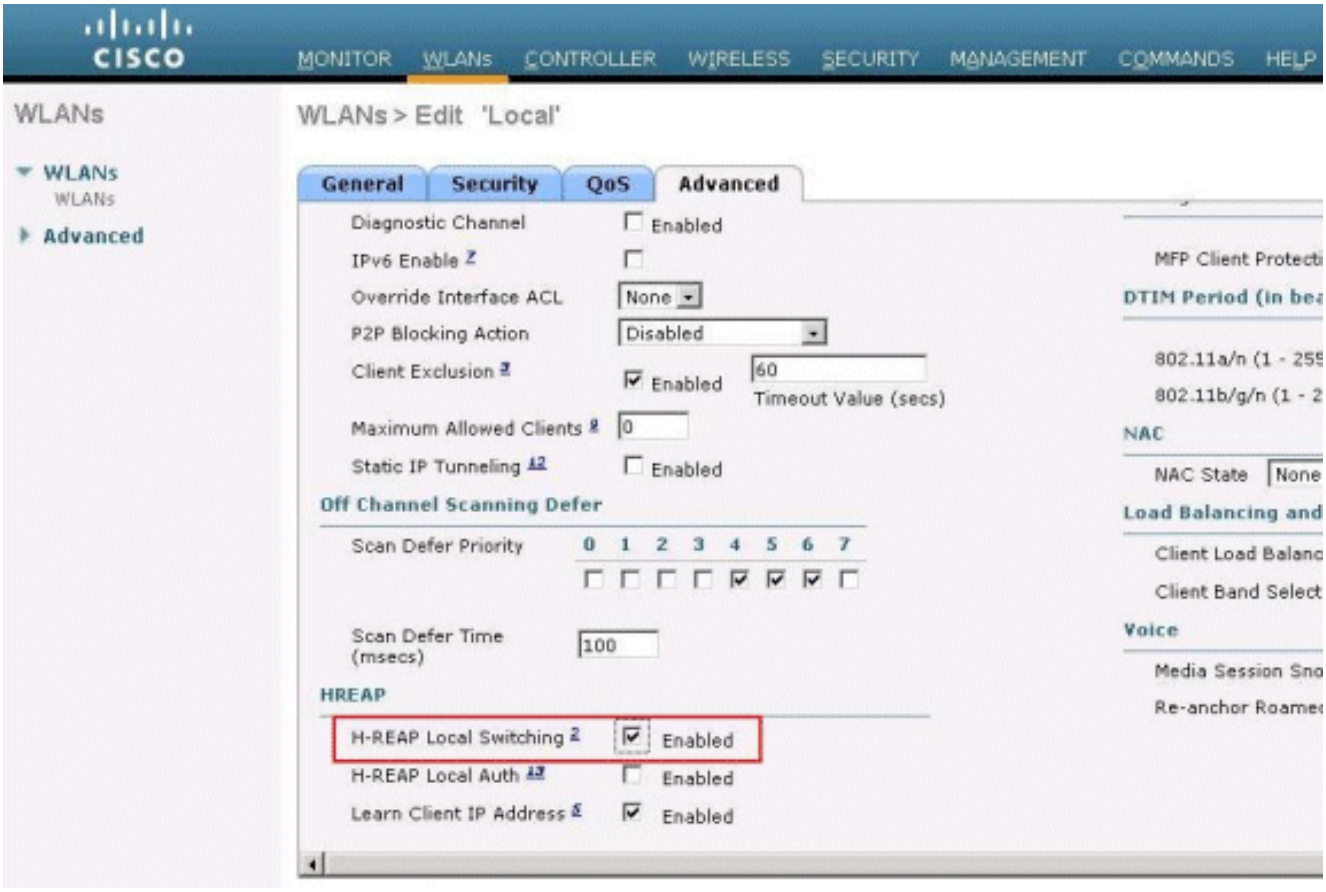
- WLAN/SSID名稱：**本地**
- 第2層安全：**WPA-PSK**
- H-REAP本地交換：**已啟用**

在控制器GUI上，完成以下步驟：

1. 按一下「**WLANs**」以建立一個名為「Local」的新WLAN，然後按一下「**Apply**」。
2. 由於此WLAN使用本地驗證，因此請選擇**WPA-PSK**或上述任何可以在「第2層安全」欄位中本地處理的安全機制。本示例使用**WPA-PSK**。



3. 選擇後，您需要配置要使用的預共用金鑰/密碼短語。客戶端必須相同，身份驗證才能成功。
4. 勾選「**H-REAP Local Switching**」覈取方塊，以便在H-REAP本地交換屬於此WLAN的客戶端流量。



驗證本地身份驗證、本地交換

請完成以下步驟：

1. 使用相同的SSID和安全配置配置客戶端。這裡的SSID是*Local*，安全方法是*WPA-PSK*。
2. 啟用客戶端中的本地SSID。客戶端在控制器處集中進行身份驗證，並與H-REAP關聯。客戶端流量配置為本地交換。現在，H-REAP處於集中身份驗證、本地交換狀態。
3. 停用連線到控制器的WAN連結。控制器會照常執行取消註冊過程。H-REAP從控制器註銷。註銷後，H-REAP進入獨立模式。但是，屬於此WLAN的客戶端仍保持與H-REAP的關聯。此外，由於此處的身份驗證型別可以在沒有控制器的AP上本地處理，因此H-REAP允許通過此WLAN關聯任何新無線客戶端。
4. 若要驗證這一點，請啟用同一WLAN上的任何其他無線使用者端。您可以看到使用者端已驗證且成功關聯。

疑難排解

- 要進一步排除H-REAP控制檯埠上的客戶端連線問題，請輸入以下命令：
  `AP_CLI#show capwap reap association`
- 若要進一步排解控制器上的使用者端連線問題並限制進一步偵錯的輸出，請使用以下命令：
  `AP_CLI#debug mac addr`
- 若要偵錯使用者端的802.11連線問題，請使用以下命令：
  `AP_CLI#debug dot11 state enable`
- 使用以下命令調試客戶端的802.1X身份驗證過程和故障：
  `AP_CLI#debug dot1x events enable`

- 使用以下命令可以調試後端控制器/RADIUS消息：
  AP_CLI#**debug aaa events enable**

- 或者，若要啟用一整套客戶端debug命令，請使用以下命令：
  AP_CLI#**debug client**

相關資訊

- 無線LAN控制器和輕量型存取點基本組態範例
- 無線 LAN 控制器上的 VLAN 組態範例
- 思科無線LAN控制器組態設定指南7.0版
- 混合REAP設計和部署指南
- 混合遠端邊緣接入點(H-REAP)基本故障排除
- 輕量接入點的WLAN控制器故障切換配置示例
- 無線產品支援
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。