配置Aironet 600系列OfficeExtend無線存取點

目錄

簡介

本文檔提供有關配置用於Cisco Aironet® 600系列OfficeExtend無線存取點(OEAP)的Cisco無線區域網(WLAN)控制器的要求的資訊。Cisco Aironet 600系列OEAP支援拆分模式操作，而且它具有需要透過WLAN控制器進行配置的設施，以及可由終端使用者在本地配置的功能。本文檔還提供了有關正確連線和支援的功能集所需的配置的資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Cisco Aironet 600系列OfficeExtend無線存取點(OEAP)。

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

設定準則

- 以下控制器支援Cisco Aironet 600系列OEAP：Cisco 5508、WiSM-2和Cisco 2504。
- 支援Cisco Aironet 600系列OEAP的第一個控制器版本是7.0.116.0
- 控制器的管理介面需要位於可路由的IP網路中。
- 需要更改公司防火牆配置以允許使用UDP埠號5246和5247的資料流。

Office Extend解決方案概述

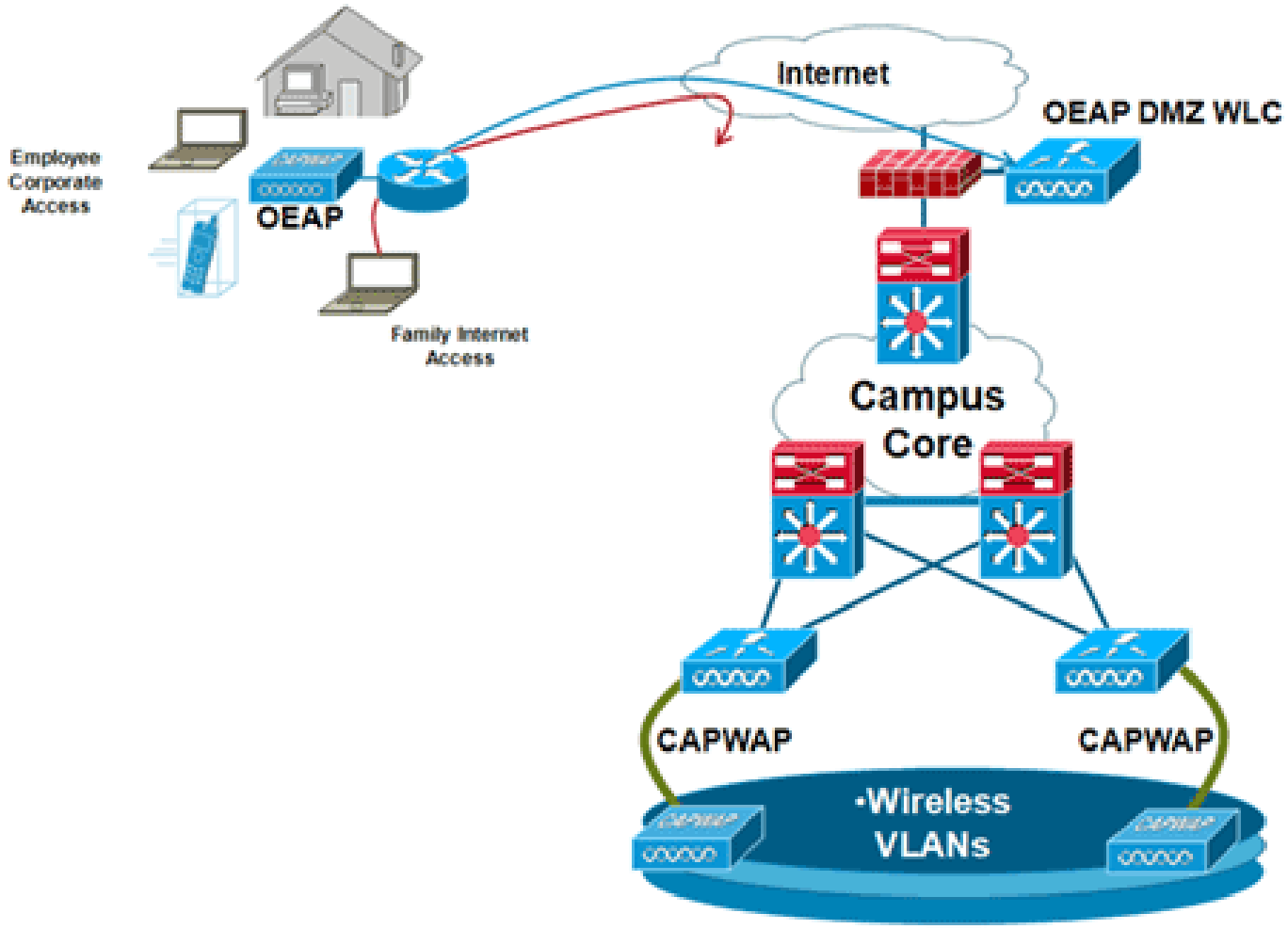
- 為使用者提供一個存取點(AP)，內含公司控制器的IP位址，或者使用者可以從組態畫面（設定HTML頁面）輸入控制器的IP位址。
- 使用者將AP插入其家庭路由器。
- AP從本地路由器獲取IP地址，加入已準備好的控制器並建立安全隧道。
- 然後，Cisco Aironet 600系列OEAP會通告公司SSID，它將相同的安全方法和服務透過WAN擴展到使用者的家庭。
- 如果配置了遠端LAN，則AP上的一個有線埠將透過隧道連線回控制器。
- 然後，使用者可另外啟用本地SSID供個人使用。

防火牆配置指南

防火牆上的常規配置是允許CAPWAP控制和CAPWAP管理埠號透過防火牆。Cisco Aironet 600系列OEAP控制器可以放在DMZ區域中。

註：需要在WLAN控制器與Cisco Aironet 600系列OEAP之間的防火牆上打開UDP 5246和5247埠。

此圖顯示DMZ上的Cisco Aironet 600系列OEAP控制器：



以下是防火牆組態範例：

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
```

```
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

為了將內部AP管理器IP地址作為CAPWAPP發現響應資料包的一部分傳輸到OfficeExtend AP，控制器管理員需要確保在AP管理器介面中啟用了NAT，並且向AP傳送了正確的NATed IP地址。

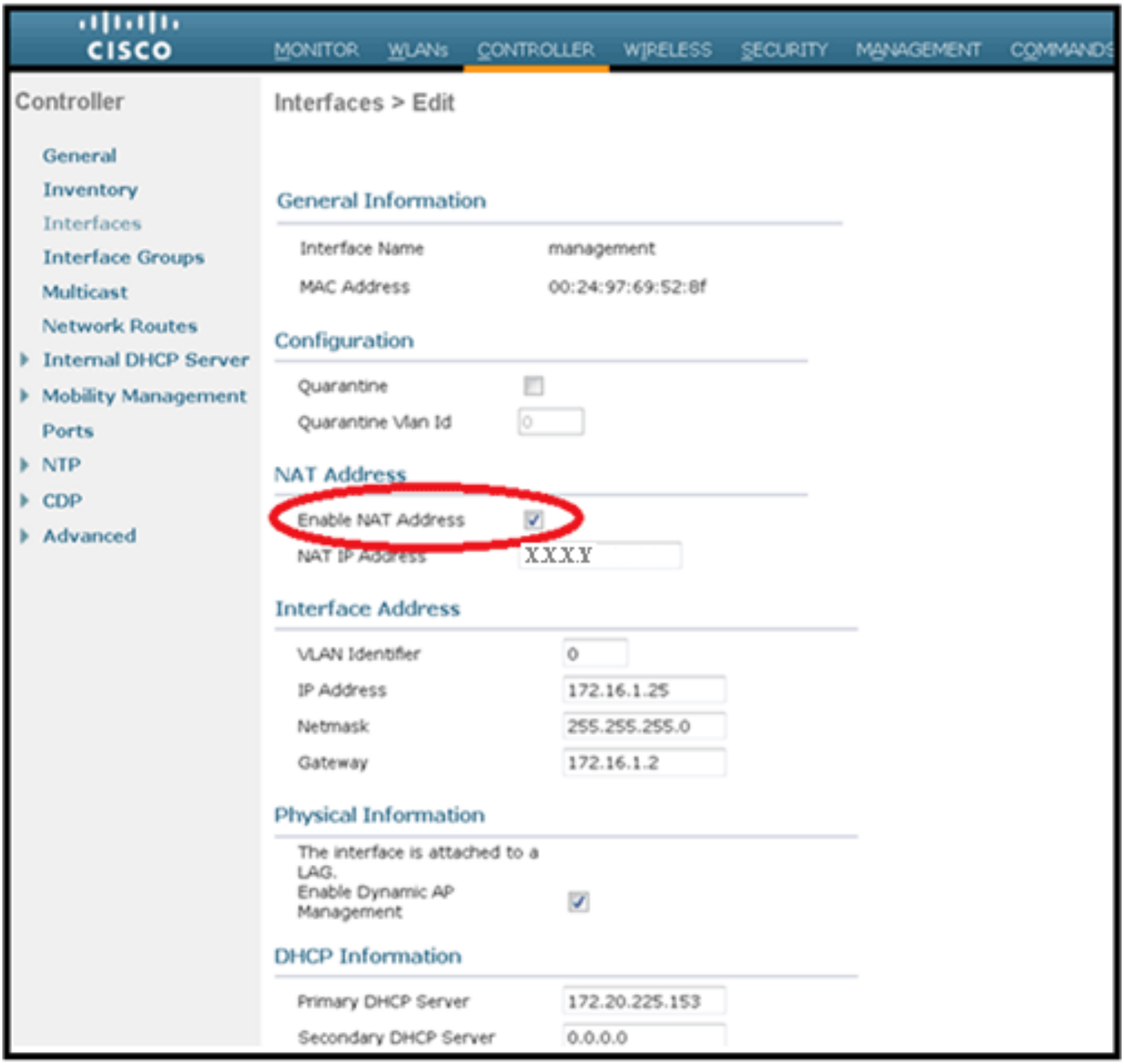
注意：預設情況下，啟用NAT時，WLC在AP發現期間僅使用NAT IP地址進行響應。如果AP存在於NAT網關的內部和外部，則發出以下命令以將WLC設定為使用NAT IP地址和非NAT（內部）管理IP地址進行響應：

<#root>

config network ap-discovery nat-ip-only disable

注意：只有在WLC具有NAT IP地址時才需要執行此操作。

下圖顯示，假設WLC具有NAT IP地址，則啟用NAT：



注意：如果控制器配置了網際網路可路由IP地址並且不在防火牆之後，則不需要此配置。

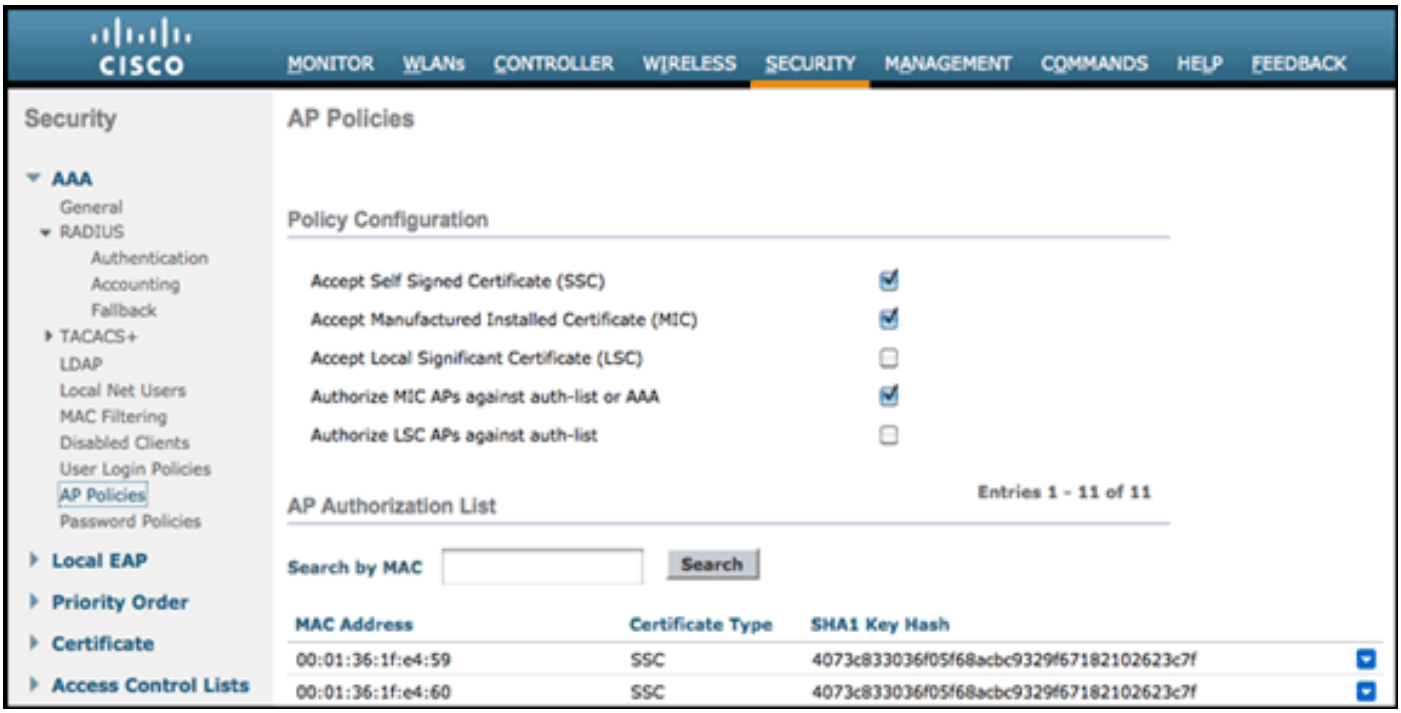
Office Extend AP-600配置步驟

Cisco Aironet 600系列OEAP將作為本地模式存取點連線到WLC。

註：600系列不支援監控模式、H-REAP、嗅探器、惡意程式檢測、網橋模式和SE-Connect模式，這些模式不可配置。

註：1040、1130、1140和3502i系列存取點中的Cisco Aironet 600系列OEAP功能要求為混合REAP (H-REAP)配置AP，並將AP的子模式設定為Cisco Aironet 600系列OEAP。這在600系列上是不行的，因為它使用本地模式，且無法更改。

MAC過濾可用於在初始加入過程中進行AP身份驗證，以防止未經授權的Cisco Aironet 600系列OEAP裝置加入控制器。下圖顯示了啟用MAC過濾和配置AP安全策略的位置：



此處輸入乙太網MAC（非無線電MAC地址）。此外，如果將MAC地址輸入Radius伺服器，則必須使用小寫。您可以檢視AP事件日誌以瞭解有關如何發現乙太網MAC地址的資訊（稍後將對此進行詳細介紹）。

WLAN和遠端LAN配置設定

Cisco Aironet 600系列OEAP上有一個物理遠端LAN埠(黃色埠#4)。其配置方式與WLAN非常相似。但是，由於它不是無線埠和AP背面的有線LAN埠，因此它被調出並作為遠端LAN埠進行管理。

雖然裝置上只有一個物理埠，但如果使用集線器或交換機，最多可以連線四個有線客戶端。

注意：遠端LAN客戶端限制支援將交換機或集線器連線到多個裝置的遠端LAN埠，或直接連線到連線到該埠的Cisco IP電話。

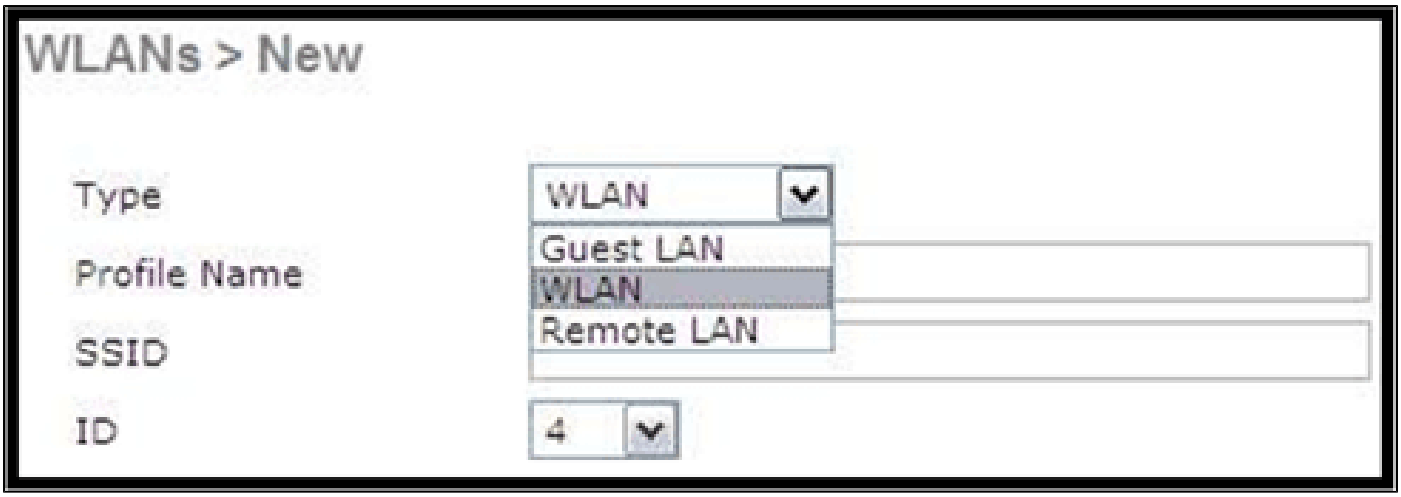
注意：只有前四個裝置可以連線，直到其中一個裝置空閒超過一分鐘。如果使用802.1x驗證，嘗試在有線連線埠上使用多個使用者端時可能會發生問題。

注意：此數字不影響為控制器WLAN強加的十五個限制。

遠端LAN的設定方式與控制器上設定的WLAN和訪客LAN類似。

WLAN是無線安全性設定檔。這些是貴公司網路使用的配置檔案。Cisco Aironet 600系列OEAP最多支援兩個WLAN和一個遠端LAN。

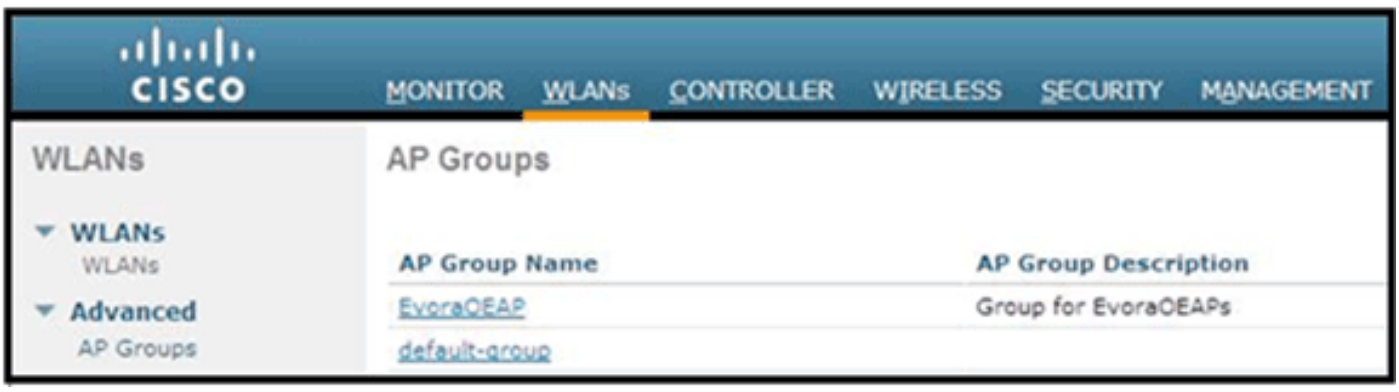
遠端LAN與WLAN類似，不同之處在於它是對映到存取點背面的有線連線埠(黃色連線埠#4)，如下圖所示：



注意：如果您有兩個以上的WLAN或一個以上的遠端LAN，則所有這些WLAN都需要放置在AP組中。

下圖顯示了WLAN和遠端LAN的配置位置：

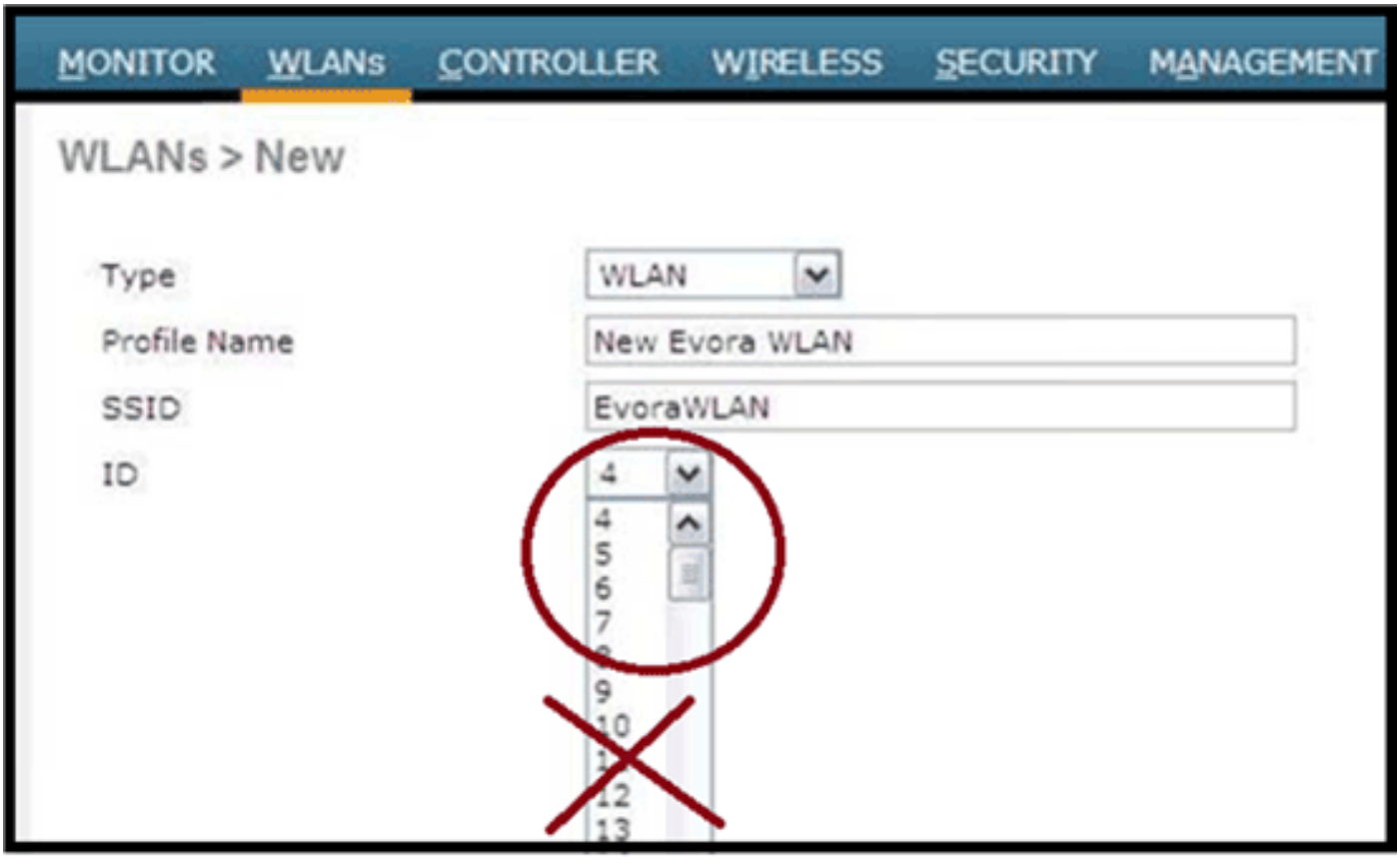
此影像顯示範例OEAP群組名稱：



此影像顯示WLAN SSID和RLAN組態：

如果Cisco Aironet 600系列OEAP輸入到AP組中，則兩個WLAN和一個遠端LAN的相同限制適用於AP組的配置。此外，如果Cisco Aironet 600系列OEAP位於預設組中（這意味著它不在定義的AP組中），則需要將WLAN/遠端LAN ID設定為小於ID 8，因為此產品不支援更高的ID集。

保留ID設定為小於8，如下圖所示：



注意：如果建立其他WLAN或遠端LAN是為了更改Cisco Aironet 600系列OEAP所使用的WLAN或遠端LAN，請在啟用600系列上的新WLAN或遠端LAN之前停用要刪除的當前WLAN或遠端LAN。如果為一個AP組啟用了多個遠端LAN，請停用所有遠端LAN，然後僅啟用一個。

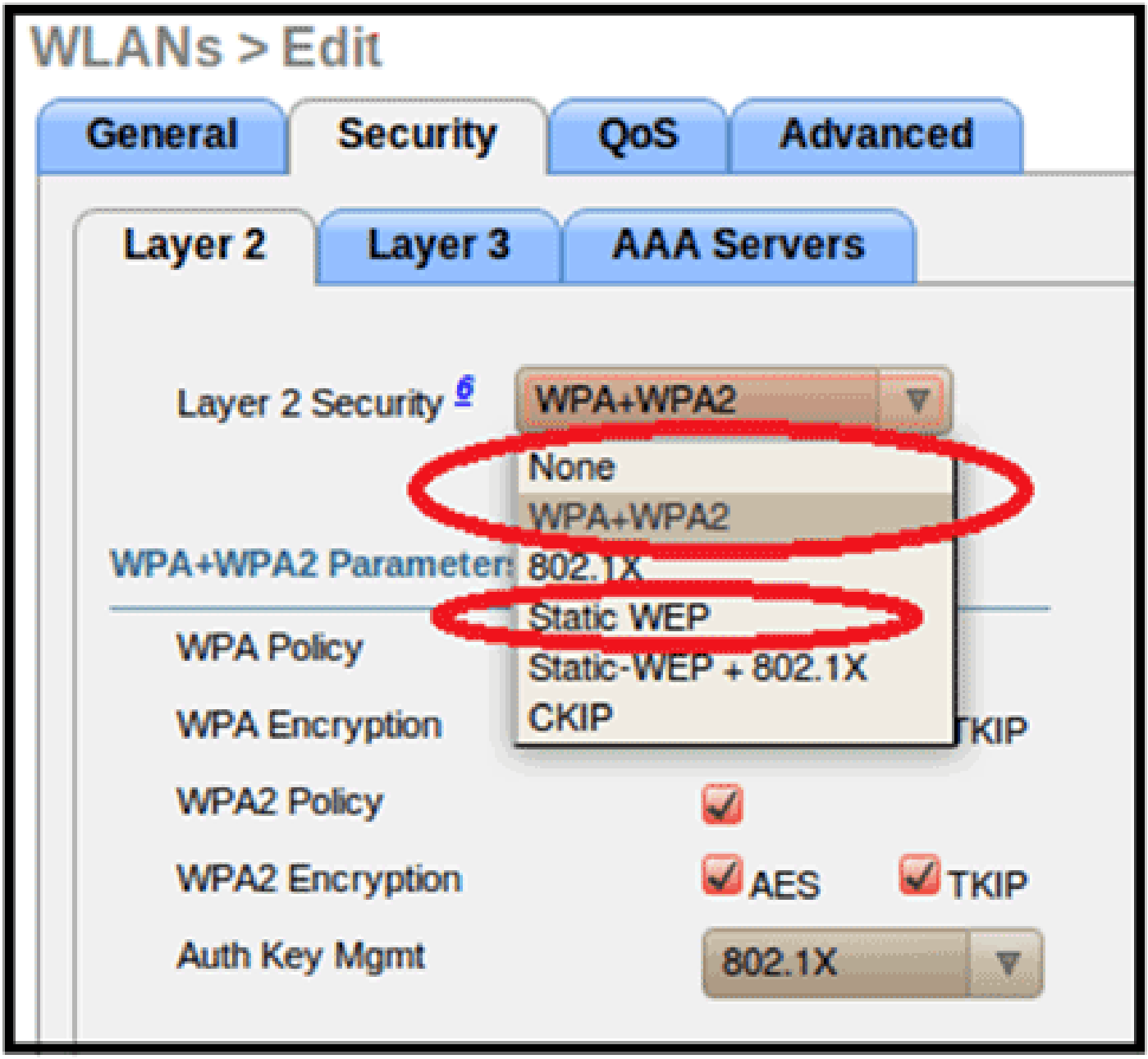
如果為一個AP組啟用了兩個以上的WLAN，請停用所有WLAN，然後僅啟用兩個WLAN。

WLAN安全性設定

在WLAN中設定安全性設定時，600系列不支援某些特定元素。

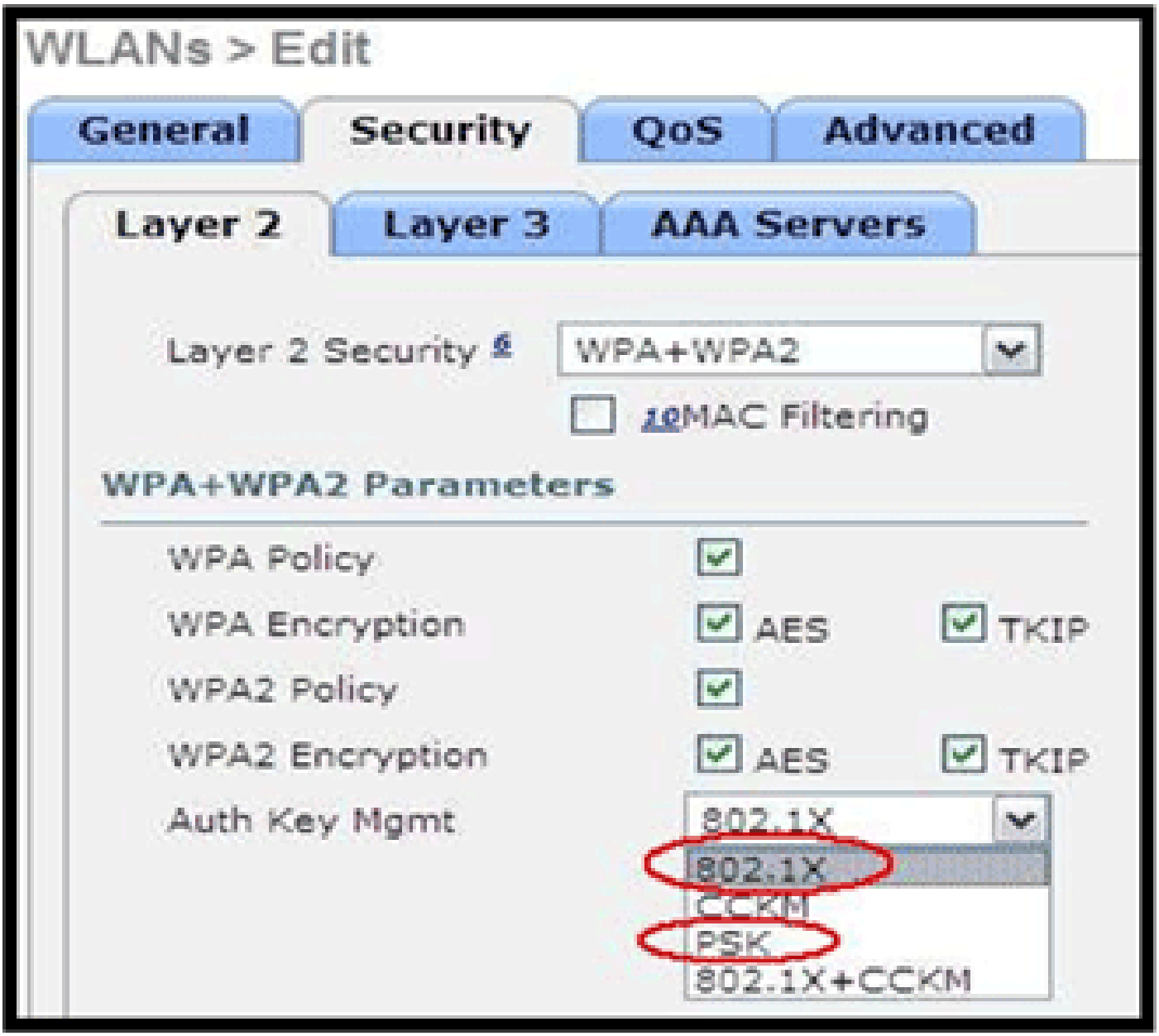
對於第2層安全，Cisco Aironet 600系列OEAP僅支援以下選項：

- 無
- WPA+WPA2
- 靜態WEP也可以使用，但不可用於。11n資料速率。

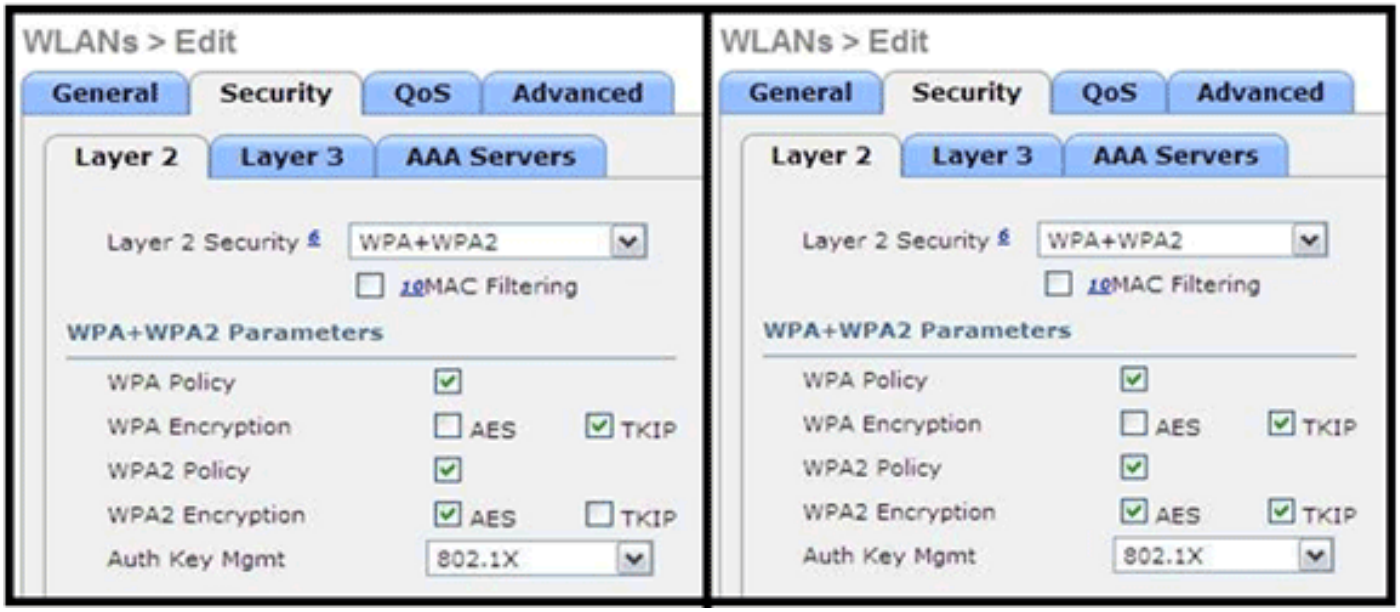


注意：只應選取802.1x或PSK。

TKIP和AES的WPA和WPA2的安全加密設定必須相同，如下圖所示：

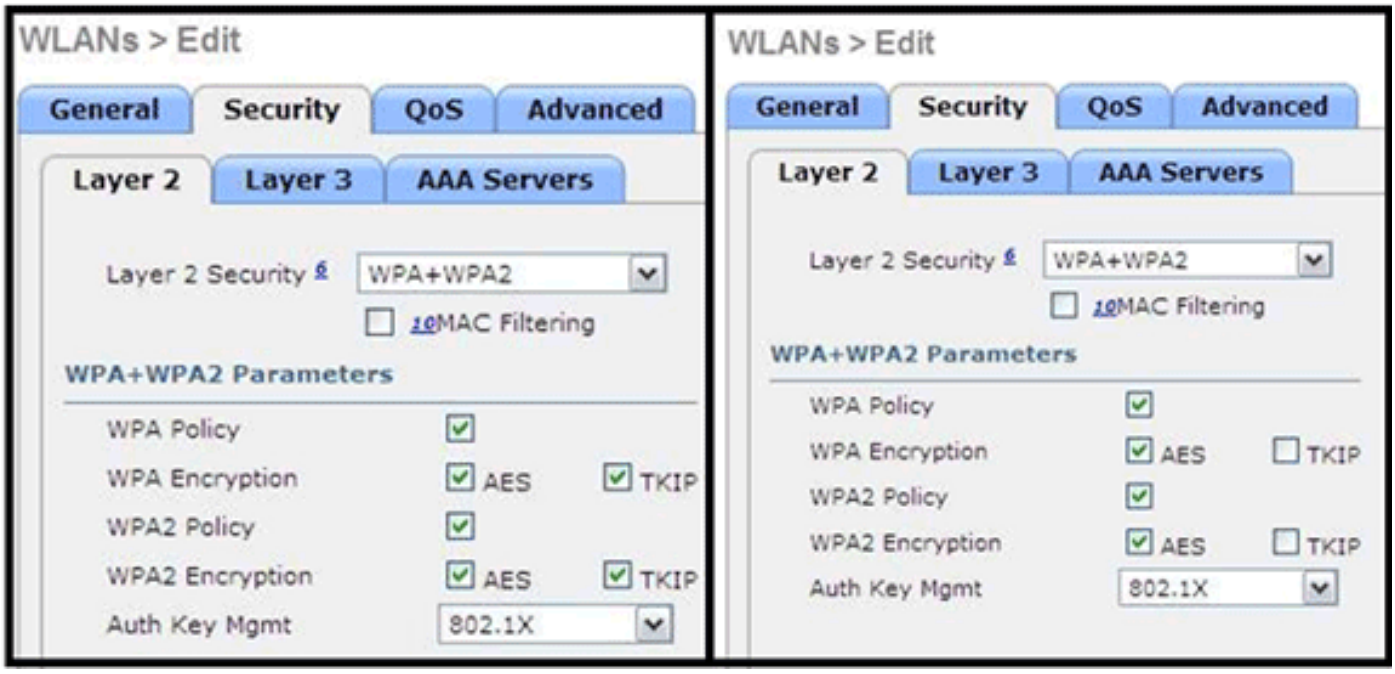


這些影像提供TKIP和AES不相容設定的範例：



注意：注意安全設定允許不支援的功能。

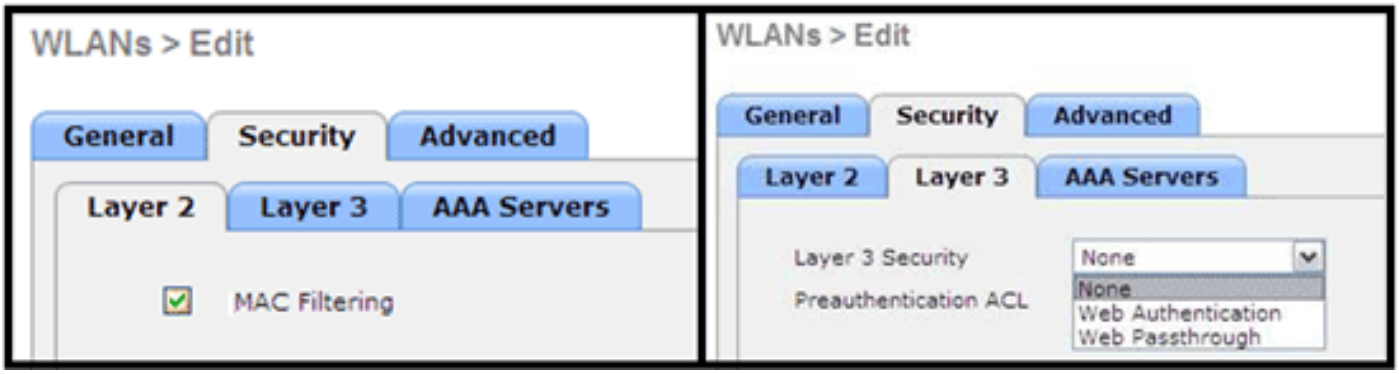
這些影像提供相容設定的範例：



MAC過濾

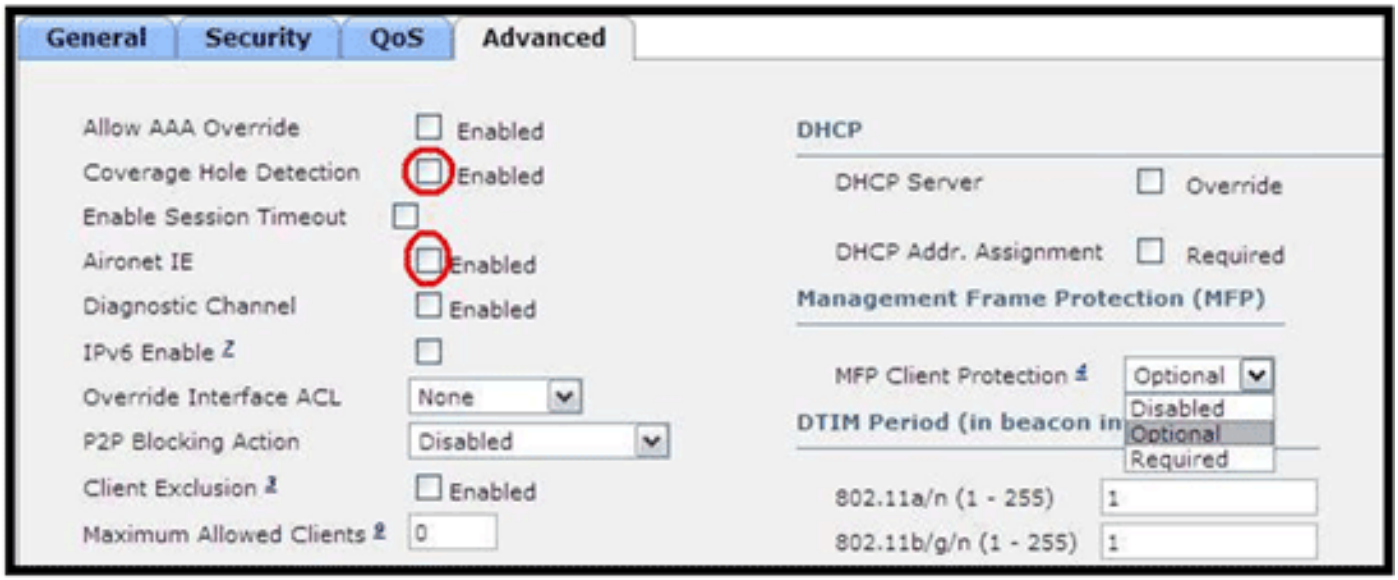
保全性設定可以保持開啟、設定為MAC過濾，或設定為Web驗證。預設使用MAC過濾。

此影像顯示第2層和第3層MAC過濾：



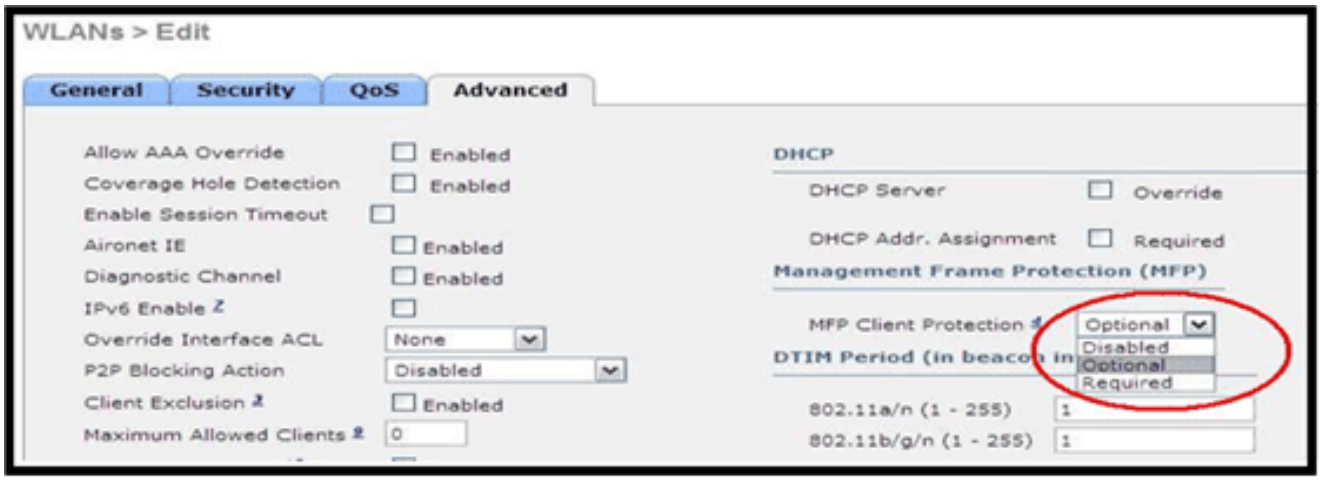
管理QoS設定：

還應管理高級設定：

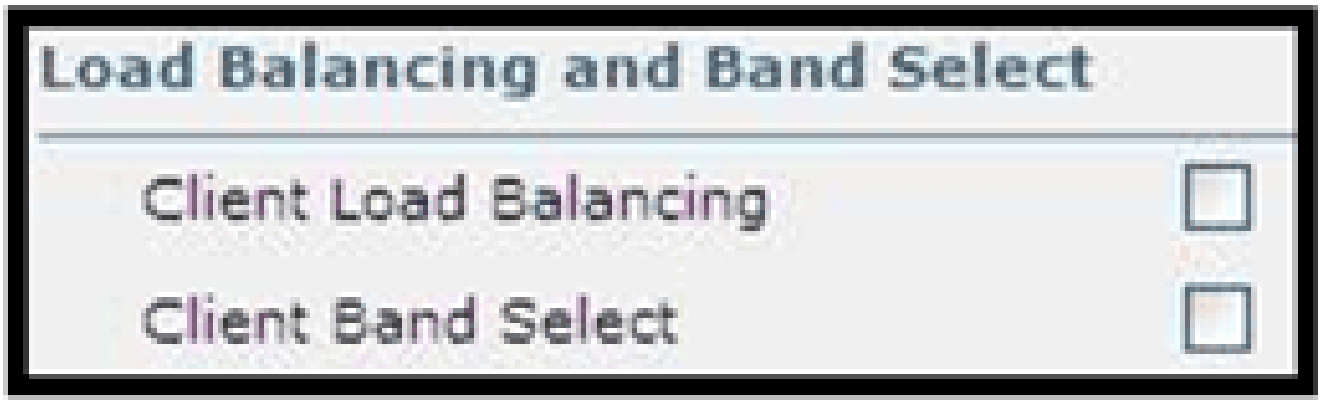


附註：

- 不應啟用覆蓋盲區檢測。
- 不應啟用Aironet IE（資訊元素），因為它們未被使用。
- 管理幀保護(MFP)也不受支援，應將其停用或配置為可選配置，如下圖所示：



- 不支援使用者端負載平衡和使用者端頻帶選取，且不應啟用：



支援的使用者計數

一次只允許十五個使用者連線到600系列上提供的WLAN控制器WLAN。在第一個客戶端之一取消身份驗證或控制器上出現超時之前，第十六個使用者無法進行身份驗證。

注意：此數字是600系列上控制器WLAN的累計數字。

例如，如果配置了兩個控制器WLAN，並且其中一個WLAN上有15個使用者，則任何使用者屆時都將無法加入600系列上的其他WLAN。此限制不適用於終端使用者在專為個人使用設計的600系列上配置的本地專用WLAN，並且連線到這些專用WLAN或有線埠上的客戶端不會影響這些限制。

通道管理和設定

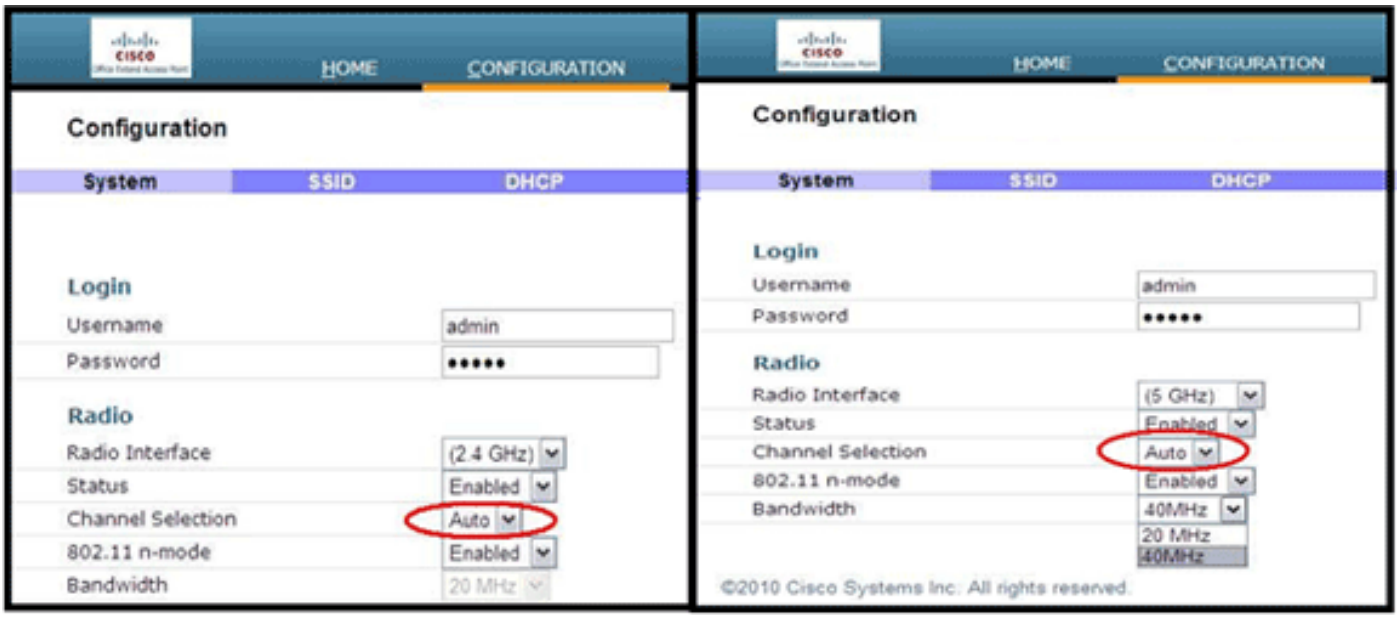
600系列的無線電透過600系列的本地GUI控制，而不是透過無線區域網控制器控制。

嘗試透過控制器控制頻譜通道、電源或停用無線電將無法對600系列產生任何影響。

600系列將在啟動期間掃描並選擇2.4 GHz和5.0 GHz的通道，前提是本地GUI上的預設設定在這兩個頻譜中均保留預設設定。

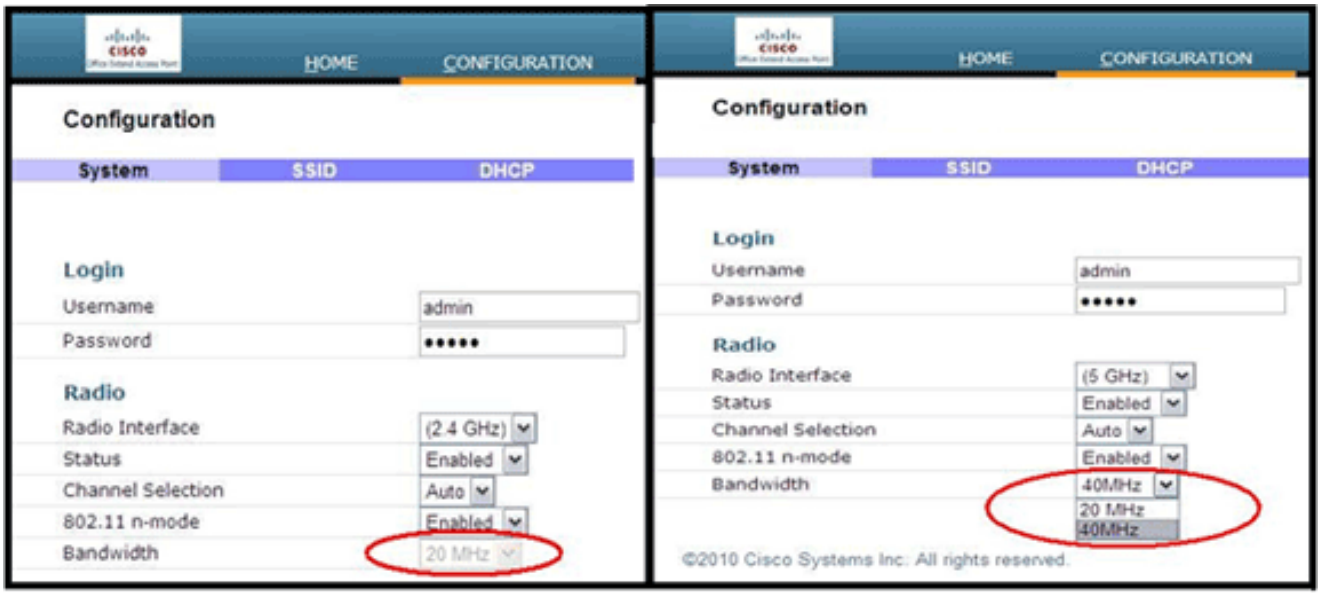
注意：如果使用者在本機停用一個或兩個無線電（該無線電也停用企業訪問）（如前所述），RRM和高級功能（如監視器、H-REAP、嗅探器）將超出定位為家庭和遠端工作者使用的Cisco Aironet 600系列OEAP的功能。

此處在Cisco Aironet 600系列OEAP的本地GUI上配置了5.0 GHz的通道選擇和頻寬。



附註：

- 20和40 MHz寬設定可用於5 GHz。
- 2.4 GHz 40 MHz寬不受支援，固定為20 MHz。
- 2.4 GHz不支援40 MHz寬（通道結合）。



其他警告

Cisco Aironet 600系列OEAP專為單AP部署而設計。因此，不支援在600系列之間漫遊客戶端。

注意：在控制器上停用802.11a/n或802.11b/g/n可能不會在Cisco Aironet 600系列OEAP上停用這些規範，因為本地SSID可能仍在正常工作。

終端使用者可以啟用/停用對Cisco Aironet 600系列OEAP內部的無線電裝置的控制。

有線連線埠上的802.1x支援

在此初始版本中，只有802.1x在命令列介面(CLI)上受支援。

注意：尚未增加GUI支援。

這是Cisco Aironet 600系列OEAP背面的有線埠(黃色埠#4)，與遠端LAN繫結（請參閱前面關於配置遠端LAN的部分）。

您可以隨時使用show命令顯示當前的遠端LAN配置：

```
<#root>

show remote-lan <remote-lan-id>
```

要更改遠端LAN配置，必須先停用它：

```
<#root>

 remote-lan disable <remote-lan-id>
```

啟用遠端LAN的802.1X驗證：

```
<#root>

 config remote-lan security 802.1X enable <remote-lan-id>
```

您可以使用此指令來復原它：

```
<#root>

 config remote-lan security 802.1X disable <remote-lan-id>
```

對於遠端LAN，「加密」始終為「無」(如show remote-lan中所示)且不可配置。

如果您要使用本機EAP（在控制器中）作為驗證伺服器：

<#root>

config remote-lan local-auth enable <*profile-name*> <*remote-lan-id*>

其中配置檔案是透過控制器GUI(Security > Local EAP)或CLI(config local-auth)定義的。有關此指令的詳細資訊，請參閱控制器指南。

您可以使用此指令來復原它：

<#root>

config remote-lan local-auth disable <*remote-lan-id*>

或者，如果您使用外部AAA身份驗證伺服器：

- config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>
- config remote-lan radius_server auth enable/disable <remote-lan-id>

其中server是透過控制器GUI (Security > RADIUS > Authentication)或CLI(config radius auth)進行設定。請參閱控制器指南以取得有關此指令的詳細資訊。

完成設定後，啟用遠端LAN：

<#root>

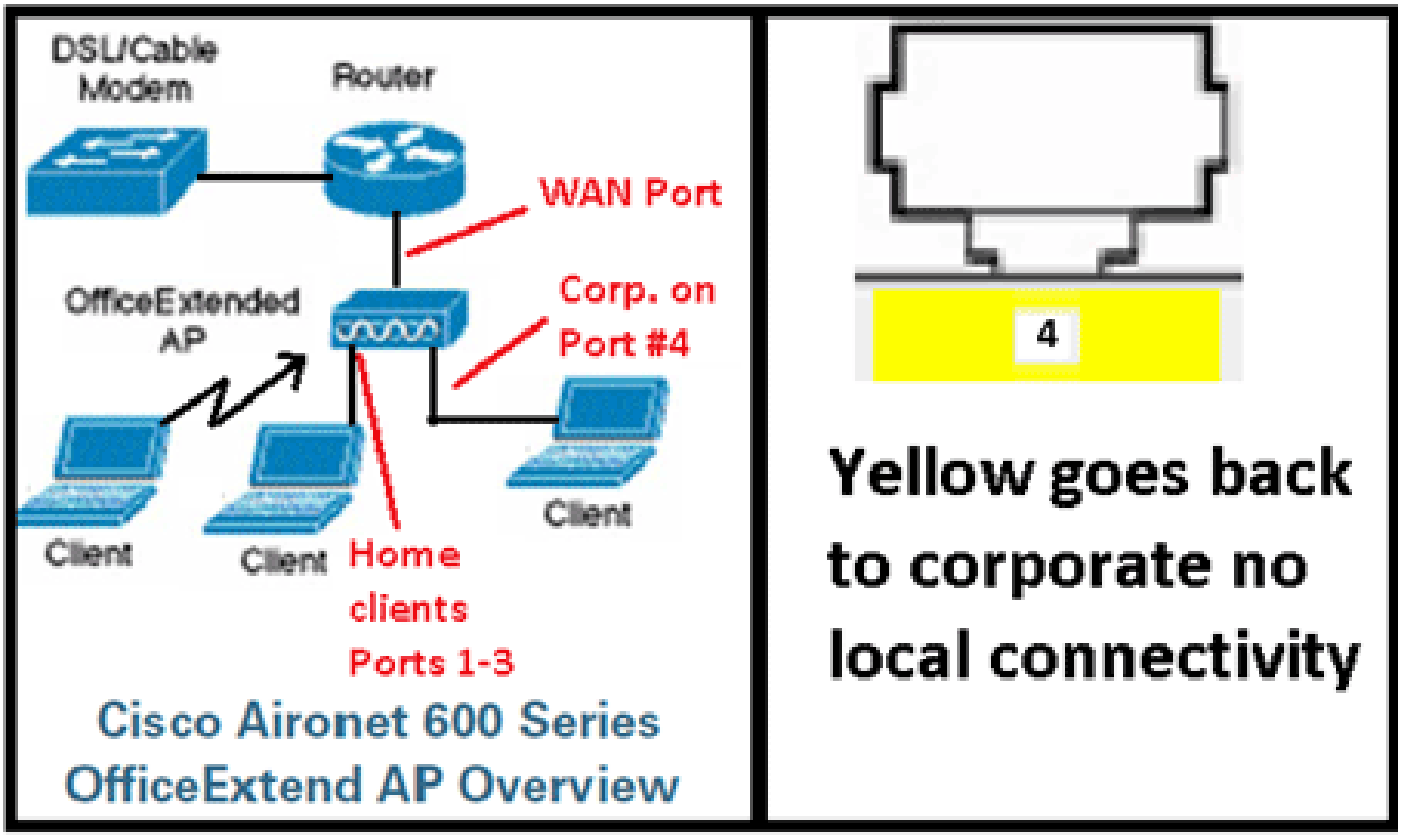
config remote-lan enable <*remote-lan-id*>

請使用show remote-lan <remote-lan-id>命令以驗證您的設定。

對於遠端LAN客戶端，您需要啟用802.1X身份驗證並相應地配置。請參閱您的裝置使用手冊。

OEAP-600存取點配置

此圖顯示Cisco Aironet 600系列OEAP的佈線圖：

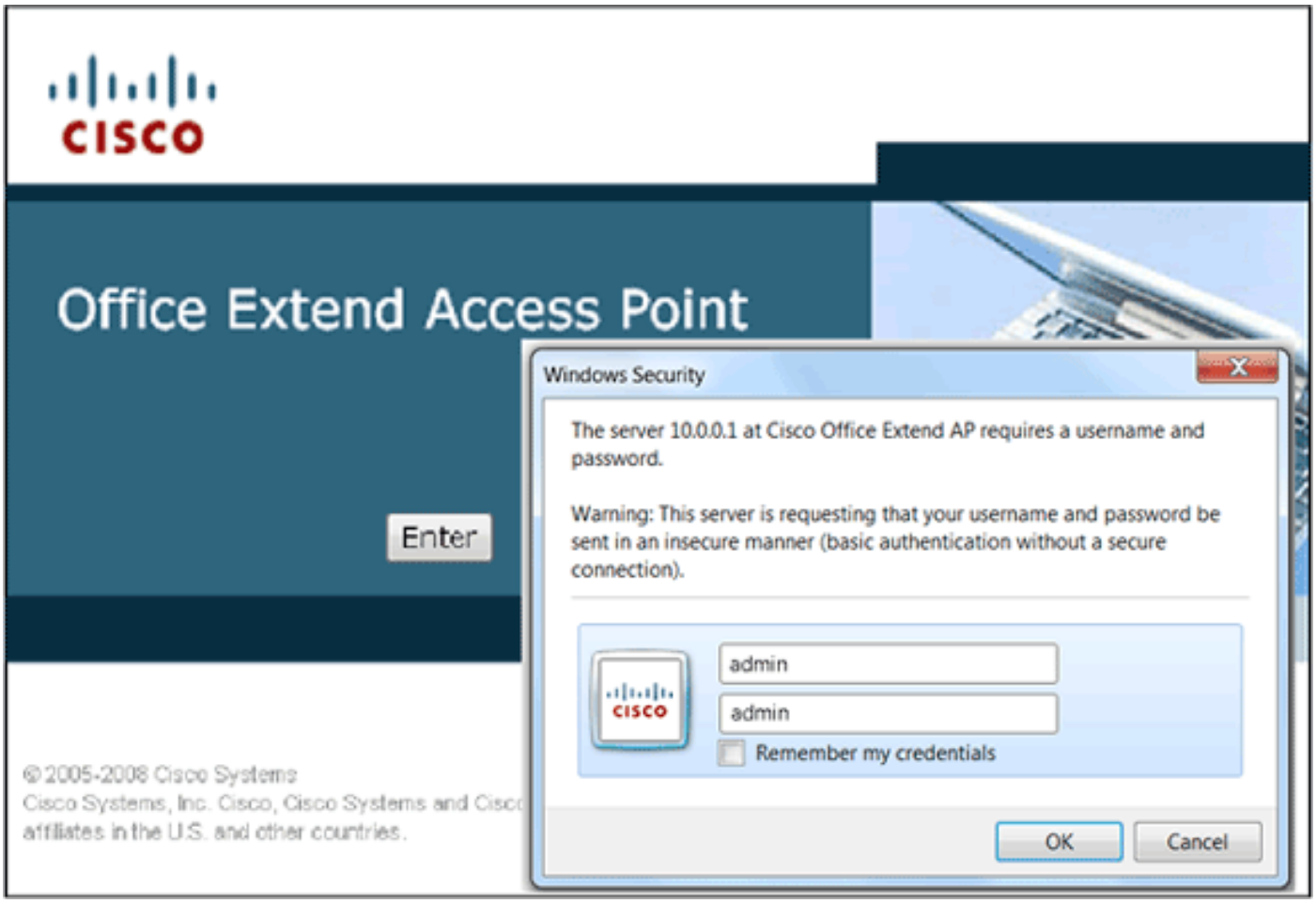


Cisco Aironet 600系列OEAP的預設DHCP作用域是10.0.0.x，因此您可以使用地址10.0.0.1瀏覽到埠1-3上的AP。預設使用者名稱和密碼為admin。

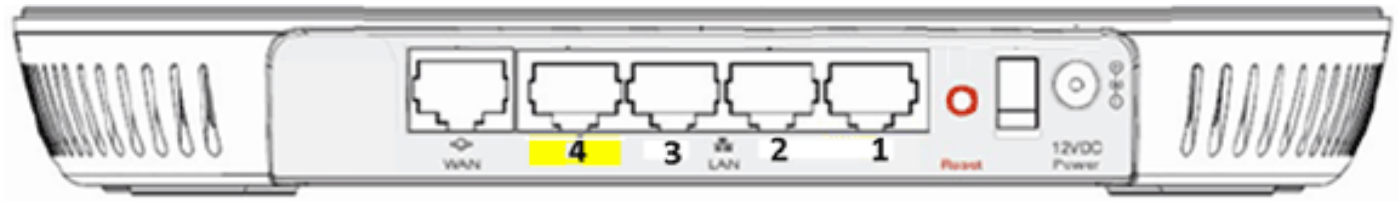
註：這不同於使用Cisco作為使用者名稱和口令的AP1040、1130、1140和3502i。

如果無線電已啟動，並且已配置個人SSID，則您可以無線訪問配置螢幕。否則，需要使用本地乙太網埠1-3。

要登入，預設使用者名稱和密碼為admin。



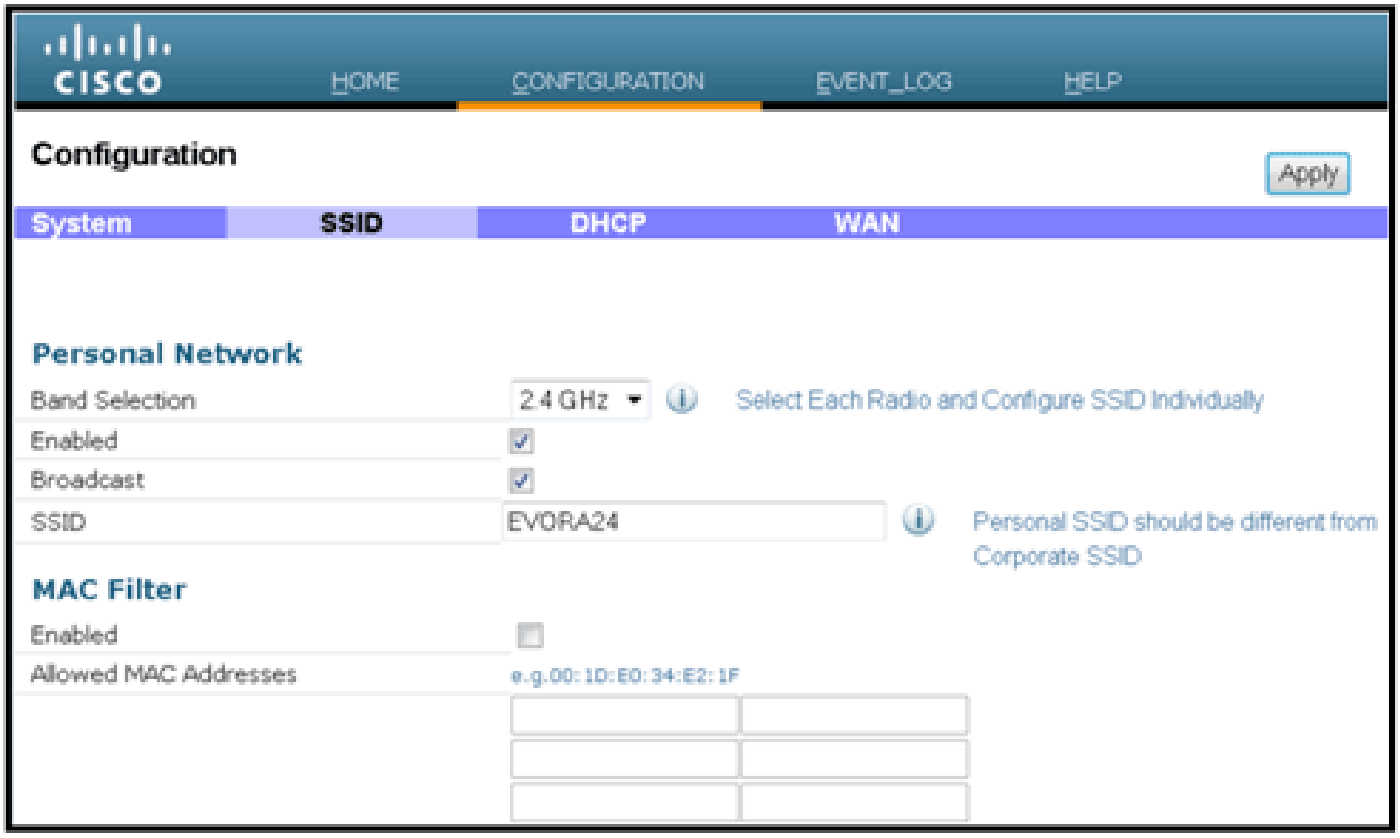
注意：黃色埠#4對於本地使用不是活動的。如果控制器上配置了遠端LAN，則此埠會在AP成功加入控制器之後返回隧道。為了瀏覽至裝置，本機使用連線埠1-3：



成功瀏覽到裝置後，您將看到主狀態螢幕。此螢幕提供無線電和MAC統計資訊。如果尚未配置無線電，配置螢幕將允許使用者啟用無線電、設定通道和模式、配置本地SSID以及啟用WLAN設定。

從SSID螢幕中，使用者可以配置個人WLAN網路。設定公司無線電SSID和安全引數，並從控制器中向下推送這些引數（在您使用控制器的IP配置WAN之後），並且成功加入。

此影像顯示SSID本機MAC過濾組態：



使用者配置個人SSID後，下方的螢幕允許使用者在專用家庭SSID上設定安全性、啟用無線電並配置MAC過濾（如果需要）。如果個人網路使用802.11n速率，建議使用者選擇驗證型別、加密型別

以及啟用WPA2-PSK和AES的密碼。

註：如果使用者選擇停用其中一個或兩個無線電（這兩個無線電，也同時停用供公司使用），則這些SSID設定與企業設定不同。

在本地訪問管理控制設定的使用者可以控制核心功能，如無線電啟用/停用，除非裝置受密碼保護並由管理員配置。因此，請務必小心不要停用兩個無線電，因為即使裝置成功加入控制器，這可能會造成連線中斷。

此影像顯示系統安全性設定：

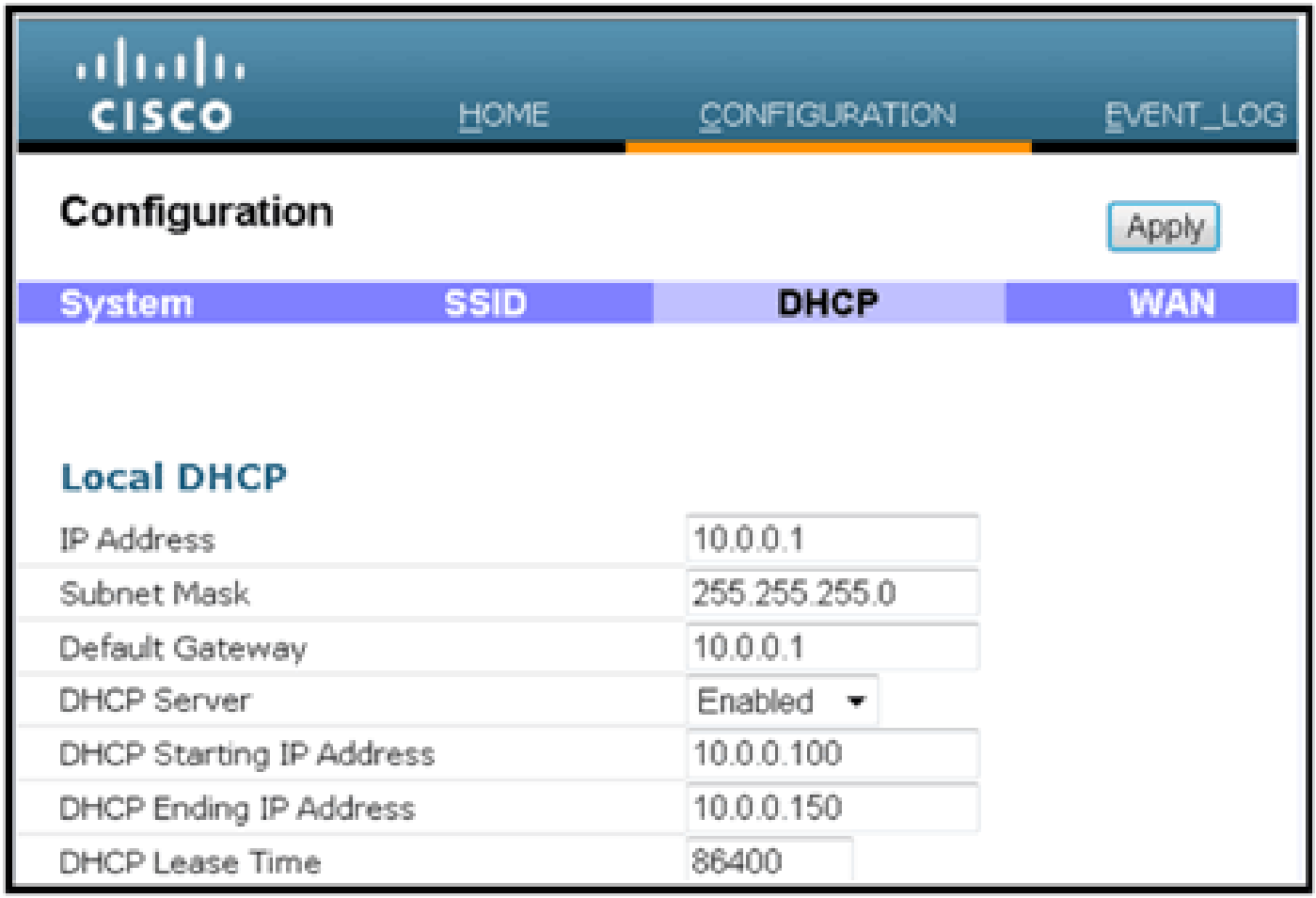
預計家庭遠端工作人員將在家庭路由器後方安裝Cisco Aironet 600系列OEAP，因為此產品並非旨在替代家庭路由器的功能。這是因為此產品的當前版本不支援防火牆、PPPoE支援或埠轉發。這些功能是客戶期望在家庭路由器中找到的功能。

雖然此產品無需家用路由器即可使用，但出於上述原因，建議不要將其定位為此類產品。此外，直接連線到某些資料機可能會發生相容性問題。

由於大多數家庭路由器的DHCP作用域在192.168.x.x範圍內，因此該裝置具有預設DHCP作用域10.0.0.x，並且可以配置。

如果家庭路由器恰好使用10.0.0.x，則必須將Cisco Aironet 600系列OEAP配置為使用192.168.1.x或相容的IP地址以避免網路衝突。

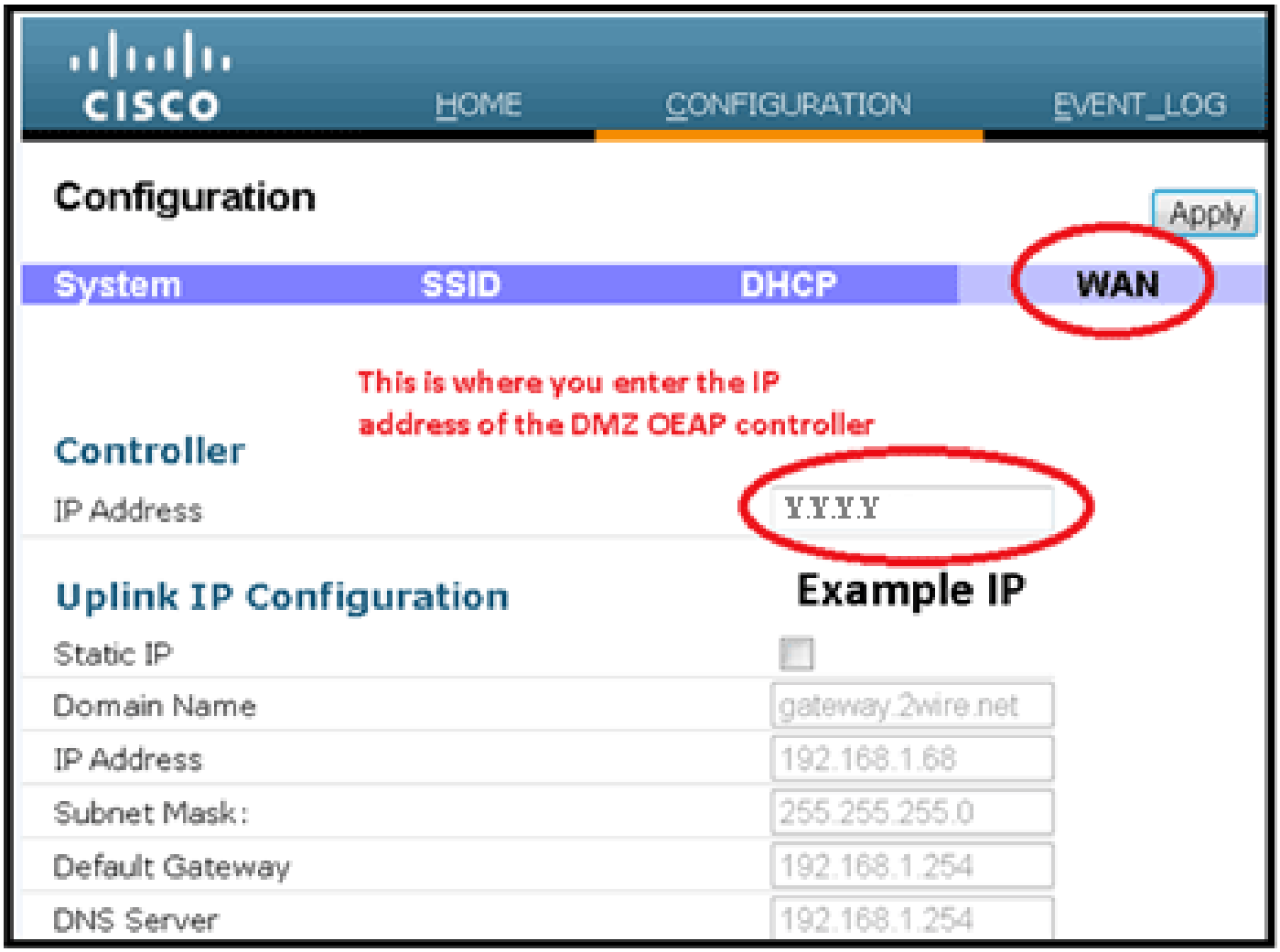
下圖顯示了DHCP作用域配置：



注意：如果Cisco Aironet 600系列OEAP未由IT管理員安裝或配置，則使用者需要輸入公司控制器的IP地址（如下所示），以便AP可以成功加入控制器。成功加入後，AP應該從控制器下載最新的映像和配置引數，如公司WLAN設定。此外，如果進行了配置，遠端LAN設定有線埠#4在Cisco Aironet 600系列OEAP的背面。

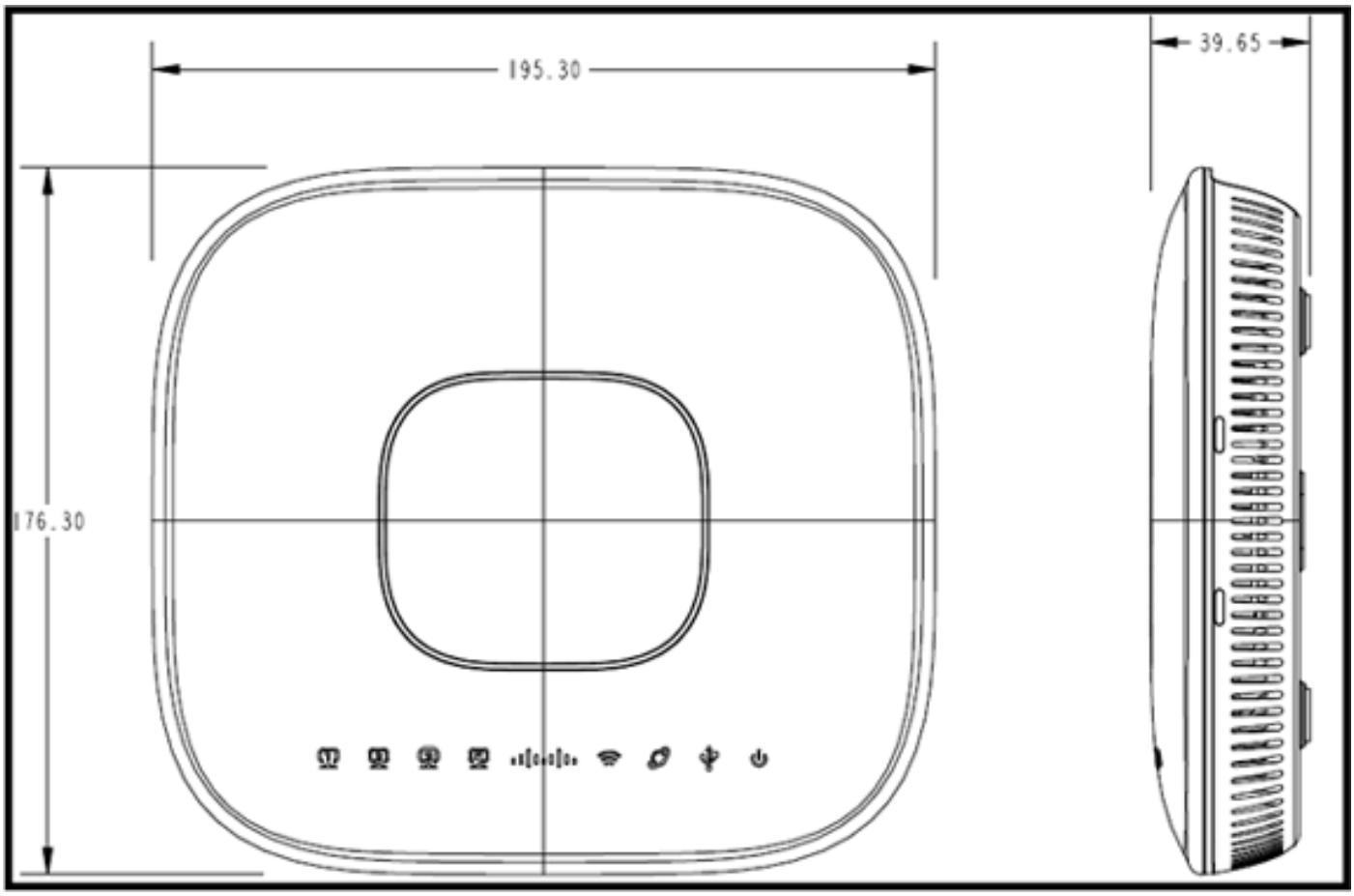
如果控制器未加入，請驗證控制器的IP位址是否可透過網際網路連線。如果已啟用MAC過濾，請確認MAC位址已順利輸入控制器中。

此圖顯示Cisco Aironet 600系列OEAP控制器的IP地址：



OEAP-600存取點硬體安裝

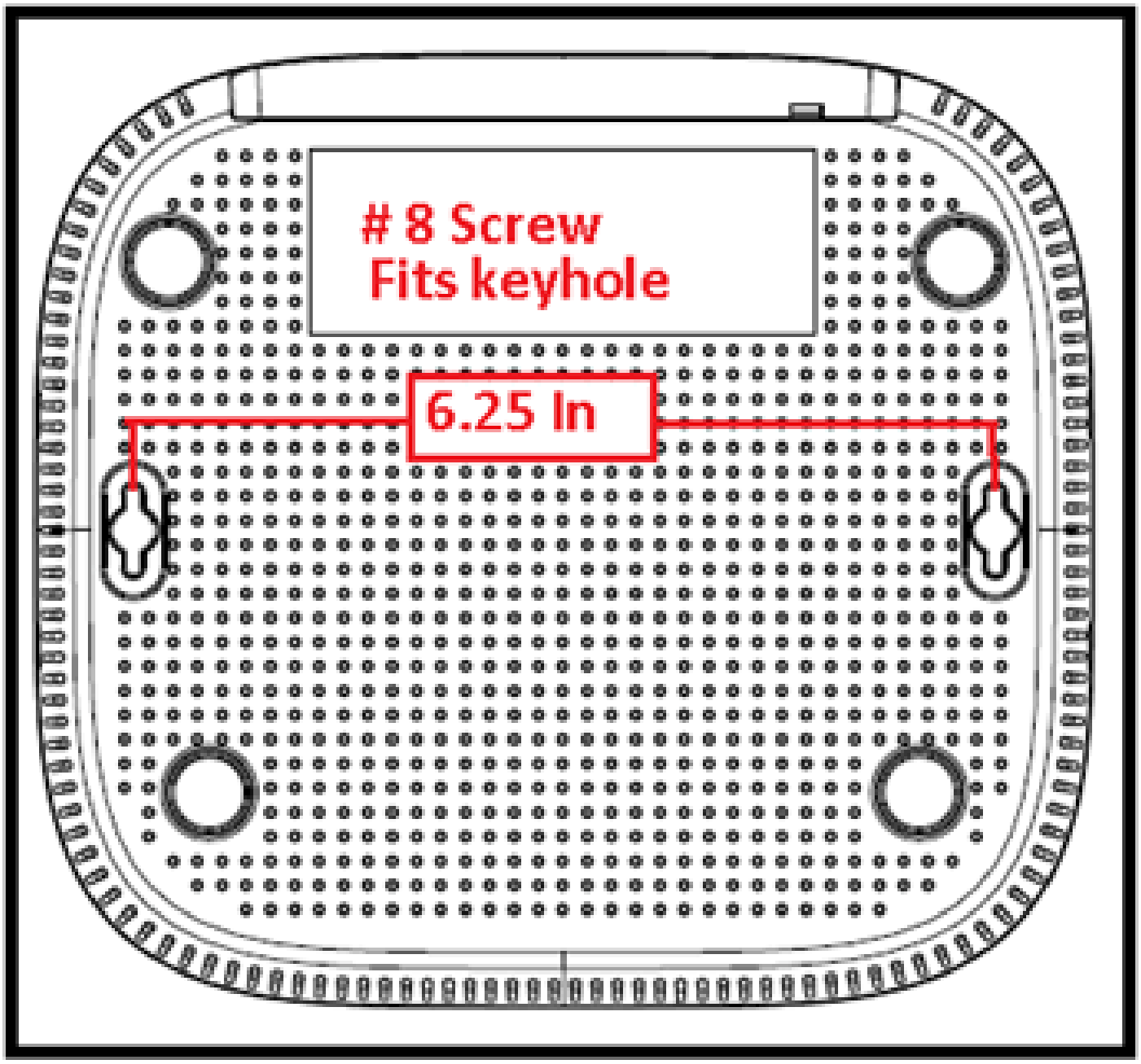
此圖顯示Cisco Aironet 600系列OEAP的物理方面：



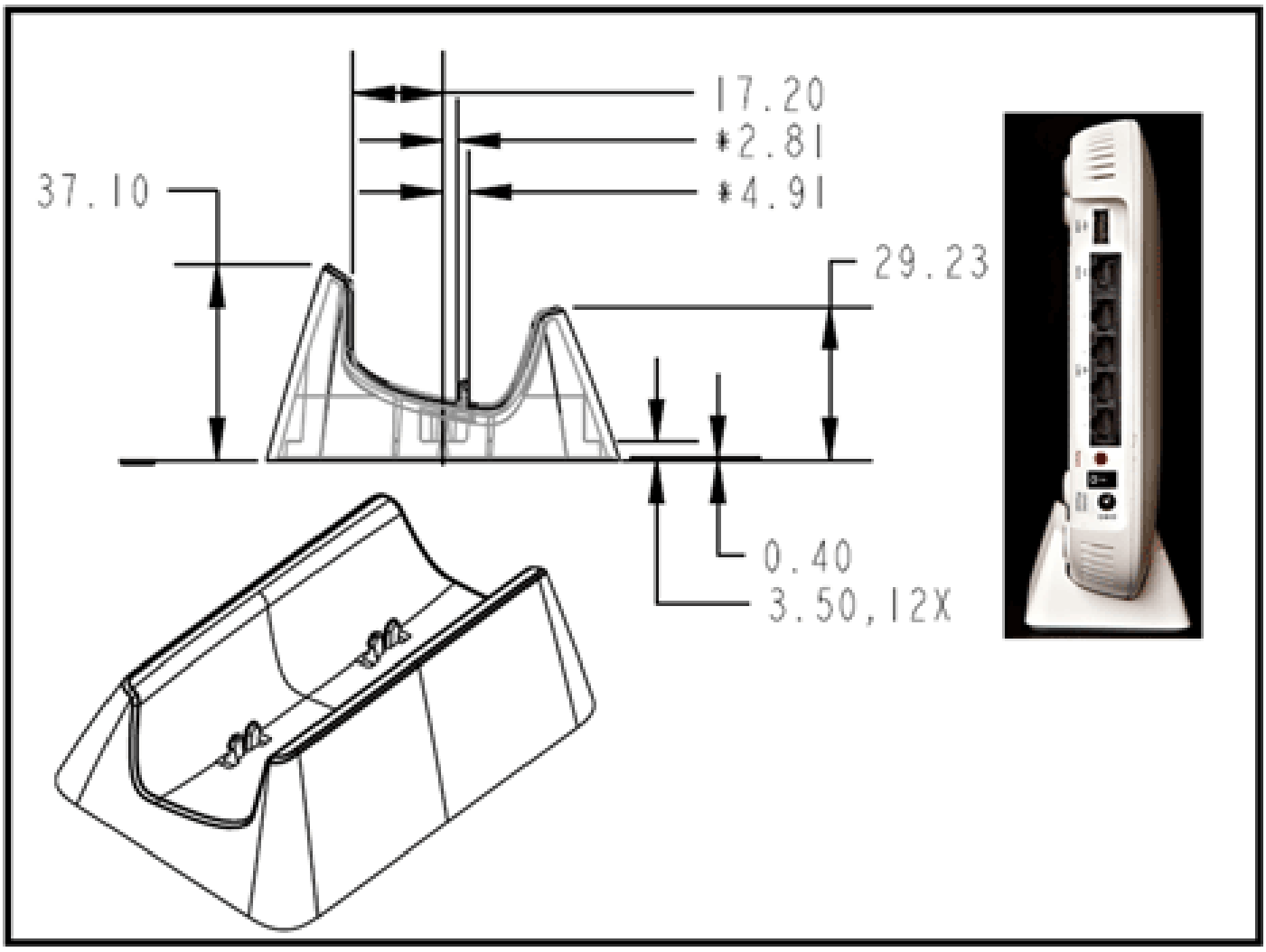
此AP設計為安裝在桌子上，並具有橡膠支腳。它也可以安裝在牆上，或者使用隨附的托架直立地坐。嘗試將AP定位在儘可能靠近目標使用者的位置。避免使用金屬表面較大的區域，例如將裝置放在金屬案頭或大型鏡子附近。AP和使用者之間的牆和物體越多，訊號強度就越低，效能也會降低。

註：此AP使用+12伏電源，不使用乙太網供電(PoE)。此外，裝置不提供PoE。確保正確的電源介面卡用於AP。此外，請確保不要使用其他裝置（如筆記型電腦和IP電話）中的其他介面卡，因為這些介面卡可能會損壞AP。

該單元可以用塑膠錨或木螺釘安裝在牆上。



該單元可使用所提供的托架直立安裝。

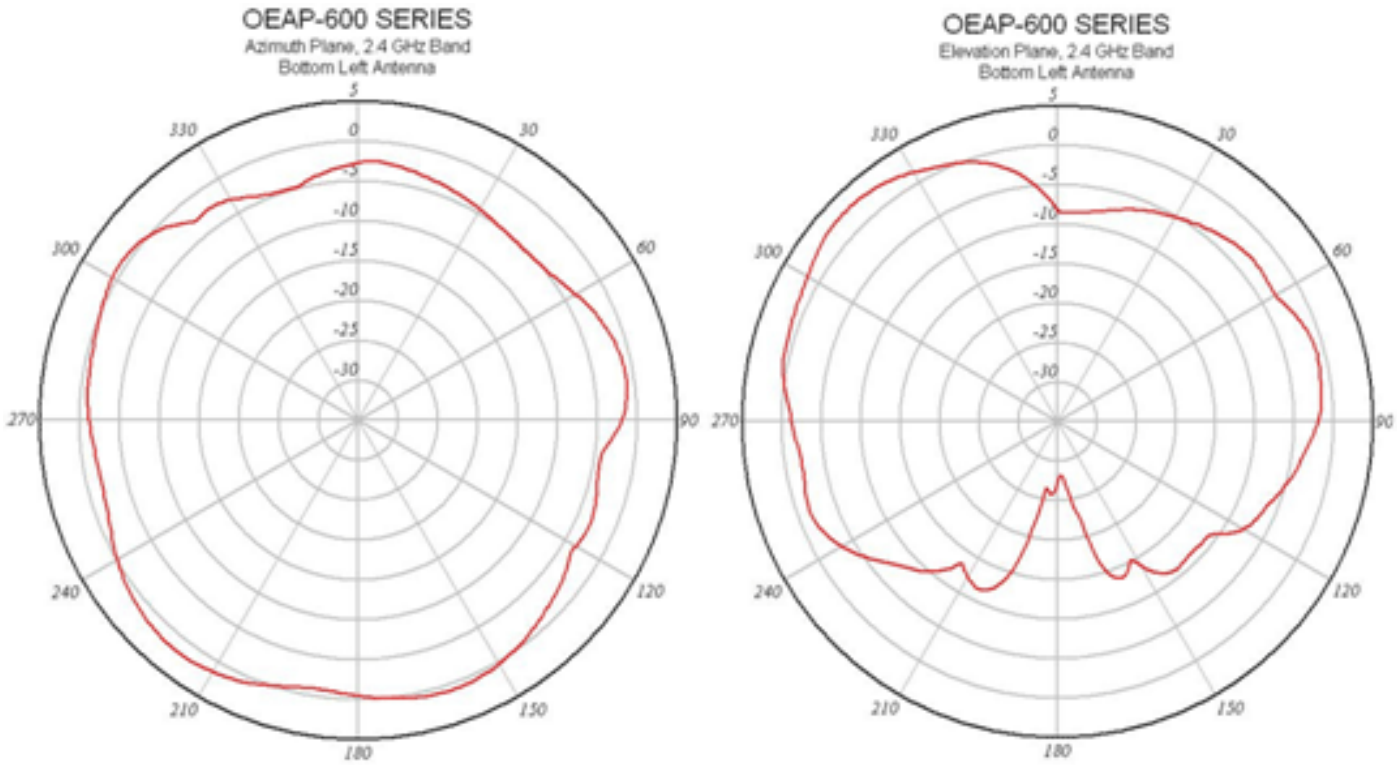


Cisco Aironet 600系列OEAP的天線位於AP的邊緣。使用者應小心不要將AP放置在金屬物體或障礙物附近，這些物體或障礙物可能導致訊號方向性變差或減弱。天線增益在兩個頻帶中均約為2 dBi，並且設計為以360度模式輻射。類似於燈泡（沒有燈罩），目標是向各個方向輻射。將AP視為燈泡，並嘗試將其放在使用者附近。

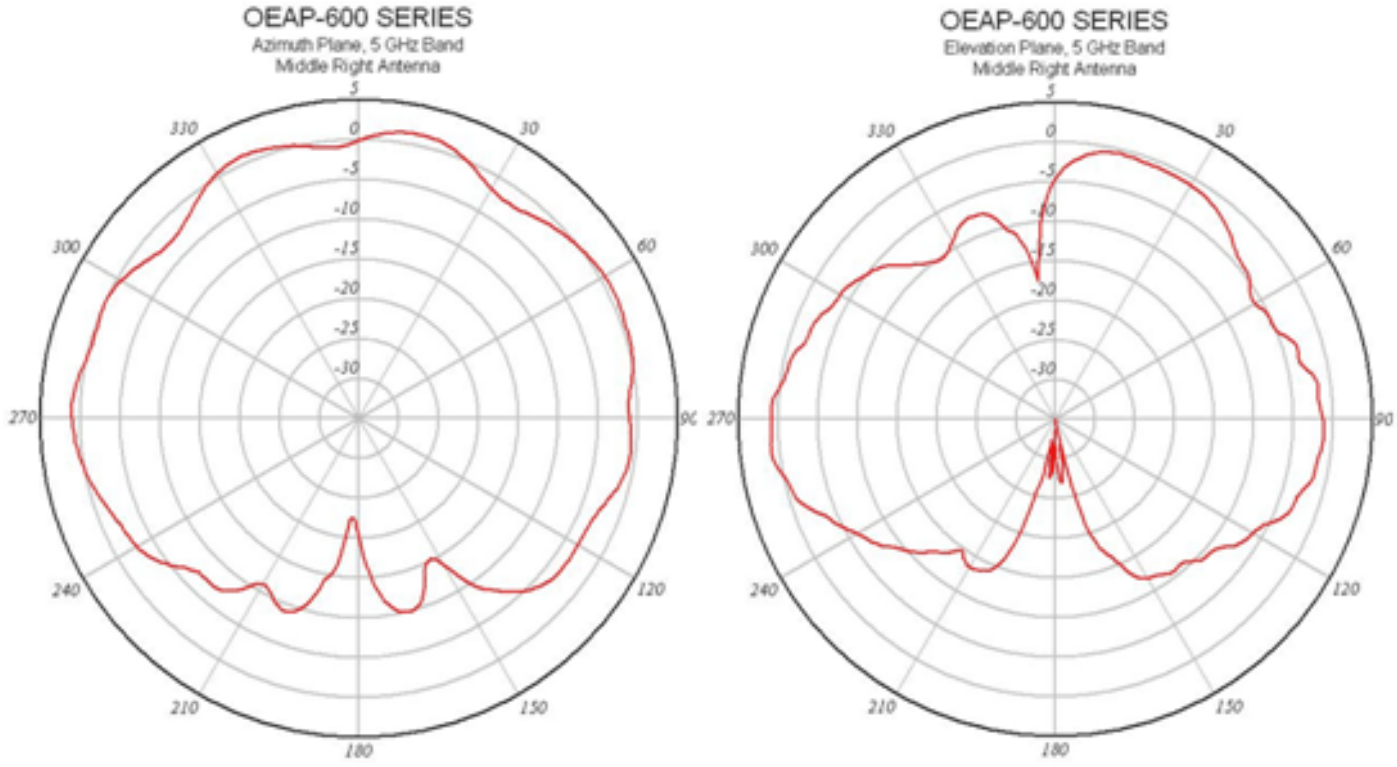
金屬物體（如鏡子）會像燈罩類比一樣阻擋訊號。如果訊號必須穿透或穿過實體物件，您可能會遇到輸送量或範圍降低的問題。如果您希望連線（例如在三層住宅中），請避免將AP放置在地下室，並嘗試將AP安裝在住宅內的中心位置。

存取點有六個天線（每個頻帶3個）。

此影像顯示2.4 GHz天線輻射圖（取自左下方天線）。



此影像顯示5 GHz天線輻射圖（取自中間偏右的天線）：



OEAP-600故障排除

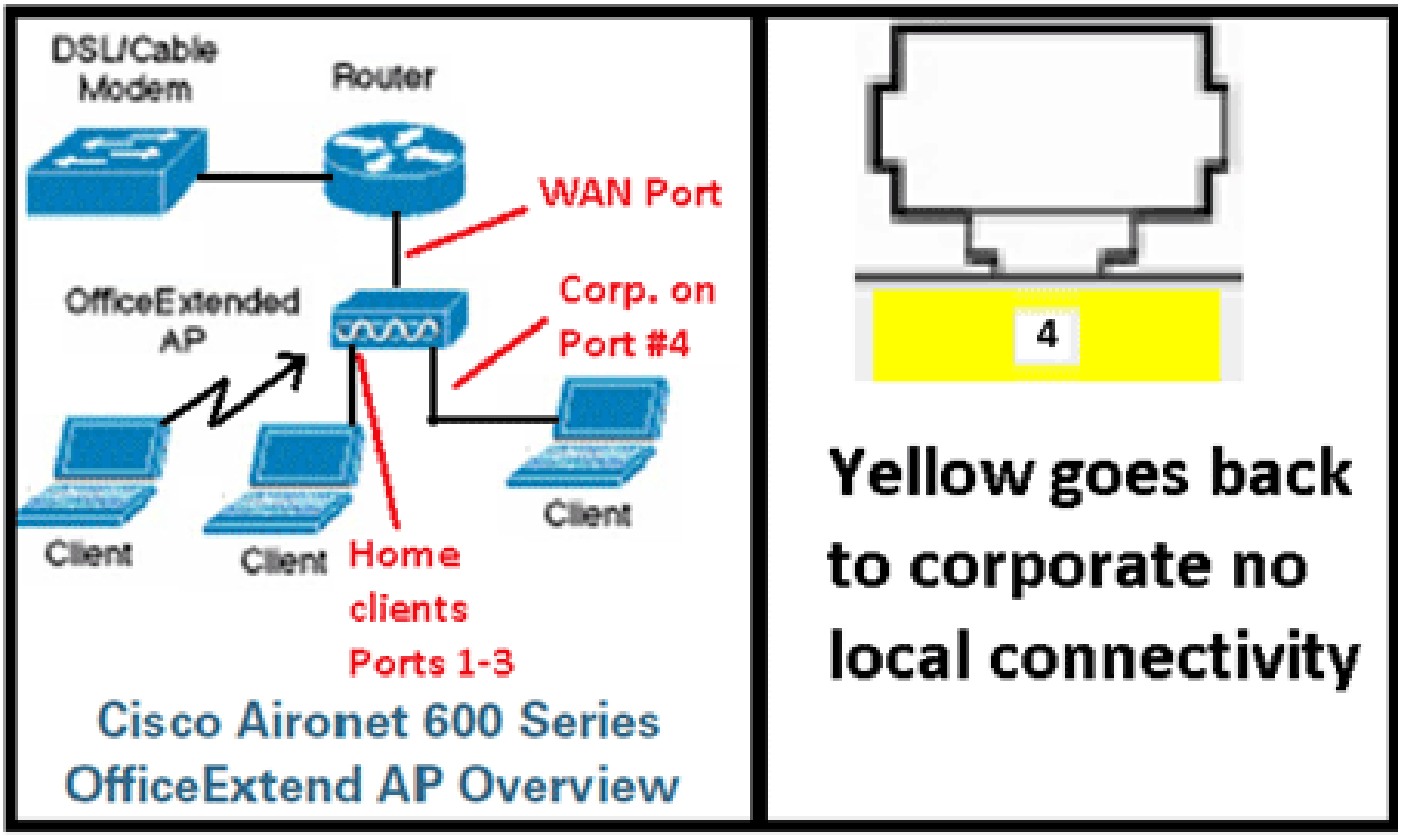
檢驗初始佈線是否正確。這可以確認Cisco Aironet 600系列OEAP上的WAN埠已連線到路由器，並且可以成功接收IP地址。如果AP似乎未加入控制器，請將PC連線到埠1-3（家庭客戶端埠），然後檢視是否可以使用預設IP地址10.0.0.1瀏覽到AP。預設使用者名稱和密碼為admin。

驗證是否已設定公司控制器的IP地址。否則，請輸入IP地址並重新啟動Cisco Aironet 600系列OEAP，以便嘗試建立到控制器的鏈路。

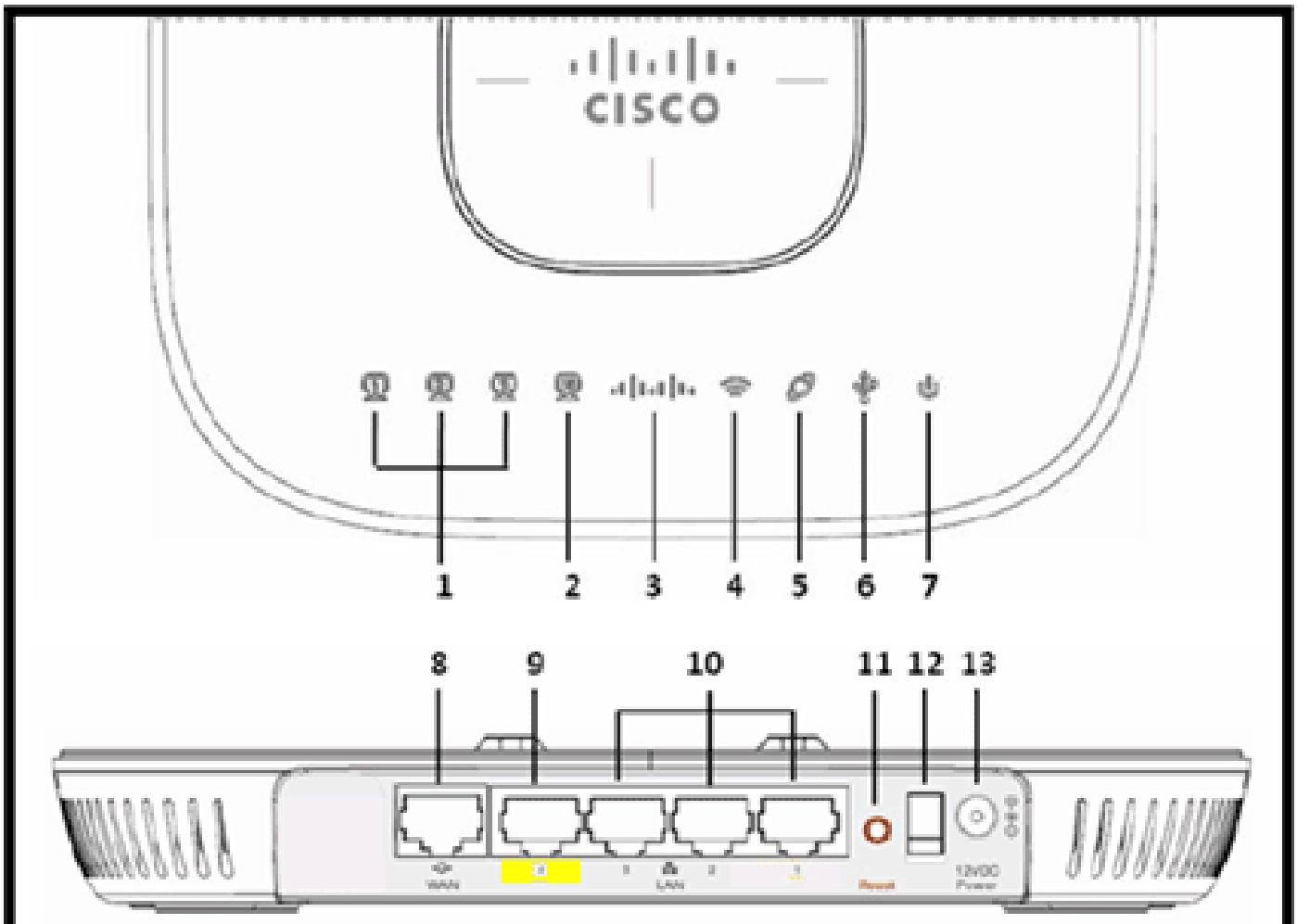
注意：公司埠#4（黃色）不能用於出於配置目的瀏覽到裝置。除非配置了遠端LAN，否則這實際上是「死埠」。然後，它將透過隧道返回公司（用於有線企業連線）

檢查事件日誌以檢視關聯如何進行（稍後將對此進行詳細說明）。

此圖顯示Cisco Aironet 600系列OEAP佈線圖：



此圖顯示Cisco Aironet 600系列OEAP連線埠：



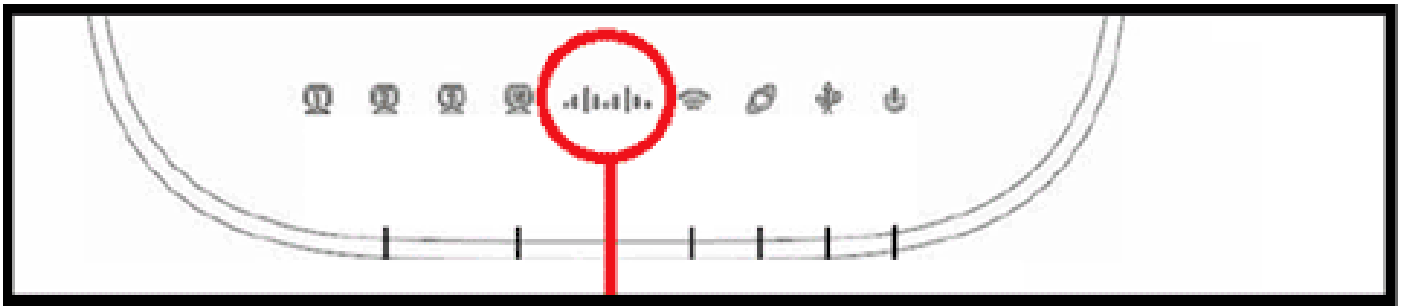
1	Local Ethernet LEDs 1 through 3	8	WAN Port
2	Remote LAN LED	9	Remote LAN Port
3	Status LED	10	Local Ethernet Ports 1 through 3
4	Wireless LED	11	Reset Button
5	WAN LED	12	Power Toggle Switch
6	USB LED (future)	13	Power Connector
7	Power Indicator LED		

如果Cisco Aironet 600系列OEAP無法加入控制器，建議您檢查以下專案：

1. 檢驗路由器是否工作正常並已連線到Cisco Aironet 600系列OEAP的WAN埠。
2. 將PC連線到Cisco Aironet 600系列OEAP的其中一個埠1-3。它應該能看到網際網路。
3. 驗證公司控制器的IP地址是否在AP中。
4. 確認控制器在DMZ上且可以透過網際網路存取。
5. 驗證加入並確認思科徽標LED是純藍色或紫色。
6. 在AP需要載入新映像並重新啟動時預留足夠時間。

7. 如果使用防火牆，請驗證UDP 5246和5247埠未被阻止。

此圖顯示Cisco Aironet 600系列OEAP徽標LED狀態：

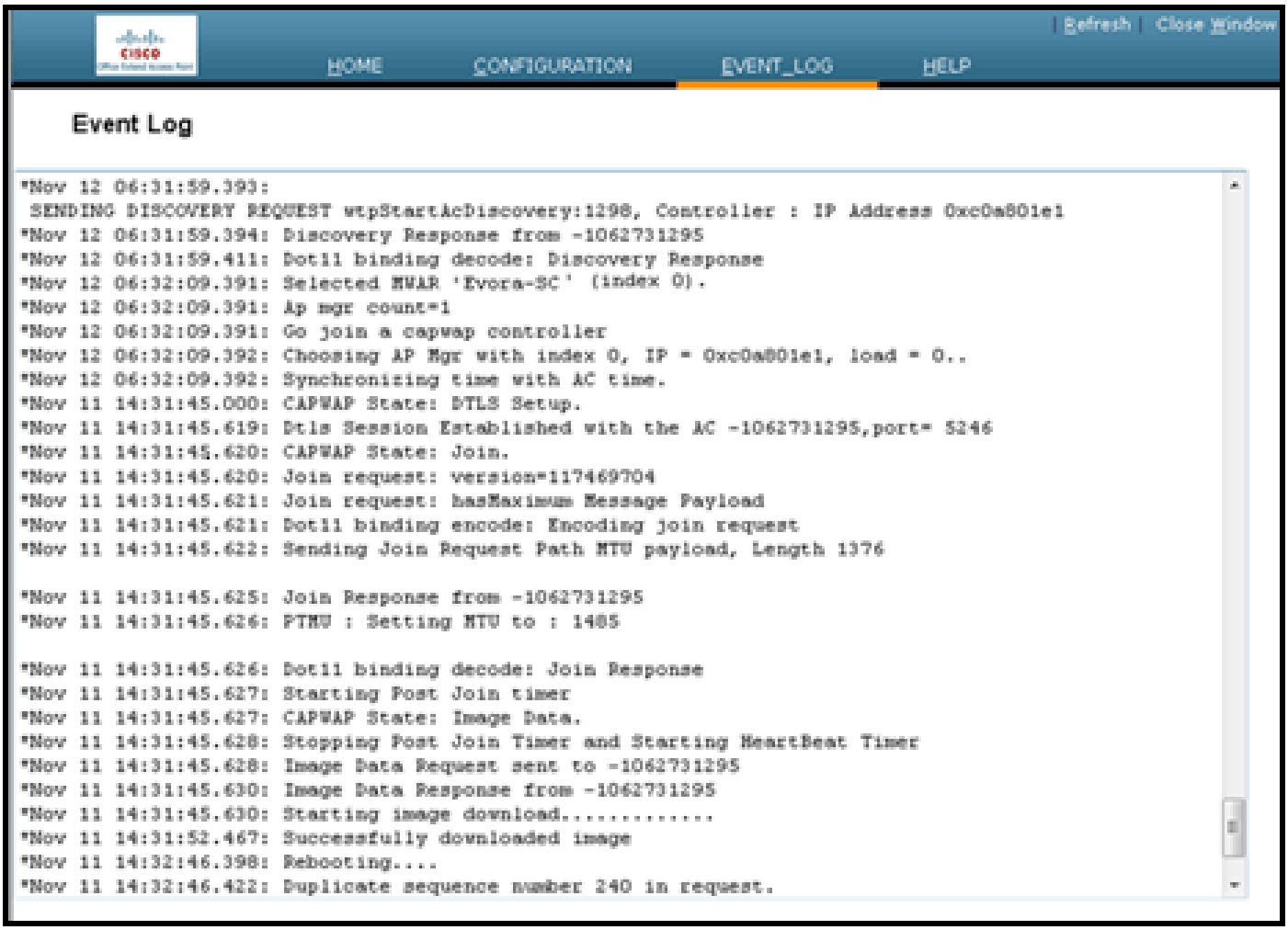


Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs

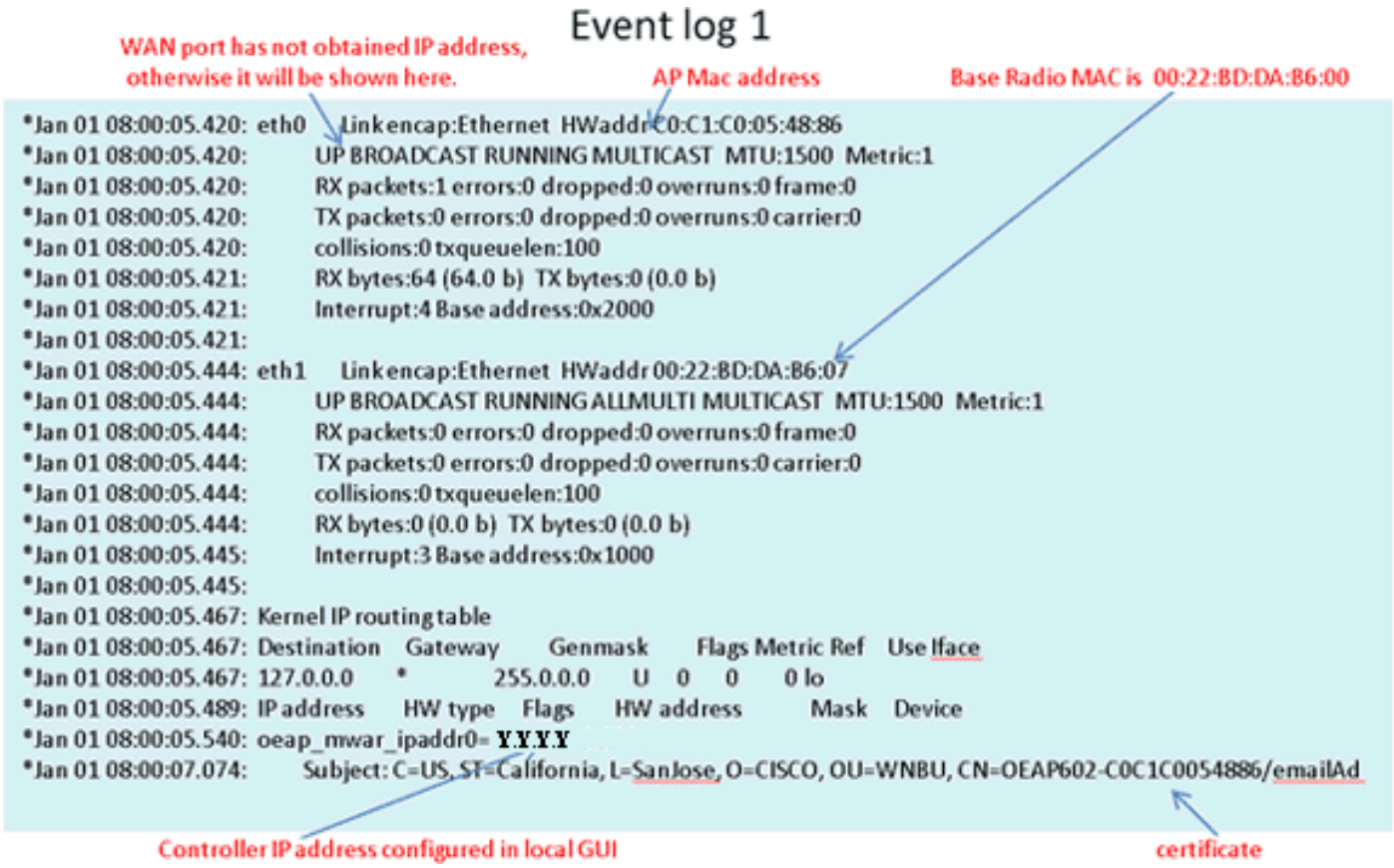
Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

如果連線過程失敗，LED會循環顯示顏色或閃爍橙色。如果發生這種情況，請檢查事件日誌以瞭解進一步的詳細資訊。要訪問事件日誌，請瀏覽到AP（使用個人SSID或有線埠1-3）並捕獲此資料供IT管理員檢視。

此圖顯示Cisco Aironet 600系列OEAP事件日誌：



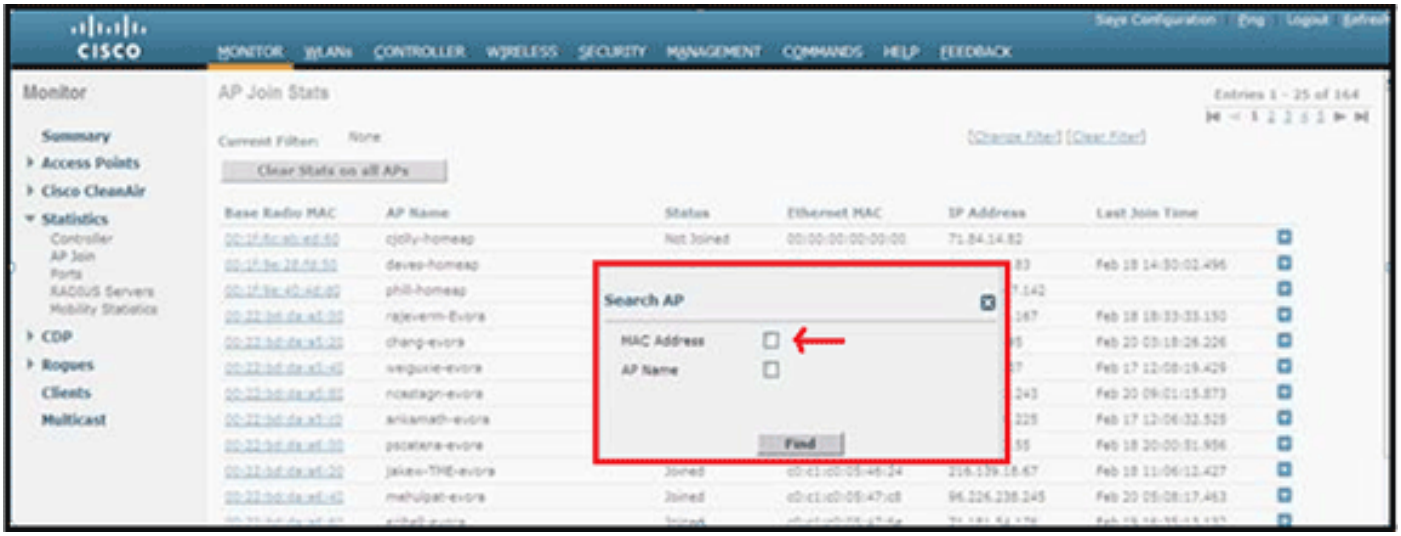
如果加入過程失敗，並且這是Cisco Aironet 600系列OEAP首次嘗試連線到控制器，請檢查Cisco Aironet 600系列OEAP的AP加入統計資訊。為此，您需要使用AP的基本無線電MAC。您可以在事件日誌中找到這個訊息。以下是一個包含註釋的事件日誌示例，可幫助您解釋以下內容：



瞭解這一點後，您可以檢視控制器監控器統計資訊，以確定Cisco Aironet 600系列OEAP是否已加入控制器或曾經加入控制器。此外，這應能說明發生故障的原因或是否發生故障。

如果需要AP身份驗證，請驗證Cisco Aironet 600系列OEAP乙太網MAC地址（非無線電MAC地址）是否已輸入到小寫的Radius伺服器。您還可以從事件日誌確定乙太網MAC地址。

在控制器上搜尋Cisco Aironet 600系列OEAP



如果確定可以從連線到本地乙太網埠的PC訪問網際網路，但AP仍無法加入控制器，並且您已確認控制器的IP地址在本地AP GUI中配置且可訪問，則確認該AP是否已成功加入。也許AP不在AAA伺服器中。或者，如果DTLS握手失敗，則AP可能在控制器上出現證書錯誤或日期/時間錯誤。

如果沒有任何Cisco Aironet 600系列OEAP裝置可以加入控制器，請驗證該控制器是否位於DMZ上

，並且是否打開UDP埠5246和5247。

如何調試客戶端關聯問題

AP正確加入控制器，但無線客戶端無法與公司SSID關聯。檢查事件日誌以檢視關聯消息是否到達AP。

下圖顯示客戶端與企業SSID與WPA或WPA2關聯的正常事件。對於採用開放式身份驗證或靜態WEP的SSID，只有一個ADD MOBILE事件。

事件日誌-客戶端關聯

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no

*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000

*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1

*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1

*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4

*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

如果(Re)Assoc-Req事件不在日誌中，請驗證客戶端具有正確的安全設定。

如果(Re)Assoc-Req事件顯示在日誌中，但客戶端無法正確關聯，請為客戶端在控制器上啟用debug client <MAC address>命令，然後以與使用其他Cisco非OEAP存取點的客戶端相同的方式調查問題。

如何解釋事件日誌

下面的事件日誌和註釋可幫助您對其他Cisco Aironet 600系列OEAP連線問題進行故障排除。

以下是從Cisco Aironet 600系列OEAP事件日誌檔案中收集的一些示例，帶有幫助解釋事件日誌的註釋：

Event log 2

*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAP State: Init.
*Jan 01 08:00:09.009: CAPWAP State: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAP State: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 1
*Jan 01 08:00:09.194:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
*Jan 01 08:00:09.195: Discovery Request sent to **Y.Y.Y.Y** with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from **Y.Y.Y.Y**
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= **Y.Y.Y.Y** , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00'(index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = **Y.Y.Y.Y** , load = 151..
*Jan 01 08:00:19.183: Synchronizing time with AC time.
*Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC **Y.Y.Y.Y** , port= 5246

Discovery Request sent
If AP can not get IP address, then Discovery Req. will not be sent

Discovery resp. received from controller. If no response from controller, then need to check whether controller is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller completed. If certificate has problem, then the failure will happen here

Event log 3

*Feb 19 23:34:16.813: CAPWAP State: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

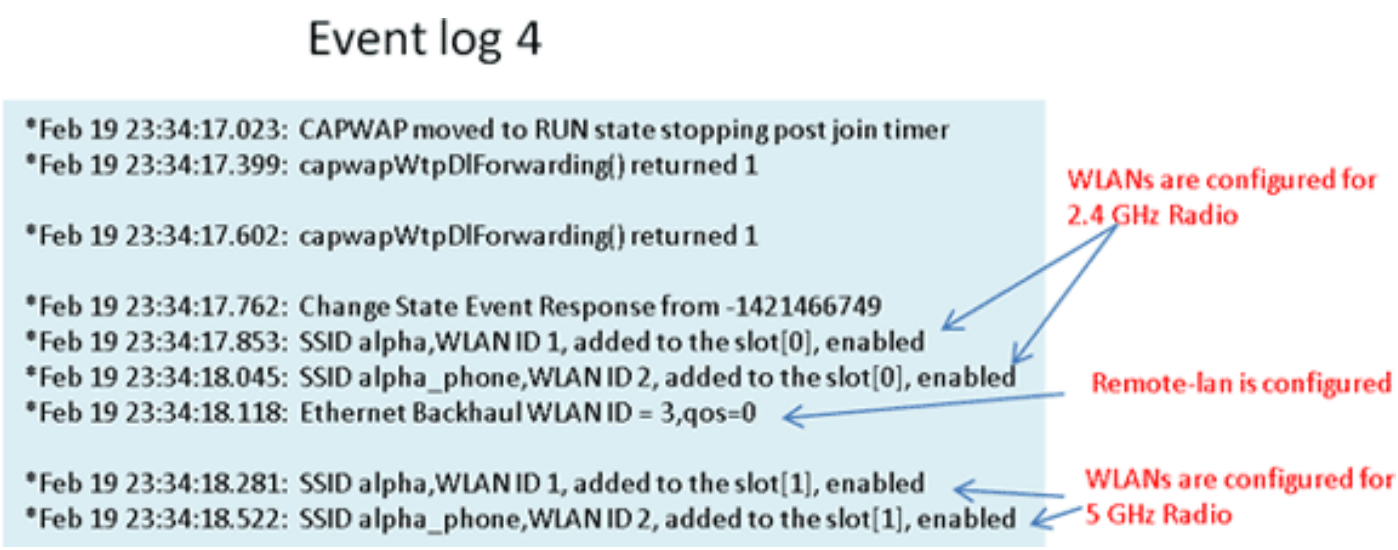
*Feb 19 23:34:16.887: Join Response from **Y.Y.Y.Y**
*Feb 19 23:34:16.888: PTMU : Setting MTU to : 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAP State: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAP State: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to **Y.Y.Y.Y**
*Feb 19 23:34:17.019: Configuration Status Response from **Y.Y.Y.Y**
*Feb 19 23:34:17.022: CAPWAP State: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAP State: Run.

Join Resp. from controller
If AP is not added to AAA server, this step will fail.

Controller and AP have same version SW, no image download is need. When controller is upgraded to new version SW, image download will happen.

Capwap configuration completes



當網際網路連線不可靠時

本節中的事件日誌示例可以在Internet連線失敗或最終非常緩慢或間歇性時發生。這可能是由您的ISP網路、ISP數據機或家庭路由器引起的。有時，來自ISP的連線會中斷或變得不可靠。發生這種情況時，CAPWAP鏈路（返回公司的隧道）可能會發生故障或發生故障。

以下是事件日誌中此類故障的範例：

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)., 2)
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAP State: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

其他調試命令

在飯店或其他付費場所使用Cisco Aironet 600系列OEAP時，在Cisco Aironet 600系列OEAP透過隧道返回控制器之前，您需要穿過有牆的花園。為此，請將筆記型電腦插入其中一個有線本地埠（埠1-3）或使用個人SSID登入飯店並滿足啟動螢幕。

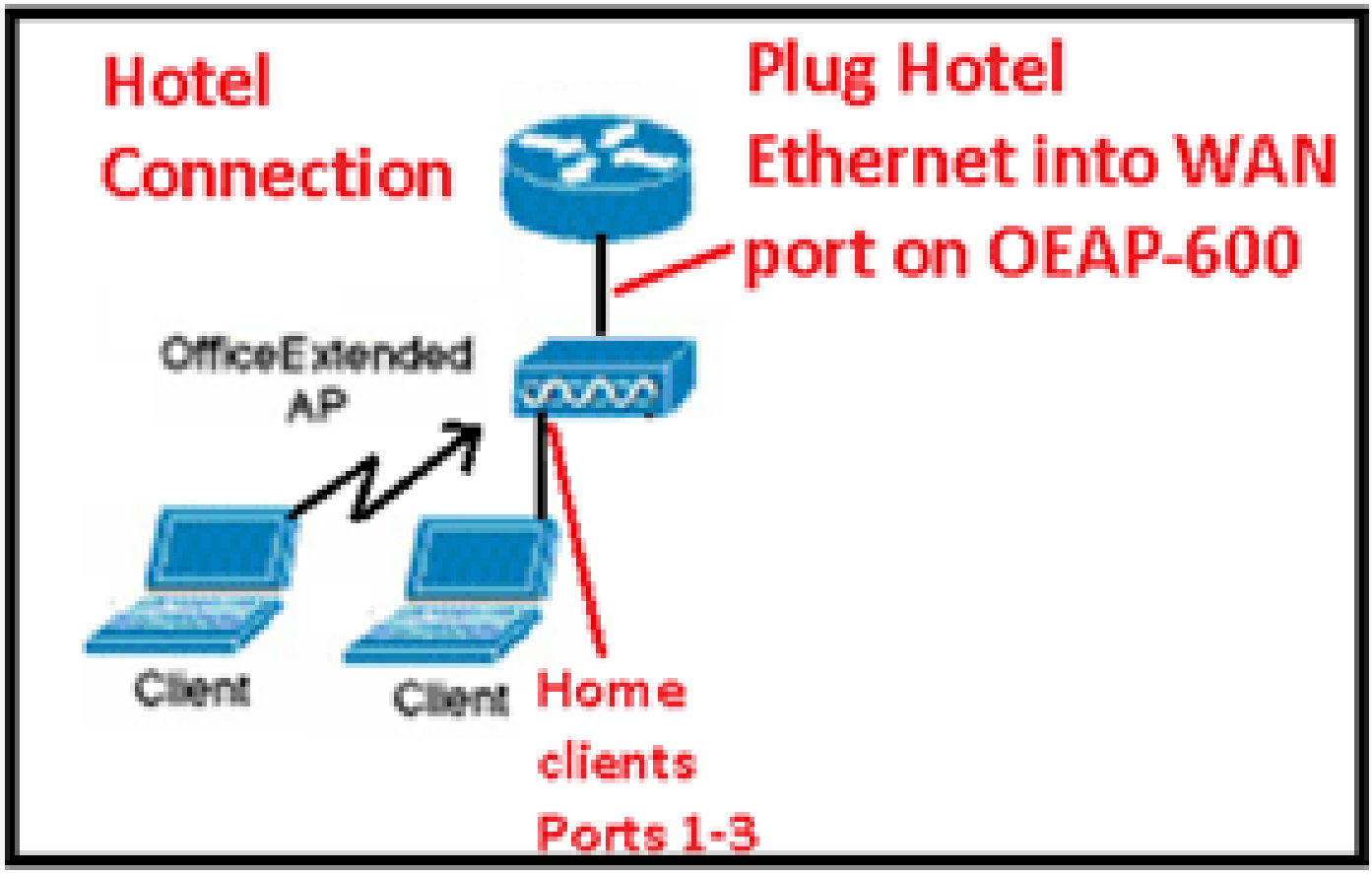
從AP的主端連線到Internet後，裝置會建立DTLS隧道和您的公司SSID。然後，有線埠#4（假設配置了遠端LAN）會變為活動狀態。

注意：這可能需要幾分鐘時間，請觀看思科徽標LED的藍色或紫色表示成功加入。此時，個人和企業連線都處於活動狀態。

注意：當飯店或其他ISP斷開連線時（通常為24小時），隧道會中斷。然後，您必須重新開始相同

的流程。這是設計好的，是正常的。

此影像顯示Office Extend的使用付費組態：



此影像顯示其他偵錯指令（無線電介面資訊）：

Below are the new diagnostics commands for the OEAP 600

The WLC CLI of "show tech" is:

debug ap enable <apname>
then:
debug ap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
debug ap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
debug ap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)

The "show eventlog" is the same as other APs:
show ap eventlog <apname>

已知問題/警告

將組態檔從控制器上傳到TFTP/FTP伺服器時，系統會將Remote-LAN組態上傳為WLAN組態。有關詳細資訊，請參閱版本7.0.116.0的Cisco無線LAN控制器和輕量存取點發行版本註釋。

在OEAP-600上，如果CAPWAP連線由於控制器上的身份驗證失敗而失敗，在OEAP-600嘗試重新啟動CAPWAP嘗試之前，OEAP-600上的Cisco徽標LED可能會關閉一段時間。這是正常現象，因此您應該注意，如果徽標LED暫時關閉，AP不會熄滅。

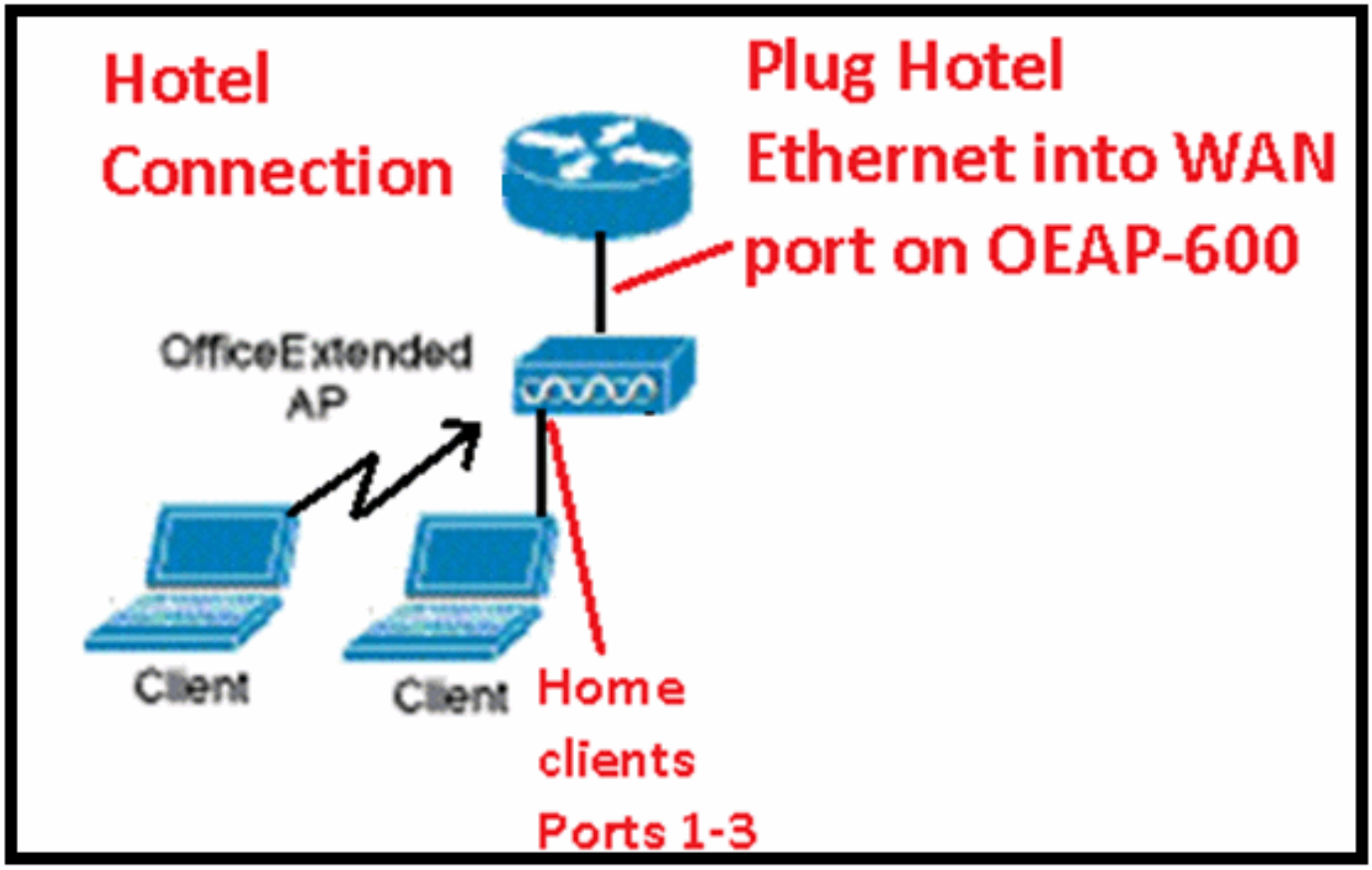
此OEAP-600產品的登入名與之前的OEAP存取點不同，為了與家庭產品（例如Linksys）一致，預設使用者名稱為admin，口令為admin；其他Cisco OEAP存取點（例如AP-1130和AP-1140）的預設使用者名稱為Cisco，口令為Cisco。

此第一版OEAP-600支援802.1x，但僅在CLI上受支援。嘗試更改GUI的使用者可能會丟失其配置。

當您在飯店或其他付費場所使用OEAP-600時，OEAP-600需要穿過帶牆的花園，才能通過隧道返回控制器。只要將筆記型電腦插入其中一個有線本機連線埠（連線埠1-3），或使用個人SSID登入飯店並滿足開機畫面。從AP的主端連線到Internet後，裝置會建立DTLS隧道和您的公司SSID和有線埠#4（假設配置了遠端LAN），然後變為活動狀態。請注意，這可能需要幾分鐘的時間，請觀看思科徽標LED的藍色或紫色，以表示成功加入。此時，個人和企業連線都處於活動狀態。

注意：當飯店或其他ISP斷開連線（通常為24小時）時，隧道可能會中斷，您必須重新啟動相同的進程。這是設計好的，是正常的。

Office Extend in pay for use場所



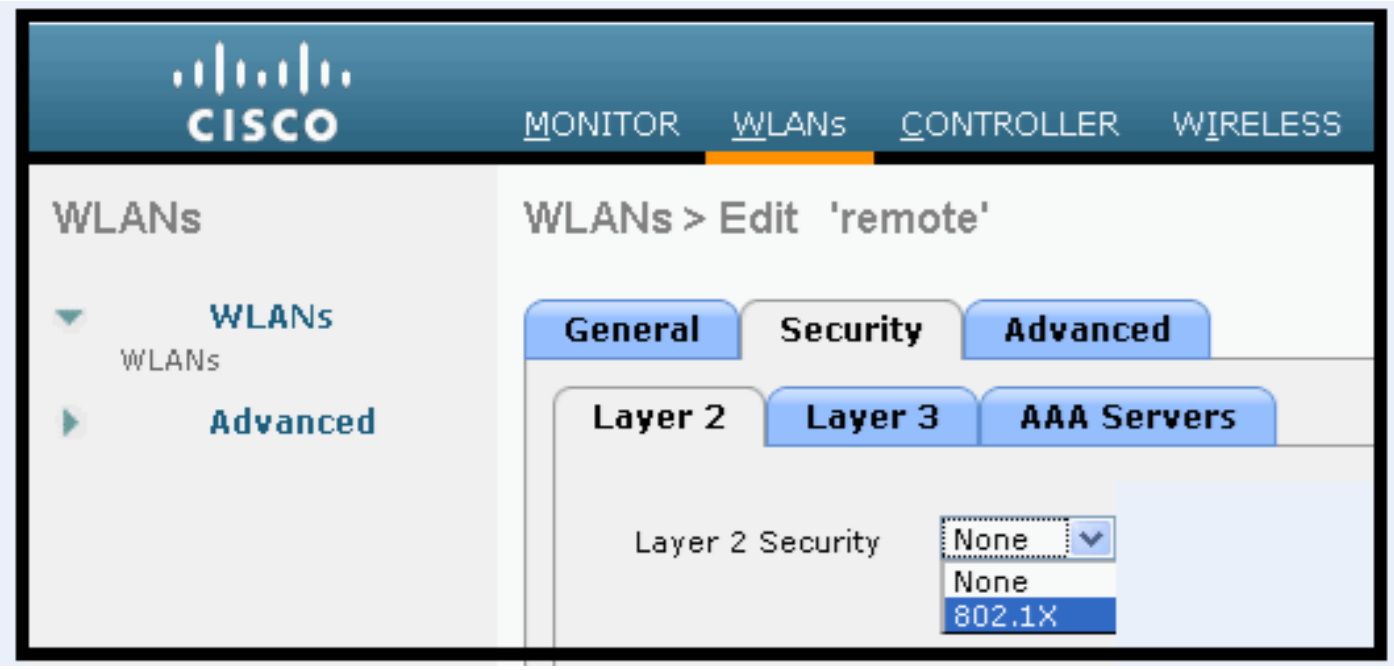
以下是Cisco 7.2版本中引入的一些其他增強功能：

- 在GUI中新增802.1x安全性
- 能夠從控制器停用AP上的本地WLAN訪問-停用個人SSID，只允許企業配置
- 頻道指派可選選項
- 支援從2個公司SSID更改為3個SSID

- 支援雙RLAN埠功能

在GUI中新增802.1x安全性

802.1x現已增加到GUI



有關遠端LAN連線埠驗證的注意事項。

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

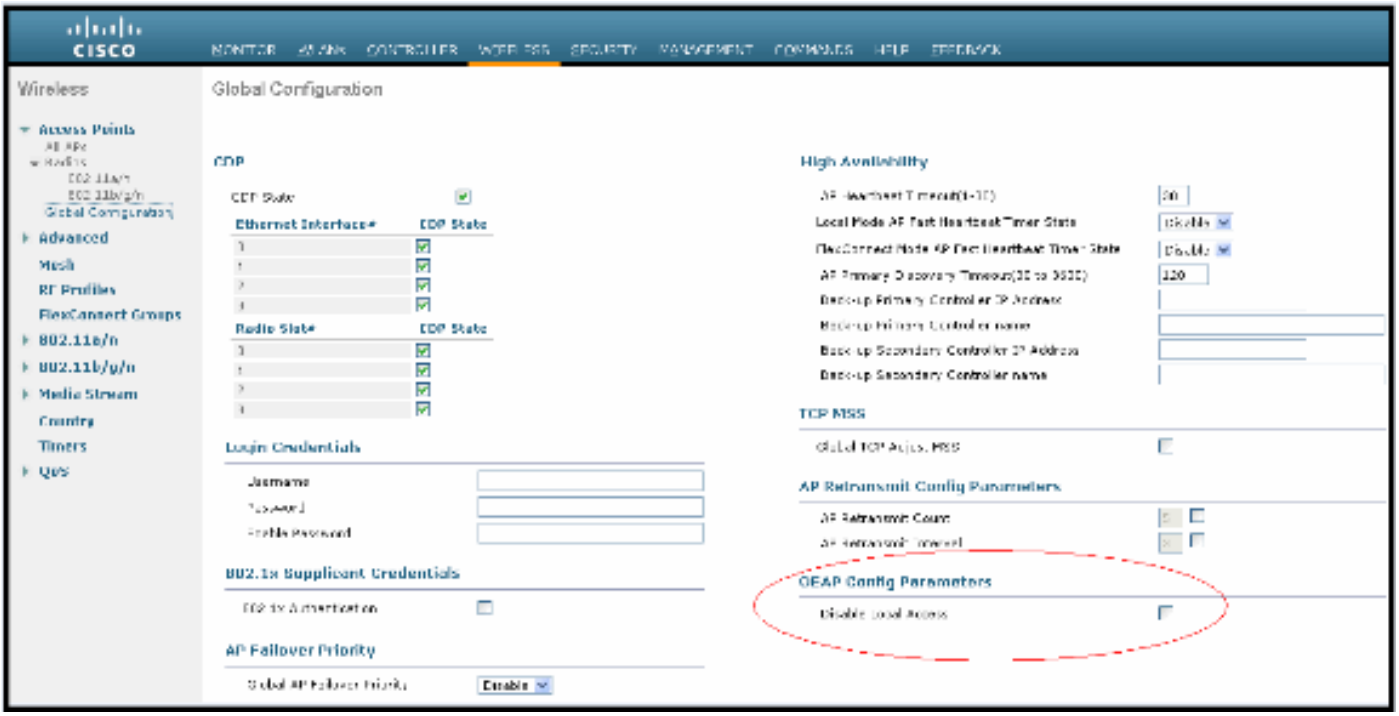
Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

能夠從控制器停用AP上的本地WLAN訪問-停用個人SSID，只允許企業配置

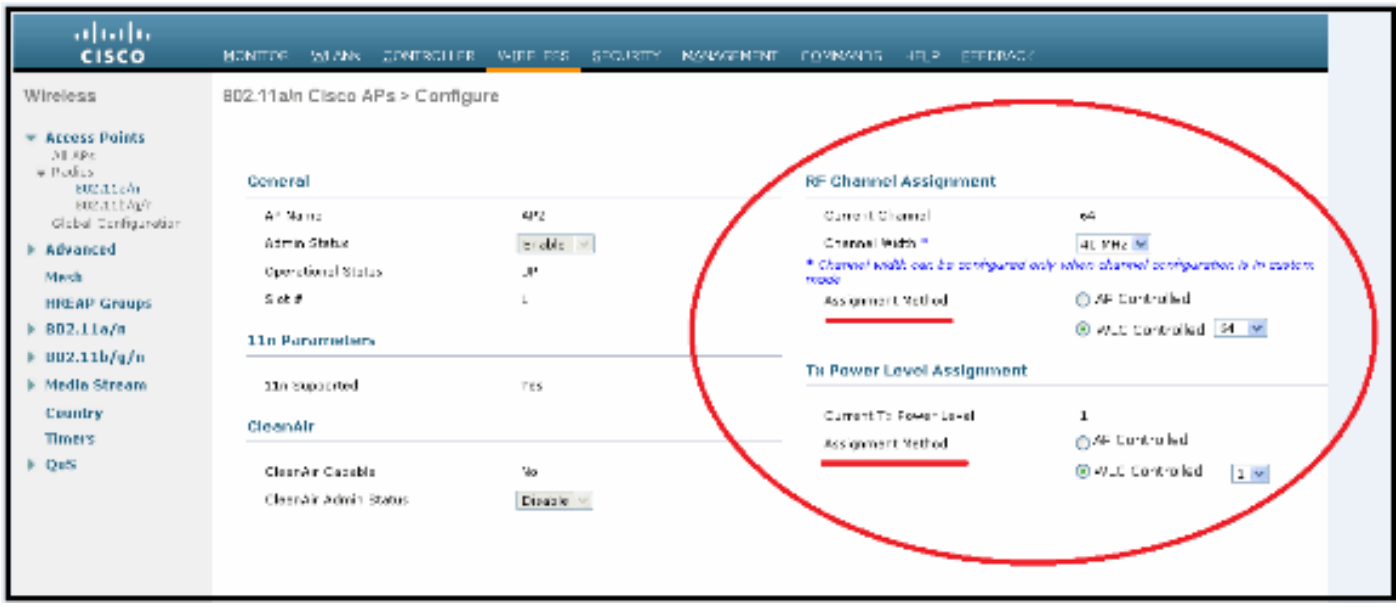
停用本地WLAN訪問



通道指派可選取的選項有：

- 本地控制的AP
- WLC控制的

RF通道和功率分配現在由本地或WLC控制



Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release; the configuration window is added back with only "General", "RF Channel Assignment" and "Tx Power Level Assignment" portions. The "Admin Status" in "General" shall be display only. The options for "Assign Method" are changed to "Custom Configured" and "AP Controlled". By default "AP Controlled" is selected. Channel and Tx power level can be configured only when they are in "Custom Configured" mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is "AP Controlled", then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is "AP controlled", then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When "Reset to Default" operation is performed, the assign method is set to "AP controlled".

支援雙RLAN連線埠功能（僅限CLI）

此注意事項適用於使用雙RLAN埠功能的OEAP-600系列AP，該功能允許OEAP-600乙太網埠3作為遠端LAN運行。僅允許透過CLI進行配置，以下是一個示例：

```
Config network oeap-600 dual-rlan-ports enable|disable
```

如果未配置此功能，則單埠4 remote-lan將繼續運行。每個埠對每個埠使用唯一的遠端LAN。遠端LAN對映不同，這取決於使用的是預設組還是AP組。

Default-group

如果使用預設組，則具有偶數遠端LAN ID的單個遠端LAN將對映到埠4。例如，remote-lan-id 2的remote-lan被對映到埠4（在OEAP-600上）。具有奇數編號的遠端LAN ID的遠端LAN對映到埠3（在OEAP-600上）。

以下列兩個遠端lan為例：

```
(Cisco Controller) >show remote-lan summary

Number of Remote LANS.............................. 2

RLAN ID  RLAN Profile Name    Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

rlan2具有偶數編號的遠端lan ID 2，因此對映到埠4。rlan3具有奇數遠端lan ID 3，因此對映到埠3。

AP組

如果使用AP組，則到OEAP-600埠的對映取決於AP組的順序。要使用AP組，必須首先從AP組中刪除所有遠端區域網和WLAN，然後將其留空。然後將兩個遠端lan增加到AP組。首先增加埠3 AP遠端LAN，然後增加埠4遠端組，最後增加任何WLAN。

清單中第一個位置的remote-lan對映到連線埠3，而清單中的第二個位置對映到連線埠4，如以下範例所示：

```
RLAN ID  RLAN Profile Name      Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

相關資訊

- Cisco無線LAN控制器組態設定指南7.0版
- 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）。