查看無線 LAN 控制器 (WLC) 設計和功能的常見問題

目錄

WLC功能常見問題解答

相關資訊

簡介

SSHv1

本文說明無線 LAN 控制器設計和功能的最新資訊。

必要條件

需求

本文件沒有特定需求。

元件使用

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您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。

WLC設計常見問題

問：如何將交換機配置為與WLC連線？

A.將WLC連線的交換機埠配置為IEEE 802.1Q中繼埠。請確保交換機上只允許必要的VLAN。通常，WLC的管理和AP-Manager介面未進行標籤。這表示它們採用所連線交換機的本地VLAN。這沒有必要。您可以為這些介面分配單獨的VLAN。有關詳細資訊，請參閱為WLC配置交換機。

問題： 在存取點(AP)註冊到控制器後，所有來往於WLAN使用者端的網路流量是否會透過無線LAN控制器(WLC)通道？

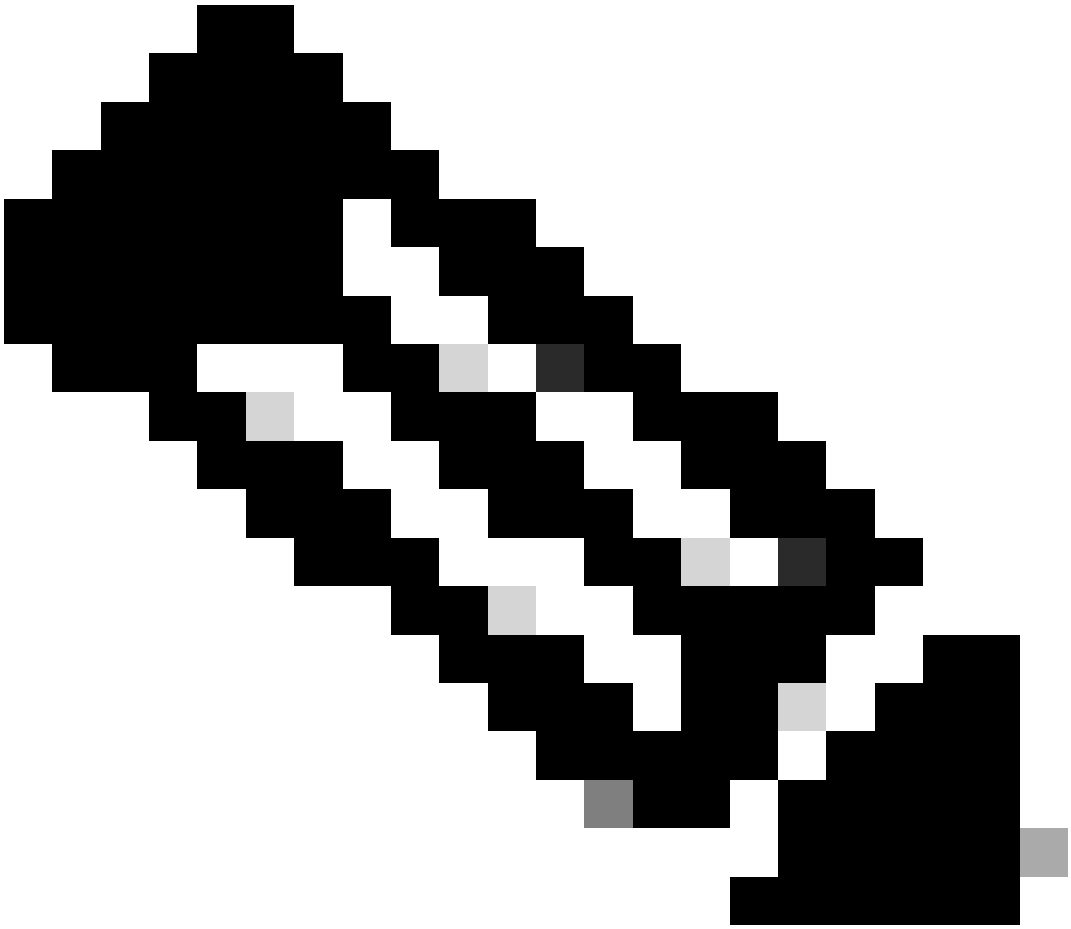
答：當AP加入WLC時，兩個裝置之間形成無線存取點協定(CAPWAP)控制和調配(CAPWAP)隧道。所有流量（包括所有客戶端流量）透過CAPWAP隧道傳送。

唯一的例外是AP處於混合REAP模式時。當與控制器的連線丟失時，混合REAP存取點可以在本地交換客戶端資料流量並在本地執行客戶端身份驗證。連線到控制器後，它們還可以將流量傳送回控制器。

問題： 是否可以在遠端辦公室安裝輕型存取點(LAP)並在總部安裝思科無線區域網控制器(WLC)？LWAPP/CAPWAP是否在WAN上工作？

答：是，您可以讓WLC透過WAN與AP連線。在遠端邊緣AP (REAP)或混合遠端邊緣AP (H-

REAP)模式下配置LAP時，LWAPP/CAPWAP可透過廣域網工作。這兩種模式中的任一種都允許透過WAN鏈路連線的遠端控制器控制AP。流量在本地橋接到LAN鏈路上，這樣就無需透過WAN鏈路傳送不必要的本地流量。這正是在您的無線網路中具有WLC的最大優勢之一。



注意：並非所有輕量AP都支援這些模式。例如，只有1131、1140、1242、1250和AP801 LAP支援H-REAP模式。只有1030 AP支援REAP模式，但1010和1020 AP不支援REAP。在計畫實施這些模式之前，請檢查以確定LAP是否支援這些模式。已轉換為LWAPP的Cisco IOS®軟體AP（自治AP）不支援REAP。

問題： REAP和H-REAP模式如何工作？

A.在REAP模式下，所有控制和管理流量（包括身份驗證流量）都透過隧道返回WLC，但是，所有資料流量都在遠端辦公室LAN中進行本地交換。當與WLC的連線丟失時，除第一個WLAN (WLAN1)外，所有WLAN都將被終止。目前與此WLAN關聯的所有使用者端都會保留。為了允許新客戶端在停機時間內成功驗證和在這個WLAN上接收服務，請將此WLAN的驗證方法配置為WEP或WPA-PSK，以便在REAP本地完成驗證。有關REAP部署的詳細資訊，請參閱分支機構的REAP部署指南。

在H-REAP模式下，存取點透過隧道將控制和管理流量（包括身份驗證流量）返回WLC。如果使用H-REAP本地交換配置了WLAN，則來自WLAN的資料流量會在遠端辦公室本地橋接，或者資料流量會傳送回WLC。當與WLC的連線丟失時，除前八個配置了H-REAP本地交換的WLAN外，所有WLAN都將被終止。目前與這些WLAN相關聯的所有使用者端都會保留。為了允許新客戶端在停機時間內成功驗證這些WLAN並接收服務，請將此WLAN的驗證方法配置為WEP、WPA PSK或WPA2 PSK，以便在H-REAP本地完成驗證。

有關H-REAP的詳細資訊，請參閱《FlexConnect無線分支控制器部署指南》。

問題： 遠端邊緣AP (REAP)和混合REAP (H-REAP)有何區別？

A. REAP 不支援IEEE 802.1Q VLAN標籤。因此，它不支援多個VLAN。來自所有服務集識別符號(SSID)的流量在同一子網中終止，但H-REAP支援IEEE 802.1Q VLAN標籤。來自每個SSID的流量可以分段為唯一的VLAN。

當與WLC的連線丟失時（即在獨立模式下），REAP僅服務於一個WLAN，即第一個WLAN。所有其他WLAN都已停用。在H-REAP中，在停機時間內最多支援8個WLAN。

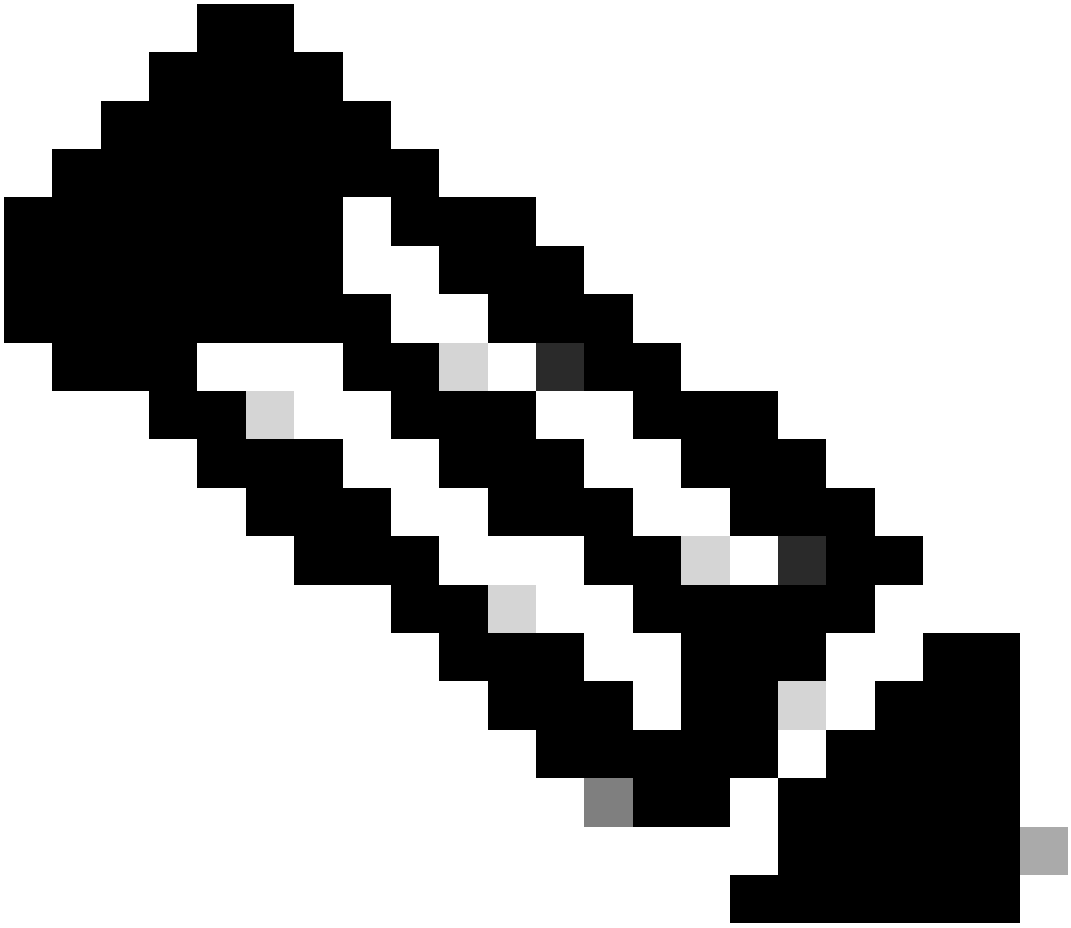
另一個主要區別是，在REAP模式下，資料流量只能進行本地橋接。它不能切換回中心辦公室，但在H-REAP模式下，您可以選擇將流量切換回中心辦公室。來自配置了H-REAP本地交換的WLAN的流量在本地交換。來自其他WLAN的資料流量交換回中心辦公室。

有關REAP的詳細資訊，請參閱「使用輕量AP和無線區域網控制器(WLC)的遠端邊緣AP (REAP)配置示例」。

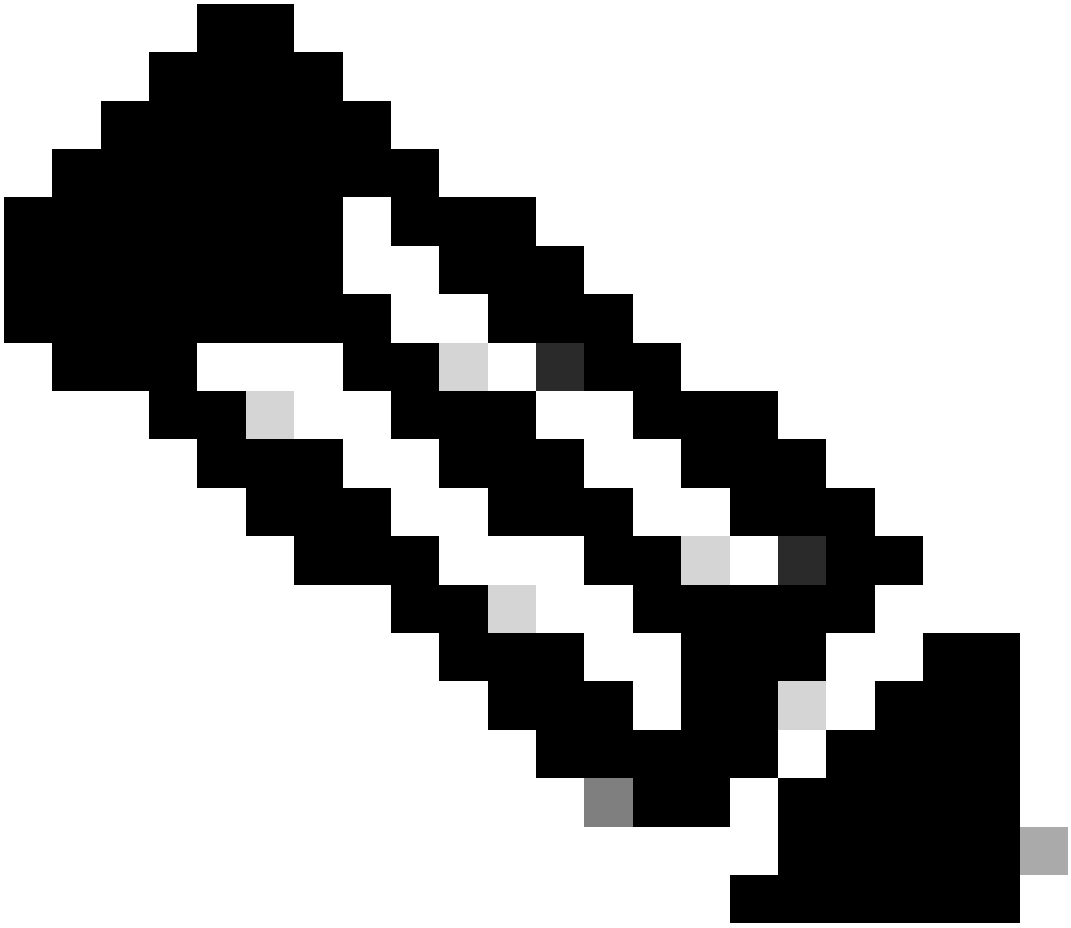
有關H-REAP的詳細資訊，請參閱配置混合REAP。

問題： WLC支援多少個WLAN？

答：從軟體版本5.2.157.0開始，WLC現在可以控制多達512個輕量存取點的WLAN。每個WLAN都有單獨的WLAN ID （1至512）、單獨的配置檔名稱和WLAN SSID，並且可以為每個WLAN分配唯一的安全策略。控制器最多會將16個WLAN發佈至每個連線的存取點，但您最多可以在控制器上建立512個WLAN，然後選擇性地將這些WLAN （使用存取點群組）發佈至不同的存取點，以更有效管理您的無線網路。



注意：Cisco 2106、2112和2125控制器僅支援最多16個WLAN。



注意：有關在WLC上配置WLAN的準則的詳細資訊，請參閱Cisco無線LAN控制器配置指南7.0.116.0版中的「建立WLAN」部分。

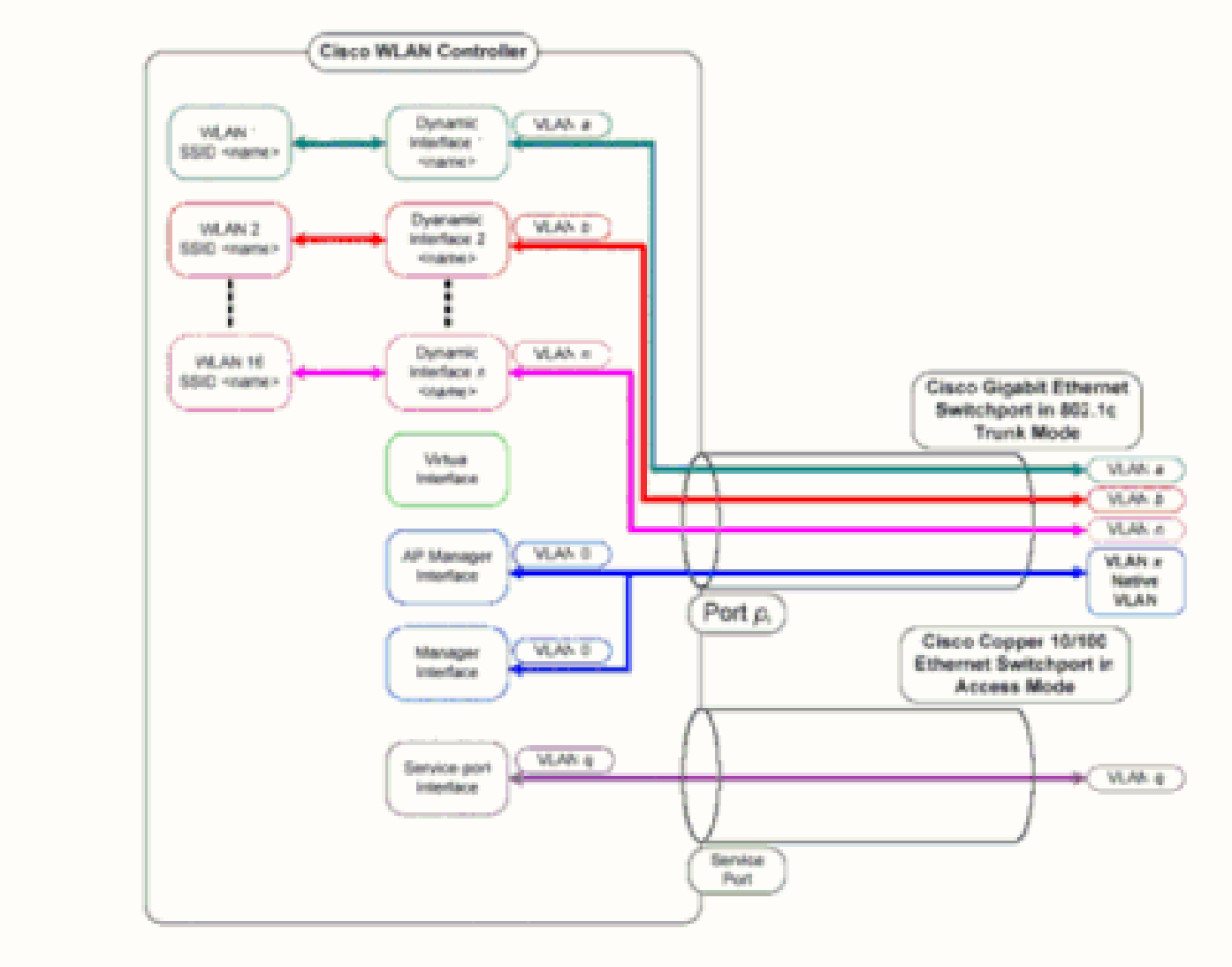
問題： 如何在無線LAN控制器(WLC)上設定VLAN？

答：在WLC中，VLAN繫結到在唯一IP子網中配置的介面。此介面對映到WLAN。然後，與此WLAN關聯的客戶端將屬於介面的VLAN，並且會從該介面所屬的子網中分配一個IP地址。要在WLC上配置VLAN，請完成無線LAN控制器上的VLAN配置示例中的過程。

問題： 我們已使用兩個不同的動態介面調配了兩個WLAN。每個介面都有自己的VLAN，與管理介面VLAN不同。這似乎可行，但我們尚未調配中繼埠來允許WLAN使用的VLAN。存取點(AP)是否使用管理介面VLAN標籤資料包？

答：AP不使用管理介面VLAN標籤資料包。AP將來自客戶端的資料包封裝在輕量AP協定(LWAPP)/CAPWAP中，然後將這些資料包傳遞到WLC。然後，WLC解除LWAPP/CAPWAP報頭並將資料包轉發到具有相應VLAN標籤的網關。VLAN標籤取決於客戶端所屬的WLAN。WLC依賴網關

將資料包路由到其目的地。為了能夠傳遞多個VLAN的流量，您必須將上行鏈路交換機配置為中繼埠。此圖說明VLAN如何使用控制器：



問題： WLC的哪個IP地址用於與AAA伺服器進行身份驗證？

答：WLC將管理介面的IP地址用於任何涉及AAA伺服器的身份驗證機制（第2層或第3層）。有關WLC上的埠和介面的詳細資訊，請參閱Cisco無線LAN控制器配置指南7.0.116.0版的「配置埠和介面」部分。

問題： 我在同一個VLAN中有十個Cisco 1000系列輕量存取點(LAP)和兩個無線區域網控制器(WLC)。如何註冊六個LAP以關聯到WLC1，另外四個LAP以關聯到WLC2？

A. LWAPP/CAPWAP允許動態冗餘和負載均衡。例如，如果您為選項43指定多個IP地址，則LAP會向AP接收的每個IP地址傳送LWAPP/CAPWAP發現請求。在WLC LWAPP/CAPWAP發現響應中，WLC會嵌入以下資訊：

- 有關當前LAP負載的資訊，定義為當時加入WLC的LAP的數量
- LAP容量

- 連線到WLC的無線客戶端的數量

然後，LAP嘗試加入負載最小的WLC，即具有最大可用LAP容量的WLC。此外，在LAP加入WLC後，LAP從其加入的WLC獲取移動組中其他WLC的IP地址。

一旦LAP加入WLC，您可以在下次重新啟動時讓LAP加入特定WLC。為此，請為LAP分配主要、次要和第三個WLC。當LAP重新啟動時，它將查詢主WLC並加入該WLC，而與該WLC上的負載無關。如果主WLC沒有響應，它將查詢輔助WLC，如果沒有響應，查詢第三WLC。有關如何為LAP配置主WLC的詳細資訊，請參閱

部分

問題： 2100系列無線LAN控制器(WLC)不支援哪些功能？

A. 2100系列控制器不支援以下硬體功能：

- 服務埠（獨立的帶外管理10/100 Mb/s乙太網介面）

2100系列控制器不支援以下軟體功能：

- VPN終端（例如IPsec和L2TP）
- 訪客控制器通道的終端（支援訪客控制器通道的產生）
- 外部Web驗證Web伺服器清單
- 第2層LWAPP
- 生成樹
- 連線埠映象
- 紅饗土
- 堡壘
- AppleTalk
- QoS每使用者頻寬合約
- IPv6傳輸
- 連結聚合(LAG)
- 組播單播模式
- 有線訪客接入

問題： 5500系列控制器不支援哪些功能？

A. 5500系列控制器不支援以下軟體功能：

- 靜態AP管理器介面

  註：對於5500系列控制器，您無需配置AP管理器介面。預設情況下，管理介面充當AP管理器介面，存取點可在此介面上加入。

- 非對稱移動隧道
- 生成樹通訊協定(STP)
- 連線埠映象
- 第2層訪問控制清單(ACL)支援
- VPN終端（例如IPSec和L2TP）
- VPN直通選項
- 配置802.3橋接、AppleTalk和乙太網點對點協定(PPPoE)

問題： 網狀網路不支援哪些功能？

A.網狀網路不支援以下控制器功能：

- 多國支援
- 基於負載的CAC（網狀網路僅支援基於頻寬或靜態CAC。）
- 高可用性（快速心跳和主發現加入計時器）
- EAP-FASTv1和802.1X驗證
- 存取點加入優先順序（網狀無線存取點具有固定優先順序。）
- 本地重要證書
- 基於位置的服務

問題： 無線LAN控制器上的製造商安裝證書(MIC)和輕量AP證書的有效期是多少？

答：WLC上的MIC的有效期為10年。建立輕量AP證書(無論是MIC證書還是自簽名證書(SSC))時，有效期均為10年。

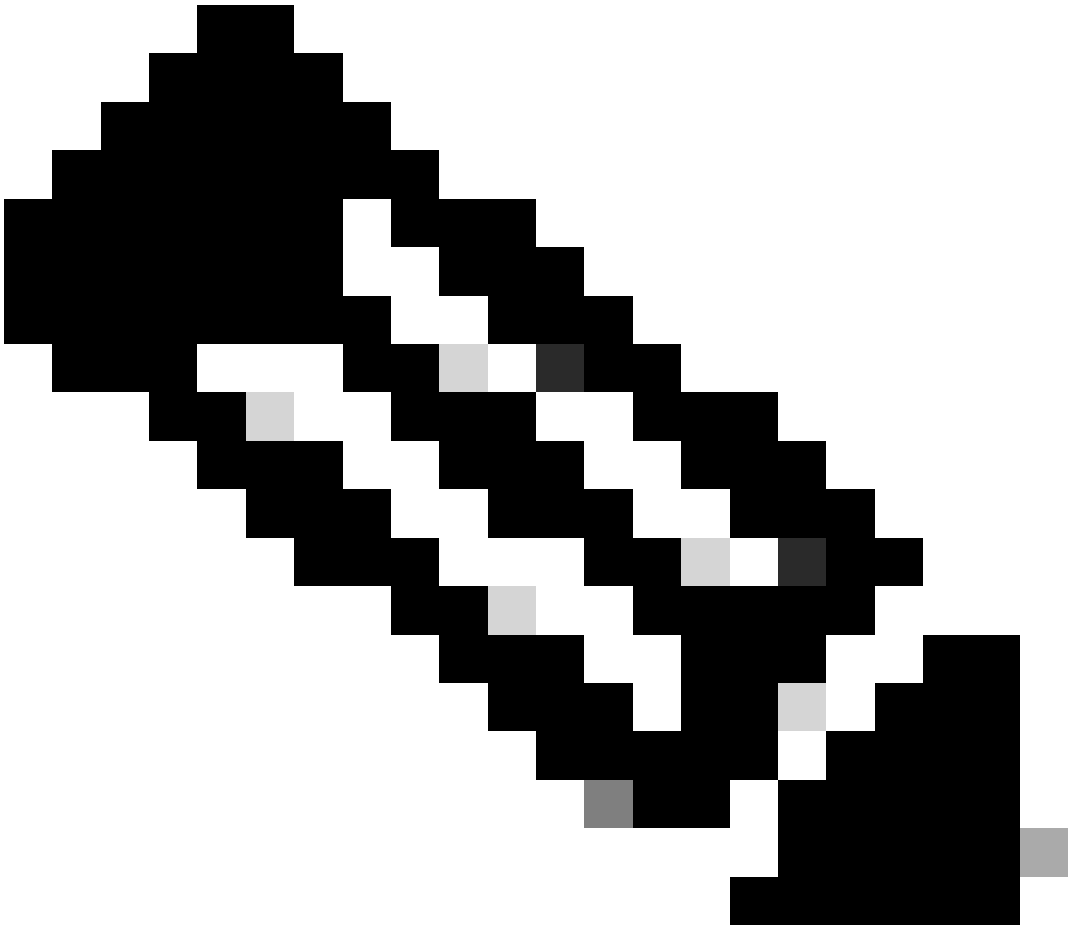
問題： 我在同一個行動群組內設定了兩個名為WLC1和WLC2的無線LAN控制器(WLC)以進行容錯移轉。我的輕量型存取點(LAP)目前已註冊到WLC1。如果WLC1發生故障，在向WLC(WLC2)過渡期間，註冊到WLC1的AP是否會重新啟動？此外，在此故障切換期間，WLAN客戶端是否丟失與LAP的WLAN連線？

A.是，LAP會從WLC1註銷並重新註冊，如果WLC1失敗，則會重新引導並重新註冊到WLC2。由於LAP重新啟動，相關的WLAN客戶端將失去與重新啟動LAP的連線。有關資訊，請參閱統一無線網

路中的AP負載均衡和AP後退。

問題： 漫遊是否依賴於無線區域網控制器(WLC)配置為使用的輕量存取點協定(LWAPP)模式？在第2層LWAPP模式下運行的WLC能否執行第3層漫遊？

A. 只要控制器上的移動分組配置正確，客戶端漫遊必須正常工作。漫遊不受LWAPP模式（第2層或第3層）的影響。但是，建議儘可能使用第3層LWAPP。



注意：只有Cisco 410x和440x系列WLC和Cisco 1000系列存取點支援第2層模式。其他無線LAN控制器和輕量存取點平台不支援第2層LWAPP。

問題： 當客戶端決定漫遊到新的存取點(AP)或控制器時，會發生什麼漫遊過程？

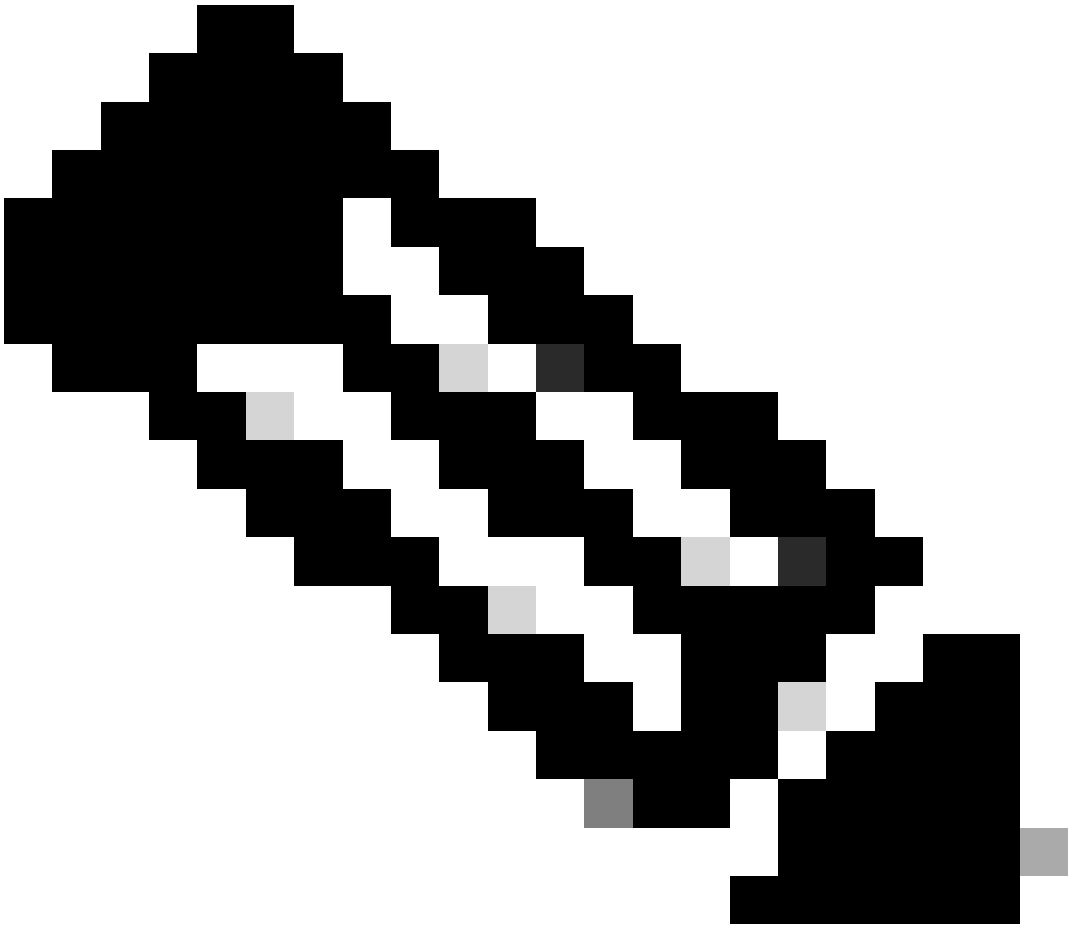
A. 這是客戶端漫遊到新AP時所發生的一系列事件：

1. 客戶端透過LAP向WLC傳送重新關聯請求。

2. WLC將移動消息傳送到移動組中的其他WLC，以找出客戶端之前與之關聯的WLC。

3. 原始WLC會透過移動消息使用有關客戶端的資訊作出響應，如MAC地址、IP地址、QoS、安全上下文等。

4. WLC會使用所提供的使用者端詳細資訊更新其資料庫；如有必要，使用者端會接著進行重新驗證程式。當前與客戶端關聯的新LAP也會與WLC資料庫中的其他詳細資訊一起更新。如此一來，使用者端IP位址在WLC之間的漫遊之間得以保留，有助於提供順暢的漫遊。



注意：無線客戶端在重新關聯過程中不發出(802.11)身份驗證請求。無線使用者端會立即傳送重新關聯訊息。然後，它可以透過802.1x身份驗證。

問題： 當網路中存在防火牆時，我需要允許哪些埠進行LWAPP/CAPWAP通訊？

A.必須啟用以下埠：

- 為LWAPP流量啟用以下UDP埠：

    - 資料- 12222
    - 控制- 12223
- 為CAPWAP流量啟用以下UDP埠：
    - 資料- 5247
    - 控制- 5246
- 為移動流量啟用以下UDP埠：
    - 16666 -安全模式
    - 16667 -非安全模式

移動和資料消息通常透過EtherIP資料包交換。 防火牆必須啟用IP協定97以允許EtherIP資料包通過。如果使用ESP封裝移動資料包，您在打開UDP埠500時必須允許ISAKMP透過防火牆。您還必須啟用IP協定50以允許加密資料透過防火牆。

這些埠是可選的（取決於您的要求）：

- 用於SNMP的TCP 161和162（用於無線控制系統[WCS]）
- 用於TFTP的UDP 69
- TCP 80和/或443用於HTTP或HTTPS用於GUI訪問
- TCP 23和/或22，用於Telnet或安全外殼(SSH)，用於CLI訪問

問題： 無線區域網控制器是否支援SSHv1和SSHv2？

答：無線區域網控制器僅支援SSHv2。

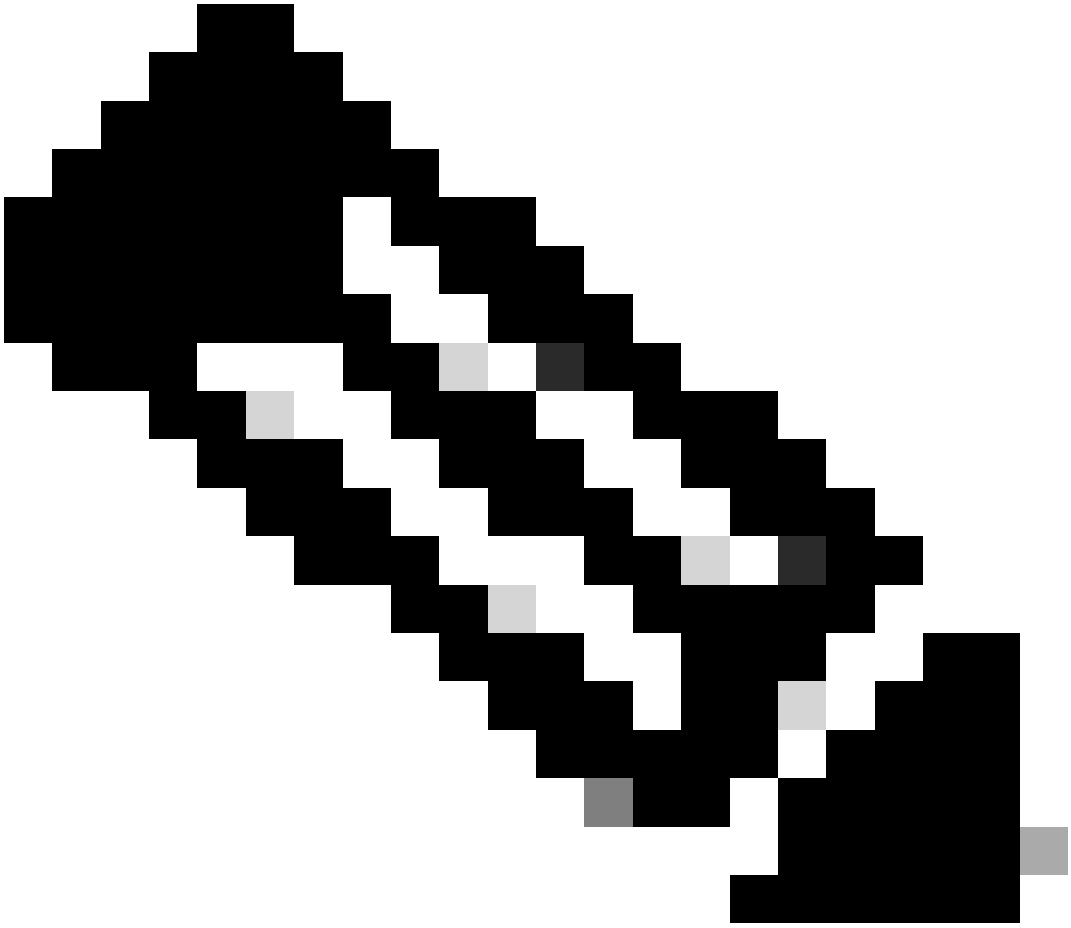
問題： 是否透過無線LAN控制器(WLC)支援反向ARP (RARP)？

A.反向位址解析通訊協定(RARP)是一種連結層通訊協定，用於取得指定連結層位址（例如乙太網路位址）的IP位址。韌體版本為4.0.217.0或更高版本的WLC支援RARP。任何舊版都不支援RARP。

問題： 能否使用無線LAN控制器(WLC)上的內部DHCP伺服器為輕量存取點(LAP)分配IP地址？

A. 控制器包含內部DHCP伺服器。此伺服器通常用於沒有DHCP伺服器的分支機構。要訪問DHCP服務，請在WLC GUI中按一下Controller選單；然後按一下頁面左側的選項Internal DHCP Server。有關如何在WLC上配置DHCP範圍的詳細資訊，請參閱Cisco無線LAN控制器配置指南7.0.116.0版中的配置DHCP部分。

內部伺服器在管理介面上向無線客戶端、LAP、裝置模式AP以及從LAP中繼的DHCP請求提供DHCP地址。WLC從不向有線網路中的上游裝置提供地址。內部伺服器上不支援DHCP選項43，因此AP必須使用替代方法查詢控制器的管理介面IP地址，如本地子網廣播、DNS、啟動或無線發現。



註：除非LAP直接連線到WLC，否則4.0以前的WLC韌體版本不支援LAP的DHCP服務。內部DHCP伺服器功能僅用於為連線到無線LAN網路的客戶端提供IP地址。

問題： WLAN下的DHCP Required欄位表示什麼？

A.DHCP Required是一個可以為WLAN啟用的選項。因此，所有與特定WLAN關聯的客戶端都必須透過DHCP獲取IP地址。具有靜態IP位址的使用者端不允許與WLAN建立關聯。此選項位於WLAN的Advanced頁籤下。只有客戶端的IP地址存在於WLC的MSCB表中，WLC才允許該客戶端之間的流量透過/通過。WLC在DHCP請求或DHCP更新期間記錄客戶端的IP地址。這要求客戶端每次重新關聯到WLC時更新其IP地址，因為每次客戶端在其漫遊過程或會話超時過程中取消關聯時，其條目都會從MSCB表中清除。使用者端必須再次進行驗證並重新建立與WLC的關聯，這會讓使用者端專案再次出現在表格中。

問題： Cisco Centralized Key Management (CCKM)如何在LWAPP/CAPWAP環境中工作？

答：在初始客戶端關聯期間，無線客戶端透過802.1x身份驗證後，AP或WLC會協商成對主金鑰(PMK)。WLC或WDS AP快取每個客戶端的PMK。當無線客戶端重新關聯或漫遊時，它會跳過802.1x驗證並立即驗證PMK。

WLC在CCKM中的唯一特殊實施是WLC透過移動資料包(例如UDP 16666)交換客戶端PMK。

問題： 如何在無線LAN控制器(WLC)和輕量存取點(LAP)上設定雙工設定？

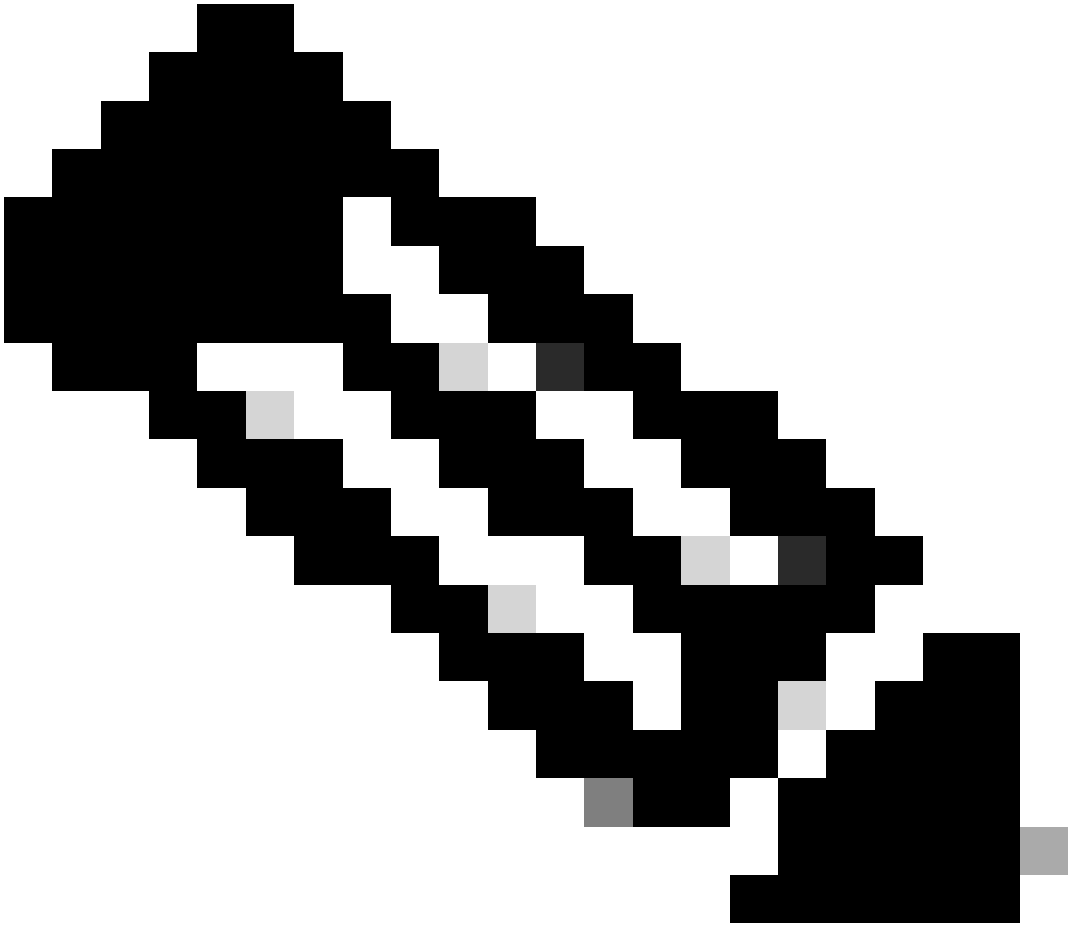
答：當速度和雙工都自動協商時，Cisco無線產品最有效，但是您確實可以選擇在WLC和LAP上設定雙工設定。為了設定AP速度/雙工設定，可以為控制器上的LAP配置雙工設定，然後依次將其推送到LAP。

設定ap乙太網路雙工<auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name>

是透過CLI設定雙工設定的命令。此命令僅在版本4.1及更高版本中受支援。

要為WLC物理介面設定雙工設定，請使用**config port physicalmode {all | port} {100h | 100f | 10h | 10f}**命令。

此命令為專用10 Mbps或100 Mbps、半雙工或全雙工操作設定指定或所有前面板10/100BASE-T乙太網埠。注意，在為埠手動配置任何物理模式之前，您必須使用**config port autoneg disable**命令停用自動協商。此外，還要注意**config port autoneg** 命令會覆蓋使用 **config port physicalmode** 命令所做的設定。預設情況下，所有埠都設定為自動協商。



註：無法更改光纖埠的速度設定。

問題： 當輕量型存取點(LAP)未註冊到控制器時，是否有方法追蹤其名稱？

A.如果AP已完全關閉並且未註冊到控制器，您將無法通過控制器跟蹤LAP。剩下的唯一方法是您可以訪問連線這些AP的交換機，並且可以使用以下命令找到它們所連線的交換機埠：

```
<#root>
```

show mac-address-table address <mac address>

這將為您顯示此AP所連線的交換機上的埠號。然後，發出以下命令：

<#root>

show cdp nei <type/num> detail

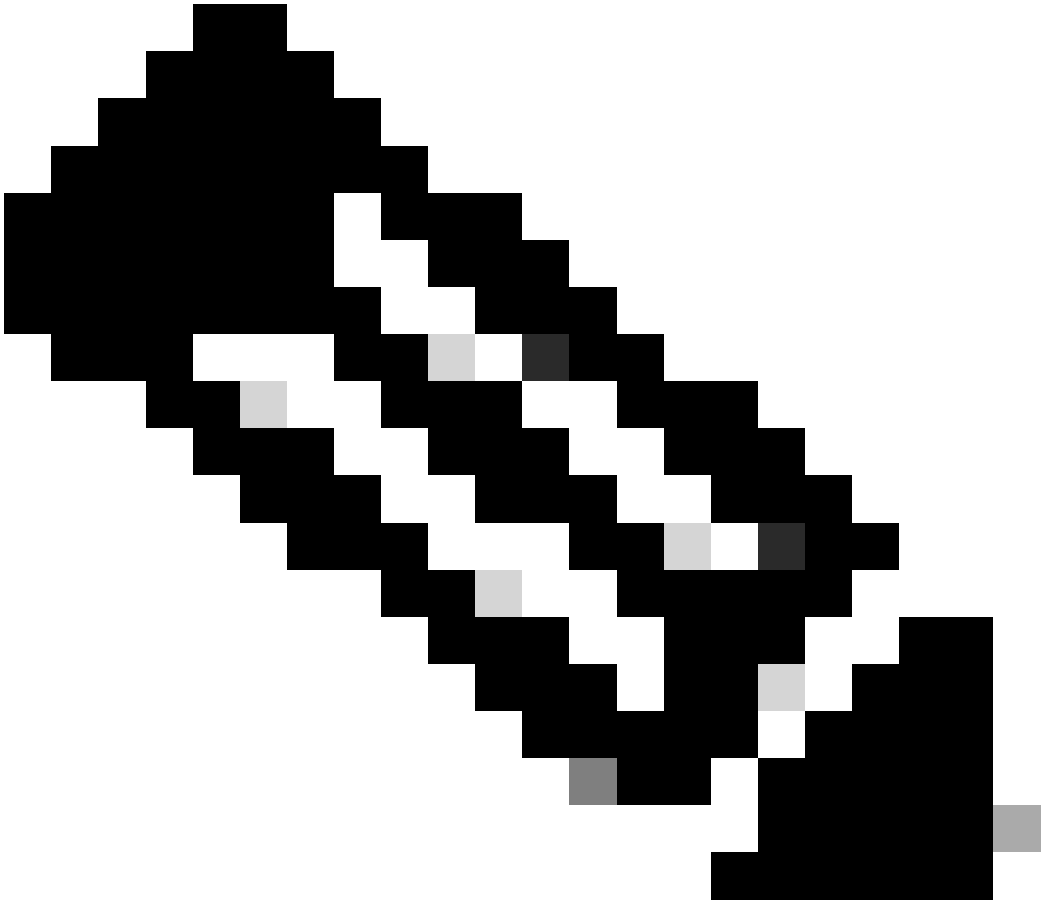
此命令的輸出還提供LAP名稱。但是，只有在AP通電並連線到交換機時，才能使用此方法。

問題： 我已在控制器上配置512個使用者。有沒有增加無線LAN控制器(WLC)上使用者人數的方法？

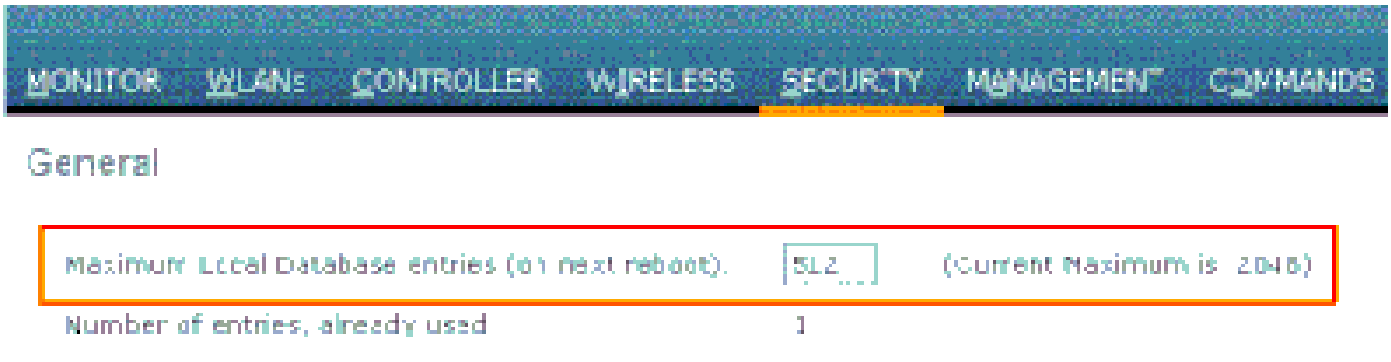
A.本地使用者資料庫在**安全**>**常規**頁面最多限制為2048個條目。此資料庫由本地管理使用者（包括接待大使）、網路使用者（包括訪客使用者）、MAC過濾器條目、存取點授權清單條目和排除清單條目共用。所有這些型別的使用者都不能超過配置的資料庫大小。

要增加本地資料庫，請從CLI使用以下命令：

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```



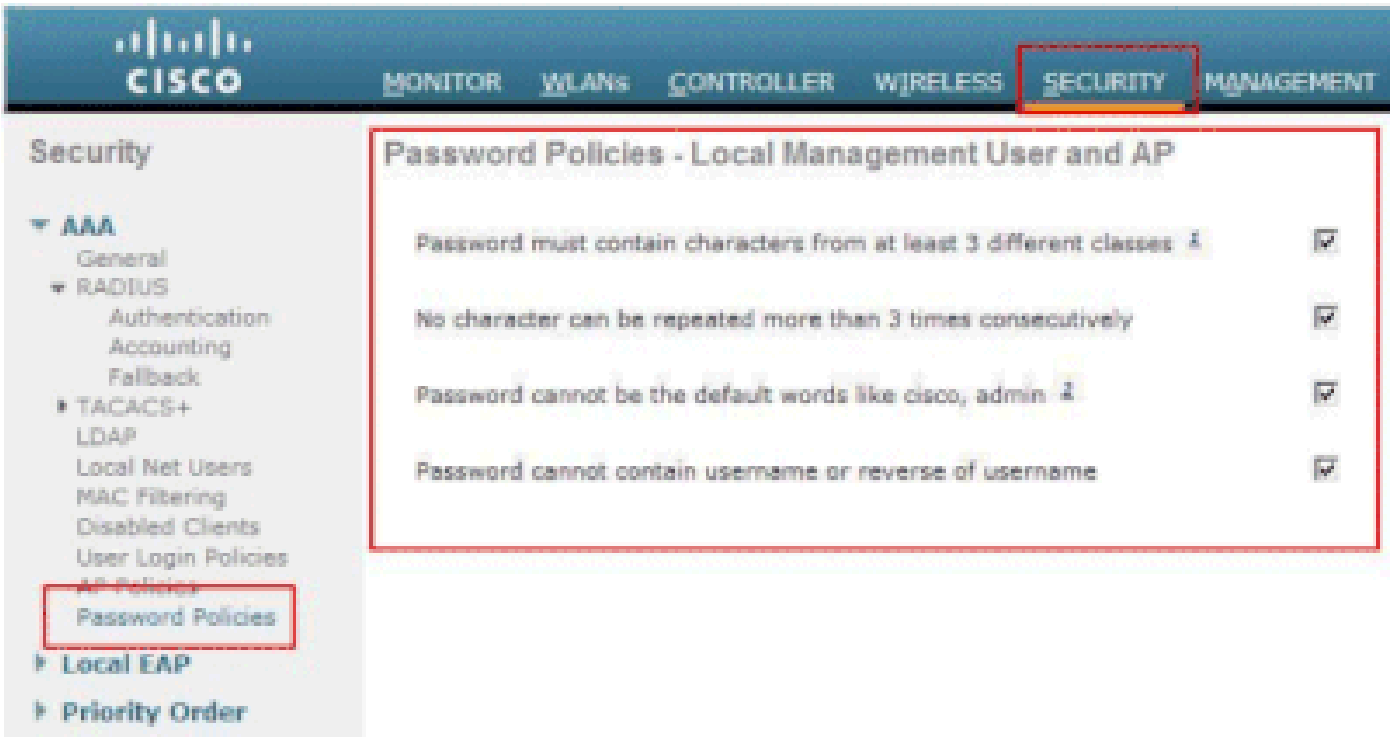
附註：您必須儲存組態並重設系統（使用reset system指令），變更才會生效。



問題： 如何在WLC上強制執行強密碼策略？

A.WLC允許您定義強密碼策略。可以使用CLI或GUI來完成此操作。

在GUI中，轉至**Security** > **AAA** > **Password Policies**。此頁面包含一系列選項，您可以選取這些選項來強制使用強式密碼。以下是範例：



問題： 無線區域網控制器上如何使用被動客戶端功能？

答：被動客戶端是無線裝置，例如配置了靜態IP地址的刻度和印表機。當這些客戶端與存取點關聯時，它們不會傳輸任何IP資訊，例如IP地址、子網掩碼和網關資訊。因此，使用被動客戶端時，除非使用DHCP，否則控制器永遠不會知道IP地址。

WLC當前充當ARP請求的代理。在收到ARP請求後，控制器會以ARP響應作出響應，而不是直接將請求傳遞給客戶端。此方案有兩個優點：

- 將ARP請求傳送到客戶端的上游裝置無法知道客戶端的位置。
-

電池操作裝置（如行動電話和印表機）的電源被保留，因為它們不必響應每個ARP請求。

由於無線控制器沒有任何有關被動客戶端的IP相關資訊，因此無法響應任何ARP請求。當前行為不允許將ARP請求傳輸到被動客戶端。任何嘗試訪問被動客戶端的應用程式都可能失敗。

被動客戶端功能允許在有線和無線客戶端之間交換ARP請求和響應。啟用此功能後，控制器就可以將來自有線客戶端的ARP請求傳遞到無線客戶端，直到所需的無線客戶端進入RUN狀態。

有關如何配置被動客戶端功能的資訊，請參閱Cisco無線LAN控制器配置指南7.0.116.0版中使用GUI配置被動客戶端部分。

問題： 如何設定使用者端每三分鐘或在任何指定的時間週期重新驗證RADIUS伺服器？

答：WLC上的會話超時引數可用於完成此操作。預設情況下，會話超時引數配置為1800秒，然後再進行身份驗證。

將此值變更為180秒，讓使用者端在三分鐘後重新進行驗證。

要訪問會話超時引數，請按一下GUI中的**WLANs**選單。它顯示在WLC中配置的WLAN的清單。按一下客戶端所屬的WLAN。轉到高級**< span**> 頁籤並找到啟用會話Timeoutparameter。將預設值更改為180，並按一下**Apply** 以使更改生效。

當以Access-Accept和RADIUS-Request的Termination-Action值傳送時，Session-Timeout屬性指定重新身份驗證前提供的服務的最大秒數。在這種情況下，Session-Timeout屬性用於在802.1X的重新身份驗證計時器狀態機中載入ReAuthPeriod常數。

問題： 我有一個訪客通道Ethernet over IP (EoIP)通道，它是在4400無線LAN控制器(WLC)（作為錨點WLC）與多個遠端WLC之間設定的。此錨點WLC能否透過EoIP隧道將子網廣播從有線網路轉發到與遠端控制器關聯的無線客戶端？

答：不，WLC 4400不會透過EoIP隧道將IP子網廣播從有線端轉發到無線客戶端。這不是支援的功能。在訪客接入拓撲中，Cisco不支援子網廣播或組播的隧道。由於訪客WLAN強制客戶端的入網點位於網路中非常特定的位置（大多數位於防火牆外部），因此子網廣播的隧道傳輸可能會帶來安全問題。

問題： 在無線LAN控制器(WLC)和輕量存取點通訊協定(LWAPP)設定中，會針對語音流量傳遞什麼差分服務代碼點(DSCP)值？如何在WLC上實施QoS？

答：Cisco Unified Wireless Network (UWN)解決方案WLAN支援四個級別的QoS：

- 白金/語音
- 金牌/影片
- 銀牌/盡力而為（預設）
- 銅色/背景

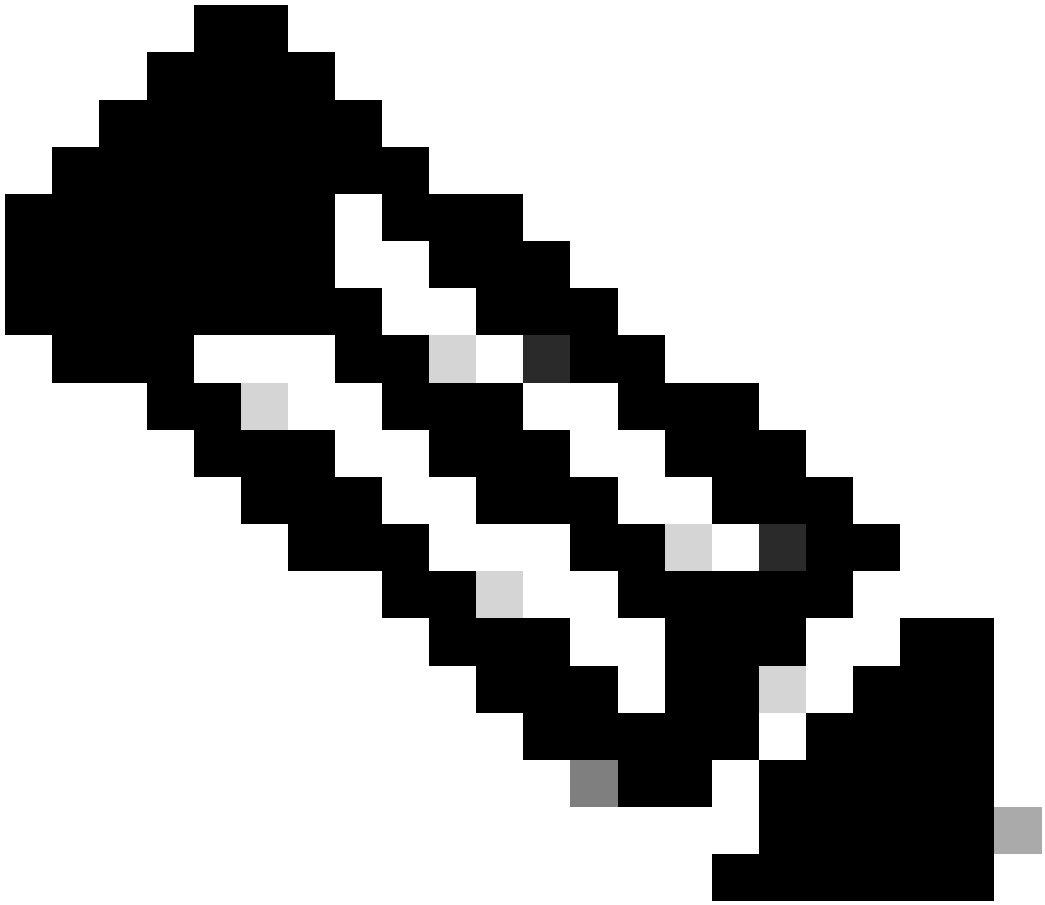
您可以將語音流量WLAN配置為使用白金QoS，將低頻寬WLAN配置為使用銅牌QoS，並在其他QoS級別之間分配所有其他流量。有關詳細資訊，請參閱為WLAN分配QoS配置檔案。

問：Cisco無線統一解決方案是否支援Linksys乙太網網橋？

答：不，WLC僅支援Cisco WGB產品。不支援Linksys WGB。雖然Cisco Wireless Unified Solution不支援Linksys WET54G和WET11B乙太網網橋，但如果您使用以下指南，則可以在無線統一解決方案配置中使用這些裝置：

- 僅將一個裝置連線到WET54G或WET11B。

- 啟用WET54G或WET11B上的MAC克隆功能以克隆連線的裝置。
- 在連線到WET54G或WET11B的裝置上安裝最新的驅動程式和韌體。本指南對JetDirect印表機特別重要，因為舊版的韌體會導致DHCP發生問題。



注意：不支援其他第三方網橋。其他第三方網橋也可以嘗試上述步驟。

問題： 如何在無線LAN控制器(WLC)上儲存組態檔？

A. WLC包含兩種記憶體：

- Volatile RAM -保留當前的活動控制器配置
- 非易失性RAM (NVRAM) -保留重新啟動配置

在WLC中配置作業系統時，您修改的是易失性RAM。您必須將來自易失性RAM的組態儲存到NVRAM，才能確保WLC以目前的組態重新啟動。

當您執行下列工作時，必須知道要修改哪些記憶體：

- 使用配置嚮導。
- 清除控制器組態。

- 儲存配置。
- 重設控制器。
- 從CLI註銷。

WLC功能常見問題解答

問：如何在無線LAN控制器(WLC)上設定可延伸驗證通訊協定(EAP)型別？我想要根據訪問控制伺服器(ACS)裝置進行身份驗證，並且我在日誌中看到「不支援的EAP」型別。

A. WLC上沒有單獨的EAP型別設定。對於輕量EAP (LEAP)、透過安全通道的EAP彈性驗證(EAP-FAST)或Microsoft保護的EAP (MS-PEAP)，只要設定IEEE 802.1x或Wi-Fi保護的存取(WPA)（如果您使用802.1x搭配WPA）。RADIUS後端和客戶端上支援的任何EAP型別都透過802.1x標籤受支援。使用者端和RADIUS伺服器上的EAP設定必須相符。

完成以下步驟，以便透過WLC上的GUI啟用EAP：

1. 從WLC GUI中，按一下**WLANs**。
2. 將會顯示WLC中配置的WLAN清單。按一下某個WLAN。
3. 在**WLANs** > **Edit**中，按一下**Security**頁籤。
4. 按一下**Layer 2**，然後選擇Layer 2 Security作為802.1x或WPA+WPA2。您也可以設定可在同一視窗中使用的802.1x引數。然後，WLC在無線客戶端和身份驗證伺服器之間轉發EAP身份驗證資料包。
5. 按一下**AAA**伺服器，然後從此WLAN的下拉選單中選擇認證伺服器。我們假設已全域設定驗證伺服器。

問題： 什麼是快速SSID更改？

A.Fast SSID更改允許客戶端在SSID之間移動。當客戶端傳送其他SSID的新關聯時，控制器連線表中的客戶端條目會被清除，然後客戶端才會增加到新的SSID中。停用快速SSID更改時，控制器會在允許客戶端移動到新SSID之前實施延遲。有關如何啟用快速SSID更改的資訊，請參閱Cisco無線LAN控制器配置指南7.0.116.0版中的「配置快速SSID更改」部分。

問題： 我是否可以對可以連線到無線LAN的客戶端數量設定限制？

答：您可以設定可連線至WLAN的從屬端數量限制，這在可連線至控制器的從屬端數量有限的情況下非常有用。您可以為每個WLAN配置的客戶端數量取決於您使用的平台。

請參閱《Cisco無線區域網控制器配置指南7.0.116.0版》中的「配置每個WLAN的最大客戶端數」一節，瞭解無線區域網控制器不同平台的每個WLAN的客戶端限制資訊。

問題： 什麼是PKC，以及它如何與無線LAN控制器(WLC)搭配使用？

A. PKC代表主動式金鑰快取。它被設計為802.11i IEEE標準的擴展。

PKC是Cisco 2006/410x/440x系列控制器中啟用的一種功能，它允許正確配備的wireleTalk與Tech Writer進行相關操作。ss客戶端無需使用AAA伺服器進行完全重新身份驗證即可漫遊。要瞭解PKC，首先需要了解金鑰快取。

金鑰快取是增加到WPA2的功能。這允許移動站快取它透過存取點(AP)的成功身份驗證獲得的主金鑰（成對主金鑰[PMK]），並**在將來與相同AP的關聯中重複使用它**。這意味著給定流動裝置需要向特定AP驗證一次，並快取金鑰以供將來使用。金鑰快取透過稱為PMK識別符號(PMKID)的機制來處理，PMK是PMK、字串、站點和AP的MAC地址的雜湊。PMKID可唯一辨識PMK。

即使使用金鑰快取，無線站台也必須向希望獲得服務的每個AP進行身份驗證。這會帶來嚴重的延遲和開銷，這會延遲移交過程，並會抑制支援即時應用程式的能力。為了解決此問題，在WPA2中引入了PKC。

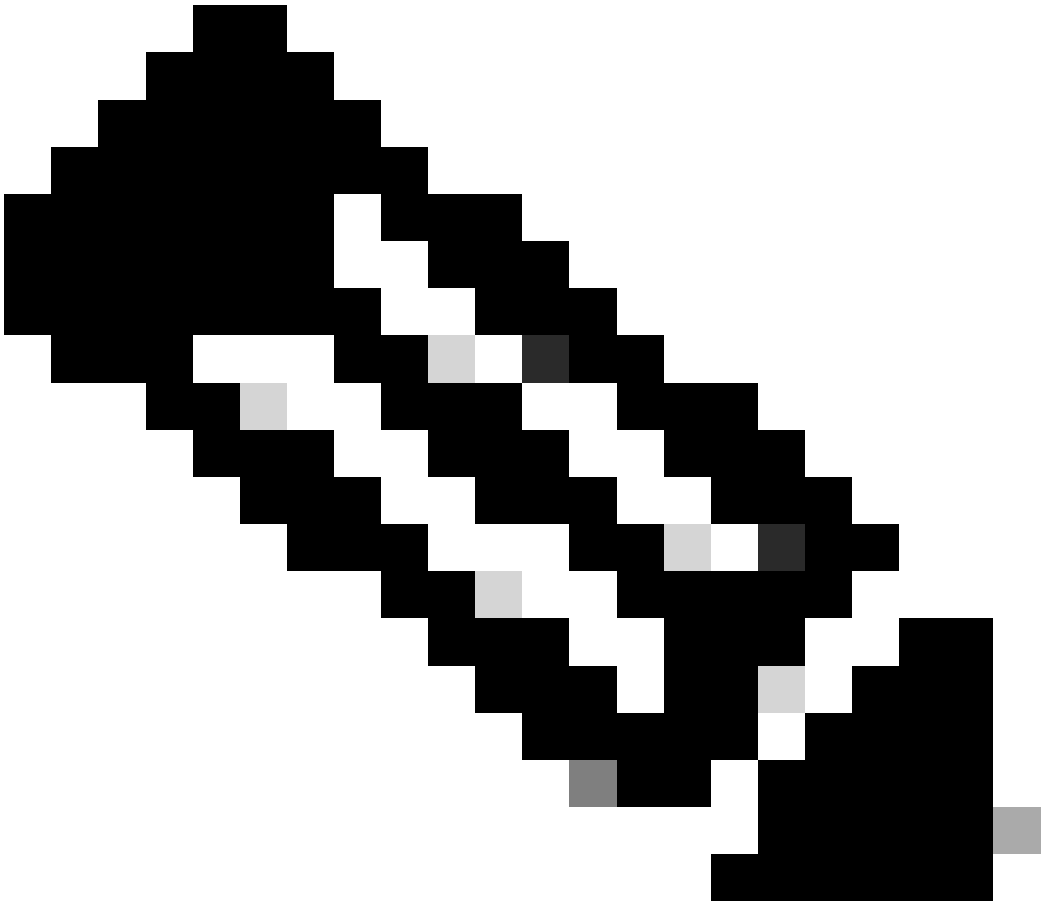
PKC可讓站台重複使用先前透過成功驗證程式獲得的PMK。這樣，在漫遊時，月台就無需對新的AP進行身份驗證。

因此，在控制器內漫遊中，當流動裝置在同一控制器上從一個AP移動到另一個AP時，客戶端使用以前使用的PMK重新計算PMKID，並在關聯過程中顯示它。WLC會搜尋其PMK快取記憶體，以判斷它是否有此類專案。如果是，它會繞過802.1x驗證程式並

立即啟動WPA2金鑰交換。如果沒有，它會透過標準的802.1X驗證程式。

預設情況下，PKC與WPA2一起啟用。因此，當您在WLC的WLAN配置下啟用WPA2作為第2層安全時，WLC上就會啟用PKC。此外，請配置AAA伺服器和無線客戶端進行相應的EAP身份驗證。

使用者端使用的請求者也必須支援WPA2，才能讓PKC運作。PKC也可以在控制器間漫遊環境中實作。

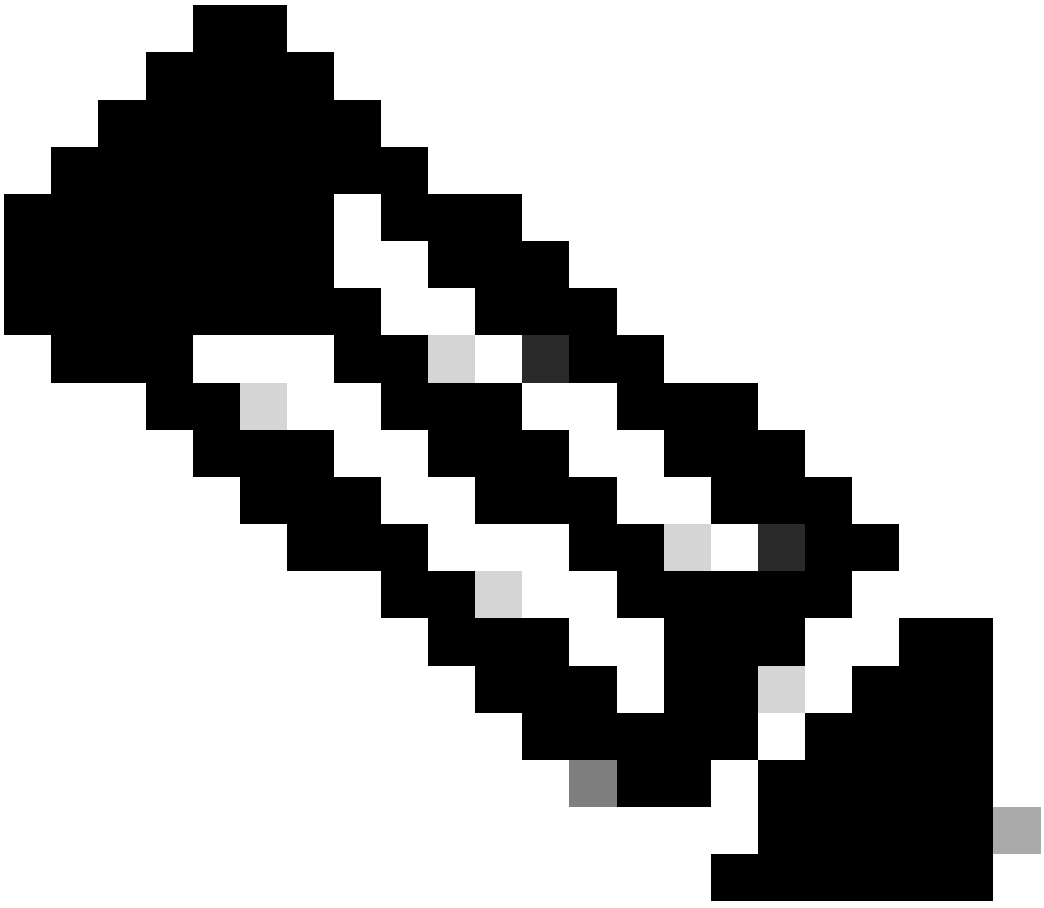


注意：PKC無法與Aironet Desktop Utility (ADU)一起作為客戶端請求方使用。

問題： 控制器上這些逾時設定的說明是什麼：位址解析通訊協定(ARP)逾時、使用者閒置逾時和作業階段逾時？

A.ARP超時用於刪除WLC上從網路中獲知的裝置的ARP條目。

TheUser Idle Timeout：當使用者在設定為User Idle Timeout的時間內未與LAP進行任何通訊而處於空閒狀態時，客戶端將由WLC取消身份驗證。使用者端必須重新驗證並重新與WLC關聯。它用於客戶端在不通知LAP的情況下從其關聯的LAP中退出的情況。如果使用者端上的電池停止運作，或使用者端連絡人移開，就可能會發生這種情況。



注意：要在WLC GUI上訪問ARP Timeout和User Idle Timeout，請轉到Controller選單。選擇左側的General以查詢ARP和User Idle

---

Timeout欄位。

Session Timeout是客戶端與WLC之間的會話的最長時間。在這段時間後，WLC會對使用者端進行解除驗證，而使用者端會再次進行整個驗證（重新驗證）程式。這是旋轉加密金鑰的安全預防措施的一部分。如果您使用具有金鑰管理的可延伸驗證通訊協定(EAP)方法，則會在每個固定間隔執行金鑰重建作業，以便衍生新的加密金鑰。如果沒有金鑰管理，此超時值是無線客戶端需要執行完全重新身份驗證的時間。會話超時是特定於WLAN的。此引數可從**WLANs**>編輯功能表存取。

問題： 何謂RFID系統？Cisco目前支援哪些RFID標籤？

A.射頻辨識(RFID)是一種使用射頻通訊來進行較短距離通訊的技術。一種基本RFID系統由RFID標籤、RFID讀取器和處理軟體組成。

目前，思科支援來自AeroScout和Pango的RFID標籤。有關如何配置AeroScout標籤的詳細資訊，請參閱《AeroScout RFID標籤的WLC配置》。

問題： 是否可以在WLC上本地執行EAP身份驗證？是否有說明此本地EAP功能的文檔？

答：是，EAP身份驗證可在WLC上本地執行。本地EAP是一種身份驗證方法，它允許使用者和無線客戶端在WLC上進行本地身份驗證。本產品專為遠端辦公室所設計，可在後端系統中斷或外部驗證伺服器故障時，維持與無線使用者端的連線能力。啟用本地EAP時，WLC充當身份驗證伺服器。有關如何為本地EAP-Fast身份驗證配置WLC的詳細資訊，請參閱使用EAP-FAST和LDAP伺服器在無線區域網控制器上配置本地EAP身份驗證的示例。

問題： WLAN覆蓋功能是什麼？如何配置此功能？當LAP故障切換到備份WLC時，LAP是否可以維護WLAN覆蓋值？

A. WLAN覆蓋功能使我們能夠從WLC上配置的WLAN中選擇WLAN，這些WLAN可針對單個LAP主動使用。要配置WLAN覆蓋，請完成以下步驟：

1. 在WLC GUI中，按一下**Wireless**選單。

2. 按一下左側的**Radios**選項並選擇**802.11 a/n**或**802.11 b/g/n**。

3. 在右側的下拉選單中按一下與要在其上配置WLAN覆蓋的AP名稱相對應的**Configure**連結。

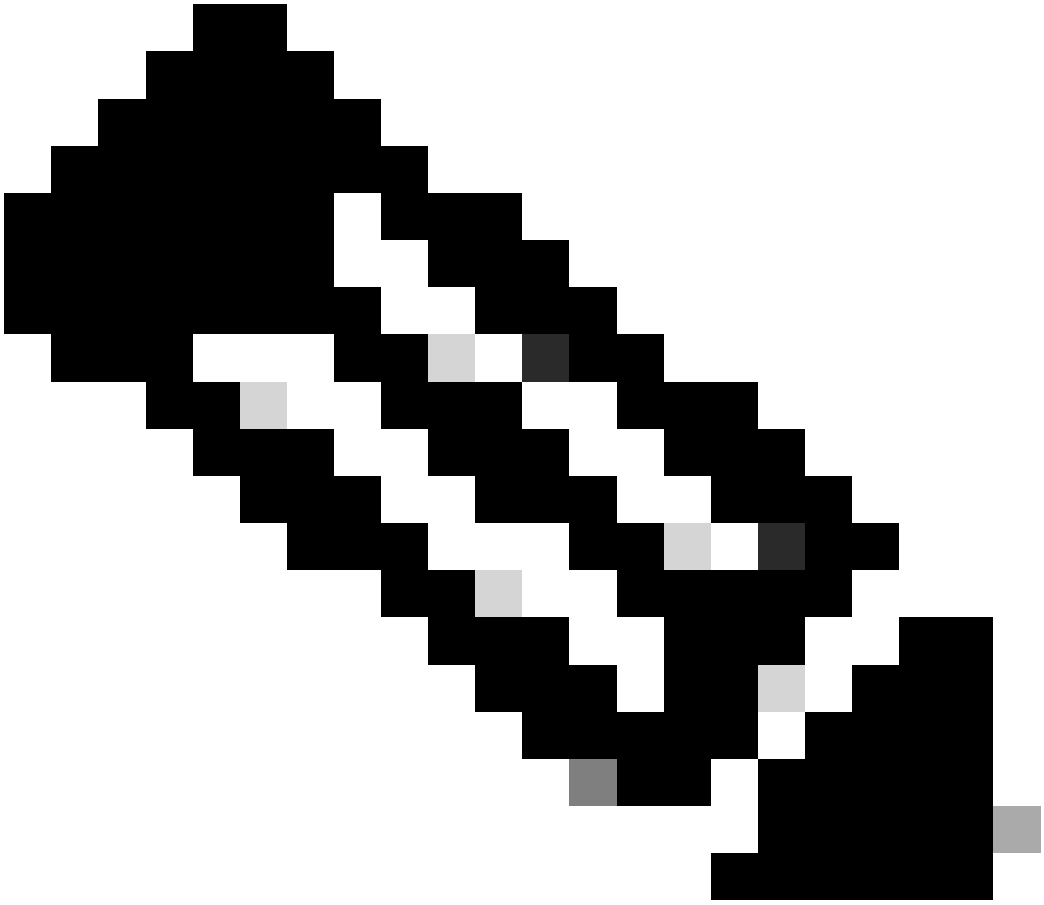
4. 從WLAN Override下拉選單中選擇**Enable**。WLAN Override選單是窗口左側的最後一個專案。

5. 將會顯示WLC上配置的所有WLAN的清單。

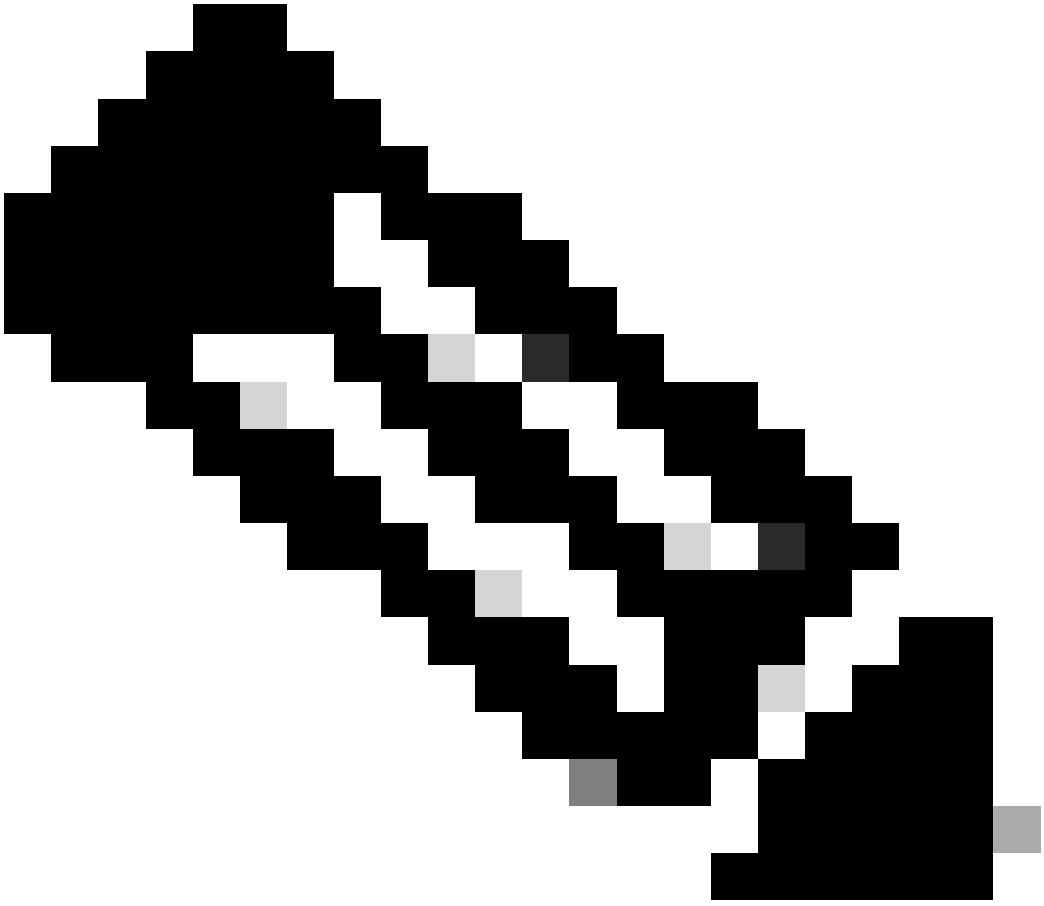
6. 在此清單中，選中要顯示在LAP上的**WLAN**，然後按一下**Apply**使更改生效。

7. 進行這些更改後儲存配置。

如果WLAN配置檔案和SSID是跨所有WLC配置的，則AP會在註冊到其他WLC時保留WLAN覆蓋值。



注意：在控制器軟體版本5.2.157.0中，WLAN覆蓋功能已從控制器GUI和CLI中刪除。如果您的控制器設定為WLAN覆寫，且您升級為控制器軟體版本5.2.157.0，則控制器會刪除WLAN組態並廣播所有WLAN。如果配置存取點組，可以指定僅傳輸某些WLAN。每個存取點僅通告屬於其存取點組的已啟用的WLAN。



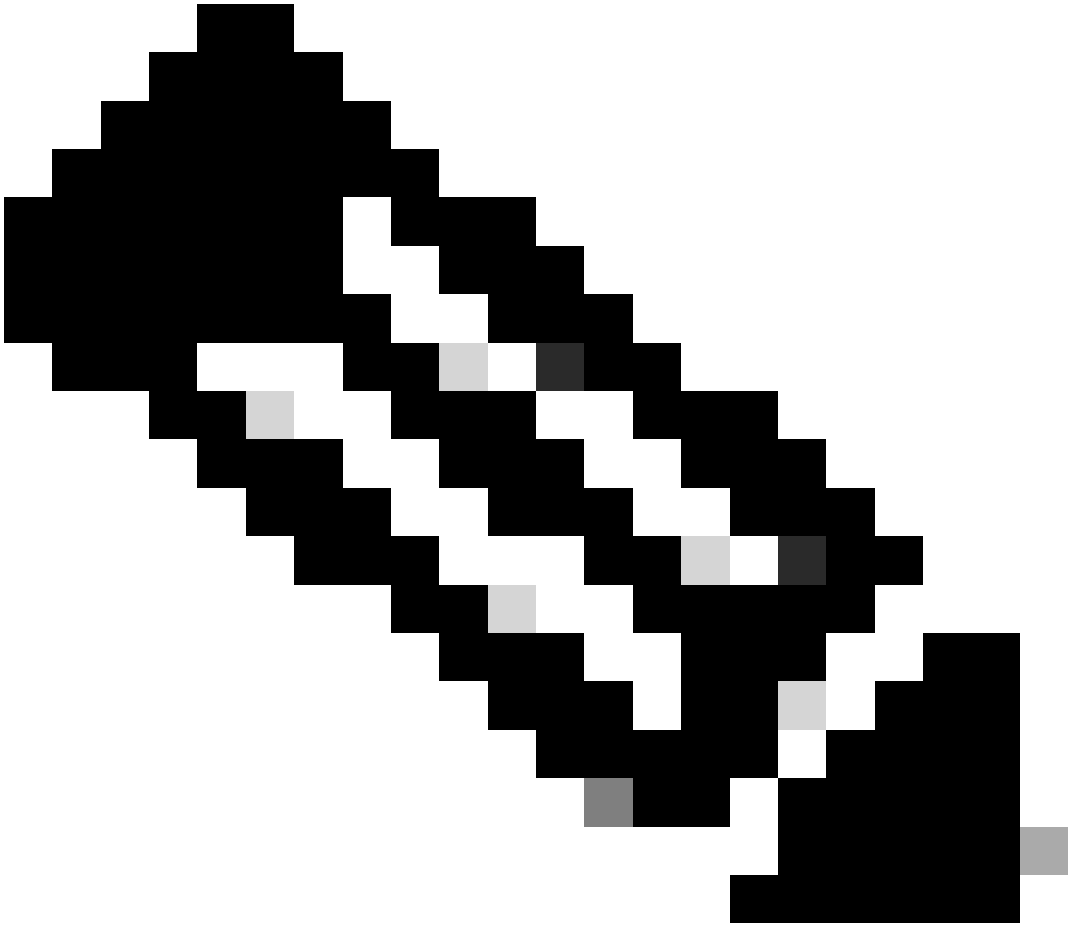
注意：存取點組無法讓WLAN在AP的每個無線介面上傳輸。

問題： 思科無線區域網控制器(WLC)和輕量存取點(LAP)是否支援IPv6？

答：目前，4400和4100系列控制器僅支援IPv6使用者端傳輸。不支援本地IPv6支援。

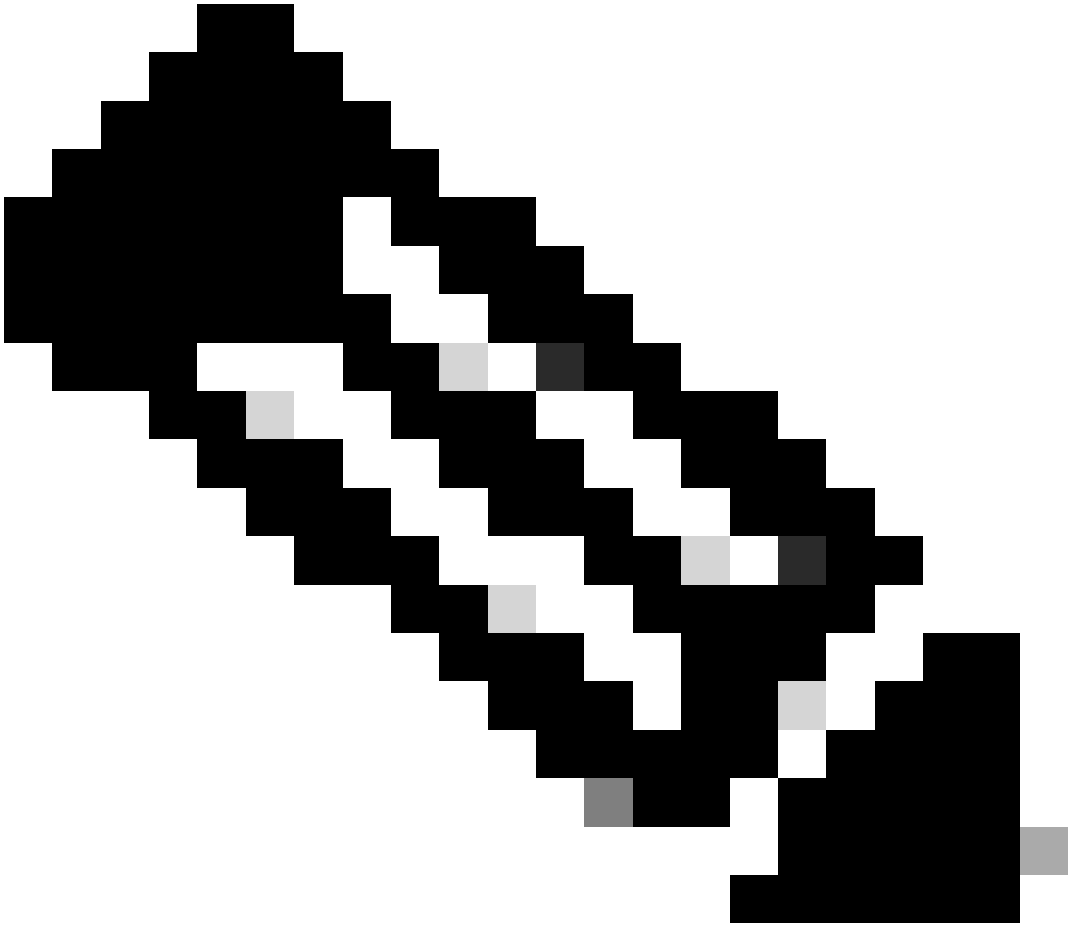
要在WLC上啟用IPv6，請在WLAN > Edit頁面的WLAN SSID配置下選中**IPv6 Enable**覈取方塊。

此外，支援IPv6還需要乙太網組播模式(EMM)。如果停用EMM，則使用IPv6的客戶端裝置會失去連線。要啟用EMM，請轉到Controller > General頁面並從Ethernet Multicast Mode下拉選單中選擇**Unicast**或**Multicast**。這樣可在單播模式或組播模式下啟用組播。當組播作為組播單播啟用時，將為每個AP複製資料包。這可能需要大量處理器，因此請謹慎使用。作為組播組播啟用的組播使用使用者分配的組播地址，向存取點(AP)進行更傳統的組播。



注意：2006控制器不支援IPv6。

此外，還存在思科漏洞ID CSCsg78176，在使用AAA覆蓋功能時，該漏洞可阻止使用IPv6直通。



注意：只有已註冊的思科使用者才能訪問內部思科工具和資訊。

問題： Cisco 2000系列無線區域網控制器(WLC)是否支援訪客使用者的Web身份驗證？

A. 所有Cisco WLC都支援Web身份驗證。Web驗證是一種第3層驗證方法，用於以簡單驗證憑證驗證使用者。不涉及加密。完成以下步驟即可啟用此功能：

1. 在GUI中，按一下**WLAN選單**。

2. 按一下某個**WLAN**（無線LAN）。

3. **轉到Security頁籤並選擇Layer 3**。

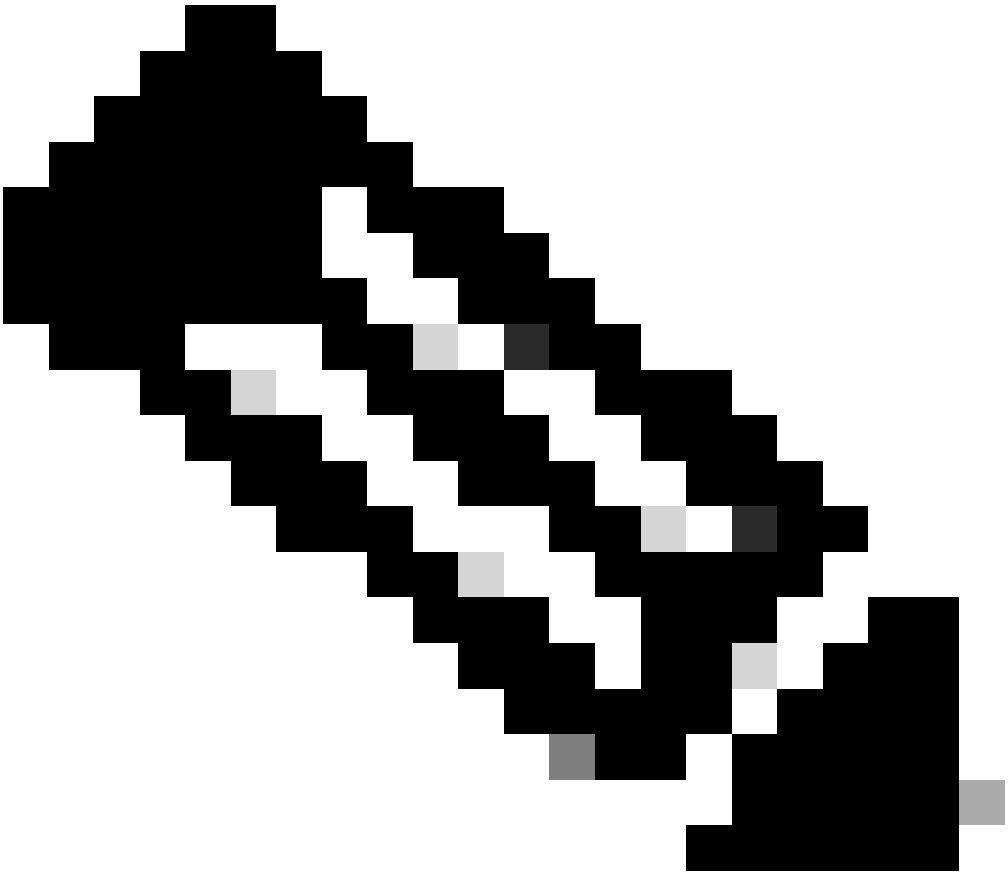
4. **選中Web Policy框並選擇Authentication**。

5. 按一下**Apply** 以儲存更改。

6. 要在WLC上建立用於認證使用者的資料庫，請轉到GUI中的**Security選單並選擇Local Net User< /strong>，然後完成以下操作**：

    a. 定義訪客用於登入的訪客使用者名稱和密碼。這些值區分大小寫。

    b. 選擇您使用的WLAN ID。



注意：如需詳細設定，請參閱無線LAN控制器Web驗證組態範例。

問題： 能否在無線模式下管理WLC？

答：啟用WLC後，可以透過無線模式對其進行管理。有關如何啟用無線模式的詳細資訊，請參閱思科無線LAN控制器配置指南7.0.116.0版的「啟用與GUI和CLI的無線連線」部分。

問題： 什麼是鏈路聚合(LAG)？如何在無線LAN控制器(WLC)上啟用LAG？

A.LAG將WLC上的所有埠捆綁到一個EtherChannel介面中。系統使用LAG動態管理流量負載均衡和埠冗餘。

通常，WLC上的介面有多個與其關聯的引數，包括IP地址、預設網關（用於IP子網）、主物理埠、輔助物理埠、VLAN標籤和DHCP伺服器。不使用LAG時，通常會將每個介面對映到物理埠，但也可以將多個介面對映到單個WLC埠。使用LAG時，系統動態地將介面對映到聚合埠通道。這有助於實現埠冗餘和負載均衡。當埠發生故障時，介面會動態對映到下一個可用的物理埠，並且跨埠平衡LAP。

在WLC上啟用LAG時，WLC會在收到資料幀的同一連線埠上轉送資料架構。WLC依賴鄰居交換機透過EtherChannel對流量進行負載均衡。WLC不會自行執行任何EtherChannel負載平衡。

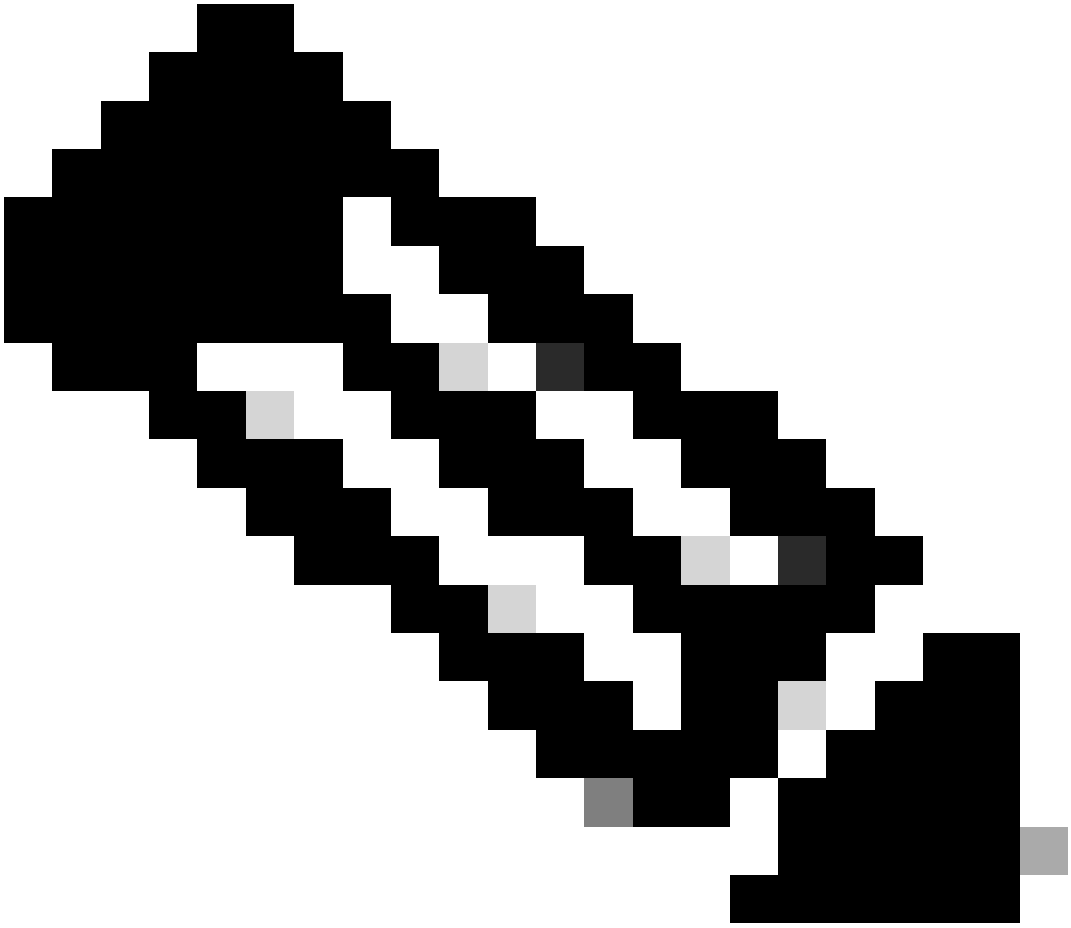
問題： 哪些型號的無線LAN控制器(WLC)支援連結集合(LAG)？

答：Cisco 5500系列控制器在軟體版本6.0或更高版本中支援LAG，Cisco 4400系列控制器在軟體版本3.2或更高版本中支援LAG，並且Cisco WiSM和Catalyst 3750G整合無線LAN控制器交換機內的控制器上自動啟用LAG。如果沒有LAG，Cisco 4400系列控制器上的每個分散式系統埠最多支援48個存取點。啟用LAG後，Cisco 4402控制器邏輯埠支援最多50個存取點，Cisco 4404控制器邏輯埠支援最多100個存取點，Catalyst 3750G整合無線LAN控制器交換機上的邏輯埠和每個Cisco WiSM控制器上的邏輯埠支援最多150個存取點。

Cisco 2106和2006 WLC不支援LAG。早期型號（如Cisco 4000系列WLC）不支援LAG。

問題： 統一無線網路中的自動錨點移動功能是什麼？

答：自動錨點移動性（或訪客WLAN移動性）用於改進無線LAN (WLAN)上漫遊客戶端的負載均衡和安全性。在正常漫遊情況下，客戶端裝置會加入WLAN並錨定到它們所連線的第一個控制器。如果客戶端漫遊到不同的子網，客戶端所漫遊到的控制器會為客戶端與錨點控制器建立外部會話。使用自動錨點行動功能時，您可以指定控制器或一組控制器作為WLAN上使用者端的錨點。



注意：不能為第3層移動性配置移動錨點。行動錨點僅用於訪客通道。

問題： 能否將Cisco 2006無線區域網控制器(WLC)配置為無線區域網的錨點？

答：Cisco 2000系列WLC無法指定為WLAN的錨點。但是，在Cisco 2000系列WLC上建立的WLAN可以將Cisco 4100系列WLC和Cisco 4400系列WLC作為其錨點。

問題： 無線LAN控制器使用哪種型別的移動隧道？

A.控制器軟體版本4.1到5.1支援非對稱和對稱行動通道。控制器軟體版本5.2或更新版本僅支援對稱行動通道，此模式現在一律會預設啟用。

在非對稱通道中，通往有線網路的使用者端流量會直接透過外部控制器路由。當上游路由器啟用反向路徑過濾(RPF)時，非對稱隧道會中斷。在這種情況下，路由器會丟棄客戶端流量，因為RPF檢查可確保返回源地址的路徑與資料包的來源路徑匹配。

啟用對稱移動隧道時，所有客戶端流量都將傳送到錨點控制器，然後可以成功透過RPF檢查。對稱移動隧道在以下情況下也非常有用：

- 如果客戶端資料包路徑中的防火牆安裝由於源IP地址與接收資料包的子網不匹配而丟棄資料包，則此操作很有用。
- 如果錨點控制器上的存取點組VLAN與外部控制器上的WLAN介面VLAN不同：在這種情況下，客戶端流量可能會在移動事件期間傳送到不正確的VLAN上。

問題： 當網路關閉時，如何存取WLC？

答：當網路發生故障時，服務埠可以訪問WLC。此埠分配的IP地址與WLC的其他埠完全不同，因此稱為帶外管理。有關詳細資訊，請參閱《Cisco無線LAN控制器配置指南7.0.116.0版》中的「配置埠和介面」部分。

問題： Cisco無線區域網控制器(WLC)是否支援故障切換（或冗餘）功能？

A.是，如果您的WLAN網路中有兩個或多個WLC，則您可以配置它們以實現冗餘。通常，LAP會連線到已配置的主WLC。一旦主WLC發生故障，LAP將重新啟動並加入移動組中的另一個WLC。故障切換是一種功能，其中LAP輪詢主WLC並在主WLC運行後加入主WLC。有關詳細資訊，請參閱輕量存取點的WLAN控制器故障切換配置示例。

問題： 預先驗證存取控制清單(ACL)在無線LAN控制器(WLC)中的用途為何？

A.使用預身份驗證ACL（顧名思義），即使在客戶端身份驗證之前，您也可以允許客戶端資料流出入特定IP地址。使用外部Web伺服器進行Web驗證時，某些WLC平台需要外部Web伺服器（Cisco 5500系列控制器、Cisco 2100系列控制器、Cisco 2000系列和控制器網路模組）的預驗證ACL。對於其他WLC平台，預身份驗證ACL不是必需的。但是，在使用外部Web身份驗證時，為外部Web伺服器配置預身份驗證ACL是很好的做法。

問題： 我的網路中有一個MAC過濾的WLAN和一個完全開放的WLAN。客戶端是否預設選擇開放的WLAN？或者，客戶端是否自動與MAC過濾器上設定的WLAN ID關聯？此外，為什麼MAC過濾器上有「interface」選項？

A.客戶端可以與客戶端配置為連線的任何WLAN關聯。MAC過濾器中的interface選項使您可以將過濾器應用於WLAN或介面。如果多個WLAN繫結到同一介面，則您可以將MAC過濾器應用於該介面，而無需為每個單獨的WLAN建立過濾器。

問題： 如何在無線LAN控制器(WLC)上為管理使用者設定TACACS驗證？

A. 從WLC版本4.1開始，WLC支援TACACS。請參閱配置TACACS+以瞭解如何配置TACACS+以驗證WLC的管理使用者。

問題： 在無線LAN控制器(WLC)中，過度驗證失敗設定有何用途？

A.此設定是客戶端排除策略之一。使用者端排除是控制器上的安全功能。此策略用於排除客戶端，以防止非法訪問網路或攻擊無線網路。

啟用這個過度Web驗證失敗原則後，當使用者端嘗試失敗Web驗證的次數超過5時，控制器會認為使用者端已超過Web驗證的嘗試上限，並將使用者端排除在外。

完成以下步驟以啟用或停用此設定：

1. 從WLC GUI中，轉到**Security > Wireless Protection Policies > Client Exclusion Policies** 。
2. 選中或取消選中**Excessive Web Authentication Failures**。

問題： 我已經將我的自主存取點(AP)轉換為輕量模式。在使用用於客戶端記賬的AAA RADIUS伺服器的輕量AP協定(LWAPP)模式下

，通常根據WLC的IP地址使用RADIUS記賬來跟蹤客戶端。能否根據與該WLC關聯的AP的MAC地址而不是WLC的IP地址來設定RADIUS記帳？

A.是，這可以用WLC端配置完成。請完成以下步驟：

1. 在控制器GUI中的**Security** > **Radius Accounting**下，有一個「Call Station ID Type」下拉框。選擇**AP MAC Address**。
2. 透過LWAPP AP日誌進行驗證。您可以在此處檢視被叫站ID欄位，該欄位顯示與特定客戶端關聯的AP的MAC地址。

問題： 如何透過CLI變更無線LAN控制器(WLC)上的Wi-Fi保護存取(WPA)交握逾時值？我知道我可以在Cisco IOS存取點(AP)上使用**dot11 wpa handshake timeoutvalue**命令進行此項更改，但如何在WLC上執行此操作？

A.軟體版本4.2及更高版本中整合了透過WLC配置WPA握手超時的能力。在舊版WLC軟體中，不需要此選項。

以下命令可用於更改WPA握手超時：

<#root>

config advanced eap eapol-key-timeout

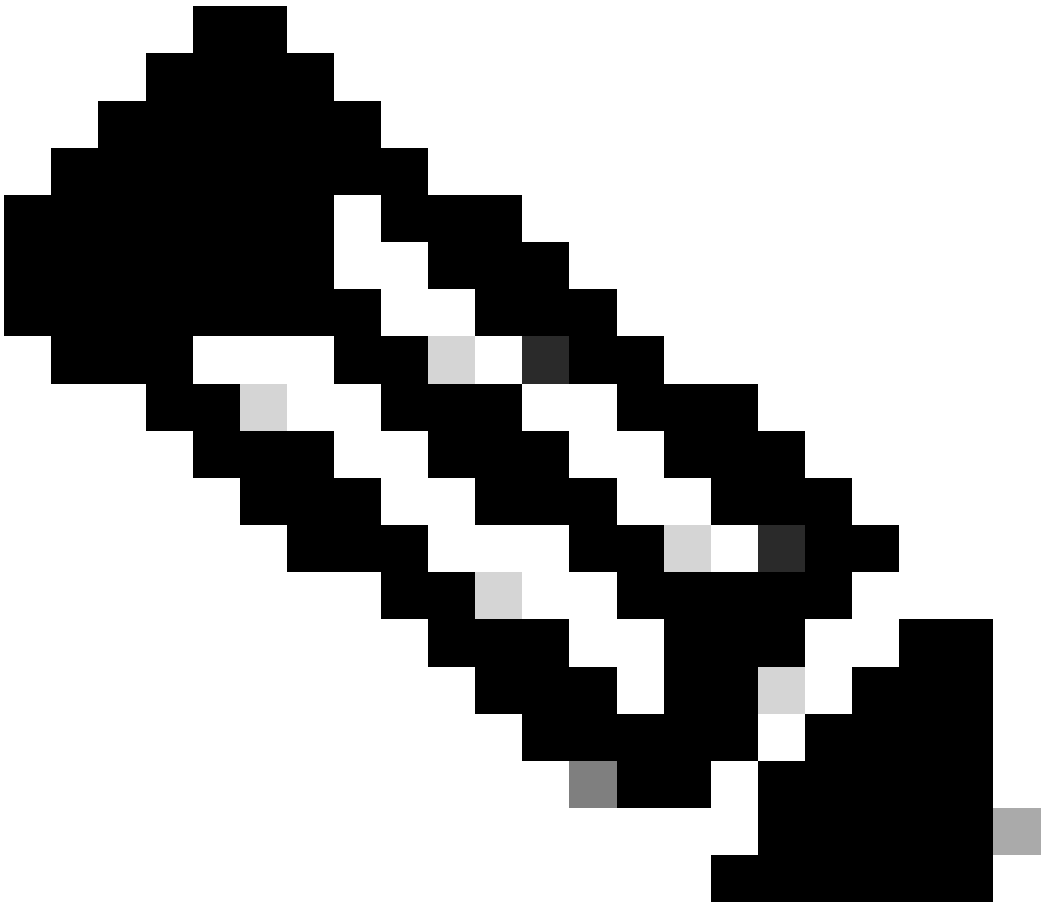
<value>

config advanced eap eapol-key-retries

<value>

預設值會繼續反映WLC目前的行為。

- the default value for eapol-key-timeout is 1 second.
- the default value for eapol-key-retries is 2 retries



注意：在Cisco IOS AP上，可使用dot11 wpa handshake命令配置此設定。

您還可以使用**config advanced eap** 命令下的選項配置其他EAP引數。

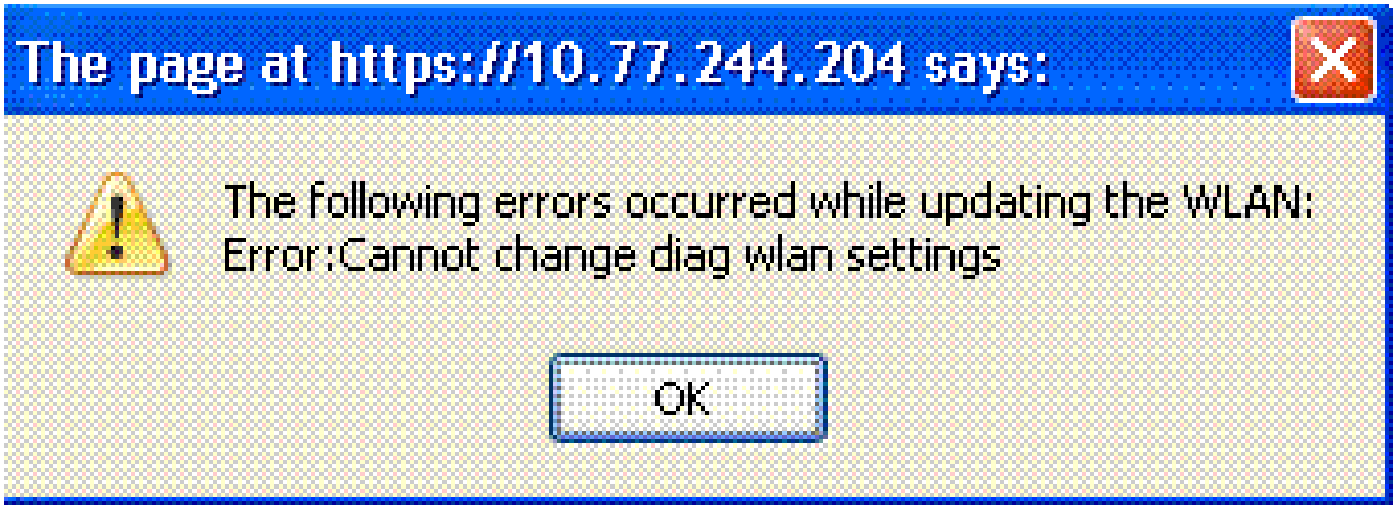
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

問題： **WLAN > Edit > Advanced**頁面上的診斷通道功能有何用途？

A.診斷通道功能使您能夠排查與WLAN相關的客戶端通訊問題。使用者端和存取點可以經過一組定義的測試，以辨識使用者端遭遇通訊困難的原因，然後允許採取修正措施來讓使用者端在網路上運作。可以使用控制器GUI或CLI啟用診斷通道，也可以使用控制器CLI或WCS運行診斷測試。

診斷通道只能用於測試。如果您嘗試在啟用診斷通道的情況下為WLAN設定驗證或加密，將會看到以下錯誤：



問題： WLC上可配置的AP組的最大數目是多少？

A. 此清單顯示可在WLC上配置的AP組的最大數量：

- Cisco 2100系列控制器和控制器網路模組最多支援50個存取點組
- Cisco 4400系列控制器、Cisco WiSM和Cisco 3750G無線LAN控制器交換機的存取點組數最多為300個
- 思科5500系列控制器最多支援500個存取點組

相關資訊

- **無線區域網路控制器(WLC)錯誤和系統訊息常見問題**
- **輕量存取點常見問題解答**
- **無線區域網控制器上的IPv6支援**
- **無線產品支援**
- **思科技術支援與下載**

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）。