

Flex 7500無線分支機構控制器部署指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[產品概觀](#)

[產品規格](#)

[產品介紹](#)

[平台功能](#)

[Flex 7500啟動](#)

[Flex 7500授權](#)

[AP基本計數許可](#)

[AP升級許可](#)

[軟體版本支援](#)

[支援的存取點](#)

[FlexConnect架構](#)

[集中接入點控制流量的優點](#)

[分配客戶端資料流量的優點](#)

[FlexConnect操作模式](#)

[WAN要求](#)

[無線分支機構網路設計](#)

[主要設計要求](#)

[概觀](#)

[優勢](#)

[解決分支機構網路設計問題的功能](#)

[IPv6支援清單](#)

[功能表](#)

[AP組](#)

[來自WLC的組態](#)

[摘要](#)

[FlexConnect組](#)

[FlexConnect組的主要目標](#)

[從WLC進行FlexConnect組配置](#)

[使用CLI驗證](#)

[FlexConnect VLAN覆蓋](#)

[摘要](#)

[程式](#)

[限制](#)

[FlexConnect VLAN型中央交換](#)

[摘要](#)

[程式](#)

[限制](#)

[FlexConnect ACL](#)

[摘要](#)

[程式](#)

[限制](#)

[FlexConnect分割通道](#)

[摘要](#)

[程式](#)

[限制](#)

[容錯能力](#)

[摘要](#)

[限制](#)

[每個WLAN的客戶端限制](#)

[主要目標](#)

[限制](#)

[WLC組態](#)

[NCS配置](#)

[點對點封鎖](#)

[摘要](#)

[程式](#)

[限制](#)

[AP預映像下載](#)

[摘要](#)

[程式](#)

[限制](#)

[FlexConnect智慧AP映像升級](#)

[摘要](#)

[程式](#)

[限制](#)

[在FlexConnect模式下自動轉換AP](#)

[手動模式](#)

[自動轉換模式](#)

[適用於本機交換WLAN的FlexConnect WGB/uWGB支援](#)

[摘要](#)

[程式](#)

[限制](#)

[支援更多的Radius伺服器](#)

[摘要](#)

[程式](#)

[限制](#)

[增強型區域模式\(ELM\)](#)

[Flex 7500中的訪客存取支援](#)

[從NCS管理WLC 7500](#)

[常見問題](#)

[相關資訊](#)

簡介

本檔案介紹如何部署Cisco Flex 7500無線分支機構控制器。本文旨在：

- 解釋Cisco FlexConnect解決方案的各種網路元素及其通訊流程。
- 提供設計Cisco FlexConnect無線分支機構解決方案的一般部署指南。
- 解釋7.2.103.0代碼版本中的軟體功能，這些功能可支援產品的資訊庫。

注意：在7.2之前，FlexConnect被稱為混合REAP(HREAP)。現在它稱為FlexConnect。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

產品概觀

圖1: Cisco Flex 7500



Cisco Flex 7500系列雲控制器是一個高度可擴展的分支控制器，適用於多站點無線部署。Cisco Flex 7500系列控制器部署在私有雲中，通過集中化控制將無線服務擴展到分散的分支機構，從而降低總運營成本。

Cisco Flex 7500系列(圖1)可在最多500個分支機構位置管理無線接入點，並允許IT管理員從資料中心配置、管理和排除最多3000個接入點(AP)和30,000個客戶端故障。Cisco Flex 7500系列控制器支援安全訪客接入、針對支付卡行業(PCI)合規性的欺詐檢測，以及分支機構內(本地交換)Wi-Fi語音和影片。

下表突出顯示Flex 7500、WiSM2和WLC 5500控制器之間的可擴充性差異：

可擴充性	Flex 7500	WiSM2	WLC 5500
接入點總數	6,000	1000	500
使用者端總數	64,000	15,000	7,000
最大FlexConnect組數	2000	100	100
每個FlexConnect組的最大AP數	100	25	25
最大AP組數	6000	1000	500

產品規格

產品介紹

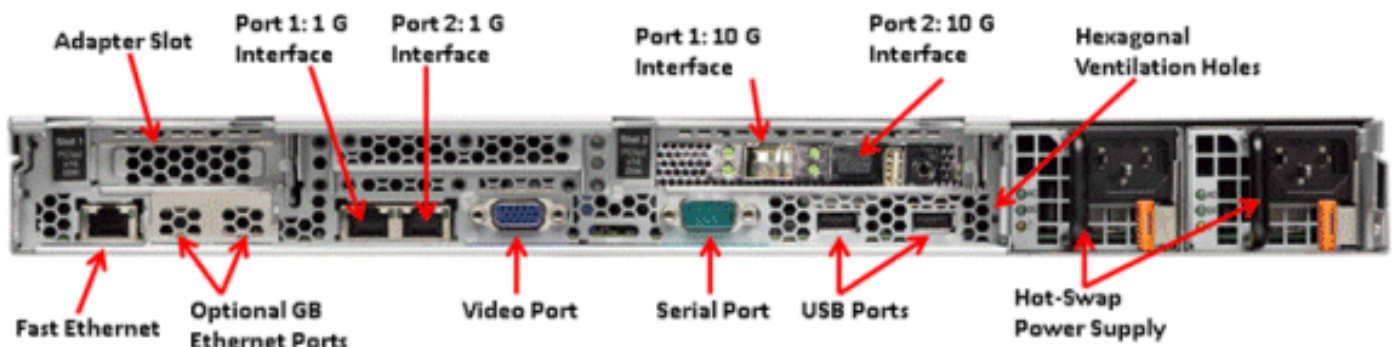
請參閱

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps11635/data_sheet_c78-650053.html。

平台功能

圖2:Flex 7500後檢視

Rear View



網路介面連線埠

介面連線埠	使用
快速乙太網路	整合式管理模組(IMM)
埠1:1G	WLC服務連線埠
埠2:1G	WLC備援連線埠(RP)
埠1:10G	WLC管理介面
埠2:10G	WLC備份管理介面連線埠 (連線埠故障)
可選千兆乙太網埠	不適用

附註：

- 2x10G介面的LAG支援允許使用快速故障切換鏈路冗餘的主用 — 主用鏈路操作。具有LAG的額

外活動10G鏈路不會更改控制器的無線吞吐量。

- 2x10G介面
- 2x10G介面僅支援SFP產品編號SFP-10G-SR的光纜。
- 交換機端SFP產品編號X2-10GB-SR

系統MAC地址

埠1:10G (管理介面)	系統/基本MAC地址
埠2:10G (備份管理介面)	基本MAC地址+ 5
埠1:1G (服務埠)	基本MAC地址+ 1
埠2:1G (冗餘埠)	基本MAC地址+ 3

序列主控台重新導向

預設情況下，WLC 7500以9600波特率啟用控制檯重定向，模擬無流量控制的Vt100終端。

庫存資訊

圖3:WLC 7500主控台

```
(Cisco Controller) >show inventory
```

```
Burned-in MAC Address..... E4:1F:13:65:DB:6C  
Maximum number of APs supported..... 2000  
NAME: "Chassis" , DESCR: "Cisco Wireless Controller"  
PID: AIR-CT7510-K9, VID: V01, SN: KQZZXWL
```

案頭管理介面(DMI)表包含伺服器硬體和BIOS資訊。

WLC 7500將BIOS版本、PID/VID和序列號顯示為清單的一部分。

Flex 7500啟動

用於軟體維護的思科引導載入程式選項與思科現有的控制器平台相同。

圖4:啟動順序

Cisco Bootloader (Version)

```
.o88b. d888888b .d8888. .o88b. .d88b.
d8P Y8 `88' 88' YP d8P Y8 .8P Y8.
8P      88 `8bo. 8P      88 88
8b      88      `Y8b. 8b      88 88
Y8b d8 .88. db 8D Y8b d8 `8b d8'
`Y88P' Y888888P `8888Y' `Y88P' `Y88P'
```

Booting Primary Image...

Press <ESC> now for additional boot options...

Boot Options

Please choose an option from below:

1. Run primary image (Version) (default)
2. Run backup image (Version)
3. Manually upgrade primary image
4. Change active boot image
5. Clear Configuration

圖5:WLC配置嚮導

```
Would you like to terminate autoinstall? [yes]:
System Name [Cisco_65:db:6c] (31 characters max):
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max): admin
Default values (admin or Cisco or its variants) in password is not allowed.
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****

Management Interface IP Address: 172.20.227.174
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 172.20.227.161
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1 ← Management Port 1: 10G
Management Interface DHCP Server IP Address: 172.20.227.161

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: mobility

Network Name (SSID): DataCenter

Configure DHCP Bridging Mode [yes][NO]: NO

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 list (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

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 09/02/10
Enter the time in HH:MM:SS format: 11:50:00

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

註：Flex 7500啟動順序等效且與現有控制器平台一致。初始啟動需要使用嚮導配置WLC。

[Flex 7500授權](#)

[AP基本計數許可](#)

AP基本數量SKU
300

500
1000
2000
3000
6000

[AP升級許可](#)

AP升級SKU
100
250
500
1000

除基本和升級數量外，涵蓋訂購、安裝和檢視的整個許可過程與思科現有的WLC 5508類似。

請參閱[WLC 7.3組態設定指南](#)，其中涵蓋整個授權程式。

[軟體版本支援](#)

Flex 7500僅支援WLC代碼版本7.0.116.x及更高版本。

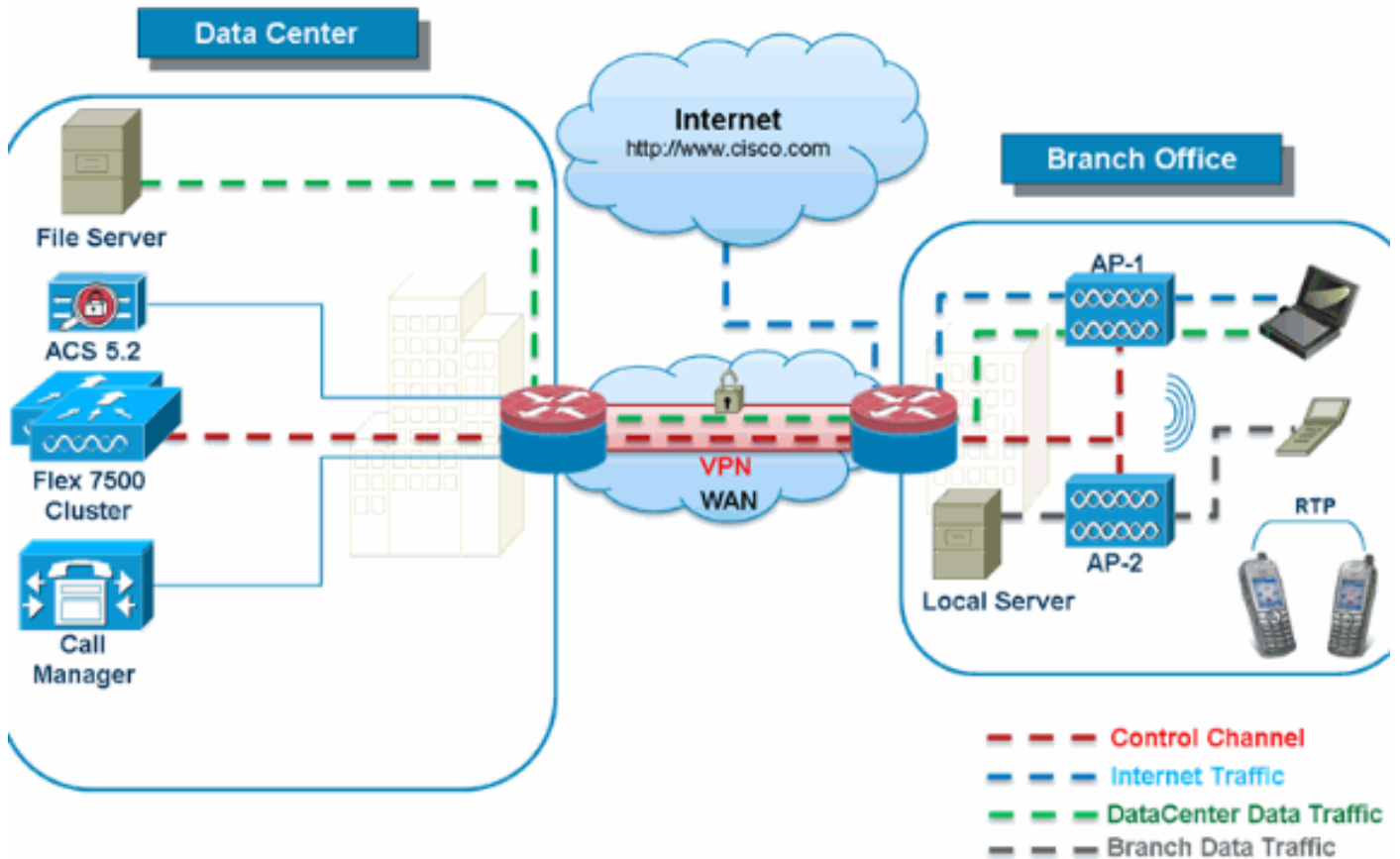
[支援的存取點](#)

Flex 7500支援接入點1040、1130、1140、1550、3500、3600、2600、1250、1260、1240、OEAP 600、ISR 891和ISR 881。

[FlexConnect架構](#)

圖6:典型的無線分支機構拓撲

FlexConnect Architecture



FlexConnect是適用於分支機構和遠端辦公室部署的無線解決方案。它也稱為混合REAP解決方案，但本文檔將稱之為FlexConnect。

FlexConnect解決方案使客戶能夠：

- 集中控制和管理來自資料中心的AP流量。圖6中，控制流量以紅色破折號標籤。
- 在每個分支機構分配客戶端資料流量。圖6中的資料流量以藍色、綠色和紫色短劃線標籤。每個資料流以最有效的方式到達其最終目的地。

集中接入點控制流量的優點

- 單一監控和故障排除窗格
- 易於管理
- 對資料中心資源的安全無縫移動訪問
- 減少分支機構佔用空間
- 增加運營節省

分配客戶端資料流量的優點

- 沒有針對整個WAN鏈路故障或控制器不可用的操作停機（生存能力）
- 在WAN鏈路故障期間，分支機構內的移動恢復能力
- 提高分支機構可擴充性。支援可擴展至100個AP和250,000平方英尺（5000平方米）英尺每無線接入點）。

Cisco FlexConnect解決方案還支援中央客戶端資料流量，但應僅限於來賓資料流量。下表介紹僅對資料流量也在資料中心集中交換的非訪客客戶端的WLAN第2層安全型別的限制。

適用於集中交換的非訪客使用者的L2安全支援

WLAN第2層安全	類型	結果
無	不適用	已允許
WPA + WPA2	802.1x	已允許
	CCKM	已允許
	802.1x + CCKM	已允許
	PSK	已允許
802.1x	WEP	已允許
靜態WEP	WEP	已允許
WEP + 802.1x	WEP	已允許
CKIP		已允許

注意：這些身份驗證限制不適用於在分支機構分配資料流量的客戶端。

適用於集中和本地交換使用者的L3安全支援

WLAN第3層安全	類型	結果
Web驗證	內部	已允許
	外部	已允許
	自定義	已允許
Web傳輸	內部	已允許
	外部	已允許
	自定義	已允許
條件式 Web 重新導向	外部	已允許
啟動顯示頁面 Web 重新導向	外部	已允許

有關Flexconnect外部WebAuth部署的詳細資訊，請參閱[Flexconnect外部WebAuth部署指南](#)

有關HREAP/FlexConnect AP狀態和資料流量交換選項的詳細資訊，請參閱[配置FlexConnect](#)。

[FlexConnect操作模式](#)

FlexConnect模式	說明
已連線	FlexConnect在返回到控制器的CAPWAP控制平面啟動並正常運行時（即WAN鏈路沒有關閉）時稱為連線模式。
獨立	獨立模式指定為FlexConnect不再連線到控制器時進入的運行狀態。獨立模式下的FlexConnect AP將繼續使用上次已知配置，即使發生電源故障和WLC或WAN故障時也是如此。

有關FlexConnect操作理論的詳細資訊，請參閱[H-Reap/FlexConnect設計和部署指南](#)。

[WAN要求](#)

FlexConnect AP部署在分支機構站點，並通過廣域網鏈路從資料中心進行管理。強烈建議保持每AP 12.8 kbps的最低頻寬限制，對於資料部署，往返延遲不超過300 ms，對於資料和語音部署，為100 ms。最大傳輸單元(MTU)必須至少為500位元組。

部署型別	WAN頻寬 (最小值)	WAN RTT延遲 (最大值)	每個分支機構 的最大 AP數	每個分支機構 的最大客戶端 數
資料	64 kbps	300毫秒	5	25
資料 +語音	128 kbps	100毫秒	5	25
監視	64 kbps	2秒	5	不適用
資料	640 kbps	300毫秒	50	1000
資料 +語音	1.44 Mbps	100毫秒	50	1000
監視	640 kbps	2秒	50	不適用

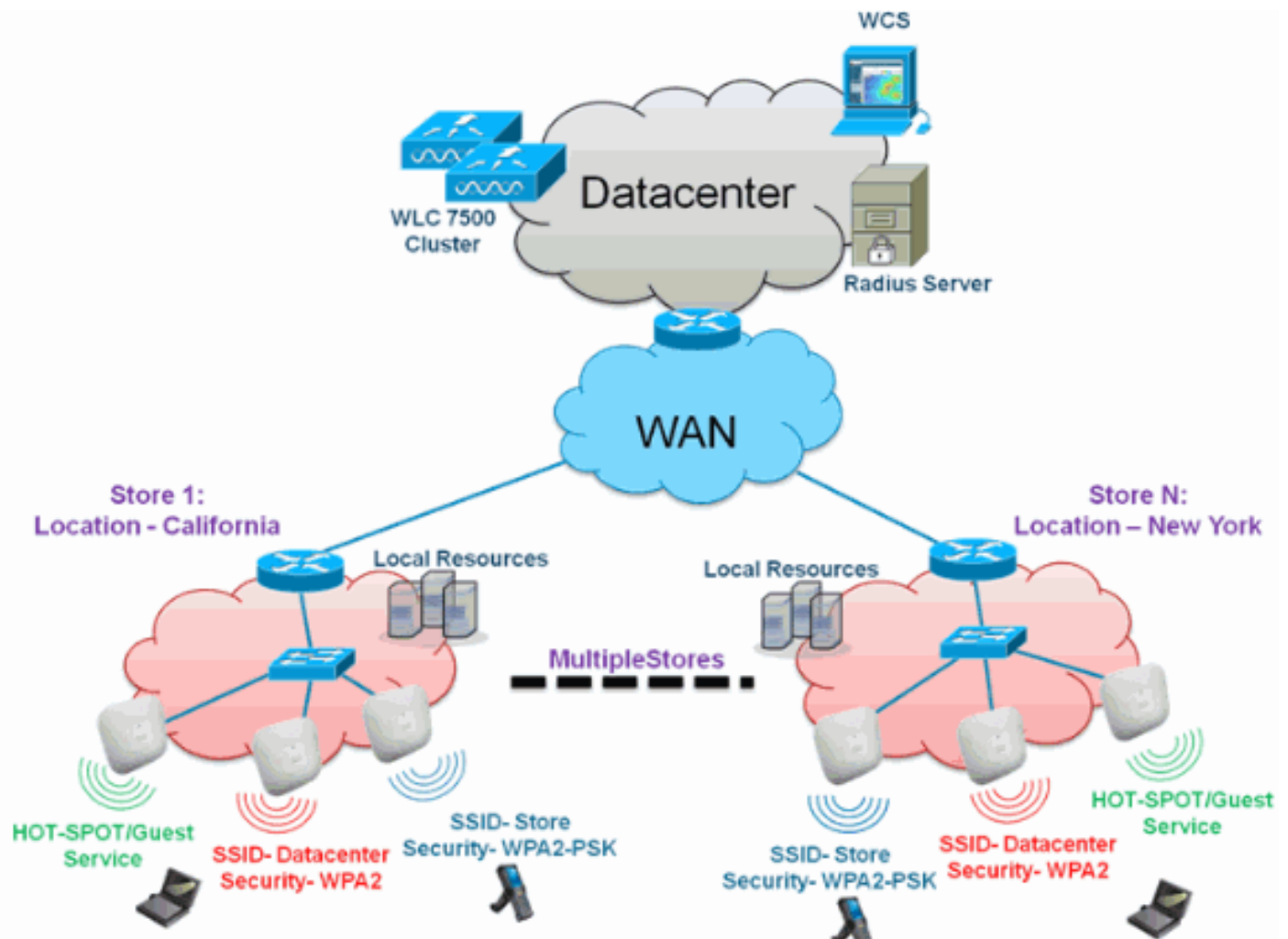
無線分支機構網路設計

本文檔的其餘部分重點介紹實施安全分散式分支機構網路的最佳實踐。對於滿足這些設計要求的無線分支網路，建議使用FlexConnect架構。

主要設計要求

- 分支機構的規模可以擴展到100個接入點和25萬平方英尺 (5000平方米) 每接入點英尺)
- 集中管理和故障排除
- 無操作停機
- 基於客戶端的流量分段
- 與企業資源無縫且安全的無線連線
- 與PCI相容
- 訪客支援

圖7:無線分支機構網路設計



概觀

分支機構客戶發現，跨地理位置提供功能齊全且可擴展且安全的網路服務越來越困難，成本也越來越高。為了支援客戶，思科推出了Flex 7500來應對這些挑戰。

Flex 7500解決方案虛擬化了資料中心內複雜的安全、管理、配置和故障排除操作，然後將這些服務透明地擴展到每個分支。使用Flex 7500的部署使IT人員更易於設定、管理以及更重要的是擴展。

優勢

- 通過6000 AP支援提高可擴充性
- 使用FlexConnect容錯提高恢復能力
- 使用FlexConnect (中央和本地交換) 增強流量分段
- 通過使用AP組和FlexConnect組複製儲存設計，簡化管理。

解決分支機構網路設計問題的功能

本指南的其餘部分將介紹實現圖7所示網路設計的功能用法和**建議**。

功能：

主要功能	亮點
AP組	在處理多個分支機構站點時提供操作/管

	理的便利性。此外，還提供了為類似分支站點複製配置的靈活性。
FlexConnect組	FlexConnect組提供本地備份Radius、CCKM/OKC快速漫遊和本地身份驗證的功能。
容錯能力	提高無線分支機構的恢復能力，並且不會造成運營中斷。
ELM (適用於自適應wIPS的增強型本機模式)	在為客戶端提供服務時提供自適應wIPS功能，而不會影響客戶端效能。
每個WLAN的客戶端限制	限制分支機構網路上的來賓客戶端總數。
AP預映像下載	在升級分支機構時減少停機時間。
在FlexConnect中自動轉換AP	用於自動轉換分支機構FlexConnect中的AP的功能。
訪客接入	使用FlexConnect繼續使用現有的思科訪客接入架構。

IPv6支援清單

功能	集中交換		本地交換	
	5500 / WiSM-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (客戶端移動性)	支援	不支援	不支援	不支援
IPv6 RA防護	支援	支援	支援	支援
IPv6 DHCP防護	支援	不支援	不支援	不支援
IPv6來源防護	支援	不支援	不支援	不支援
RA限制/速率限制	支援	不支援	不支援	不支援
IPv6 ACL	支援	不支援	不支援	不支援
IPv6客戶端可視性	支援	不支援	不支援	不支援
IPv6鄰居發現快取	支援	不支援	不支援	不支援
IPv6橋接	支援	不支援	支援	支援

功能表

有關FlexConnect功能的功能矩陣，請參閱[FlexConnect功能矩陣](#)。

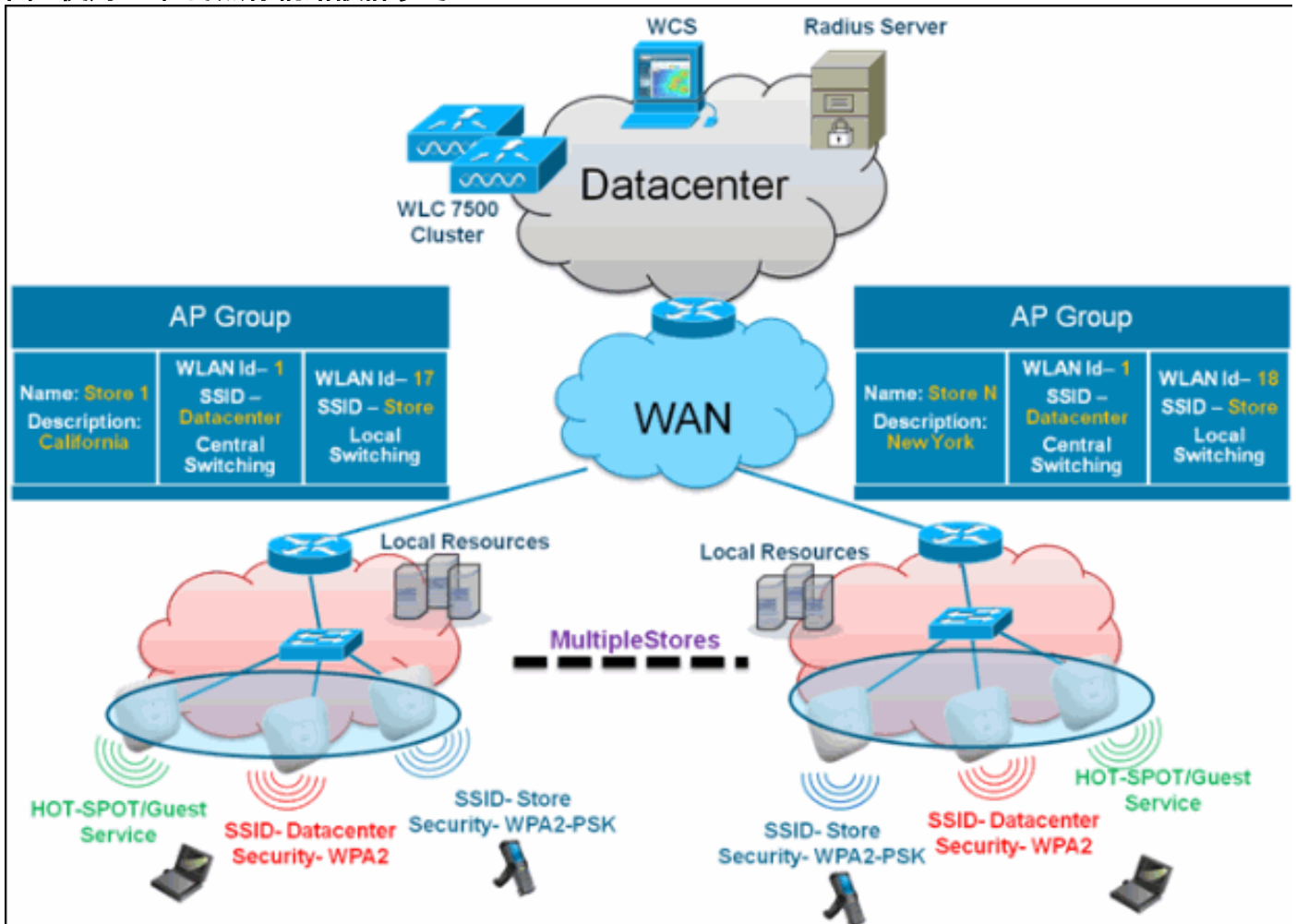
AP組

在控制器上建立WLAN後，您可以選擇性將其（使用存取點群組）發佈到不同的存取點，以便更好地管理您的無線網路。在典型部署中，WLAN中的所有使用者都對映到控制器上的單個介面。因此，與該WLAN相關聯的所有使用者都位於同一個子網或VLAN中。但是，您可以通過建立接入點組，選擇根據特定標準(如各個部門(如行銷、工程或運營))在多個介面之間或將負載分配給使用者組。此外，這些接入點組可以在單獨的VLAN中進行配置，以簡化網路管理。

本文檔使用AP組簡化跨地理位置管理多個儲存區的網路管理。為便於操作，本文檔為每個儲存區建立一個AP組以滿足以下要求：

- 跨所有儲存集中交換SSID **Datacenter**，用於本地儲存管理器管理訪問。
- 本地交換SSID **Store** (在手持掃描器的所有儲存區中具有不同的WPA2-PSK金鑰)。

圖8:使用AP組的無線網路設計參考



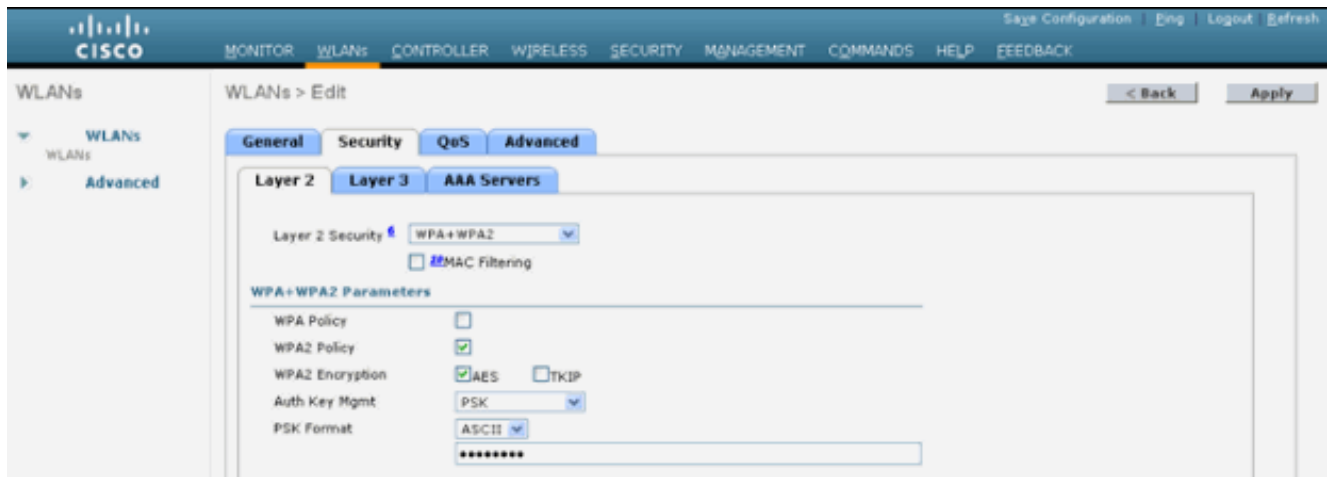
來自WLC的組態

請完成以下步驟：

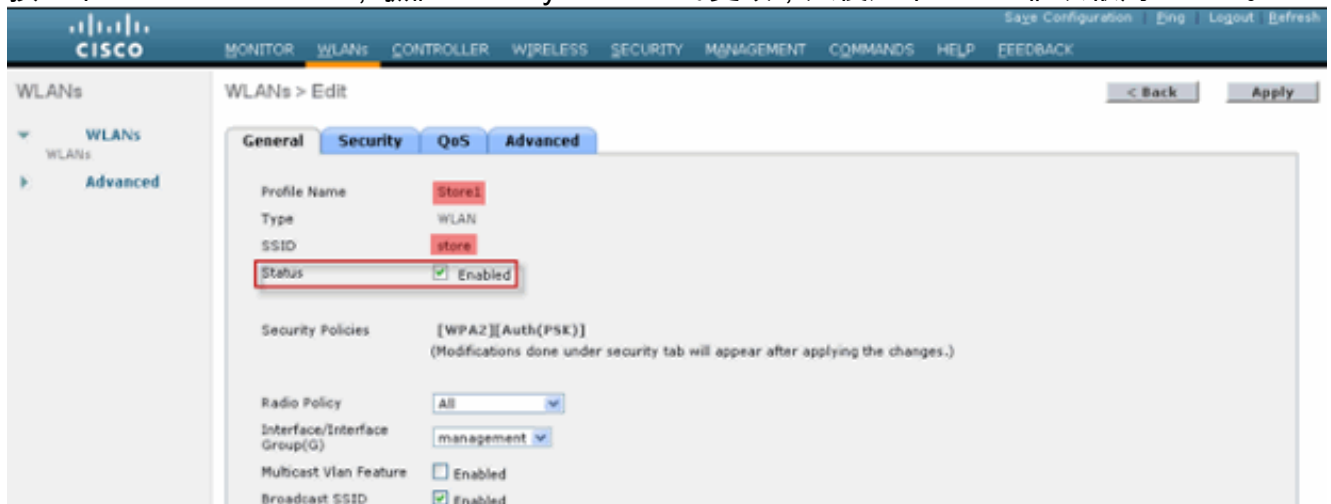
1. 在WLANs > New頁面上，在Profile Name欄位中輸入**Store1**，在SSID欄位中輸入**store**，然後從ID下拉選單中選擇**17**。**注意**：WLAN ID 1-16是預設組的一部分，無法刪除。為了滿足我們對使用不同WPA2-PSK的每個儲存使用同一SSID儲存的要求，您需要使用WLAN ID 17及更高版本，因為這些不是預設組的一部分，並且可能限制到每個儲存。



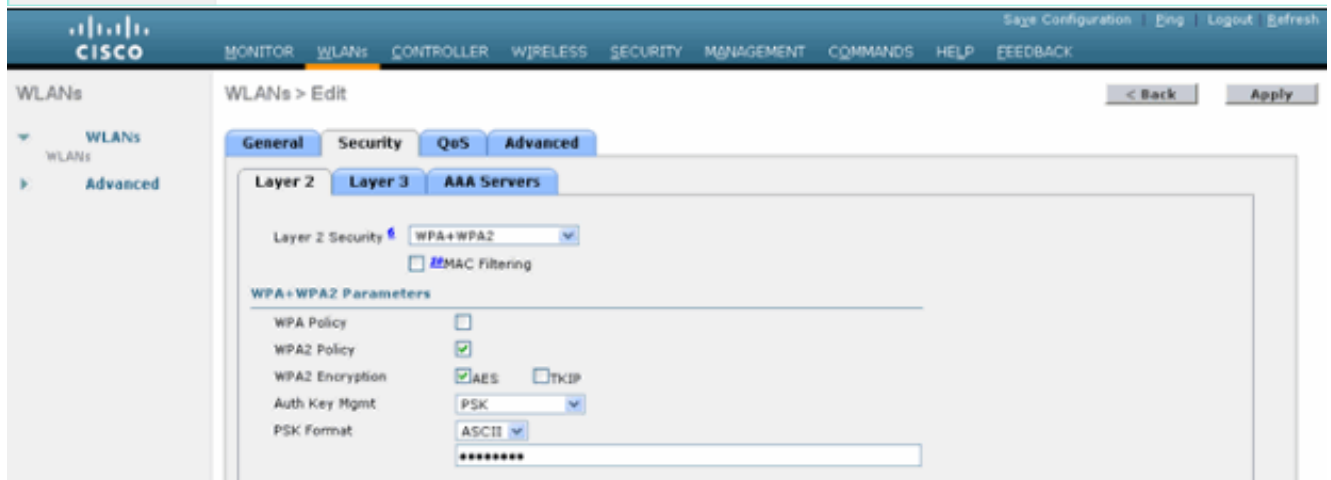
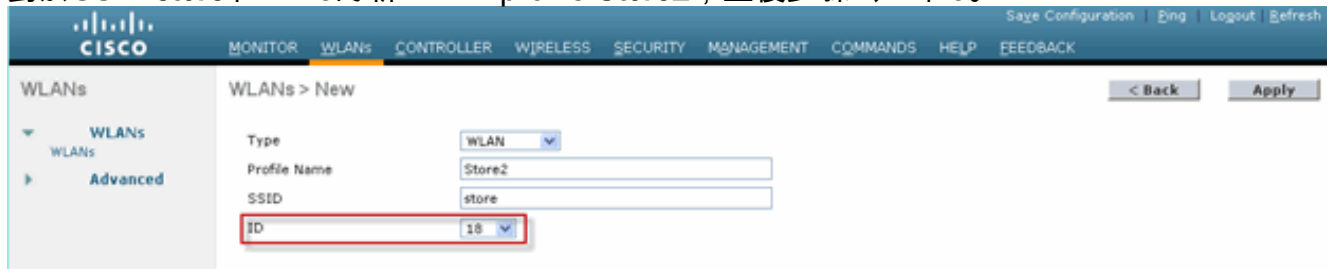
2. 在WLAN > Security下，從Auth Key Mgmt下拉選單中選擇**PSK**，從PSK Format下拉選單中選擇**ASCII**，然後按一下**Apply**。

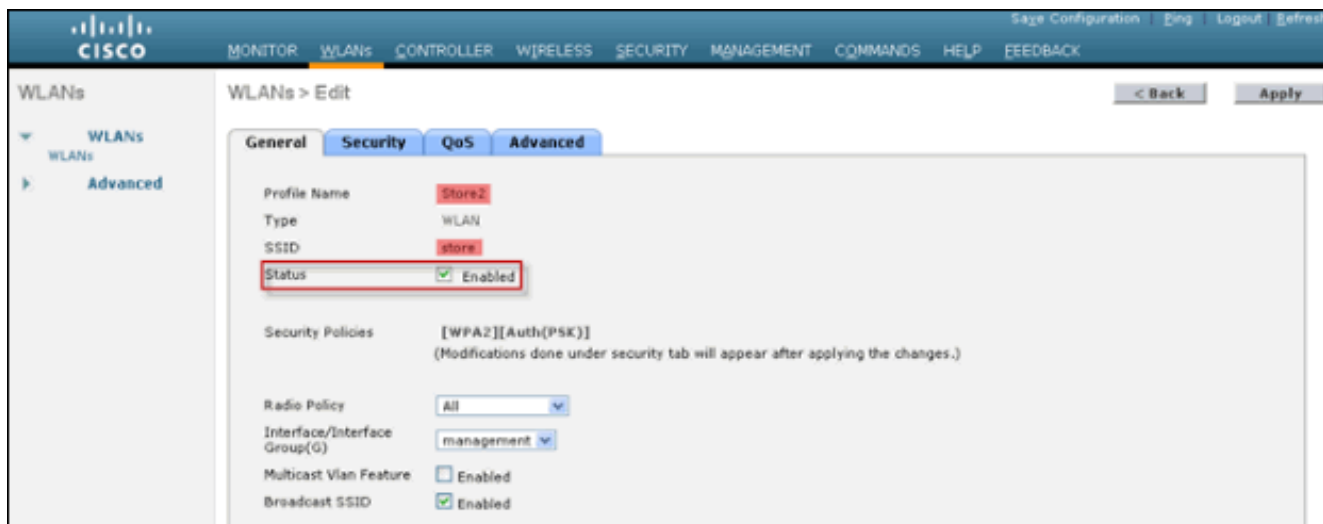


3. 按一下WLAN > General，驗證Security Policies的更改，然後選中Status框以啟用WLAN。

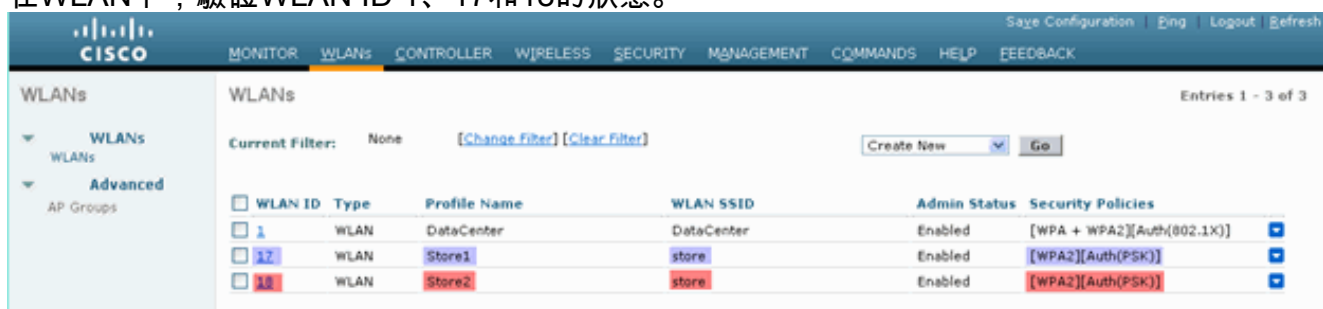


4. 對於SSID store和ID 18的新WLAN profile Store2，重複步驟1、2和3。

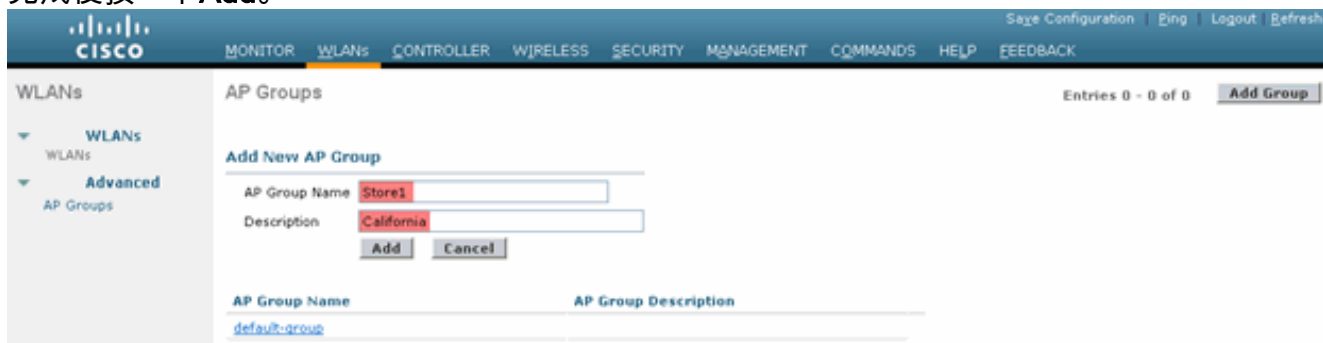




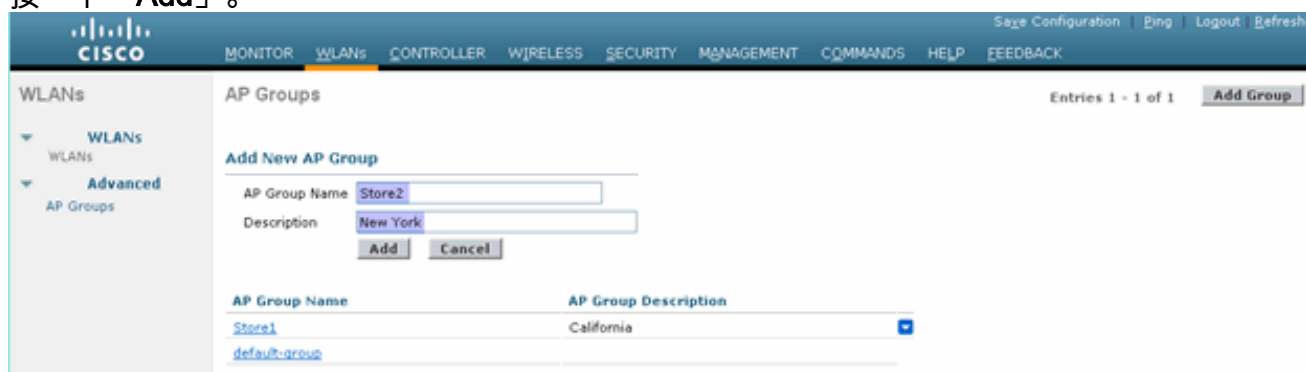
5. 使用Profile Name **DataCenter**、SSID **DataCenter**和ID 1建立並啟用WLAN配置檔案。注意：建立時，1-16的WLAN ID自動成為default-ap-group的一部分。
6. 在WLAN下，驗證WLAN ID 1、17和18的狀態。



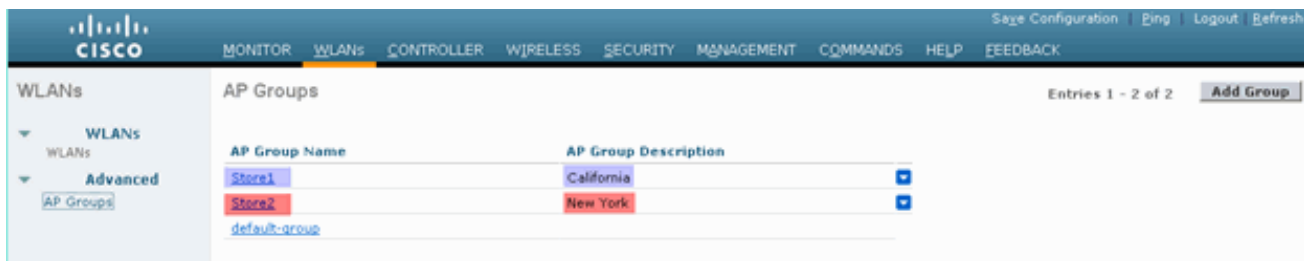
7. 按一下**WLAN > Advanced > AP group > Add Group**。
8. 新增AP組名稱**Store1**，與WLAN配置檔案Store1相同，新增Description作為儲存的位置。在此示例中，California用作商店的位置。
9. 完成後按一下**Add**。



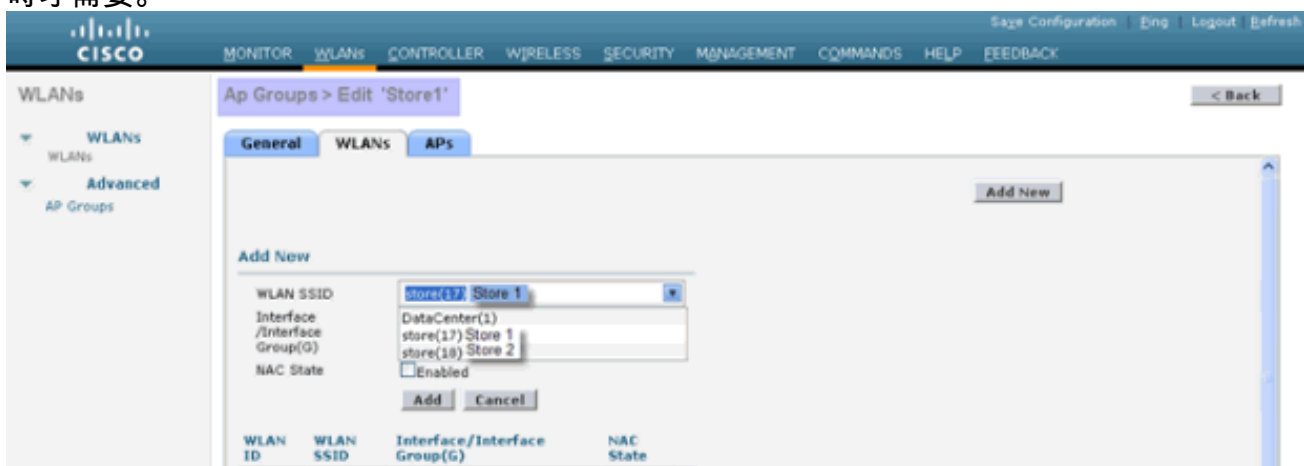
10. 按一下**Add Group**並建立AP組名稱**Store2**和Description **New York**。
11. 按一下「**Add**」。



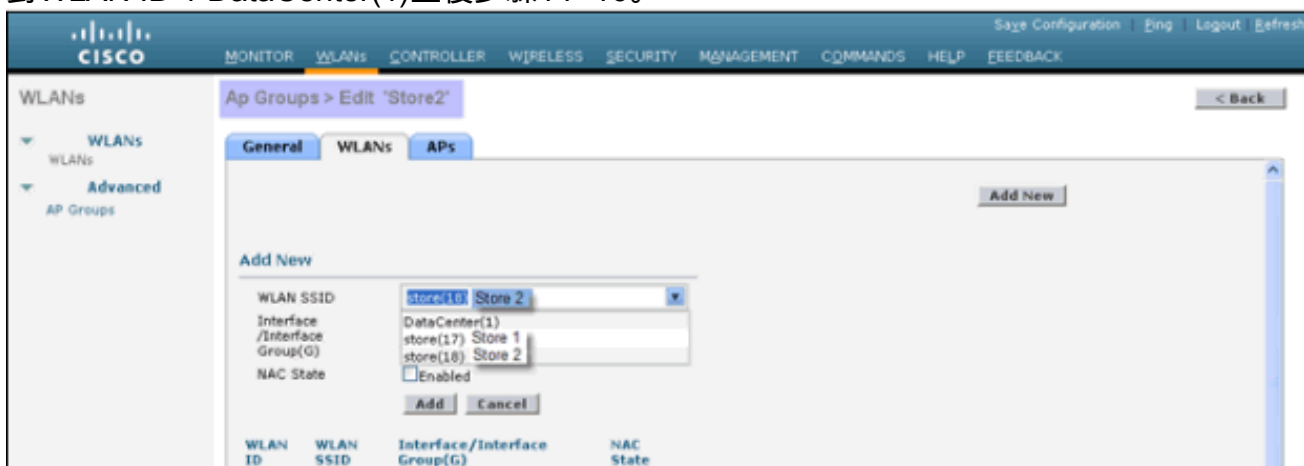
12. 按一下**WLAN > Advanced > AP Groups**以驗證組的建立。



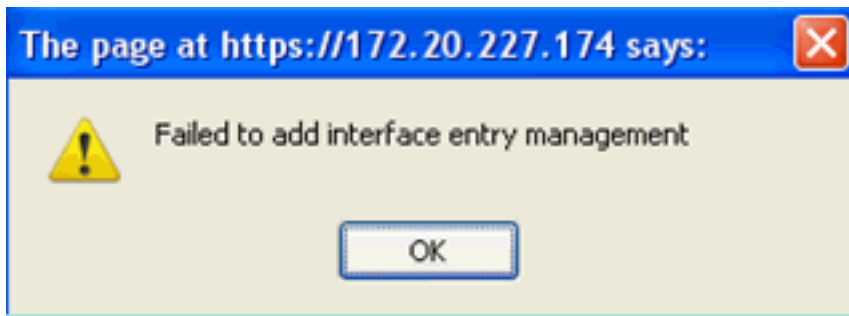
13. 按一下AP Group Name **Store1**新增或編輯WLAN。
14. 按一下**Add New**以選擇WLAN。
15. 在WLAN下，從WLAN SSID下拉選單中選擇**WLAN ID 17 store(17)**。
16. 選擇WLAN ID 17後，按一下**Add**。
17. 對WLAN ID 1 DataCenter(1)重複步驟14 -16。此步驟是可選的，僅在要允許遠端資源訪問時才需要。



18. 返回**WLAN > Advanced > AP Groups**螢幕。
19. 點選AP Group Name **Store2**新增或編輯WLAN。
20. 按一下**Add New**以選擇WLAN。
21. 在WLAN下，從WLAN SSID下拉選單中選擇**WLAN ID 18 store(18)**。
22. 選擇WLAN ID 18後，按一下**Add**。
23. 對WLAN ID 1 DataCenter(1)重複步驟14 -16。



注意：不允許在單個AP組下新增具有相同SSID的多個WLAN配置檔案。



注意：本文檔中未捕獲向AP組

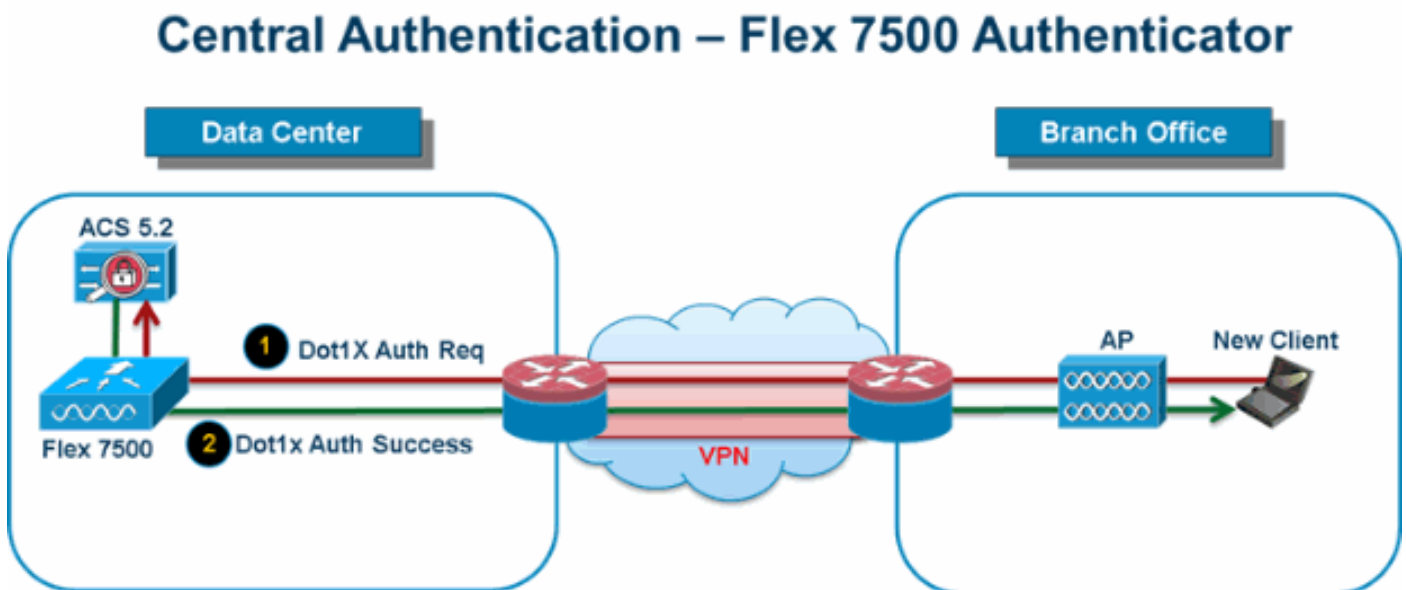
新增AP，但客戶端訪問網路服務需要新增AP。

摘要

- AP組簡化了網路管理。
- 通過每個分支細分度輕鬆進行故障排除
- 更高的靈活性

FlexConnect組

圖9:中央Dot1X驗證 (Flex 7500充當驗證器)



在大多數典型的分支機構部署中，很容易預見到客戶端802.1X身份驗證會在資料中心集中進行，如圖9所示。由於上述場景完全有效，因此會引起以下擔憂：

- 如果Flex 7500發生故障，無線客戶端如何執行802.1X身份驗證並訪問資料中心服務？
- 如果分支機構和資料中心之間的WAN鏈路發生故障，無線客戶端如何執行802.1X身份驗證？
- 在WAN故障期間是否會對分支機構移動性產生影響？
- FlexConnect解決方案是否不提供運行分支機構的停機時間？

FlexConnect Group主要旨在解決這些難題，應建立該組。此外，由於每個分支站點的所有FlexConnect接入點都屬於單個FlexConnect組，因此它簡化了每個分支站點的組織工作。

注意：FlexConnect組與AP組不同。

FlexConnect組的主要目標

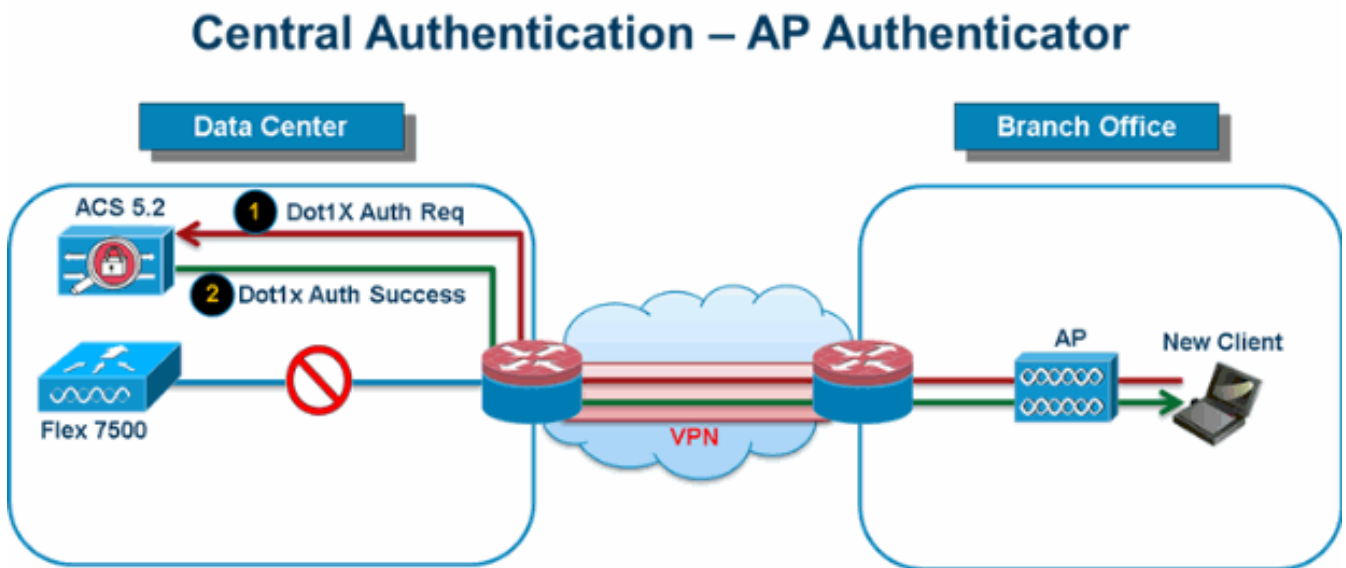
備份RADIUS伺服器故障轉移

- 您可以將控制器配置為允許處於獨立模式的FlexConnect接入點對備份RADIUS伺服器執行完整的802.1X身份驗證。為了提高分支機構的恢復能力，管理員可以配置主備份RADIUS伺服器或主備份與輔助備份RADIUS伺服器。僅當FlexConnect接入點未連線到控制器時，才使用這些伺服器。

注意：不支援備份RADIUS記帳。

本地身份驗證

- 在7.0.98.0代碼發行之之前，只有當FlexConnect處於獨立模式時，才支援本地身份驗證，以確保在WAN鏈路故障期間不會影響客戶端連線。在7.0.116.0版本中，即使FlexConnect接入點處於連線模式，現在仍支援此功能。**圖10:中央Dot1X驗證 (用作驗證器的FlexConnect AP)**

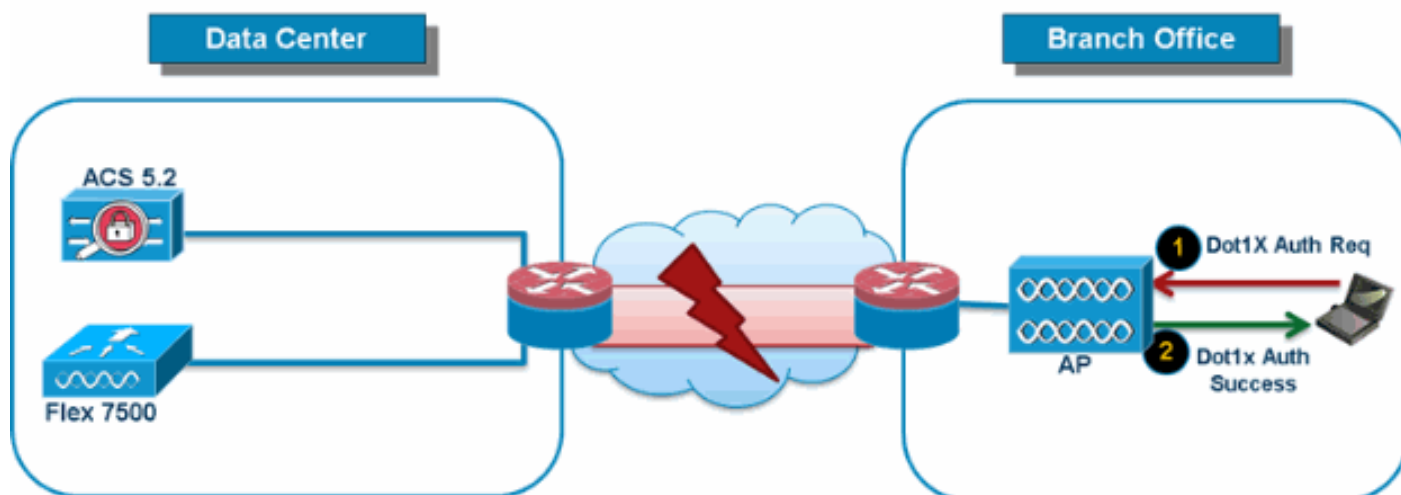


如圖10所示，當FlexConnect分支AP與Flex 7500失去連線時，分支客戶端可以繼續執行802.1X身份驗證。只要RADIUS/ACS伺服器可從分支機構站點訪問，無線客戶端就會繼續驗證和訪問無線服務。換句話說，如果RADIUS/ACS位於分支機構內，則客戶端即使在廣域網中斷期間也會進行身份驗證並訪問無線服務。**注意：**此功能可與FlexConnect備份RADIUS伺服器功能結合使用。如果FlexConnect組配置了備份RADIUS伺服器和本地身份驗證，則FlexConnect接入點總是首先嘗試使用主備份RADIUS伺服器對客戶端進行身份驗證，然後嘗試使用輔助備份RADIUS伺服器（如果主伺服器無法訪問），最後嘗試使用FlexConnect接入點上的本地EAP伺服器（如果主伺服器和輔助伺服器無法訪問）。

本地EAP (本地身份驗證繼續)

圖11:Dot1X身份驗證 (FlexConnect AP充當本地EAP伺服器)

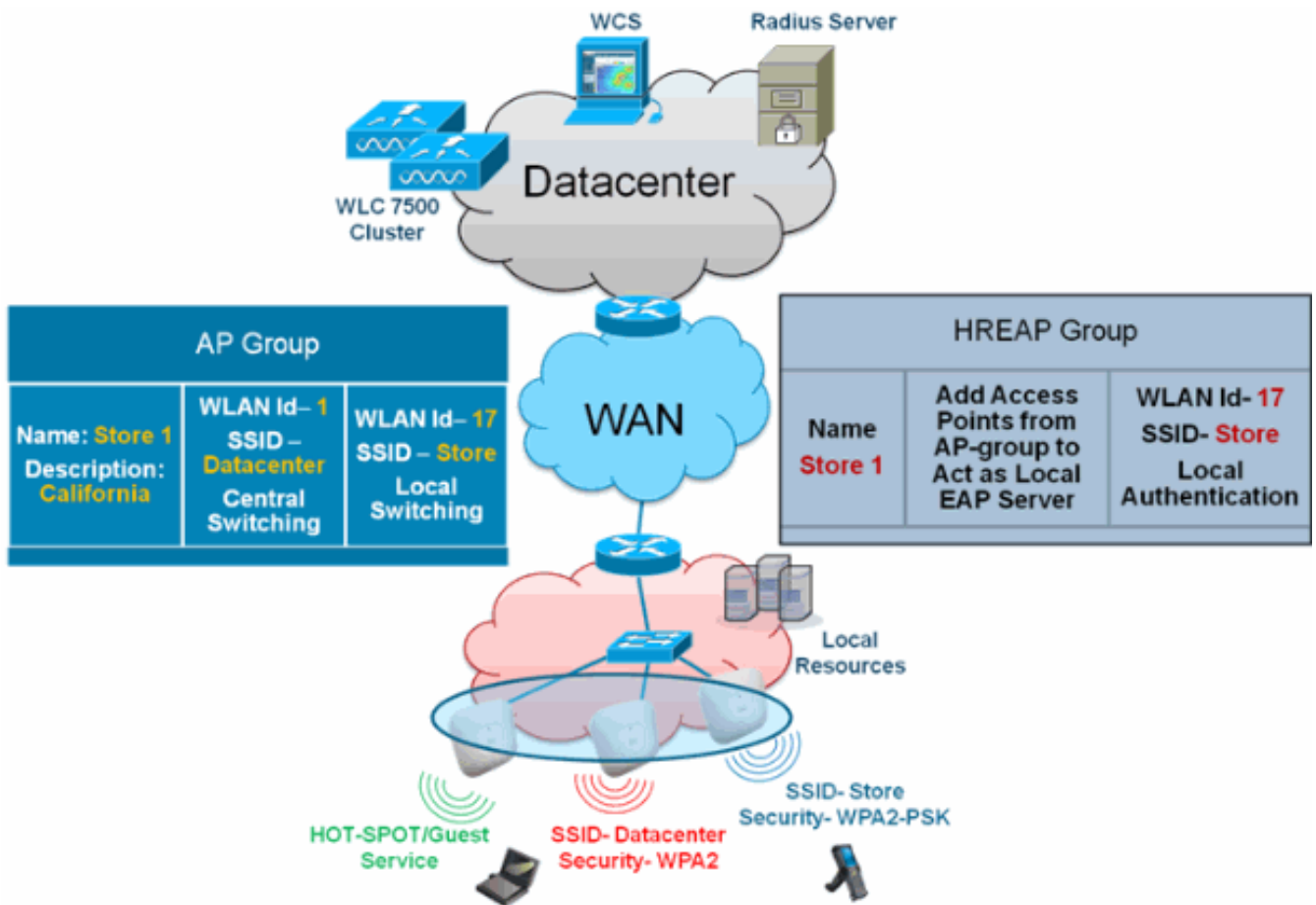
Local Branch Authentication – AP as Radius Server



- 您可以將控制器配置為允許處於獨立或連線模式的FlexConnect AP對最多100個靜態配置的使用者執行LEAP或EAP-FAST身份驗證。當控制器加入控制器時，控制器將使用者名稱和密碼的靜態清單傳送給該特定FlexConnect組的每個FlexConnect接入點。組中的每個接入點僅對自己的關聯客戶端進行身份驗證。
- 對於正在從自主接入點網路遷移到輕量FlexConnect接入點網路，且無意維護大型使用者資料庫，或者希望新增其他硬體裝置來替換自主接入點中可用的RADIUS伺服器功能的客戶，此功能為理想之選。
- 如圖11所示，如果資料中心內的RADIUS/ACS伺服器無法訪問，則FlexConnect AP自動充當本地EAP伺服器，為無線分支客戶端執行Dot1X身份驗證。

CCKM/OKC快速漫遊

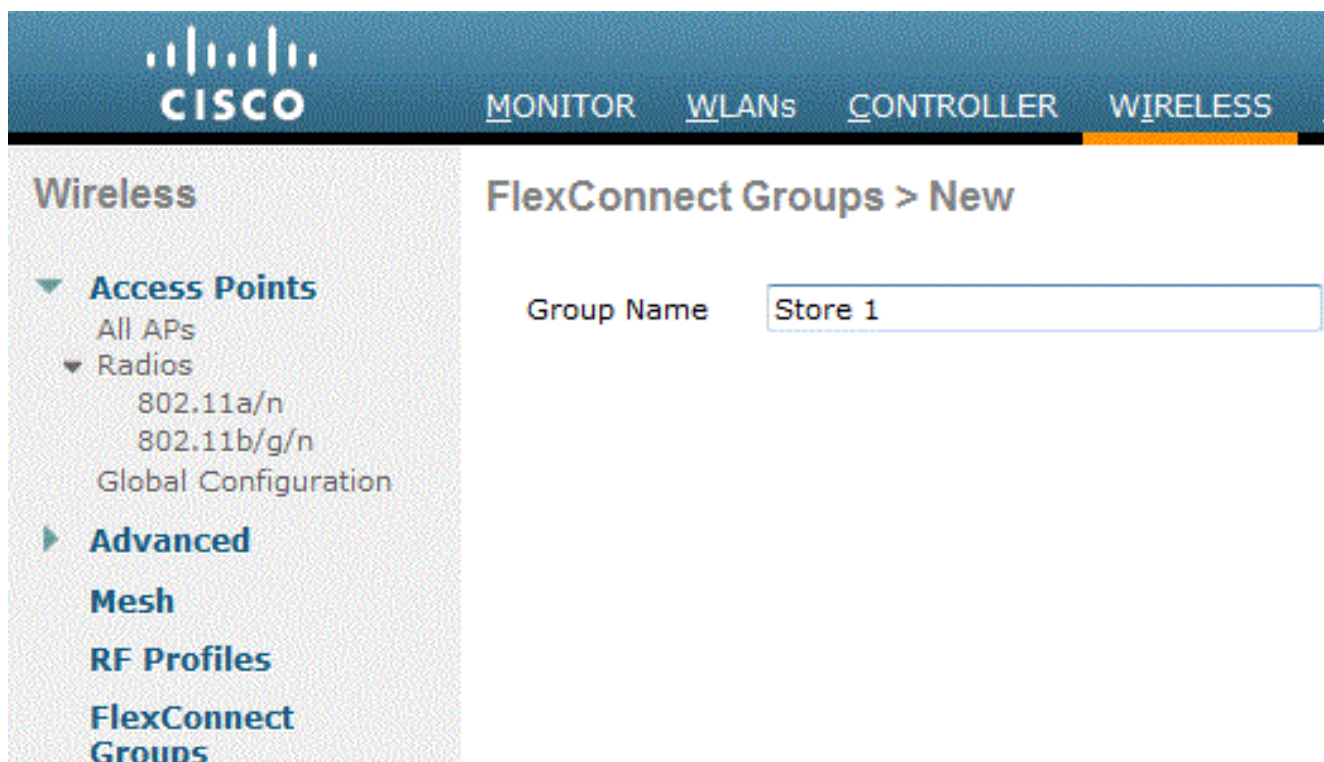
- CCKM/OKC快速漫遊需要FlexConnect組才能與FlexConnect接入點配合使用。快速漫遊是通過快取來自完全EAP身份驗證的主金鑰的派生項來實現的，以便當無線客戶端漫遊到不同的接入點時，可以發生簡單和安全的金鑰交換。此功能可防止客戶端從一個接入點漫遊到另一個接入點時，需要執行完整的RADIUS EAP身份驗證。FlexConnect接入點需要獲取所有可能關聯的客戶端的CCKM/OKC快取資訊，以便快速處理該資訊，而不是將其傳送回控制器。例如，如果控制器具有300個接入點和100個可能關聯的客戶端，則為所有100個客戶端傳送CCKM/OKC快取是不切實際的。如果建立包含有限數量接入點的FlexConnect組（例如，為遠端辦公室中的四個接入點建立一個組），則客戶端僅在這四個接入點之間漫遊，並且僅當客戶端與其中一個接入點關聯時，CCKM/OKC快取才會分佈在這四個接入點中。
- 此功能與備份Radius和本地身份驗證(Local-EAP)相結合，可確保分支站點不會出現操作中斷的情況。**注意：**不支援FlexConnect和非FlexConnect接入點之間的CCKM/OKC快速漫遊。圖12:使用FlexConnect組的無線網路設計參考



從WLC進行FlexConnect組配置

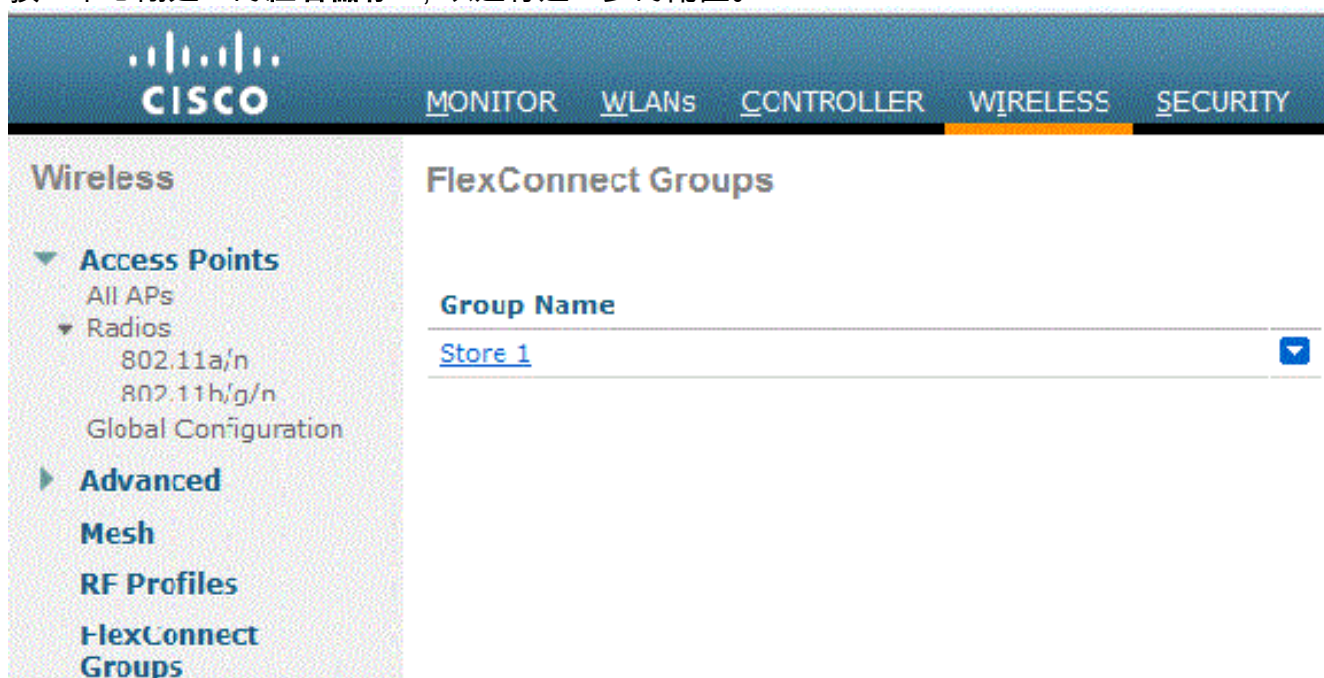
完成本節中的步驟，以便當FlexConnect處於連線或獨立模式時，配置FlexConnect組以支援使用LEAP的本地身份驗證。圖12中的配置示例說明了AP組和FlexConnect組之間的目標差異和1:1對映。

1. 在Wireless > FlexConnect Groups下按一下**New**。
2. 分配組名稱儲存1，類似於圖12中所示的示例配置。
3. 設定「組名」後，按一下**Apply**。



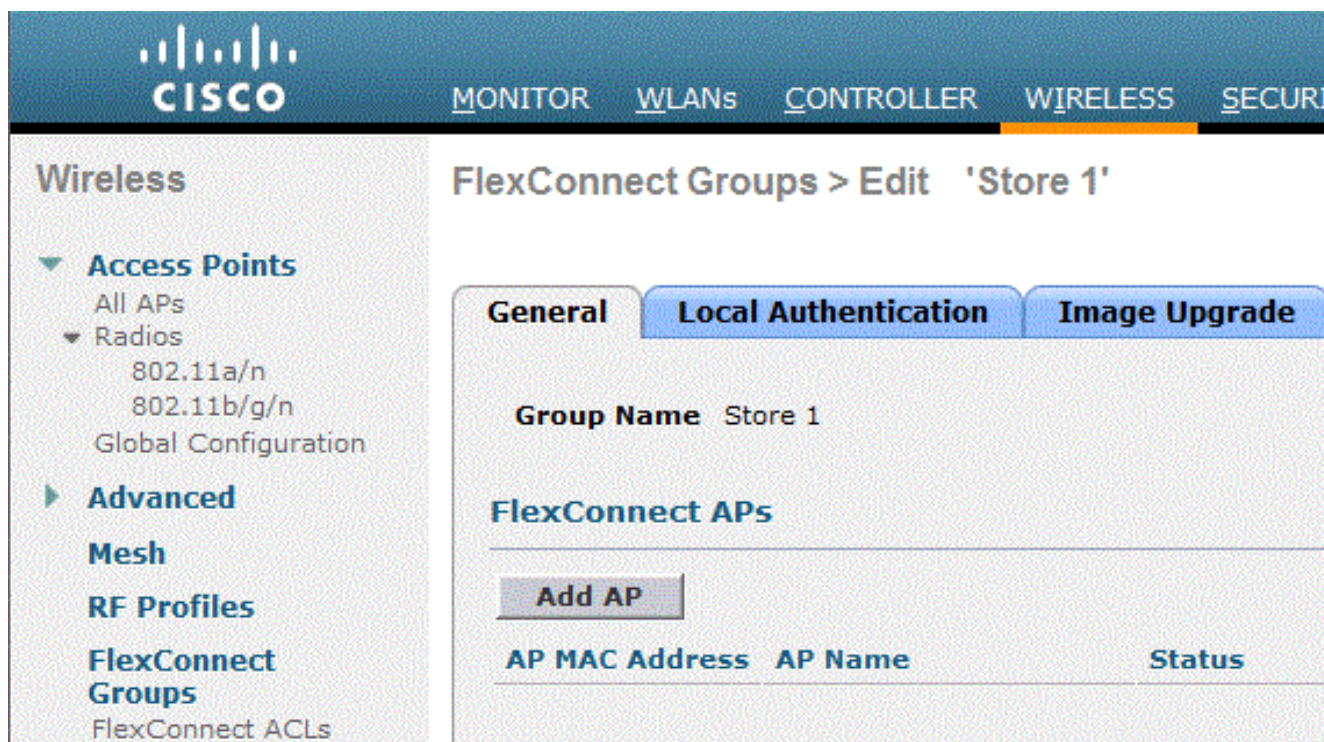
The screenshot shows the Cisco FlexConnect Groups configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11b/g/n, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'FlexConnect Groups > New' and features a 'Group Name' input field containing the text 'Store 1'.

4. 按一下您剛建立的組名儲存1，以進行進一步的配置。



The screenshot shows the Cisco FlexConnect Groups configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios: 802.11a/n, 802.11h/g/n, Global Configuration), 'Advanced', 'Mesh', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'FlexConnect Groups' and features a 'Group Name' dropdown menu with 'Store 1' selected and a blue downward arrow icon.

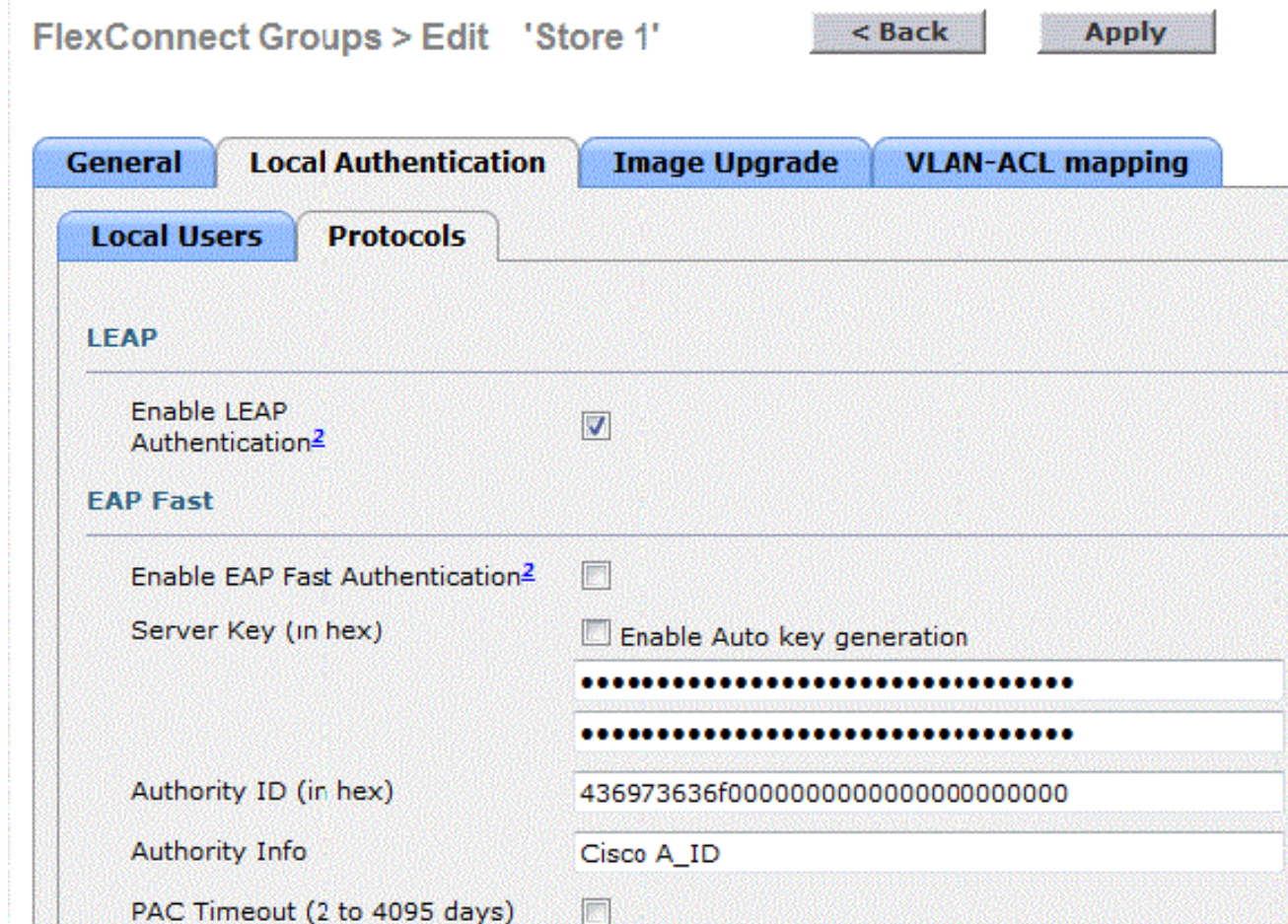
5. 按一下「Add AP」。



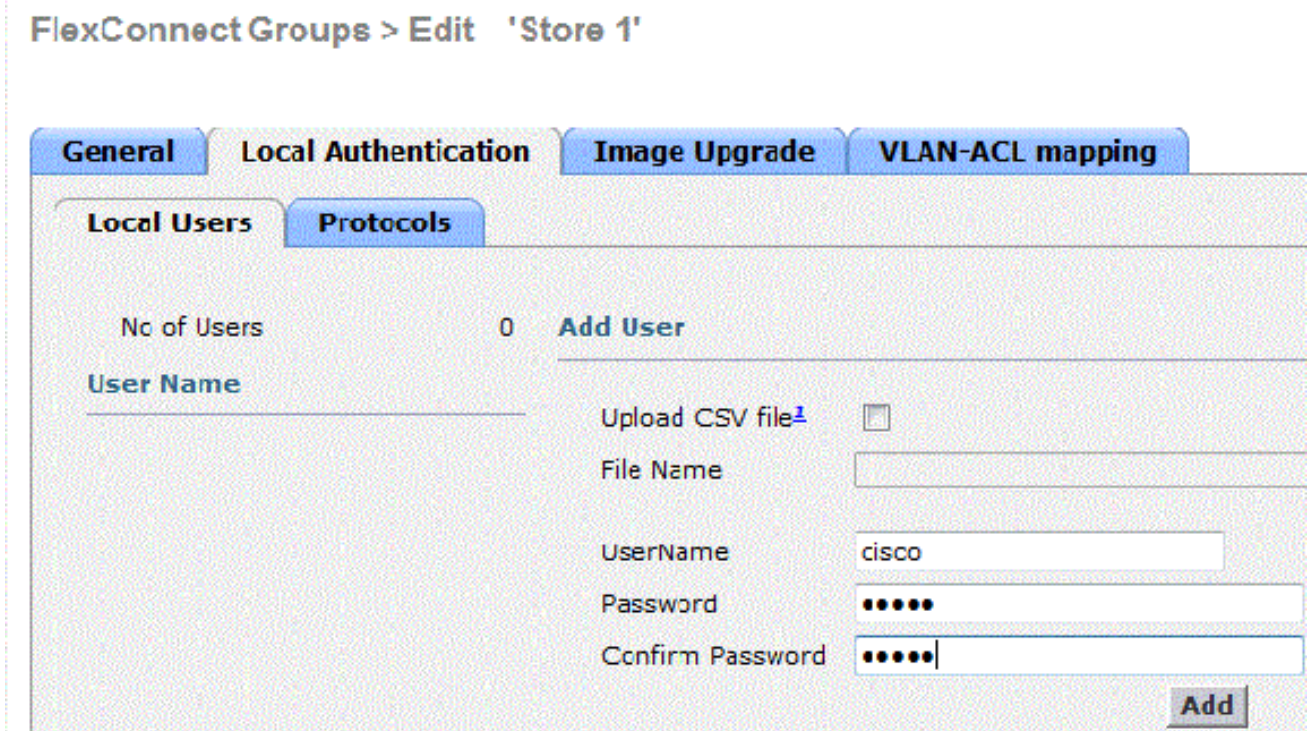
- 選中**Enable AP Local Authentication**框，以便當AP處於獨立模式時啟用Local Authentication。**注意**：步驟20顯示如何為連線模式AP啟用本地身份驗證。
- 選中**Select APs from current controller**框以啟用AP Name下拉選單。
- 從需要成為此FlexConnect組一部分的下拉選單中選擇AP。
- 從下拉選單中選擇AP後，按一下**Add**。
- 重複步驟7和8，將所有屬於AP組儲存1的AP新增到此FlexConnect組。請參閱圖12以瞭解AP組和FlexConnect組之間的1:1對映。如果您已為每個儲存區建立一個AP組(圖8)，則理想情況下，該AP組的所有AP都應屬於此FlexConnect組(圖12)。維持AP組和FlexConnect組之間保持1:1的比率可簡化網路管理。



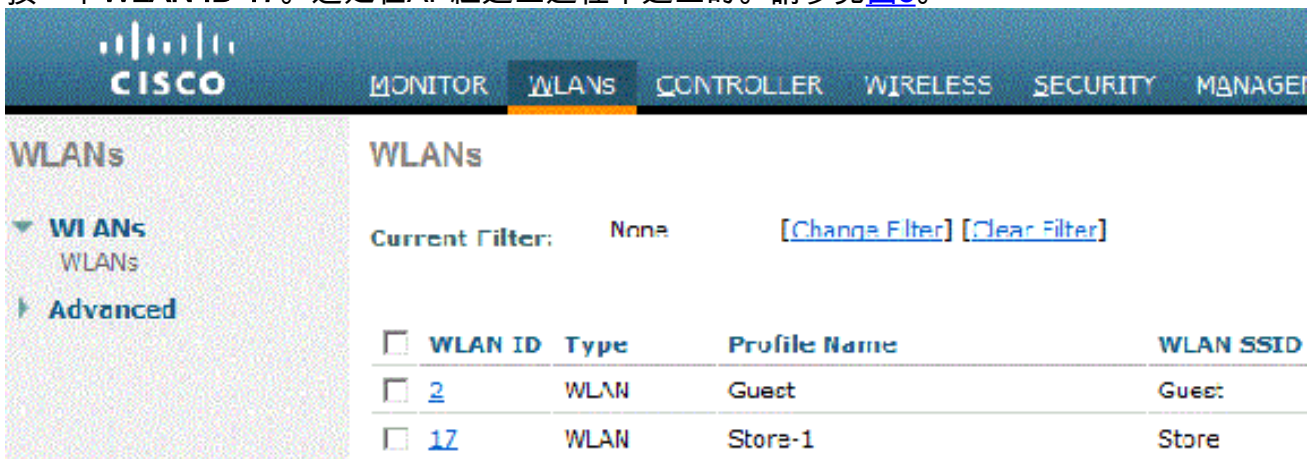
11. 按一下 **Local Authentication > Protocols**，然後選中 **Enable LEAP Authentication** 框。
12. 設定覈取方塊後，按一下 **Apply**。注意：如果您有備份控制器，請確保 FlexConnect 組相同，每個 FlexConnect 組都包含 AP MAC 地址條目。



13. 在Local Authentication下，按一下**Local Users**。
14. 設定Username、Password和Confirm Password欄位，然後點選**Add**以在駐留在AP上的本地EAP伺服器中建立使用者條目。
15. 重複步驟13，直到您的本地使用者名稱清單用盡。您無法配置或新增超過100個使用者。
16. 完成步驟14並驗證No of Users計數後，按一下**Apply**。



17. 在頂部窗格中，按一下**WLANs**。
18. 按一下**WLAN ID 17**。這是在AP組建立過程中建立的。請參見圖8。



19. 在WLAN > Edit for WLAN ID 17下，按一下**Advanced**。
20. 勾選「**FlexConnect Local Auth**」方塊，以在連線模式下啟用本地身份驗證。**注意：僅支援使用本地交換的FlexConnect進行本地身份驗證。注意：始終確保在啟用WLAN下的本地身份驗證之前建立FlexConnect組。**

WLANs > Edit 'Store-1'

General	Security	QoS	Advanced
P2P Blocking Action			Disabled
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled		60 Timeout Value (secs)
Maximum Allowed Clients 8		0	
Static IP Tunneling 11	<input type="checkbox"/> Enabled		
Wi-Fi Direct Clients Policy			Disabled
Maximum Allowed Clients Per AP Radio		200	
Off Channel Scanning Defer			
Scan Defer Priority		0	1
		2	3
		4	5
		6	7
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scan Defer Time (msecs)		100	
FlexConnect			
FlexConnect Local Switching 2	<input checked="" type="checkbox"/> Enabled		
FlexConnect Local Auth 12	<input checked="" type="checkbox"/> Enabled		
Learn Client IP Address 5	<input checked="" type="checkbox"/> Enabled		

NCS還提

供FlexConnect Local Auth覈取方塊，以在連線模式下啟用本地身份驗證，如下所示：

Properties > System > **WLANs** > WLAN Configuration > AP Groups > FlexConnect > Security > Access Points > 802.11 > 802.11a/n > 802.11b/g/n > Mesh > Ports > Management > Location

WLAN Configuration Details : 1

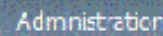
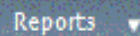
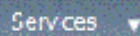
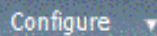
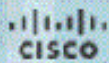
Configure > Controllers > [Controller] > WLANs > WLAN Configuration :

General Security QoS **Advanced**

HexConnect Local Switching	<input checked="" type="checkbox"/>	Enable
FlexConnect Local Auth ⓘ	<input checked="" type="checkbox"/>	Enable
Learn Client IP Address	<input checked="" type="checkbox"/>	Enable
Session Timeout	<input type="checkbox"/>	Enable
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enable
Aironet IE	<input checked="" type="checkbox"/>	Enable
IPv6 ⓘ	<input type="checkbox"/>	Enable
Diagnostic Channel ⓘ	<input type="checkbox"/>	Enable
Override Interface ACL	IPv4	NONE
Peer to Peer Blocking ⓘ		Disable
Wi-Fi Direct Clients Policy		Disabled
Client Exclusion ⓘ	<input checked="" type="checkbox"/>	Enable
Timeout Value		60 (secs)

NCS還提供過濾和監控FlexConnect本地身份驗證客戶端的功能，如下所示

:



Clients and Users



Refresh



Test



Useful



Remove



More



Track Clients



Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name
<input type="radio"/>	00:22:90:1b:17:42		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	1c:df:0f:66:86:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:6e:97:9b:bc		IPv4	husl/vikal...		Intel	oeap-ta-war-2
<input type="radio"/>	00:22:90:1b:96:48		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:90:1b:17:8c		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	00:25:0b:4d:77:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	c4:7d:4f:3a:c5:d5		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:21:a0:d5:03:c4		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	f3:66:f2:67:7f:50		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:17:ca:bc:d1:b4		IPv4	Uniku10w11		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	88:43:e1:d1:df:02		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:22:bd:1b:e2:b5		IPv4	Unknown		Cisco	WCS_SW-0.1.0.22
<input type="radio"/>	f3:66:f2:ab:1e:69		IPv4	Unknown		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1c:58:dc:b4:4e		IPv4	Uniku10w11		Cisco	WCS_SW-9.1.0.22
<input type="radio"/>	00:1e:7a:0b:21:8d		IPv4	ssimm		Cisco	oeap-ta-war-2

Virtual Domain: ROOT-DOMAIN root ▼ Log Out 🔍

Total 299

Location	VLAN	Status	Interface
Unknown	109	Associated	Gi1/0/34
Unknown	109	Associated	Gi1/0/26
Root Area	310	Associated	data
Unknown	109	Associated	Gi1/0/36
Unknown	109	Associated	Gi1/0/32
Unknown	109	Associated	Gi1/0/30
Unknown	109	Associated	Gi1/0/13
Unknown	109	Associated	Gi1/0/27
Unknown	109	Associated	Gi1/0/12
Unknown	109	Associated	Gi1/0/15
Unknown	109	Associated	Gi1/0/28
Unknown	109	Associated	Gi1/0/14
Unknown	109	Associated	Gi1/0/9
Unknown	109	Associated	Gi1/0/29
Root Area	311	Associated	voice

Associated Clients

- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- 2.4GHz Clients
- 5GHz Clients
- All Lightweight Clients
- All Autonomous Clients
- All Wired Clients
- Associated Clients
- Clients known by ISE
- Clients detected by MSE
- Clients detected in the last 24 hours
- Clients with Problems
- Excluded Clients
- FlexConnect Locally Authenticated
- New clients detected in last 24 hours
- On Network Clients

使用CLI驗證

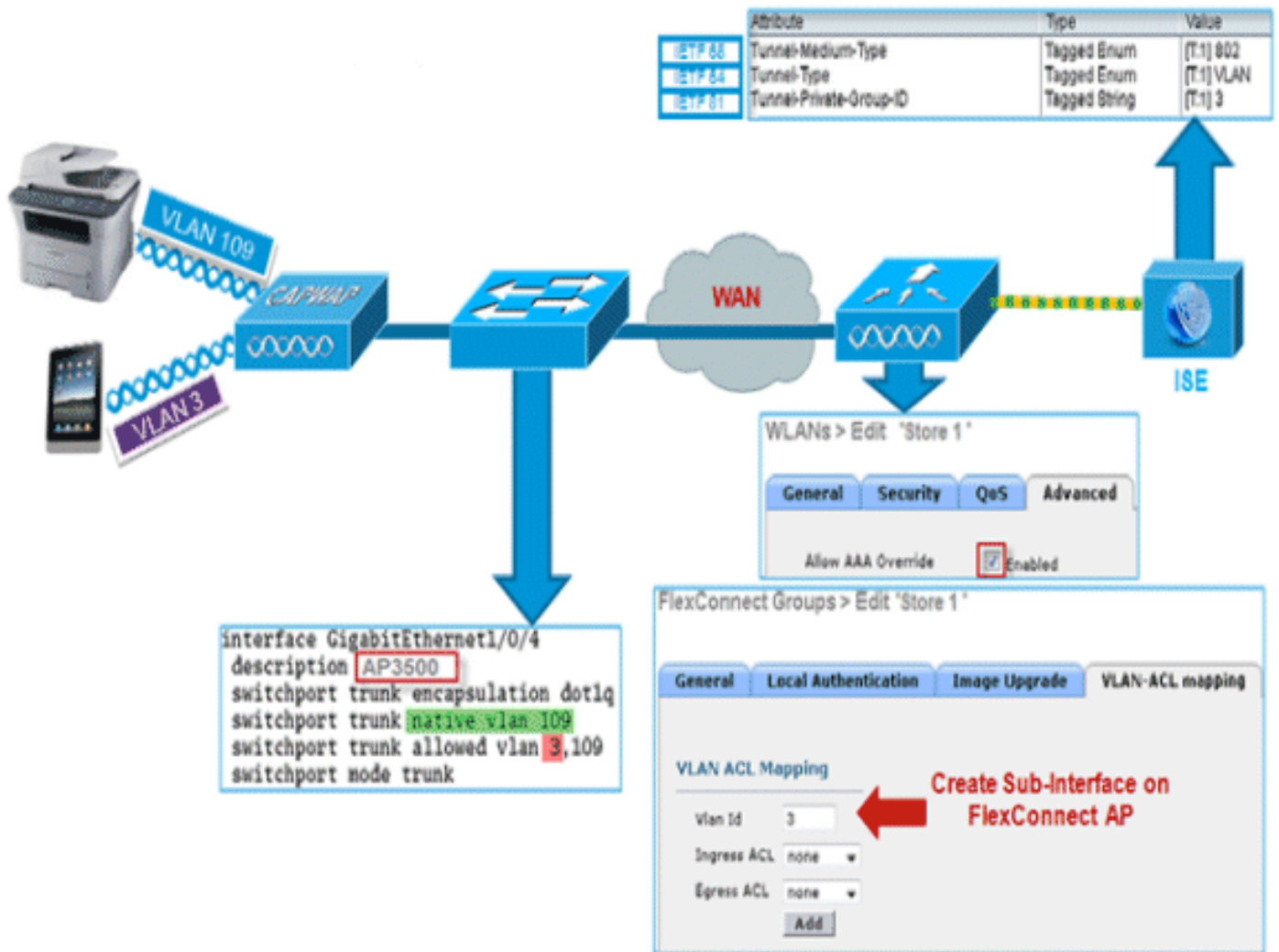
在WLC上使用以下CLI可以快速驗證使用者端驗證狀態和交換模式：

```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
Client MAC Address..... 00:24:d7:2b:7c:0c
Client Username ..... N/A
AP MAC Address..... d0:57:4c:08:e6:70
Client State..... Associated
H-REAP Data Switching..... Local
H-REAP Authentication..... Local
```

FlexConnect VLAN覆蓋

在當前的FlexConnect架構中，WLAN到VLAN的對映非常嚴格，因此在FlexConnect AP上關聯到特定WLAN的客戶端必須遵守對映到該客戶端的VLAN。此方法有侷限性，因為它要求客戶端與不同的SSID關聯以繼承不同的基於VLAN的策略。

從7.2版本開始，支援為本地交換配置的單個WLAN上的AAA覆蓋VLAN。為了進行動態VLAN分配，AP將根據配置預先建立VLAN的介面，使用單個FlexConnect AP的現有WLAN-VLAN對映或FlexConnect組上的ACL-VLAN對映。WLC用於在AP上預先建立子介面。



摘要

- 從7.2版起，對於在中央和本地身份驗證模式下配置為本地交換的WLAN，支援AAA VLAN覆蓋。
- 應在為本地交換配置的WLAN上啟用AAA覆蓋。
- FlexConnect AP應從WLC預建立VLAN，以便進行動態VLAN分配。
- 如果AAA覆蓋返回的VLAN不在AP客戶端上，它們將從AP的預設VLAN介面獲取IP。

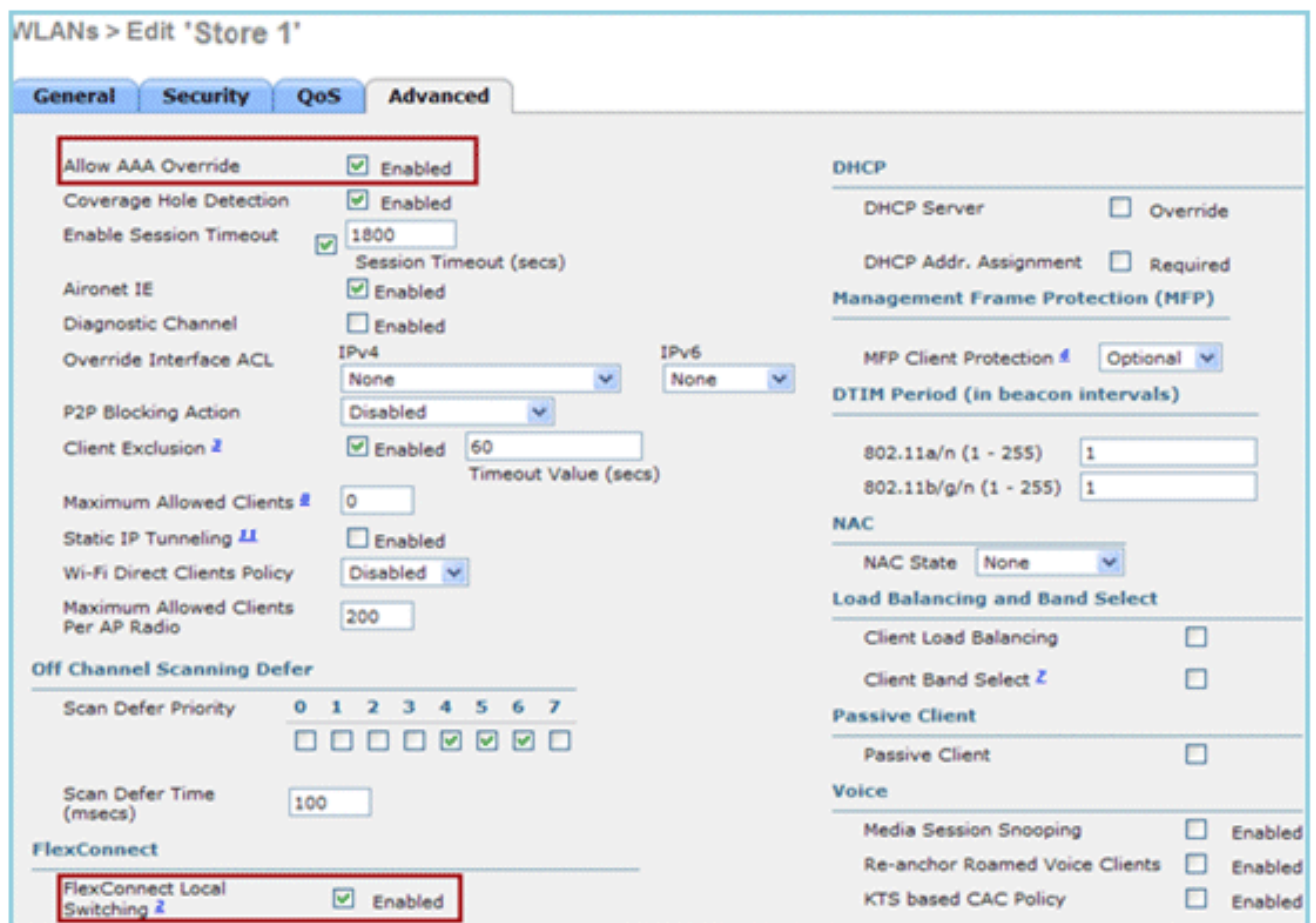
程式

請完成以下步驟：

1. 建立用於802.1x身份驗證的WLAN。



2. 在WLC上啟用本地交換WLAN的AAA覆寫支援。導覽至WLAN GUI > WLAN > WLAN ID > Advanced索引標籤。



3. 在控制器上新增AAA伺服器詳細資訊以進行802.1x身份驗證。若要新增AAA伺服器，請導覽至WLC GUI > Security > AAA > Radius > Authentication > New。

Security **RADIUS Authentication Servers > Edit**

AAA
 General
 RADIUS
 Authentication
 Accounting
 Fallback
 TACACS+
 LDAP
 Local Net Users
 MAC Filtering
 Disabled Clients
 User Login Policies
 AP Policies
 Password Policies
 Local EAP
 Priority Order
 Certificate
 Access Control Lists
 Wireless Protection Policies

Server Index: 1
 Server Address: [Redacted]
 Shared Secret Format: ASCII
 Shared Secret: [Redacted]
 Confirm Shared Secret: [Redacted]

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
 Port Number: 1812
 Server Status: Enabled
 Support for RFC 3576: Enabled
 Server Timeout: 2 seconds
 Network User: Enable
 Management: Enable
 IPSec: Enable

4. AP預設處於本地模式，因此將該模式轉換為FlexConnect模式。通過轉至無線 > 所有AP，然後按一下單個AP，可以將本地模式AP轉換為FlexConnect模式。

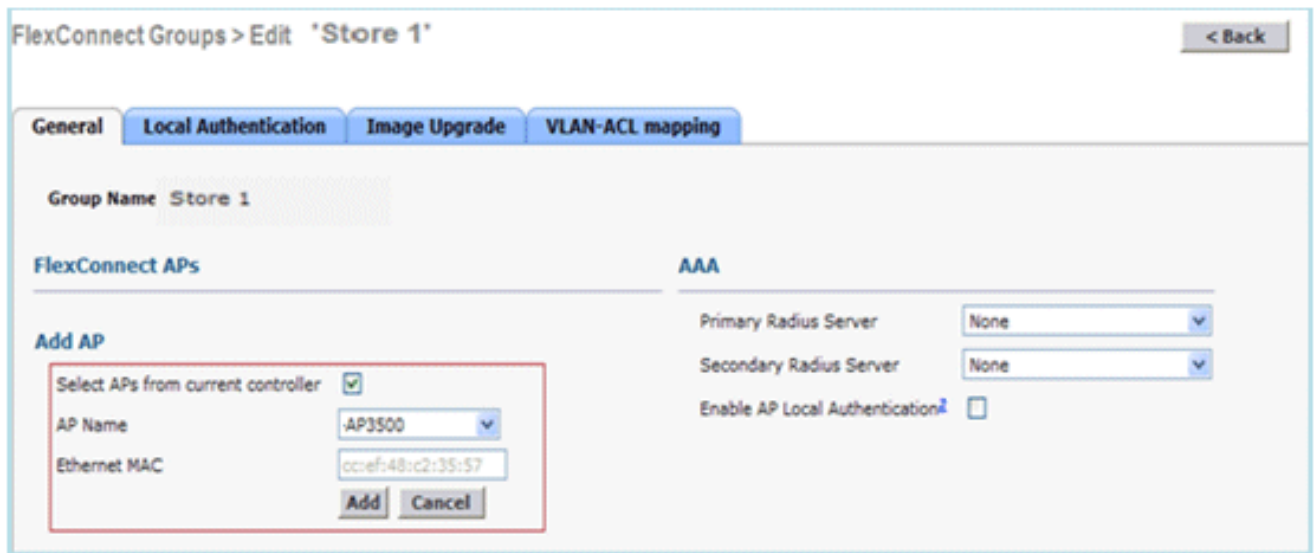
All APs > Details for AP3500

General Credentials Interfaces High Availability Inventory Advanced

General

AP Name	AP3500	Primary Software Version	7.2.1.69
Location	default location	Backup Software Version	7.2.1.72
AP MAC Address	cc:ef:48:c2:35:57	Predownload Status	None
Base Radio MAC	2c:3f:38:f6:98:b0	Predownloaded Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	12.4.23.0
Operational Status	REG	IOS Version	12.4(20111122:141426)\$
Port Number	1	Mini IOS Version	7.0.112.74
Venue Group	Unspecified	IP Config	
Venue Type	Unspecified	IP Address	10.10.10.132
Venue Name		Static IP	<input type="checkbox"/>
Language		Time Statistics	
Network Spectrum Interface Key	0D45BA896226F4117D98BA920FBA8A16	UP Time	0 d, 00 h 01 m 14 s
		Controller Associated Time	0 d, 00 h 00 m 14 s
		Controller Association Latency	0 d, 00 h 00 m 59 s

5. 將FlexConnect AP新增到FlexConnect組。導覽至WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General索引標籤 > Add AP。



6. FlexConnect AP應在中繼埠上連線，並且應在中繼埠上允許WLAN對映VLAN和AAA覆蓋

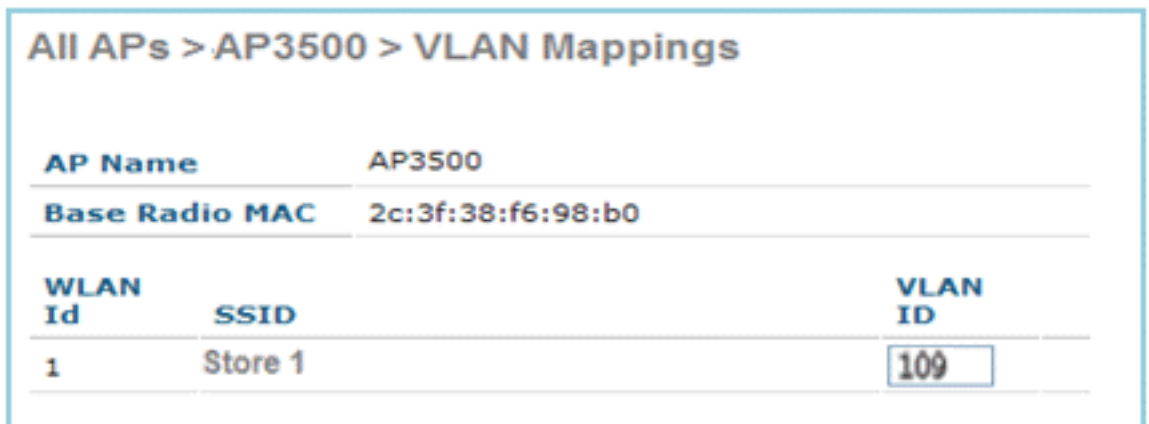
```
interface GigabitEthernet1/0/4
description AP3500
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk
```

VLAN。

注意：在此配置中，vlan 109用於

WLAN VLAN對映，vlan 3用於AAA覆蓋。

7. 為FlexConnect AP配置WLAN到VLAN的對映。根據此配置，AP將具有VLAN介面。當AP收到VLAN配置時，會建立相應的dot11和乙太網子介面，並將其新增到網橋組中。在此WLAN上關聯客戶端，當該客戶端關聯時，分配其VLAN（預設基於WLAN-VLAN對映）。導覽至WLAN GUI > **Wireless** > **All APs** > 按一下特定的AP > **FlexConnect**標籤，然後按一下VLAN

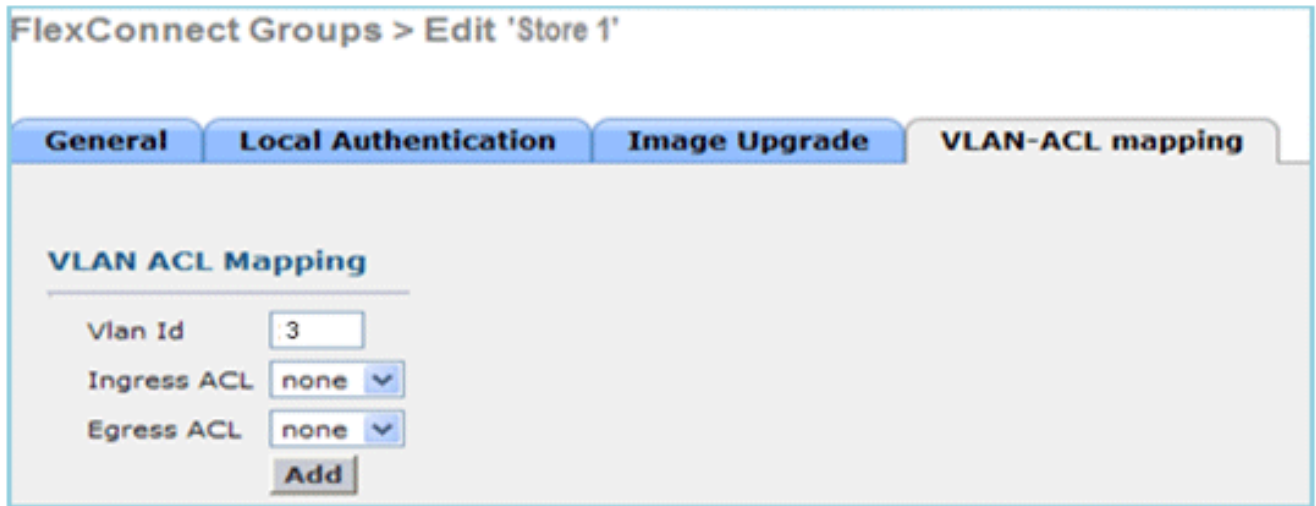


Mapping。

8. 在AAA伺服器中建立使用者，並將使用者配置為返回IETF Radius屬性中的VLAN ID。

Attribute	Type	Value
IETF 65	Tunnel-Medium-Type	Tagged Enum [T:1] 802
IETF 64	Tunnel-Type	Tagged Enum [T:1] VLAN
IETF 81	Tunnel-Private-Group-ID	Tagged String [T:1] 3

9. 為了進行動態VLAN分配，AP將使用單個FlexConnect AP的現有WLAN-VLAN對映或FlexConnect組上的ACL-VLAN對映根據配置預先建立動態VLAN的介面。若要在FlexConnect AP上設定AAA VLAN，請導覽至WLC GUI > **Wireless** > **FlexConnect Group** > 按一下特定的FlexConnect群組 > **VLAN-ACL對映**，然後在Vlan ID欄位中輸入VLAN。



10. 在此WLAN上關聯客戶端，並使用AAA伺服器中配置的使用者名稱進行身份驗證，以返回AAA VLAN。
11. 客戶端應從通過AAA伺服器返回的動態VLAN接收IP地址。
12. 若要驗證，請按一下WLC GUI > Monitor > Client >按一下特定使用者端MAC位址以檢查使用者端詳細資訊。

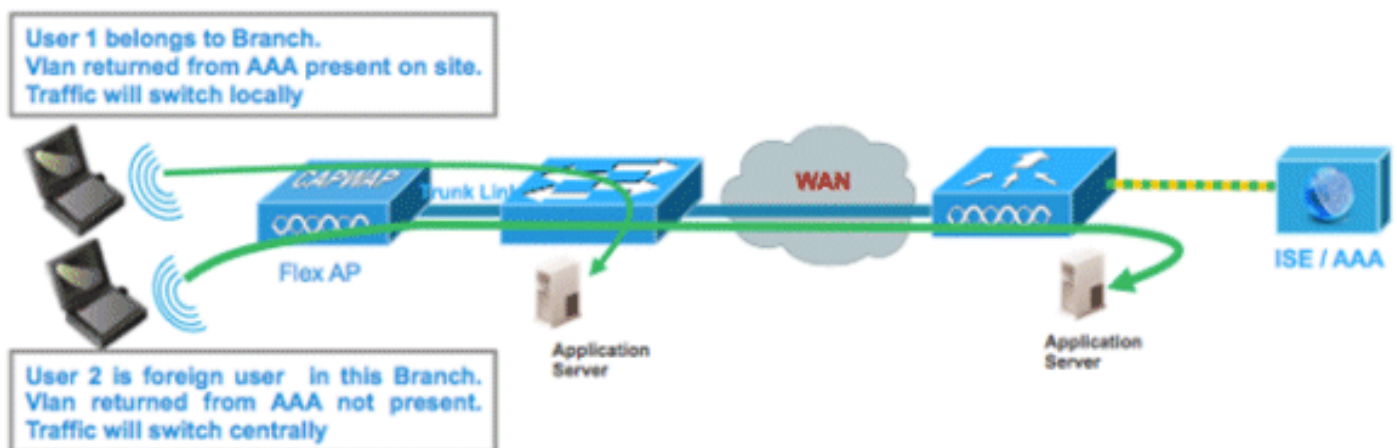
限制

- 不支持Cisco Airespace特定的屬性，並且僅支援IETF屬性VLAN ID。
- 通過單個FlexConnect接入點的WLAN-VLAN對映或使用FlexConnect組上的ACL-VLAN對映，每個AP配置中最多可配置16個VLAN。

FlexConnect VLAN型中央交換

在控制器軟體版本7.2中，本地交換WLAN的VLAN（動態VLAN分配）的AAA覆寫會將無線使用者端放到AAA伺服器提供的VLAN中。如果AAA伺服器提供的VLAN在AP上不存在，則客戶端被置於該AP上的WLAN對映VLAN中，流量將在該VLAN上本地交換。此外，在7.3版之前，來自FlexConnect AP的特定WLAN流量可以根據WLAN配置進行集中或本地交換。

從7.3版開始，根據FlexConnect AP上是否存在VLAN，來自FlexConnect AP的流量可以集中交換或本地交換。



摘要

當Flex AP處於連線模式時，為本地交換配置的WLAN上的流量傳輸：

- 如果VLAN作為AAA屬性之一返回，且該VLAN不存在於Flex AP資料庫中，則流量將集中交換，並且如果VLAN存在於WLC上，客戶端將被分配從AAA伺服器返回的此VLAN/介面。
- 如果VLAN作為AAA屬性之一返回，且該VLAN不在Flex AP資料庫中，則流量將集中交換。如果WLC上不存在該VLAN，則會為使用者端指派一個對應到WLC上的WLAN的VLAN/介面。
- 如果VLAN作為AAA屬性之一返回，且該VLAN存在於FlexConnect AP資料庫中，則流量將在本地交換。
- 如果沒有從AAA伺服器返回VLAN，將為客戶端分配該FlexConnect AP上的WLAN對映VLAN，並且流量將在本地交換。

當Flex AP處於獨立模式時，為本地交換配置的WLAN上的流量傳輸：

- 如果AAA伺服器傳回的VLAN不存在於Flex AP資料庫中，則使用者端將被置於預設VLAN中（即Flex AP上的WLAN對應VLAN）。當AP連線回時，此客戶端將取消身份驗證並集中交換流量。
- 如果AAA伺服器返回的VLAN存在於Flex AP資料庫中，則客戶端將被置於返回的VLAN中，流量將在本地交換。
- 如果未從AAA伺服器返回VLAN，則將為客戶端分配該FlexConnect AP上的WLAN對映VLAN，並且流量將在本地交換。

程式

請完成以下步驟：

1. 為本地交換配置WLAN並啟用AAA覆蓋。

WLANs > Edit 'Store 1'

General	Security	QoS	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
Diagnostic Channel	<input type="checkbox"/>	Enabled	
Override Interface ACL		IPv4 None <input type="button" value="v"/>	IPv6 None <input type="button" value="v"/>
P2P Blocking Action		Disabled <input type="button" value="v"/>	
Client Exclusion ³	<input checked="" type="checkbox"/>	Enabled	60 Timeout Value (secs)
Maximum Allowed Clients ⁶		<input type="text" value="0"/>	
Static IP Tunneling ¹¹	<input type="checkbox"/>	Enabled	
Wi-Fi Direct Clients Policy		Disabled <input type="button" value="v"/>	
Maximum Allowed Clients Per AP Radio		<input type="text" value="200"/>	
FlexConnect			
FlexConnect Local Switching ²	<input checked="" type="checkbox"/>	Enabled	

2. 在新建立的WLAN上啟用基於Vlan的集中交換。

WLANs > Edit 'Store 1'

General

Security

QoS

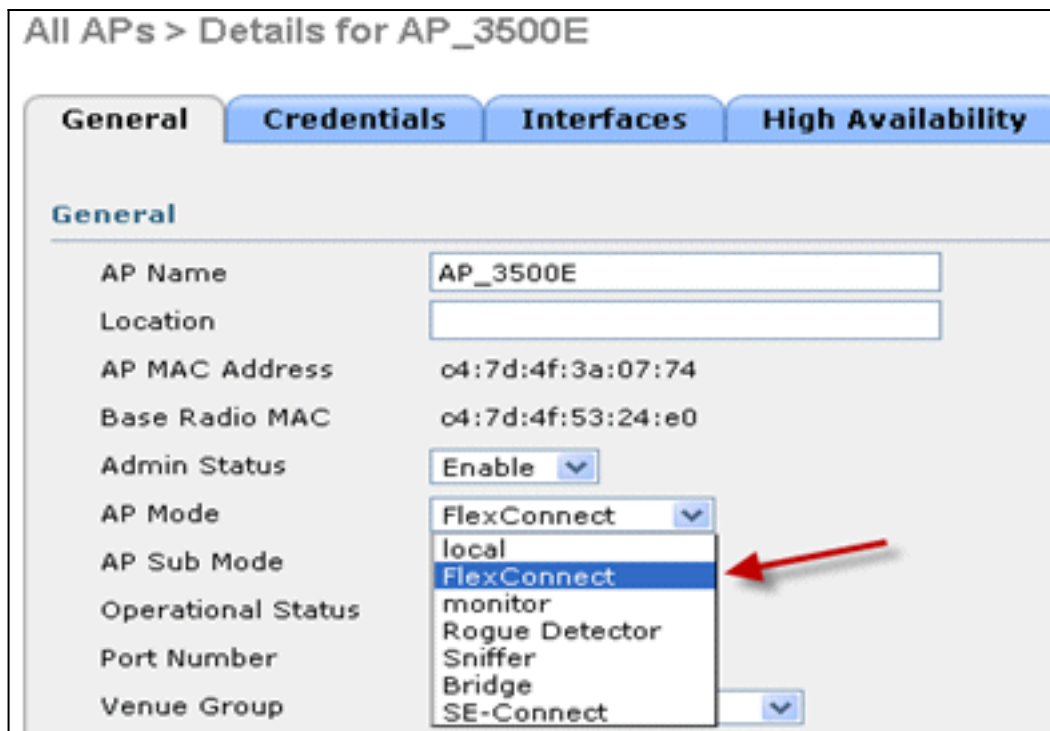
Advanced

Allow AAA Override	<input checked="" type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> <input type="text" value="1800"/> Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <input type="text" value="None"/> IPv6 <input type="text" value="None"/>
P2P Blocking Action	<input type="text" value="Disabled"/>
Client Exclusion 3	<input checked="" type="checkbox"/> Enabled <input type="text" value="60"/> Timeout Value (secs)
Maximum Allowed Clients 8	<input type="text" value="0"/>
Static IP Tunneling 11	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	<input type="text" value="Disabled"/>
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>

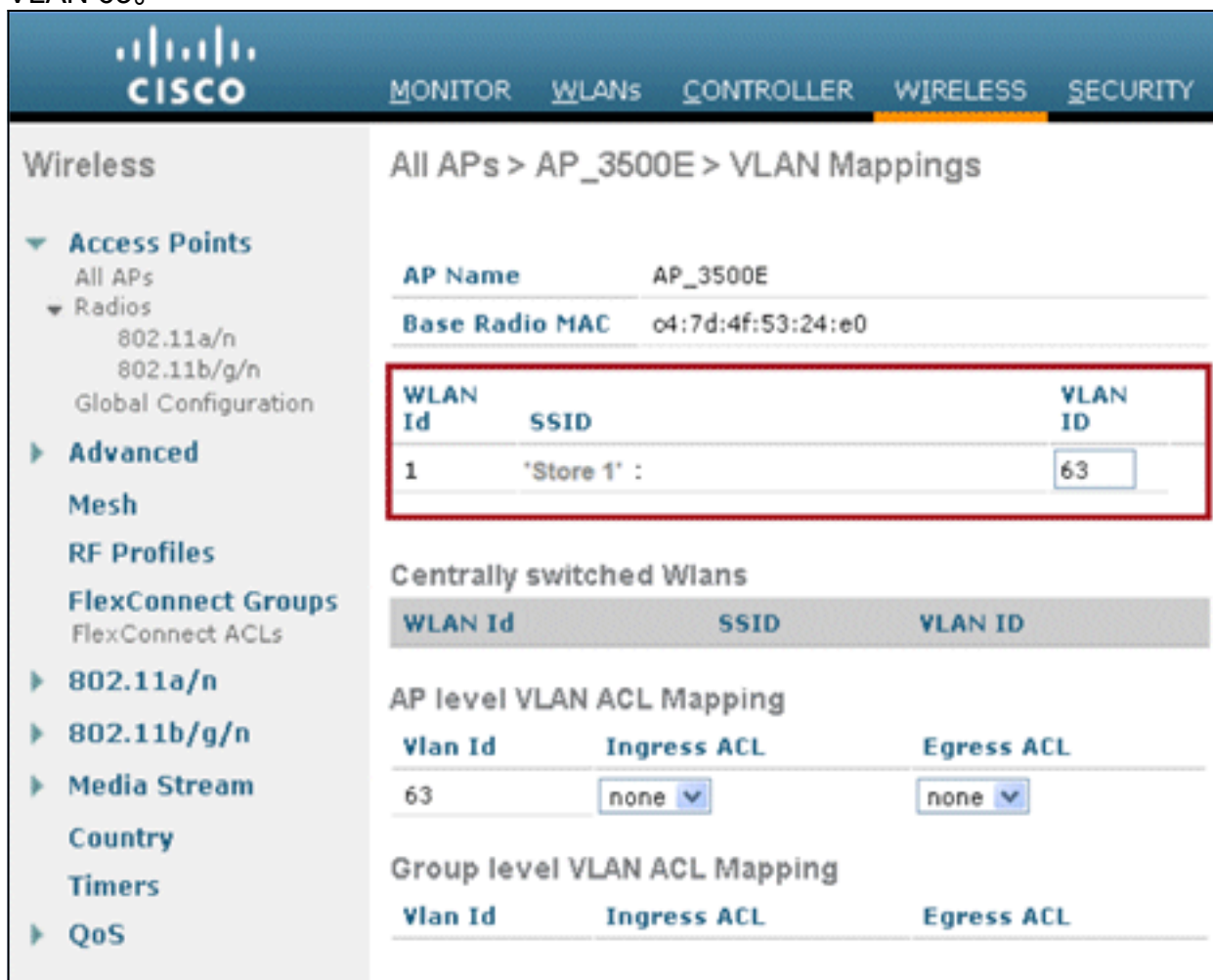
FlexConnect

FlexConnect Local Switching 2	<input checked="" type="checkbox"/> Enabled
FlexConnect Local Auth 12	<input type="checkbox"/> Enabled
Learn Client IP Address 5	<input checked="" type="checkbox"/> Enabled
Vlan based Central Switching 13	<input checked="" type="checkbox"/> Enabled

3. 將AP模式設定為FlexConnect。



4. 確保FlexConnect AP的資料庫中存在一些子介面，或者通過特定Flex AP上的WLAN-VLAN對映，或者通過從Flex組配置VLAN。在本示例中，在Flex AP上的WLAN-VLAN對映中配置了VLAN 63。



5. 在本範例中，WLC上的VLAN 62設定為其中一個動態介面，且不會對映到WLC上的WLAN。WLC上的WLAN對映到管理VLAN (即VLAN 61)。

Cisco					
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK					
Controller	Interfaces				
General					
Inventory					
Interfaces					
Interface Groups					
Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	
dyn	62	9.6.62.10	Dynamic	Disabled	▼
management	61	9.6.61.2	Static	Enabled	

6. 將客戶端與此Flex AP上步驟1中配置的WLAN關聯並從AAA伺服器返回VLAN 62。此Flex AP上不存在VLAN 62，但WLC上卻將其作為動態介面存在，因此流量將集中交換，並在WLC上為客戶端分配VLAN 62。在此捕獲的輸出中，為客戶端分配了VLAN 62，並將資料交換和身份驗證設定為**Central**。

Monitor		Clients > Detail	
Summary			
Access Points			
Cisco CleanAir			
Statistics			
CDP			
Rogues			
Redundancy			
Clients			
Multicast			
Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.62.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	3
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented
Client Type	Regular		
User Name	betouser		
Port Number	1		
Interface	dyn		
VLAN ID	62		

注意：請注意，雖然WLAN配置為本地交換，但基於VLAN的存在（即從AAA伺服器返回的VLAN 62不在AP資料庫中），此客戶端的「資料交換」欄位為「中心」。

7. 如果另一個使用者與此建立的WLAN上的相同AP建立關聯，且一些VLAN從AAA伺服器傳回（AP上並不存在）以及WLC上，流量會集中交換，且使用者端會分配到WLC上的WLAN對應介面（也就是此範例設定中的VLAN 61），因為WLAN會對應到為VLAN 61設定的管理介面

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Central
		Authentication	Central
Client Type	Regular	Status	Associated
User Name	betauser2	Association ID	1
Port Number	1	802.11 Authentication	Open System
Interface	management	Reason Code	3
VLAN ID	61	Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Not Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented

注意：請注意，儘管WLAN配置為本地交換，但基於VLAN的存在，此客戶端的「資料交換」欄位為「中心」。即，從AAA伺服器返回的VLAN 61不在AP資料庫中，但在WLC資料庫中也不存在。因此，系統會為客戶端分配一個對映到WLAN的預設介面VLAN/介面。在本例中，WLAN對映到管理介面（即VLAN 61），因此客戶端從VLAN 61收到IP地址。

8. 如果另一個使用者在此建立的WLAN上與其建立關聯，並且VLAN 63從AAA伺服器（該Flex AP上存在）返回，則將為客戶端分配VLAN 63，流量將在本地交換。

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

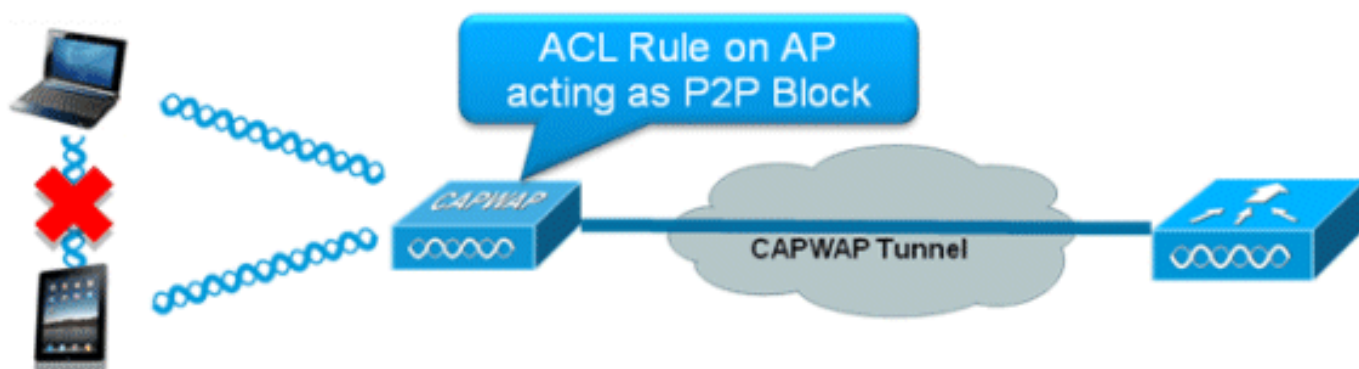
限制

- 只有為中央身份驗證和本地交換配置的WLAN支援基於VLAN的中央交換。
- 應在FlexConnect AP上配置AP子介面（即VLAN對映）。

FlexConnect ACL

在FlexConnect上引入ACL後，有一種機制可以滿足FlexConnect AP的訪問控制需求，從而保護來自AP的本地交換資料流量並保持其完整性。FlexConnect ACL在WLC上建立，然後應使用VLAN-

ACL對映 (將用於AAA覆蓋VLAN) 配置FlexConnect AP或FlexConnect組上存在的VLAN。然後，將這些內容推送到無線接入點。



摘要

- 在控制器上建立FlexConnect ACL。
- 將其應用於AP級別VLAN ACL對映下的FlexConnect AP上的VLAN。
- 可以應用於VLAN-ACL對映下FlexConnect組中的VLAN (通常用於AAA覆蓋的VLAN) 。
- 在VLAN上套用ACL時，請選擇要套用的方向，即「ingress」、「egress」或「ingress and egress」。

程式

請完成以下步驟：

1. 在WLC上建立FlexConnect ACL。導覽至WLC GUI > Security > Access Control List > FlexConnect ACLs。

The screenshot shows the 'FlexConnect Access Control Lists' configuration page in the WLC GUI. The page title is 'FlexConnect Access Control Lists' and it shows 'Entries 0 - 0 of 0'. There is a 'New...' button in the top right corner. Below the title, there is a table with one column labeled 'Acl Name'.

2. 按一下「New」。
3. 配置ACL名稱。

Access Control Lists > New

Access Control List Name

4. 按一下「Apply」。
5. 為每個ACL建立規則。若要建立規則，請導覽至WLC GUI > Security > Access Control List > FlexConnect ACL，然後按一下上述建立的ACL。

Access Control Lists > Edit

General

Access List Name Flex-ACL-Ingress

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP

6. 按一下「Add New Rule」。

Access Control Lists > Rules > New

Sequence

Source IP Address Netmask

Destination IP Address Netmask

Protocol

DSCP

Action

注意： 根據需要配置規則。如果在終端未配置permit any any規則，則存在將阻止所有流量的隱式deny。

7. 建立FlexConnect ACL後，可以將其對映為單個FlexConnect AP下的WLAN-VLAN對映，也可以將其應用於FlexConnect組上的VLAN-ACL對映。
8. 在每個FlexConnect AP的VLAN對映下，將上面配置的各VLAN的AP級別的FlexConnect ACL對映。導覽至WLC GUI > Wireless > All AP >按一下特定的AP > FlexConnect標籤> VLAN對映。

All APs > AP3500 > VLAN Mappings

AP Name	AP3500	
Base Radio MAC	2c:3f:38:f6:98:b0	
WLAN Id	SSID	VLAN ID
1	Store 1	109

Centrally switched Wlans

WLAN Id	SSID	VLAN ID
2	Store 3	N/A

AP level VLAN ACL Mapping

Vlan Id	Ingress ACL	Egress ACL
109	Flex-ACL-Ingress	Flex-ACL-Egress

9. FlexConnect ACL還可以應用於FlexConnect組中的VLAN-ACL對映。在FlexConnect組中的VLAN-ACL對映下建立的VLAN主要用於動態VLAN覆蓋。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade **VLAN-ACL mapping**

VLAN ACL Mapping

Vlan Id

Ingress ACL Flex-ACL-Egress

Egress ACL Flex-ACL-Egress

Add

Vlan Id	Ingress ACL	Egress ACL
3	Flex-ACL-Ingress	Flex-ACL-Egress

限制

- WLC上最多可以設定512個FlexConnect ACL。
- 每個單獨的ACL可以配置64條規則。
- 每個FlexConnect組或每個FlexConnect AP最多可對映32個ACL。
- 在任何給定的時間點，FlexConnect AP上最多有16個VLAN和32個ACL。

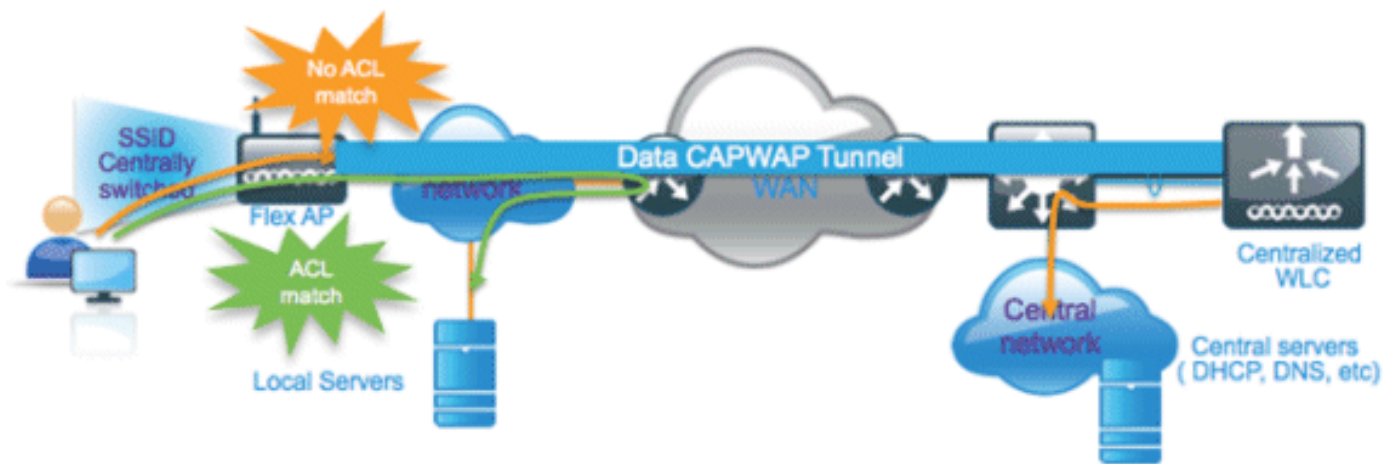
FlexConnect分割通道

在7.3之前的WLC版本中，如果連線到與中央交換WLAN關聯的FlexConnect AP上的客戶端需要將某些流量傳送到本地站點/網路中的裝置，則它們需要通過CAPWAP將流量傳送到WLC，然後通過CAPWAP或使用某些帶外連線將相同的流量返回到本地站點。

從7.3版開始，**分割通道**引入了一種機制，通過該機制，客戶端傳送的流量將使用**Flex ACL**根據封包內容進行分類。從Flex AP本地交換匹配資料包，其餘資料包通過CAPWAP集中交換。

分割隧道功能是OEAP AP設定的一個額外優勢，在該設定中，公司SSID上的客戶端可以直接與本地網路中的裝置（印表機、遠端LAN埠上的有線電腦或個人SSID上的無線裝置）進行通訊，而無需通過CAPWAP傳送資料包來消耗WAN頻寬。OEAP 600 AP不支援拆分隧道。可以使用規則建立Flex ACL，以允許本地站點/網路上的所有裝置。當來自公司SSID上無線客戶端的資料包與在OEAP AP上配置的Flex ACL中的規則匹配時，該流量將在本地交換，而其餘的流量（即隱式拒絕流量）將通過CAPWAP集中交換。

分割隧道解決方案假設本地站點中不存在與中心站點中的客戶端相關聯的子網/VLAN（即，從中心站點上的子網接收IP地址的客戶端的流量將無法進行本地交換）。分割隧道功能旨在本地交換屬於本地站點的子網的流量，以避免WAN頻寬消耗。與Flex ACL規則匹配的流量在本地交換，並執行NAT操作，將客戶端的源IP地址更改為Flex AP的BVI介面IP地址，該地址可在本地站點/網路路由。



摘要

- 為僅由Flex AP通告的中央交換配置的WLAN支援分割隧道功能。
- 應在為分割隧道配置的WLAN上啟用所需的DHCP。
- 分割通道組態會套用每個WLAN，且設定為每個Flex AP上的中央交換或FlexConnect組中的所有Flex AP。

程式

請完成以下步驟：

1. 為中央交換配置WLAN(即不應啟用Flex Local Switching)。

WLANs > Edit 'Store 1'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

FlexConnect

FlexConnect Local Switching Enabled

Flex Local Switching should not be enabled

2. 將DHCP地址分配設定為必需。

WLANs > Edit 'Store 1'

General **Security** **QoS** **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

DHCP

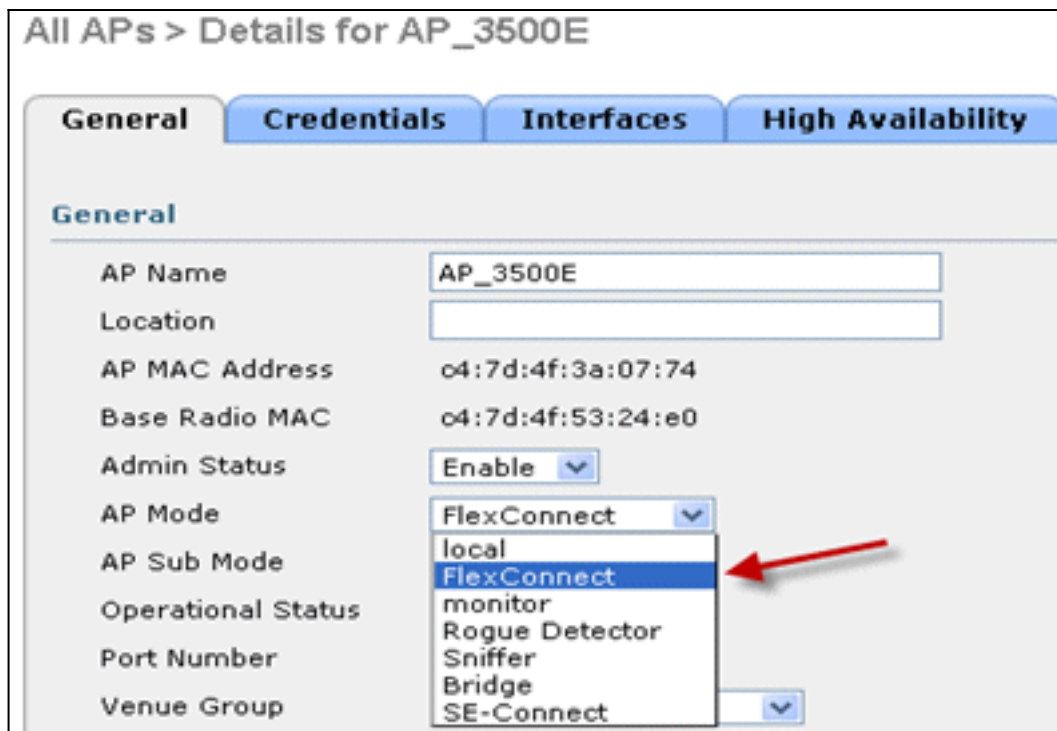
DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection

3. 將AP模式設定為FlexConnect。



4. 為應該在中央交換機WLAN上本地交換的流量配置FlexConnect ACL的允許規則。在本例中，FlexConnect ACL規則配置為在對Flex AP應用NAT操作後，向9.6.61.0子網（即存在於中心站點）上的所有客戶端向9.1.0.150發出警報，以本地交換來自FlexAP的所有客戶端的ICMP流量。其餘流量將到達隱式拒絕規則，並通過CAPWAP進行集中交換。



5. 此建立的FlexConnect ACL可以作為拆分隧道ACL推送到各個Flex AP，也可以推送到一個Flex Connect組中的所有Flex AP。完成以下步驟，將Flex ACL作為本地拆分ACL推送到各個Flex AP:按一下「Local Split ACLs」。

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main content area is titled 'All APs > Details for AP_3500E'. The 'FlexConnect' tab is selected and highlighted with a red box. Below the tabs, the 'VLAN Support' checkbox is checked, and the 'Native VLAN ID' is set to 57. The 'FlexConnect Group Name' is 'Not Configured'. Under the 'PreAuthentication Access Control Lists' section, the 'Local Split ACLs' link is highlighted with a red box and a red arrow pointing to it.

選擇應啟用分割隧道功能的WLAN Id，選擇Flex-ACL，然後按一下Add。

The screenshot shows the 'All APs > AP_3500E > ACL Mappings' configuration page. The 'AP Name' is 'AP_3500E' and the 'Base Radio MAC' is '04:7d:4f:53:24:e0'. The 'WLAN ACL Mapping' form is highlighted with a red box. It contains the following fields: 'WLAN Id' with the value '1', 'Local-Split ACL' with a dropdown menu set to 'Flex-ACL', and an 'Add' button. Two callout boxes with red arrows provide instructions: one points to the 'WLAN Id' field with the text 'Enter WLAN ID on which Split Tunnel should be enabled', and another points to the 'Add' button with the text 'Click Add after selecting Flex ACL'. Below the form is a table with columns for 'WLAN Id', 'WLAN Profile Name', and 'Local-Split ACL'.

Flex-ACL會作為本地拆分ACL推送到Flex AP。

All APs > AP_3500E > ACL Mappings

AP Name AP_3500E

Base Radio MAC 04:7d:4f:53:24:e0

WLAN ACL Mapping

WLAN Id

Local-Split ACL ▼

Add

WLAN Id	WLAN Profile Name	Local-Split ACL
1	'Store 1'	Flex-ACL ▼

完成

以下步驟，將Flex ACL作為本地拆分ACL推送到FlexConnect組：選擇應啟用分割隧道功能的WLAN ID。在「WLAN-ACL mapping」頁籤上，從新增了特定Flex AP的FlexConnect組中選擇FlexConnect ACL，然後按一下Add。

Wireless FlexConnect Groups > Edit Flex-Group'

General Local Authentication Image Upgrade AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id WebAuth ACL ▼ Add

Local Split ACL Mapping

WLAN Id Local Split ACL ▼ Add

Enter WLAN ID on which Split Tunnel should be enabled

Click ADD after selecting Flex ACL

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL
			1	'Store 1'	Flex-ACL ▼

將Flex-ACL作為本地拆分ACL推送到該Flex組中的Flex AP。

Wireless FlexConnect Groups > Edit Flex-Group'

General Local Authentication Image Upgrade AAA VLAN-ACL mapping **WLAN-ACL mapping** WebPolicies

Web Auth ACL Mapping

WLAN Id WebAuth ACL ▼ Add

Local Split ACL Mapping

WLAN Id Local Split ACL ▼ Add

WLAN Id	WLAN Profile Name	WebAuth ACL	WLAN Id	WLAN Profile Name	LocalSplit ACL
			1	'Store 1'	Flex-ACL ▼

限制

- 不應使用permit/deny語句配置Flex ACL規則，該語句的子網與源和目標相同。
- 只有在無線客戶端為本地站點上存在的主機發起流量時，為分割隧道配置的集中交換WLAN上的流量才能在本機交換。如果流量由本地站點上的客戶端/主機為這些已配置的WLAN上的無線客戶端發起，則流量將無法到達目的地。
- 多點傳送/廣播流量不支援分割通道。即使組播/廣播流量與Flex ACL匹配，也會集中進行交換。

容錯能力

FlexConnect容錯允許在以下情況下對分支機構客戶端進行無線訪問和服務：

- FlexConnect分支機構AP與主Flex 7500控制器失去連線。
- FlexConnect分支機構AP正在切換到輔助Flex 7500控制器。
- FlexConnect分支機構AP正在重新建立與主Flex 7500控制器的連線。

FlexConnect容錯和上述本地EAP一起在網路故障期間提供零分支停機時間。此功能預設啟用，無法禁用。不需要在控制器或AP上進行配置。但是，為確保容錯順利運行且適用，應保持以下標準：

- WLAN的訂購和配置必須在主控制器和備用Flex 7500控制器上完全相同。
- VLAN對映必須在主控制器和備用Flex 7500控制器之間完全相同。
- 移動域名必須在主控制器和備用Flex 7500控制器之間完全相同。
- 建議使用Flex 7500作為主要和備份控制器。

摘要

- 如果AP連線到同一控制器，且控制器上的配置沒有更改，則FlexConnect不會斷開客戶端連線。
- 如果配置沒有變化，並且備份控制器與主控制器相同，則FlexConnect在連線到備份控制器時不會斷開客戶端連線。
- 如果控制器上的配置沒有更改，FlexConnect在連線回主控制器時不會重置其無線電。

限制

- 僅支援使用本地交換的中央/本地身份驗證的FlexConnect。
- 如果客戶端會話計時器在FlexConnect AP從獨立模式切換到連線模式之前到期，集中身份驗證的客戶端需要完全重新身份驗證。
- Flex 7500主控制器和備份控制器必須位於同一個移動域中。

每個WLAN的客戶端限制

隨著流量分割，需要限制訪問無線服務的客戶端總數。

範例：限制從分支機構隧道返回到資料中心的訪客客戶端總數。

為了解決這一難題，思科推出了「每個WLAN的客戶端限制」功能，該功能可以限制每個WLAN允許的客戶端總數。

主要目標

- 設定最大客戶端限制
- 易於操作

注意：這不是一種QoS形式。

預設情況下，該功能處於禁用狀態，不會強制限制。

限制

當FlexConnect處於獨立操作狀態時，此功能不會強制實施客戶端限制。

WLC組態

請完成以下步驟：

1. 選擇帶有SSID **DataCenter**的集中交換WLAN ID 1。此WLAN是在建立AP組期間建立的。請參見圖8。
2. 按一下**Advanced**頁籤以檢視WLAN ID 1。
3. 為「允許的最大客戶端數」文本欄位設定客戶端限制值。
4. 在設定「允許的最大客戶端數」文本欄位後，按一下**Apply**。

WLANs > Edit

General Security QoS **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout 1800
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

IPv6 Enable

Override Interface ACL

P2P Blocking Action

Client Exclusion 60
Timeout Value (secs)

Maximum Allowed Clients

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7

Scan Defer Time(msecs)

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

Management Frame Protection (MFP)

MFP Client Protection

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC OOB State Enabled

Posture State Enabled

Load Balancing and Band Select

Client Load Balancing

Client Band Select

Foot Notes

2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication

3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)

4 Client MFP is not active unless WPA2 is configured

5 Learn Client IP is configurable only when HREAP Local Switching is enabled

6 WMM and open or AES security should be enabled to support higher II in rates

7 Multicast Should Be Enabled For IPV6.

8 Band Select is configurable only when Radio Policy is set to 'All'.

9 Value zero implies there is no restriction on maximum clients allowed.

10 MAC Filtering is not supported with HREAP Local authentication

「允許的最大客戶端數」的預設值設定為0，這意味著沒有限制，該功能被禁用。

NCS配置

若要從NCS啟用此功能，請前往Configure > Controllers > Controller IP > WLANs > WLAN Configuration > WLAN Configuration Details。

WLAN Configuration Details : 17

Configure > Controllers > 172.20.225.154 > WLANs > WLAN Configuration > **WLAN Configuration Details**

General Security QoS **Advanced**

FlexConnect Local Switching	<input type="checkbox"/> Enable	
FlexConnect Local Auth ⁱ	<input type="checkbox"/> Enable	
Learn Client IP Address	<input type="checkbox"/> Enable	
Session Timeout	<input checked="" type="checkbox"/> Enable	1800 (secs)
Coverage Hole Detection	<input checked="" type="checkbox"/> Enable	
Aironet IE	<input checked="" type="checkbox"/> Enable	
IPv6 [?]	<input type="checkbox"/> Enable	
Diagnostic Channel [?]	<input type="checkbox"/> Enable	
Override Interface ACL	IPv4	NONE ^v
	IPv6	NONE ^v
Peer to Peer Blocking ⁱ		Disable ^v
Wi-Fi Direct Clients Policy		Disabled ^v
Client Exclusion [!]	<input checked="" type="checkbox"/> Enable	
Timeout Value		60 (secs)
Maximum Clients ⁱ		0

DHCP

DHCP Server
DHCP Address Assignment

Management Frame Protection

MFP Client Protection [?]
MFP Version

Load Balancing and Band Sel

Client Load Balancing
Client Band Select

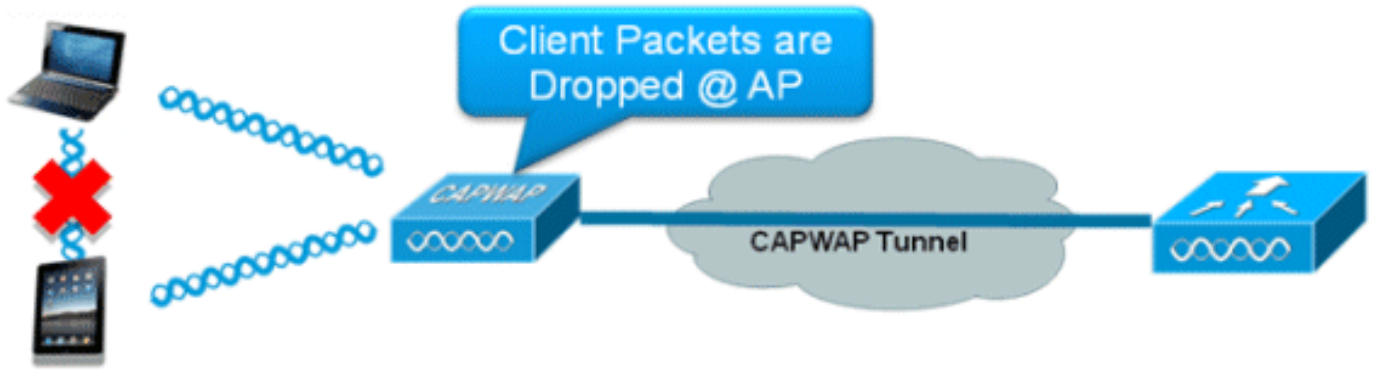
NAC

點對點封鎖

在7.2之前的控制器軟體版本中，只有中央交換WLAN支援對等(P2P)封鎖。可以使用以下三種操作中的任一種在WLAN上配置對等阻塞：

- **Disabled** — 為相同子網中的使用者端在控制器內本地停用對等封鎖和橋接流量。這是預設值。
- **Drop** — 使控制器丟棄同一子網中客戶端的資料包。
- **Forward Up-Stream** — 使資料包在上游VLAN上轉發。控制器上方的裝置決定對封包採取什麼動作。

自7.2版起，本地交換WLAN上關聯的客戶端支援點對點阻塞。根據WLAN，對等配置由控制器推送到FlexConnect AP。



摘要

- 每WLAN配置點對點阻塞
- 根據WLAN，WLC會將點對點封鎖組態推送到FlexConnect AP。
- 在WLAN上配置為丟棄或上游轉發的對等阻塞操作被視為在FlexConnect AP上啟用的對等阻塞。

程式

請完成以下步驟：

1. 啟用點對點阻止操作，作為為FlexConnect本地交換配置的WLAN上的Drop。

2. 將P2P阻塞操作配置為為本地交換配置的WLAN上的Drop或Forward-Upstream後，它將從WLC推送到FlexConnect AP。FlexConnect AP將此資訊儲存在快閃記憶體中的reap配置檔案中。這樣，即使FlexConnect AP處於獨立模式，它也可以在相應的子介面上應用P2P配置。

限制

- 在FlexConnect中，解決方案P2P阻塞配置不能僅應用於特定FlexConnect AP或AP子集。它適用於廣播SSID的所有FlexConnect AP。
- 適用於中央交換客戶端的統一解決方案支援P2P上行轉發。但是，FlexConnect解決方案不支援

此操作。這被視為P2P丟棄，客戶端資料包被丟棄，而不是轉發到下一個網路節點。

- 適用於中央交換客戶端的統一解決方案支援與不同AP關聯的客戶端的P2P封鎖。但是，此解決方案僅針對連線到同一AP的客戶端。FlexConnect ACL可用作此限制的解決方法。

AP預映像下載

此功能允許AP在運行時下載代碼。AP映像前下載在減少軟體維護或升級期間的網路停機時間方面非常有用。

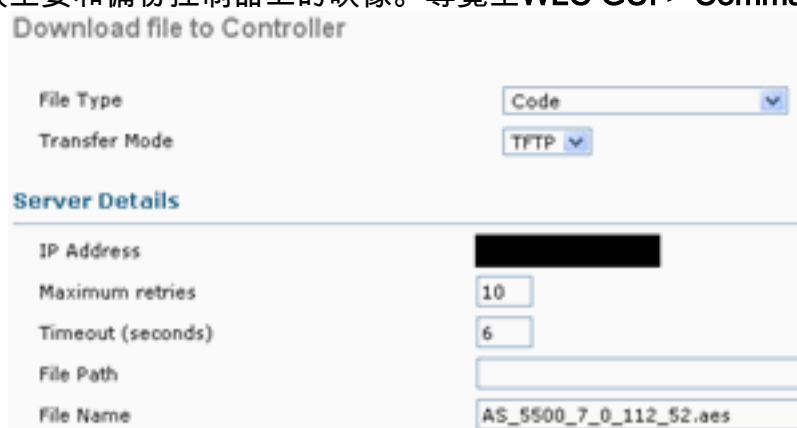
摘要

- 易於軟體管理
- 計畫每個商店的升級：ncs需要完成此任務
- 減少停機時間

程式

請完成以下步驟：

1. 升級主要和備份控制器上的映像。導覽至WLC GUI > Commands > Download File下以開始下



載。

2. 儲存控制器上的組態，但不要重新啟動控制器。
3. 從主控制器發出AP預映像下載命令。導覽至WLC GUI > Wireless > Access Points > All APs，然後選擇接入點以開始預映像下載。選擇接入點後，按一下Advanced頁籤。按一下「Download Primary」，開始預映像下載。



```
*Sep 13 21:21:14 903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image [REDACTED] not found in flash, predownloading.
examining image...!
extracting info (326 bytes)
Image info:
  Version Suffix: k9w8-.wnbu_j_mr.201009101910
  Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
  Ios Image Size: 5530112
  Total Image Size: 5550592
  Image Feature: WIRELESS LAN|LWAPP
  Image Family: C1250
  Wireless Switch Management Version: [REDACTED]
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre [REDACTED].
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!
!!!!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds

New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.█
```

4. 下載所有存取點映像後，重新啟動控制器。現在，AP會回退到獨立模式，直到控制器重新啟動。**注意：在獨立模式下，容錯功能將保持客戶端關聯。控制器恢復後，AP自動使用預先下載的映像重新啟動。重新啟動後，AP重新加入主控制器並恢復客戶端服務。**

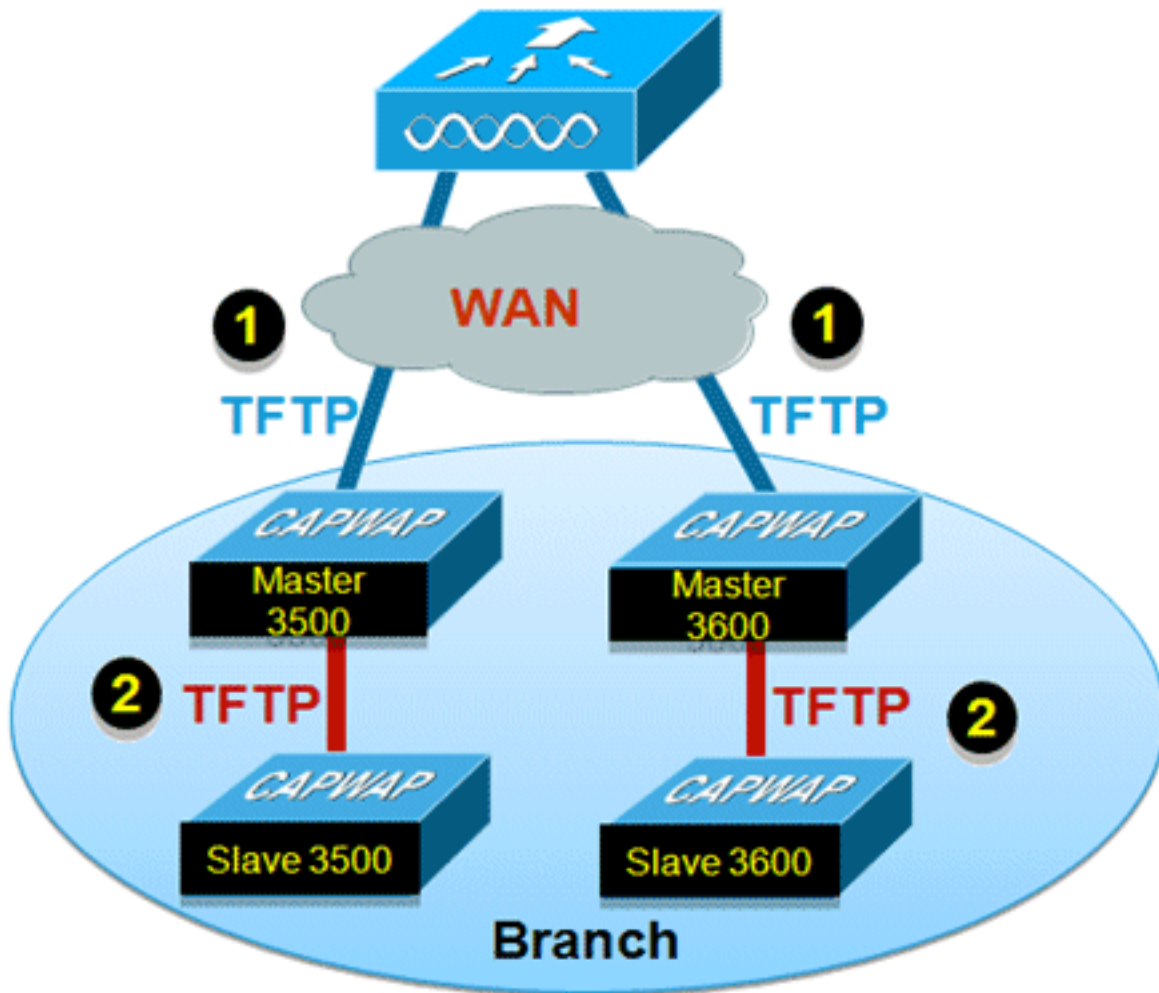
限制

- 僅適用於CAPWAP AP。

FlexConnect智慧AP映像升級

預映像下載功能可在一定程度上縮短停機時間，但所有FlexConnect AP仍必須通過WAN鏈路預下載各自的AP映像，延遲較高。

高效的AP映像升級將減少每個FlexConnect AP的停機時間。基本思想是每個AP型號中只有一個AP從控制器下載映像並充當主/伺服器，同一型號的其餘的AP將充當從/客戶端並預先從主控制器下載AP映像。從伺服器到客戶端的AP映像分佈將位於本地網路上，不會遇到WAN鏈路的延遲。因此，該過程將更快。



摘要

- 每個FlexConnect組的每個AP型號均選擇主和從AP
- 主機從WLC下載映像
- 從裝置從主AP下載映像
- 減少停機時間並節省廣域網頻寬

程式

請完成以下步驟：

1. 升級控制器上的映像。導覽至WLC GUI > Commands > Download File，開始下載。

Download file to Controller	
File Type	Code
Transfer Mode	TFTP
Server Details	
IP Address	[Redacted]
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_2_1_72.oes

2. 儲存控制器上的組態，但不要重新啟動控制器。
3. 將FlexConnect AP新增到FlexConnect組。導覽至WLC GUI > Wireless > FlexConnect Groups > select **FlexConnect Group** > **General**索引標籤> **Add AP**。

FlexConnect Groups > Edit 'Store 1' < Back

General Local Authentication Image Upgrade VLAN-ACL mapping

Group Name Store 1

FlexConnect APs AAA

Add AP

Select APs from current controller

AP Name AP3500

Ethernet MAC 0c:ef:48:c2:35:57

Add Cancel

Primary Radius Server None

Secondary Radius Server None

Enable AP Local Authentication

4. 按一下**FlexConnect AP Upgrade**釁取方塊以實現高效的AP映像升級。導覽至WLC GUI > Wireless > FlexConnect Groups > select **FlexConnect Group** > **Image Upgrade**選項。

FlexConnect Groups > 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

FlexConnect Master APs

AP Name AP3500

Add Master

Master AP Name AP Model Manual

5. 可以手動或自動選擇主AP:若要手動選擇主AP，請導覽至WLC GUI > Wireless > FlexConnect Groups > select **FlexConnect Group** > **Image Upgrade**索引標籤> **FlexConnect Master APs**，從下拉選單中選擇AP，然後按一下**Add Master**。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
AP3500	c3500I	yes

注意：每個型號只能配置一個AP作為主AP。如果手動配置主AP，則手動欄位將更新為是。若要自動選擇主AP，請導覽至WLC GUI > Wireless > FlexConnect Groups > select FlexConnect Group > Image Upgrade索引標籤，然後按一下FlexConnect Upgrade。

FlexConnect Groups > Edit 'Store 1'

General Local Authentication Image Upgrade VLAN-ACL mapping

FlexConnect AP Upgrade

Slave Maximum Retry Count

Upgrade Image

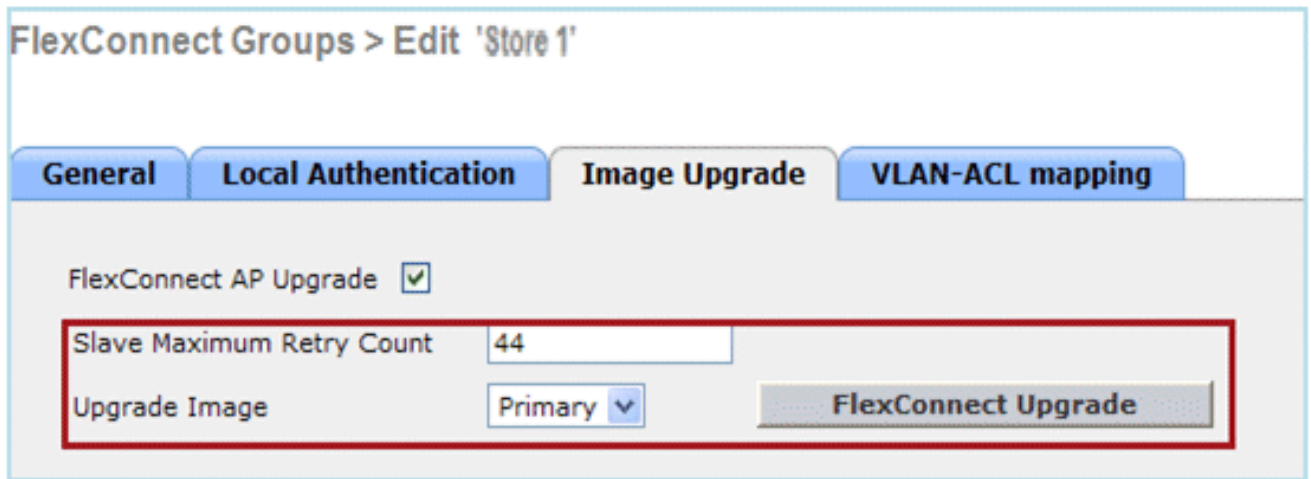
FlexConnect Master APs

AP Name

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

註：如果自動選擇主AP，則「手動」欄位將更新為否。

- 若要為特定FlexConnect組下的所有AP啟動有效的AP映像升級，請按一下FlexConnect Upgrade。導覽至WLC GUI > Wireless > FlexConnect Groups > select FlexConnect group > Image Upgrade索引標籤，然後按一下FlexConnect Upgrade。



註：Slave Maximum Retry Count是從AP從主AP下載映像時將進行的嘗試次數（預設情況下為44次），之後它將回退以從WLC下載映像。它會對WLC進行20次嘗試下載新映像，之後管理員必須重新啟動下載過程。

- FlexConnect升級啟動後，只有主AP將從WLC下載映像。在「所有AP」頁面下，「升級角色」將更新為**Master/Central**，這表示主AP已從位於中心位置的WLC下載映像。從屬AP將從位於本地站點的主要AP下載映像，這是「Upgrade Role」下的所有AP頁面將更新為「**Slave/Local**」的原因。若要驗證這一點，請導覽至WLC GUI > Wireless。

AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)
AP3500	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None	
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central

- 下載所有存取點映像後，重新啟動控制器。現在，AP會回退到獨立模式，直到控制器重新啟動。**注意：在獨立模式下，容錯功能將保持客戶端關聯。**控制器恢復後，AP自動使用預先下載的映像重新啟動。重新啟動後，AP重新加入主控制器並恢復客戶端服務。

限制

- 主AP選擇是每個FlexConnect組和每個組中的每個AP型號。
- 只有3個相同型號的從AP可以從其主AP同時升級，其餘的從AP將使用隨機回退計時器重試主AP以下載AP映像。
- 當從屬AP由於某種原因無法從主AP下載映像時，它會轉到WLC以提取新映像。
- 這僅適用於CAPWAP AP。

在FlexConnect模式下自動轉換AP

Flex 7500提供以下兩個選項來將AP模式轉換為FlexConnect:

- 手動模式
- 自動轉換模式

手動模式

此模式在所有平台上都可用，僅允許對每個AP進行更改。

1. 導覽至WLC GUI > Wireless > All APs，然後選擇AP。
2. 選擇FlexConnect作為AP模式，然後按一下Apply。
3. 更改AP模式會導致AP重新啟動。

All APs > Details for AP3500

此選項也可

在所有目前的WLC平台上使用。

自動轉換模式

此模式僅適用於Flex 7500控制器，且僅使用CLI支援。此模式觸發所有連線的AP上的更改。啟用此CLI之前，建議先將Flex 7500部署到與現有WLC園區控制器不同的移動域中：

```
(Cisco Controller) >config ap autoconvert ?
```

```
disable          Disables auto conversion of unsupported mode APs to supported
                  modes when AP joins
flexconnect      Converts unsupported mode APs to flexconnect mode when AP joins
monitor         Converts unsupported mode APs to monitor mode when AP joins
```

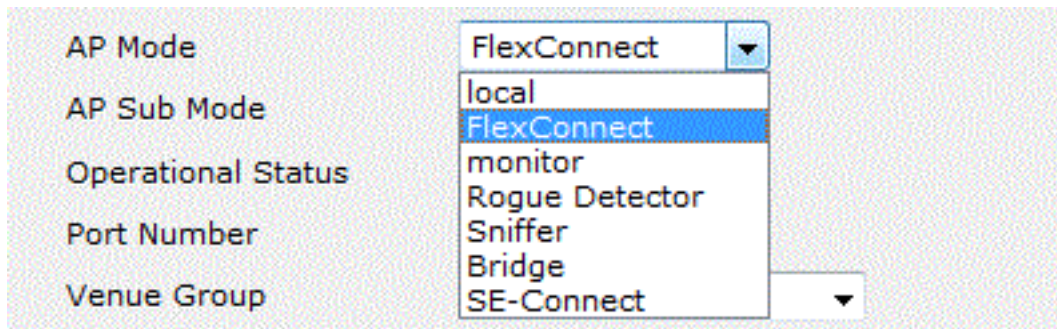
```
(Cisco Controller) >
```

1. 自動轉換功能預設為停用，可以使用以下show指令進行驗證：

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... Disabled
```

不支援的AP模式=本地模式、監聽器、欺詐檢測器和網橋。



此選項當前僅通過

CLI可用。這些CLI僅在WLC 7500上可用。

2. 執行**config ap autoconvert flexconnect** CLI將網路中具有不受支援的AP模式的所有AP轉換為FlexConnect模式。任何已處於FlexConnect或監控模式的AP都不會受到影響。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... FlexConnect
```

```
(Cisco Controller) >
```

3. 執行**config ap autoconvert monitor** CLI將網路中支援不支援的AP模式的所有存取點轉換為監控模式。任何已處於FlexConnect或監控模式的AP都不會受到影響。

```
(Cisco Controller) >config ap autoconvert monitor
```

```
(Cisco Controller) >show ap autoconvert
```

```
AP Autoconvert ..... Monitor
```

沒有選項可同時執行**config ap autoconvert flexconnect**和**config ap autoconvert monitor**。

[適用於本機交換WLAN的FlexConnect WGB/uWGB支援](#)

自7.3版起，支援WGB/uWGB和WGB背後的有線/無線客戶端，並將作為為本地交換配置的WLAN上的正常客戶端工作。

關聯後，WGB會為其每個有線/無線客戶端傳送IAPP消息，並且Flex AP的行為方式如下：

- 當Flex AP處於連線模式時，它將所有IAPP消息轉發到控制器，並且控制器會以與本地模式AP相同的方式處理IAPP消息。有線/無線客戶端的流量將從Flex AP本地交換。
- 當AP處於獨立模式時，它會處理IAPP消息，WGB上的有線/無線客戶端必須能夠註冊和取消註冊。在轉換為連線模式後，Flex AP會將有線客戶端的資訊傳送回控制器。當Flex AP從獨立模式轉換到連線模式時，WGB將傳送三次註冊消息。

有線/無線客戶端將繼承WGB的配置，這意味著對於WGB後面的客戶端，不需要像AAA身份驗證、AAA覆蓋和FlexConnect ACL這樣的單獨配置。



摘要

- 在WLC上不需要特殊組態即可在Flex AP上支援WGB。
- WGB和WGB後的客戶端支援容錯功能。
- IOS AP支援WGB:1240、1130、1140、1260和1250。

程式

請完成以下步驟：

1. 對於配置為本地交換的WLAN，無需特殊配置即可在FlexConnect AP上啟用WGB/uWGB支援。此外，WGB後的使用者端會被Flex AP視為本地交換已設定WLAN上的正常使用者端。在WLAN上啟用FlexConnect本地交換。

WLANS > Edit 'Store 1'

General

Security

QoS

Advanced

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout
Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel Enabled

Override Interface ACL IPv4 IPv6

P2P Blocking Action

Client Exclusion Enabled
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling Enabled

Wi-Fi Direct Clients Policy

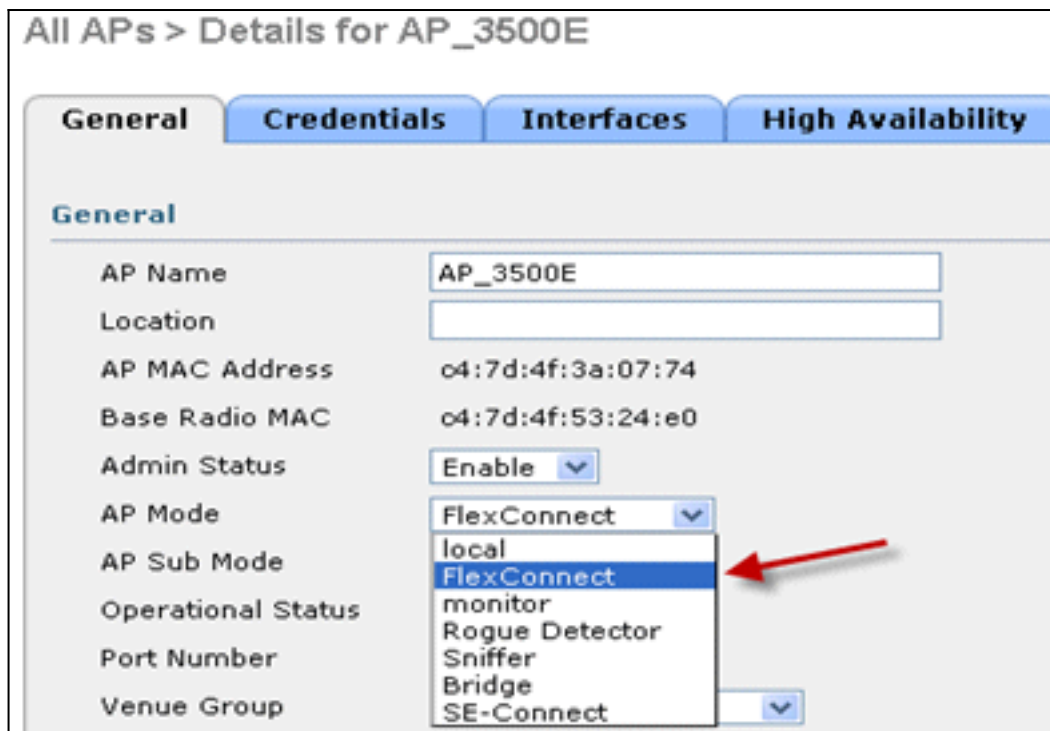
Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration Enabled

FlexConnect

FlexConnect Local Switching Enabled

2. 將AP模式設定為FlexConnect。



3. 將WGB與此已配置的WLAN後面的有線客戶端關聯。

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status	Auth	Port	WGB
00:40:96:38:d4:be	AP_3500E	'Store 1'	'Store 1'	N/A	Associated	Yes	1	No
00:50:b6:09:e5:3b	AP_3500E	'Store 1'	'Store 1'	N/A	Associated	Yes	1	No
04:7d:4f:3a:08:10	AP_3500E	'Store 1'	'Store 1'	802.11an	Associated	Yes	1	Yes

4. 若要檢查WGB的詳細資訊，請轉到Monitor > Clients，然後從客戶端清單中選擇WGB。

Client Properties		AP Properties	
MAC Address	04:7d:4f:3a:08:10	AP Address	04:7d:4f:53:24:e0
IPv4 Address	9.6.63.102	AP Name	AP_3500E
IPv6 Address		AP Type	802.11an
Client Type	WGB	WLAN Profile	'Store 1'
Number of Wired Client(s)	2	Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented

5. 若要檢查WGB背後的有線/無線使用者端的詳細資訊，請前往Monitor > Clients，然後選擇使用

者端。

Client Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	04:7d:4f:53:24:e0
IPv4 Address	96.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	0
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
Client Type	WGB Client		
WGB MAC Address	04:7d:4f:3a:08:10		

限制

- WGB後面的有線客戶端將始終與WGN本身位於同一個VLAN中。為本地交換配置的WLAN的Flex AP不支援對WGB後的客戶端提供多個VLAN支援。
- 當與為本地交換配置的WLAN上的Flex AP相關聯時，WGB最多支援20個客戶端（有線/無線）。此數字與我們目前本地模式AP上的WGB支援數量相同。
- 為本地交換設定的WLAN上，WGB背後的使用者端不支援Web驗證。

支援更多的Radius伺服器

在版本7.4之前，在FlexConnect組上配置RADIUS伺服器是在控制器上的RADIUS伺服器全域性清單中進行的。在此全域性清單中可配置的RADIUS伺服器的最大數量為17。隨著分支機構數量的增加，要求能夠為每個分支機構站點配置RADIUS伺服器。從7.4版本開始，可以配置每個FlexConnect組的主要RADIUS伺服器和備用RADIUS伺服器，這些伺服器可以是或不是控制器上配置的17個RADIUS身份驗證伺服器的全域性清單的一部分。

還將支援RADIUS伺服器的AP特定配置。AP特定配置的優先順序將高於FlexConnect組配置。

FlexConnect組中的現有配置命令需要控制器上全域性RADIUS伺服器清單中的RADIUS伺服器索引，該命令將被棄用，並替換為配置命令，該配置命令使用伺服器的IP地址和共用金鑰配置Flexconnect組中的RADIUS伺服器。

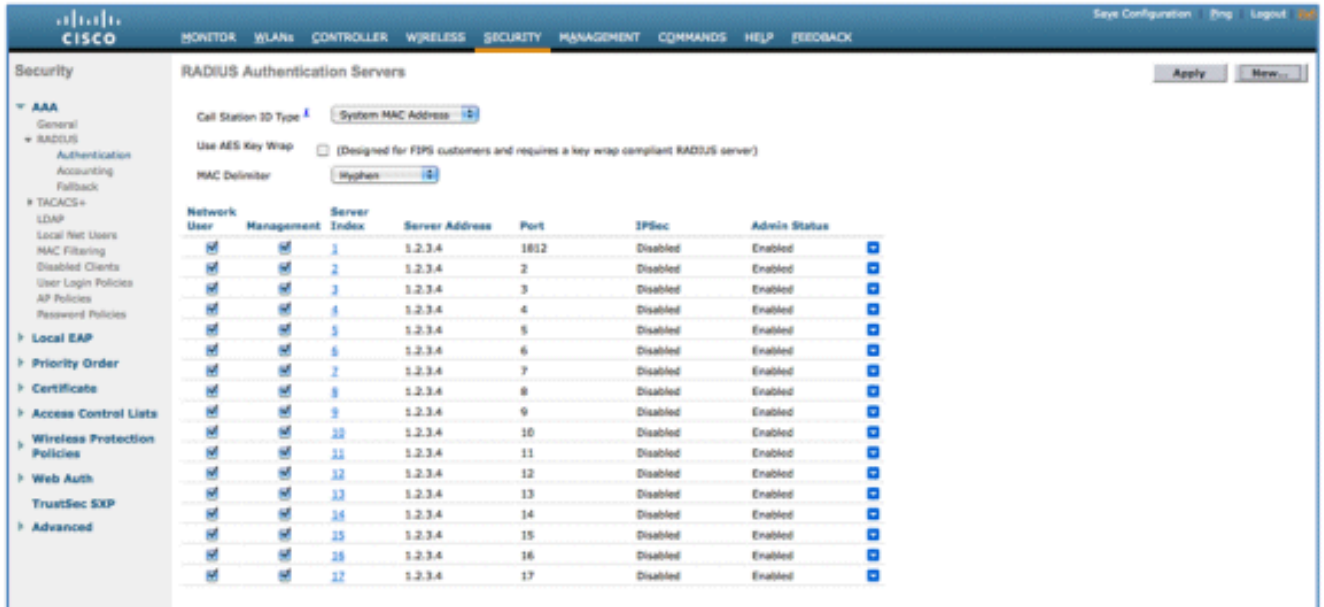
摘要

- 支援每個FlexConnect組的主要RADIUS伺服器和備用RADIUS伺服器的配置，這些伺服器可能存在，也可能不在RADIUS身份驗證伺服器的全域性清單中。
- 可在一個WLC上新增的唯一RADIUS伺服器的最大數量是給定平台上可設定的FlexConnect群組數乘以二。例如，每個FlexConnect組有一個主RADIUS伺服器和一個輔助RADIUS伺服器。
- 從早期版本升級到7.4版不會導致任何RADIUS配置丟失。

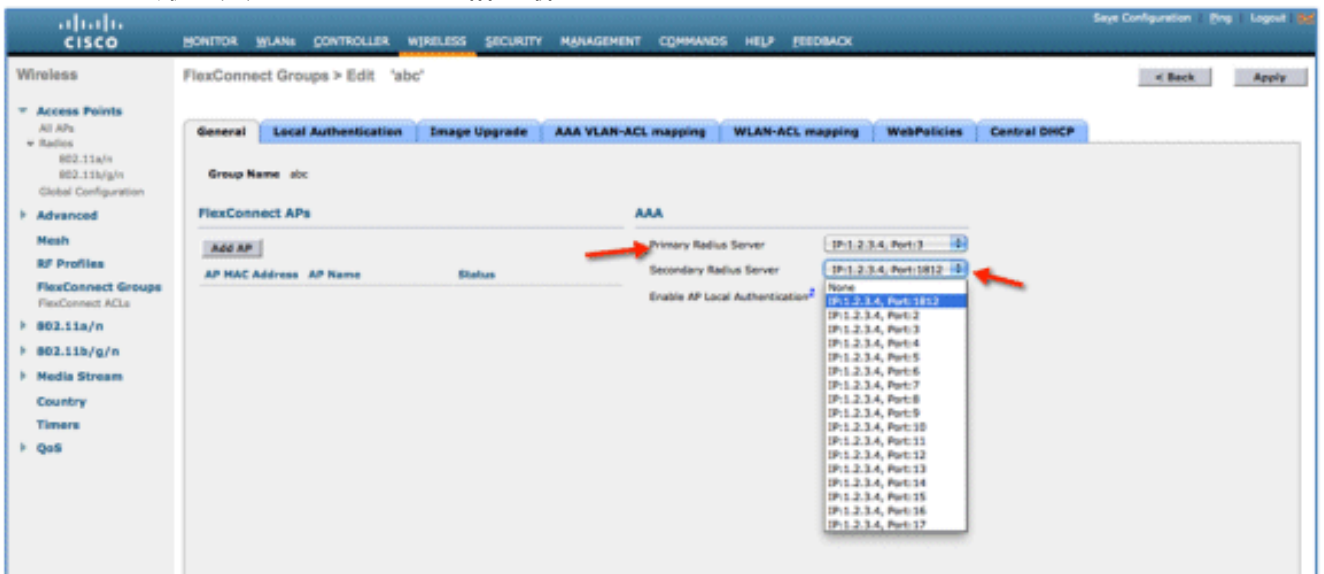
- 允許刪除主RADIUS伺服器，而不必刪除輔助RADIUS伺服器。這與RADIUS伺服器的當前FlexConnect組配置一致。

程式

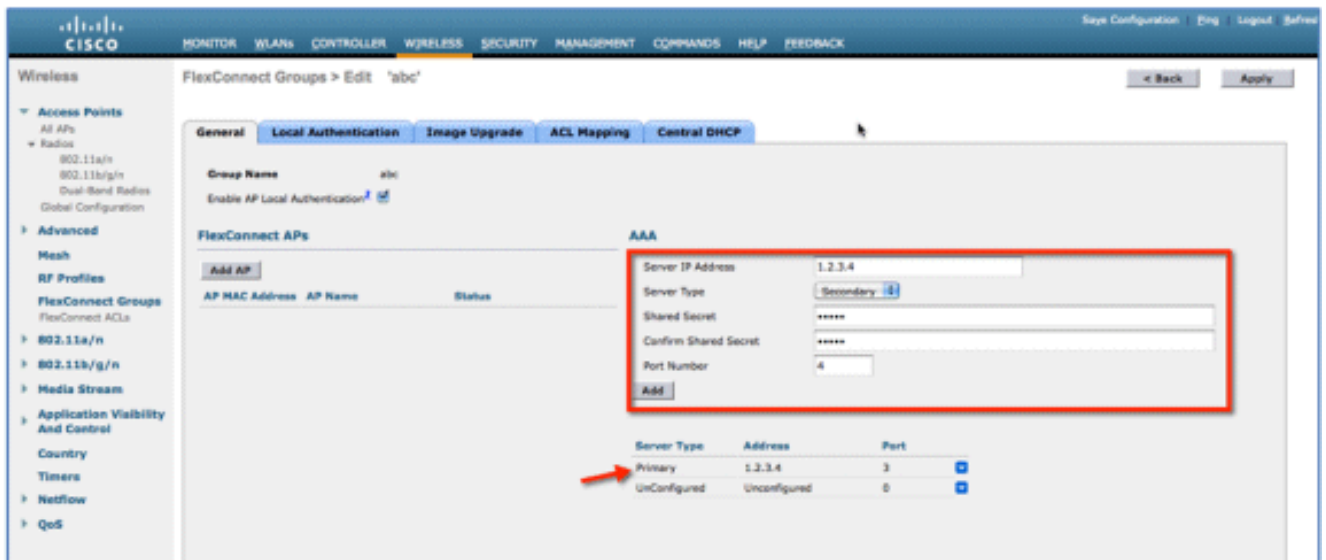
1. 7.4之前的配置模式。在AAA身份驗證配置下，最多可配置17台RADIUS伺服器。



2. 使用包含在AAA Authentication頁面上配置的RADIUS伺服器的下拉選單，可以將主和輔助RADIUS伺服器與FlexConnect組相關聯。



3. 版本7.4中FlexConnect組的配置模式。可以在FlexConnect組下使用IP地址、埠號和共用金鑰配置主RADIUS伺服器和輔助RADIUS伺服器。



限制

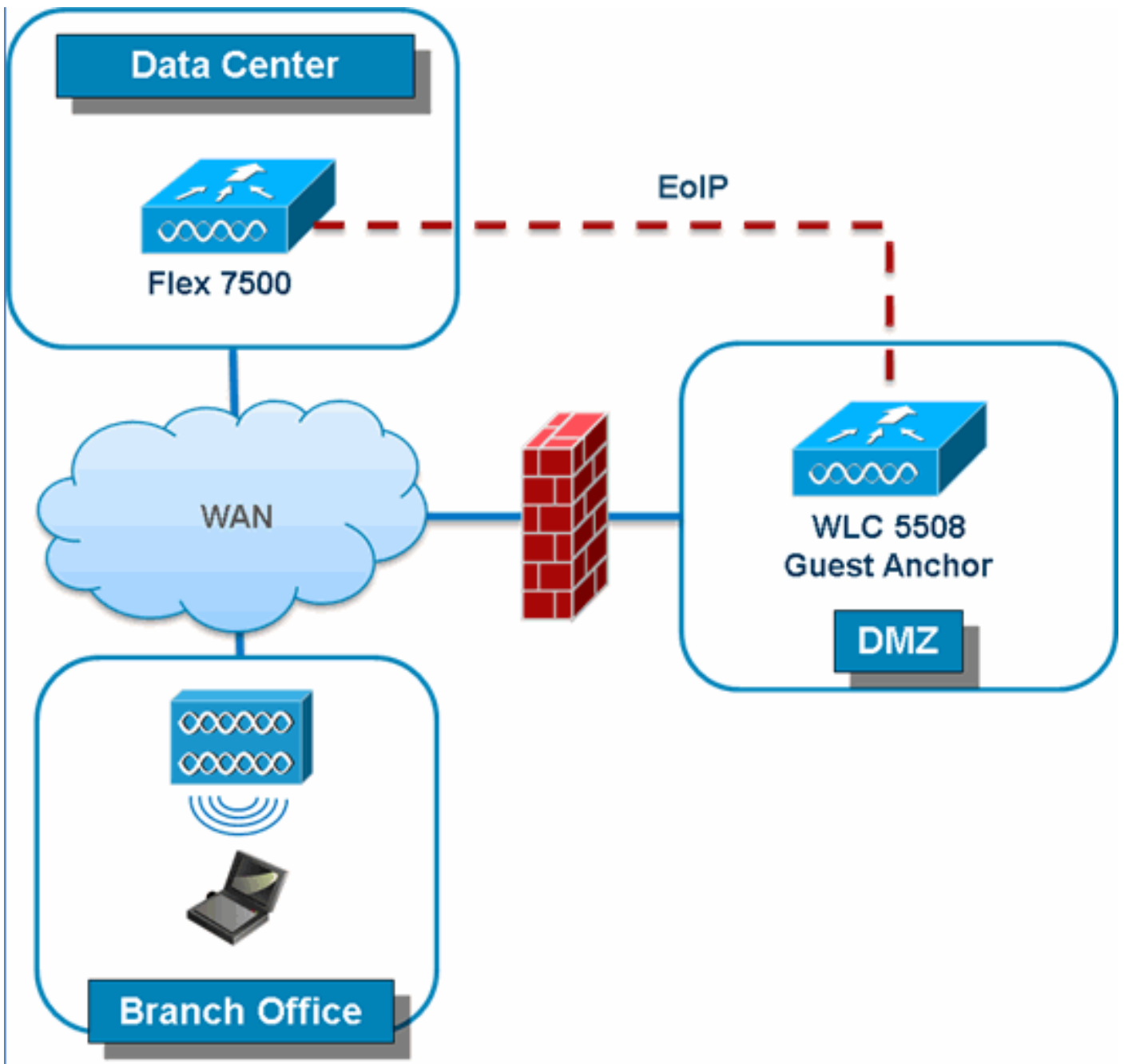
- 從版本7.4降級至先前版本的軟體將保留組態，但有一些限制。
- 配置主/輔助RADIUS伺服器時，配置上一個主伺服器/輔助RADIUS伺服器將導致舊條目被新條目替換。

增強型區域模式(ELM)

FlexConnect解決方案支援ELM。有關詳細資訊，請參閱ELM上的最佳實踐指南。

Flex 7500中的訪客存取支援

圖13:Flex 7500中的訪客存取支援



Flex 7500將允許並繼續支援建立通往DMZ中訪客錨點控制器的EoIP隧道。有關無線訪客接入解決方案的最佳實踐，請參閱《訪客部署指南》。

[從NCS管理WLC 7500](#)

從NCS對WLC 7500的管理與思科現有的WLC相同。

Monitor ▾ Reports ▾ Configure ▾ Services ▾

Add Controllers

Configure > Controllers > Add Controllers

General Parameters

Add Format Type: Device Info ▾

IP Addresses: **WLC 7500 IP Address**

Network Mask: 255.255.255.0

Verify Telnet/SSH Capabilities ⓘ

SNMP Parameters ⓘ

Version: v2c ▾

Retries: 2

Timeout: 10 (secs)

Community: private

Telnet/SSH Parameters ⓘ

User Name: admin

Password: ●●●●●●

Confirm Password: ●●●●●●

Retries: 3

Timeout: 60 (secs)

OK Cancel

Controllers

Configure > Controllers

-- Select a command --

IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
172.20.227.174 ⓘ	Ambassador	7500		7.0.112.62	mobility	Reachable	Identical
172.20.227.172 ⓘ	5508-Primary	5500		7.0.112.52	mobility	Reachable	Identical

有關管理WLC和發現模板的詳細資訊，請參閱[思科無線控制系統配置指南7.0.172.0版](#)。

常見問題

問題： 如果我在遠端位置將LAP配置為FlexConnect，是否可以向這些LAP提供主控制器和輔助控制器？

範例： 站點A有一個主控制器，站點B有一個輔助控制器。如果站點A的控制器發生故障，LAP會故障切換到站點B的控制器。如果兩個控制器均不可用，LAP是否會進入FlexConnect獨立模式？

是的。 首先，LAP故障切換到其輔助裝置。所有本地交換的WLAN均無變化，而所有集中交換的WLAN僅將流量傳送到新控制器。此外，如果輔助路由器發生故障，標籤為進行本地交換（以及開放/預共用金鑰身份驗證/您正在執行AP身份驗證程式）的所有WLAN將保持運行。

問題： 在本地模式下配置的接入點如何處理使用FlexConnect本地交換配置的WLAN？

A.本地模式接入點將這些WLAN視為常規WLAN。驗證和資料流量通過隧道傳回WLC。在WAN連結失敗期間，此WLAN完全關閉，在恢復與WLC的連線之前，此WLAN上沒有使用者端處於使用中狀態。

問題： 是否可以使用本地交換執行Web身份驗證？

答：是，您可以啟用Web驗證的SSID，並在Web驗證後本地丟棄流量。使用本機交換的Web驗證運作正常。

問題： 我是否可以將控制器上的訪客門戶用於H REAP本地處理的SSID?如果是，如果與控制器的連線斷開會發生什麼情況？當前客戶端是否立即刪除？

是的。由於此WLAN是在本地交換的，因此WLAN可用，但由於網頁不可用，因此沒有新客戶端能夠進行身份驗證。但是，現有客戶端不會丟失。

問題： FlexConnect能否認證PCI合規性？

是的。FlexConnect解決方案支援欺詐檢測，以滿足PCI合規性。

相關資訊

- [HREAP設計和部署指南](#)
- [Cisco 4400系列無線LAN控制器](#)
- [Cisco 2000系列無線LAN控制器](#)
- [思科無線控制系統](#)
- [思科3300系列行動化服務引擎](#)
- [Cisco Aironet 3500 系列](#)
- [思科安全存取控制系統](#)
- [技術支援與文件 - Cisco Systems](#)