

Flex 7500无线分支控制器部署指南

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[产品概述](#)

[产品规格](#)

[数据表](#)

[平台功能](#)

[Flex 7500启动](#)

[Flex 7500许可](#)

[AP基本计数许可](#)

[AP升级许可](#)

[软件版本支持](#)

[支持的接入点](#)

[FlexConnect架构](#)

[集中接入点控制流量的优势](#)

[分布客户端数据流量的优势](#)

[FlexConnect操作模式](#)

[WAN要求](#)

[无线分支机构网络设计](#)

[主要设计要求](#)

[概述](#)

[优势](#)

[功能编址分支机构网络设计](#)

[IPv6支持列表](#)

[功能表](#)

[AP组](#)

[来自WLC的配置](#)

[摘要](#)

[FlexConnect组](#)

[FlexConnect组的主要目标](#)

[从WLC配置FlexConnect组](#)

[使用CLI进行验证](#)

[FlexConnect VLAN覆盖](#)

[摘要](#)

[步骤](#)

[限制](#)

[基于FlexConnect VLAN的中央交换](#)

[摘要](#)

[步骤](#)

[限制](#)

[FlexConnect ACL](#)

[摘要](#)

[步骤](#)

[限制](#)

[FlexConnect拆分隧道](#)

[摘要](#)

[步骤](#)

[限制](#)

[容错](#)

[摘要](#)

[限制](#)

[每个WLAN的客户端限制](#)

[主要目标](#)

[限制](#)

[WLC 配置](#)

[NCS配置](#)

[点对点阻塞](#)

[摘要](#)

[步骤](#)

[限制](#)

[AP预映像下载](#)

[摘要](#)

[步骤](#)

[限制](#)

[FlexConnect智能AP映像升级](#)

[摘要](#)

[步骤](#)

[限制](#)

[在FlexConnect模式下自动转换AP](#)

[手动模式](#)

[自动转换模式](#)

[FlexConnect WGB/uWGB支持本地交换WLAN](#)

[摘要](#)

[步骤](#)

[限制](#)

[支持更多的Radius服务器](#)

[摘要](#)

[步骤](#)

[限制](#)

[增强的本地模式\(ELM\)](#)

[Flex 7500中的访客接入支持](#)

[从NCS管理WLC 7500](#)

[常见问题](#)

[相关信息](#)

简介

本文档介绍如何部署Cisco Flex 7500无线分支控制器。本文档旨在：

- 解释Cisco FlexConnect解决方案的各种网络元素及其通信流。
- 提供设计Cisco FlexConnect无线分支机构解决方案的一般部署指南。
- 解释7.2.103.0代码版本中用于增强产品信息库的软件功能。

注意：在7.2之前，FlexConnect称为混合REAP(HREAP)。现在它称为FlexConnect。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

产品概述

图 1：思科Flex 7500



Cisco Flex 7500系列云控制器是一个高度可扩展的分支机构控制器，用于多站点**无线部署**。思科Flex 7500系列控制器部署在私有云中，通过集中控制将无线服务扩展到分布式分支机构，从而降低总运营成本。

Cisco Flex 7500系列([图1](#))可管理多达500个分支机构位置的**无线接入点**，并允许IT经理从数据中心配置、管理多达3000个接入点(AP)和30,000个客户端并对其进行故障排除。Cisco Flex 7500系列控制器支持安全访客接入、支付卡行业(PCI)合规性欺诈检测以及分支内（本地交换）Wi-Fi语音和视频。

下表重点介绍了Flex 7500、WiSM2和WLC 5500控制器之间的可扩展性差异：

可扩展性	Flex 7500	WiSM2	WLC 5500
总接入点数	6,000	1000	500
客户端总数	64,000	15,000	7,000
最大FlexConnect组数	2000	100	100
每个FlexConnect组的最大AP数	100	25	25
最大AP组数	6000	1000	500

产品规格

数据表

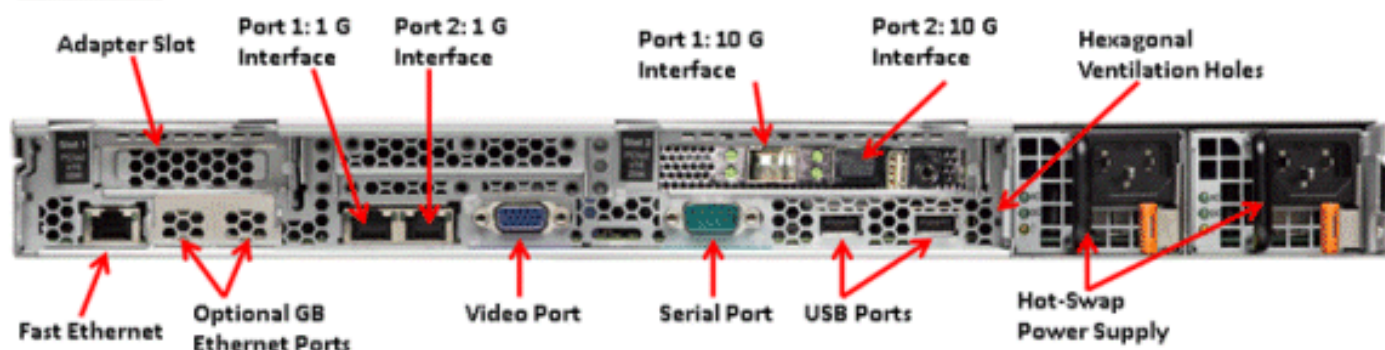
请参阅

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

平台功能

图 2：Flex 7500后视图

Rear View



网络接口端口

接口端口	使用率
快速以太网	集成管理模块(IMM)
端口 1：1G	WLC服务端口
端口 2：1G	WLC冗余端口(RP)
端口 1：10G	WLC管理接口
端口 2：10G	WLC备份管理接口端口 (端口故障)
可选千兆以太网端口	不适用

注意：

- 对2x10G接口的LAG支持允许主用 — 主用链路操作，并提供快速故障切换链路冗余。带LAG的

额外活动10G链路不会更改控制器无线吞吐量。

- 2个10G接口
- 2x10G接口仅支持SFP产品# SFP-10G-SR的光缆。
- 交换机端SFP产品编号X2-10GB-SR

系统MAC地址

端口 1 : 10G (管理接口)	系统/基本MAC地址
端口 2 : 10G (备份管理接口)	基本MAC地址+ 5
端口 1 : 1G (服务端口)	基本MAC地址+ 1
端口 2 : 1G (冗余端口)	基本MAC地址+ 3

串行控制台重定向

默认情况下，WLC 7500以9600波特率启用控制台重定向，模拟无流量控制的Vt100终端。

库存信息

图 3 : WLC 7500控制台

```
(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
```

桌面管理接口(DMI)表包含服务器硬件和BIOS信息。

WLC 7500显示BIOS版本、PID/VID和序列号作为资产的一部分。

Flex 7500启动

用于软件维护的思科引导加载器选项与思科现有控制器平台相同。

图 4 : 启动顺序

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

图 5 : WLC配置向导

```
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
```

注意：Flex 7500启动顺序与现有控制器平台等效且一致。初始启动需要使用向导进行WLC配置。

[Flex 7500许可](#)

[AP基本计数许可](#)

AP基本计数SKU
300

500
1000
2000
3000
6000

[AP升级许可](#)

AP升级SKU
100
250
500
1000

除基本和升级计数外，涵盖订购、安装和查看的整个许可过程与思科现有的WLC 5508类似。

请参阅[WLC 7.3配置指南](#)，该指南涵盖整个许可过程。

[软件版本支持](#)

Flex 7500仅支持WLC代码版本7.0.116.x及更高版本。

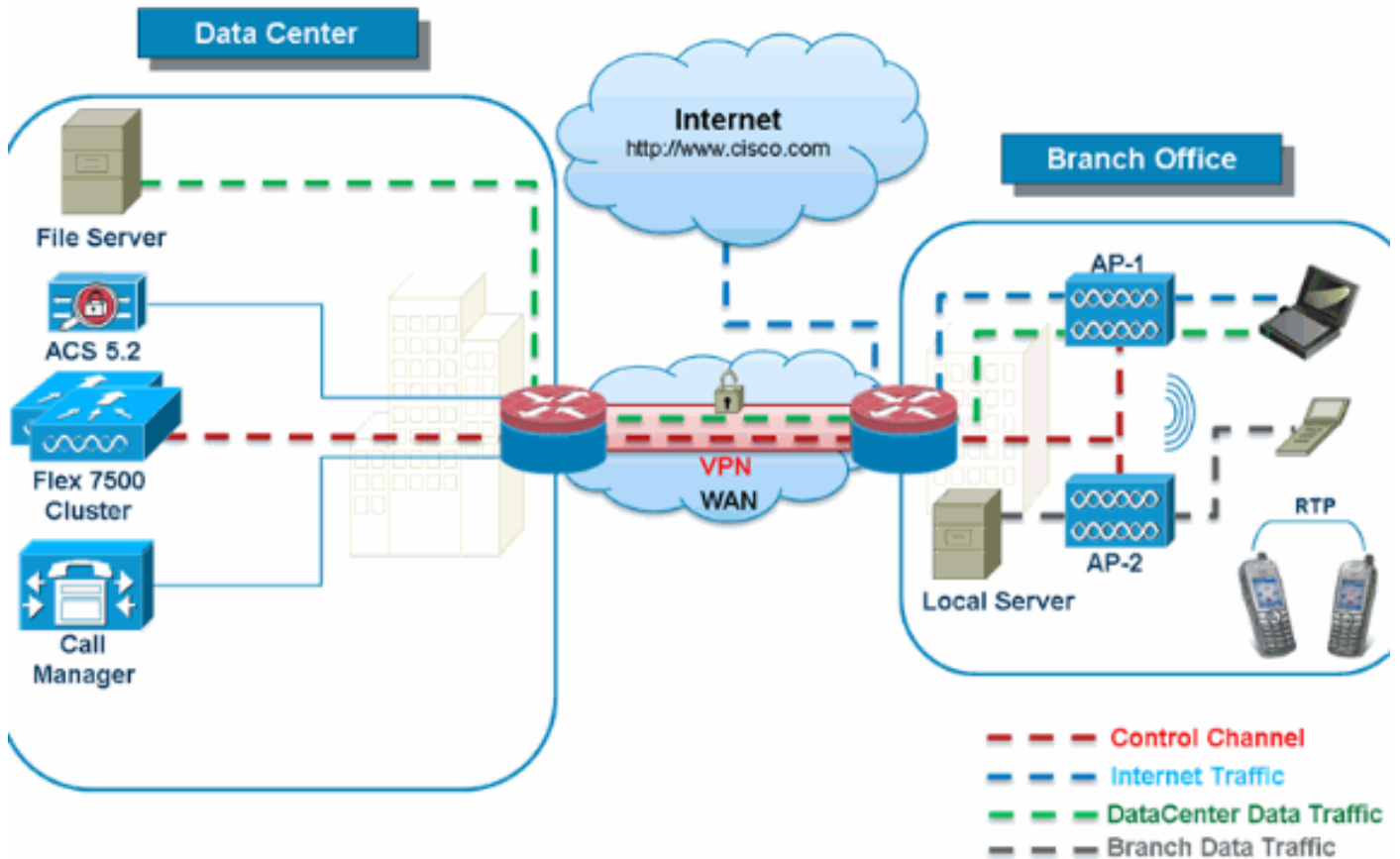
[支持的接入点](#)

接入点1040、1130、1140、1550、3500、3600、2600、1250、1260、1240、OEAP 600、ISR 89Flex 7500支持1和ISR 881。

[FlexConnect架构](#)

图 6：典型的无线分支拓扑

FlexConnect Architecture



FlexConnect是适用于分支机构和远程办公室部署的无线解决方案。它也称为混合REAP解决方案，但本文档将其称为FlexConnect。

FlexConnect解决方案使客户能够：

- 集中控制和管理来自数据中心的AP流量。控制流量在图6中标有红色短划线。
- 在每个分支机构分配客户端数据流量。图6中的数据流量标有蓝色、绿色和紫色短划线。每个流量以最有效的方式到达最终目的地。

集中接入点控制流量的优势

- 监控和故障排除的单一窗格
- 易于管理
- 安全无缝地移动访问数据中心资源
- 减少分支机构占用空间
- 运营节省增加

分布客户端数据流量的优势

- 在广域网链路完全故障或控制器不可用时不会出现运营中断（生存能力）
- 广域网链路故障期间分支机构内的移动恢复能力
- 提高分支机构的可扩展性。支持可扩展至100个AP和250,000平方英尺（5000平方英尺）的分支机构规模每个AP的英尺）。

思科FlexConnect解决方案还支持中央客户端数据流量，但应仅限于访客数据流量。下表介绍仅对在数据中心集中交换数据流量的非访客客户端的WLAN L2安全类型的限制。

集中交换非访客用户的L2安全支持

WLAN L2安全	类型	结果
无	不适用	允许
WPA + WPA2	802.1x	允许
	CCKM	允许
	802.1x + CCKM	允许
	PSK	允许
802.1x	WEP	允许
静态 WEP	WEP	允许
WEP + 802.1x	WEP	允许
CKIP		允许

注意：这些身份验证限制不适用于在分支机构分发数据流量的客户端。

集中和本地交换用户的L3安全支持

WLAN L3安全	类型	结果
Web 身份验证	内部	允许
	外部	允许
	定制	允许
Web直通	内部	允许
	外部	允许
	定制	允许
条件Web重定向	外部	允许
启动页Web重定向	外部	允许

有关Flexconnect外部WebAuth部署的详细信息，请参阅[Flexconnect外部WebAuth部署指南](#)

有关HREAP/FlexConnect AP状态和数据流量交换选项的详细信息，请参阅[配置FlexConnect](#)。

FlexConnect操作模式

Flex Connect模式	描述
已连接	当FlexConnect返回控制器的CAPWAP控制平面处于启用状态且运行正常时，即表示WAN链路未关闭，则FlexConnect将处于连接模式。
独立	独立模式被指定为FlexConnect在不再具有与控制器的连接时进入的操作状态。独立模式下的FlexConnect AP将继续使用上次已知配置运行，即使在电源故障和WLC或WAN故障的情况下也是如此。

有关FlexConnect运营理论的详细信息，请参阅[《H-Reap/FlexConnect设计和部署指南》](#)。

WAN要求

FlexConnect AP部署在分支机构站点，并通过广域网链路从数据中心进行管理。强烈建议最低带宽限制保持为每个AP 12.8 kbps，对于数据部署，往返延迟不大于300 ms，对于数据+语音部署，为100 ms。最大传输单位(MTU)必须至少为500字节。

部署类型	WAN带宽 (最小)	WAN RTT延迟 (最大)	每个分支机构的最大AP数	每个分支机构的最大客户端数
数据	64 kbps	300 ms	5	25
数据+语音	128 kbps	100 ms	5	25
监控	64 kbps	2 秒	5	不适用
数据	640 kbps	300 ms	50	1000
数据+语音	1.44 Mbps	100 ms	50	1000
监控	640 kbps	2 秒	50	不适用

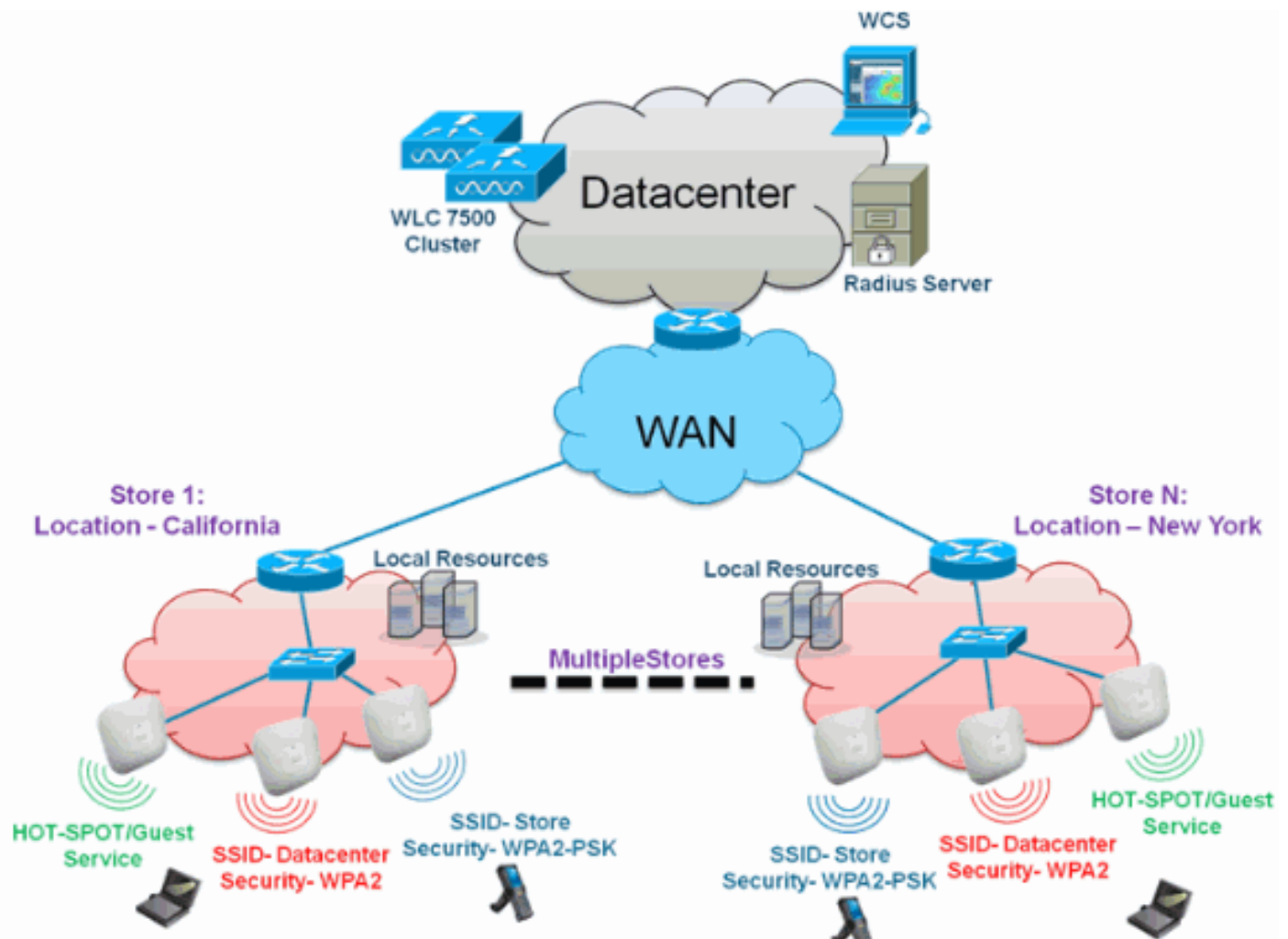
无线分支机构网络设计

本文档的其余部分重点介绍实施安全分布式分支机构网络的指导原则和最佳实践。FlexConnect架构推荐用于满足这些设计要求的无线分支机构网络。

主要设计要求

- 分支机构规模，可扩展至100个AP和250,000平方英尺(5000平方每个AP的英尺)
- 集中管理和故障排除
- 无运营停机
- 基于客户端的流量分段
- 与公司资源的无缝且安全的无线连接
- 符合PCI
- 支持访客

图 7：无线分支机构网络设计



概述

分支机构客户发现，跨地理位置提供功能齐全的可扩展安全网络服务越来越困难，成本也越来越高。为了支持客户，思科正通过引入Flex 7500来解决这些挑战。

Flex 7500解决方案可虚拟化数据中心内复杂的安全、管理、配置和故障排除操作，然后将这些服务透明地扩展到每个分支机构。使用Flex 7500的部署使IT部门更易于设置、管理，最重要的是更易于扩展。

优势

- 通过6000个AP支持提高可扩展性
- 使用FlexConnect容错功能提高恢复能力
- 使用FlexConnect（中央和本地交换）增加流量分段
- 使用AP组和FlexConnect组复制存储设计，从而简化管理。

功能编址分支机构网络设计

本指南的其余部分将介绍实现图7所示网络设计的功能使用和[建议](#)。

功能：

主要功能	亮点
------	----

AP组	处理多个分支站点时，可简化操作/管理。此外，还为类似分支机构站点提供复制配置的灵活性。
FlexConnect组	FlexConnect组提供本地备份RADIUS、CCKM/OKC快速漫游和本地身份验证的功能。
容错	提高无线分支机构的恢复能力，不会造成运营中断。
ELM (自适应wIPS的增强本地模式)	在为客户端提供服务时提供自适应wIPS功能，而不会对客户端性能造成任何影响。
每个WLAN的客户端限制	限制分支机构网络上的访客客户端总数。
AP预映像下载	在升级分支机构时减少停机时间。
在FlexConnect中自动转换AP	在FlexConnect中为分支机构自动转换AP的功能。
访客权限	使用FlexConnect继续现有的思科访客接入架构。

IPv6支持列表

功能	集中交换		本地交换	
	5500 / WiSM-2	Flex 7500	5500 / WiSM-2	Flex 7500
IPv6 (客户端移动)	受支持	Not Supported	Not Supported	Not Supported
IPv6 RA防护	受支持	受支持	受支持	受支持
IPv6 DHCP防护	受支持	Not Supported	Not Supported	Not Supported
IPv6源防护	受支持	Not Supported	Not Supported	Not Supported
RA限制/速率限制	受支持	Not Supported	Not Supported	Not Supported
IPv6 ACL	受支持	Not Supported	Not Supported	Not Supported
IPv6客户端可视性	受支持	Not Supported	Not Supported	Not Supported
IPv6邻居发现缓存	受支持	Not Supported	Not Supported	Not Supported

IPv6桥接	受支持	Not Supported	受支持	受支持
--------	-----	---------------	-----	-----

功能表

有关FlexConnect[功能的功能矩阵](#)，请参阅FlexConnect功能矩阵。

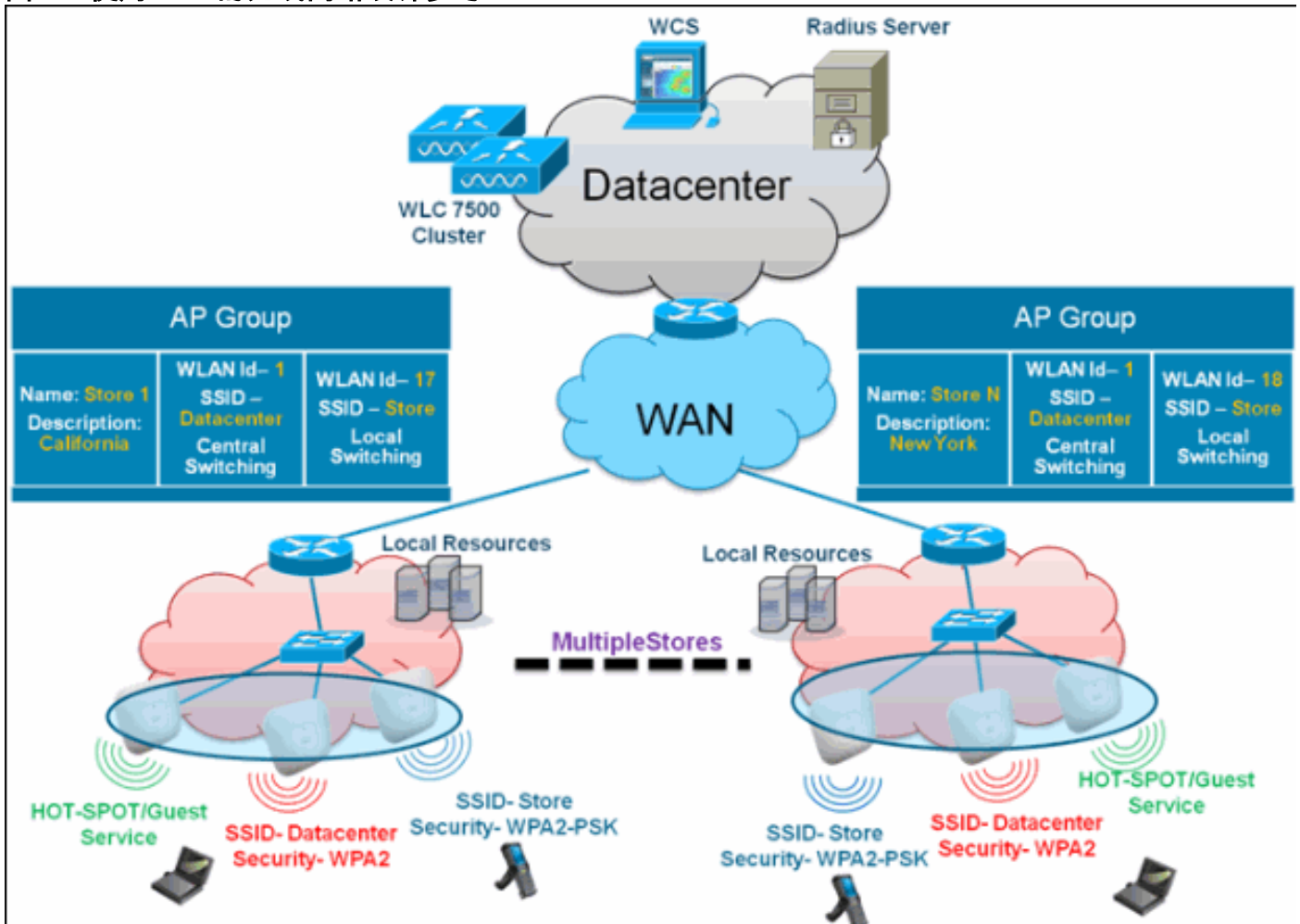
AP组

在控制器上创建WLAN后，您可以选择性地将其（使用接入点组）发布到不同的接入点，以便更好地管理无线网络。在典型部署中，WLAN上的所有用户都映射到控制器上的单个接口。因此，与该WLAN关联的所有用户都位于同一子网或VLAN中。但是，您可以通过创建接入点组，根据特定标准（如“营销”、“工程”或“运营”），选择在多个接口之间或向一组用户分配负载。此外，这些接入点组可以配置在单独的VLAN中，以简化网络管理。

本文档使用AP组来简化跨地理位置管理多个存储时的网络管理。为便于操作，本文档为每个存储创建一个AP组以满足以下要求：

- 跨所有存储集中交换SSID数据中心，用于本地存储管理器管理访问。
- 本地交换SSID存储区，在所有存储区中为手持扫描仪提供不同的WPA2-PSK密钥。

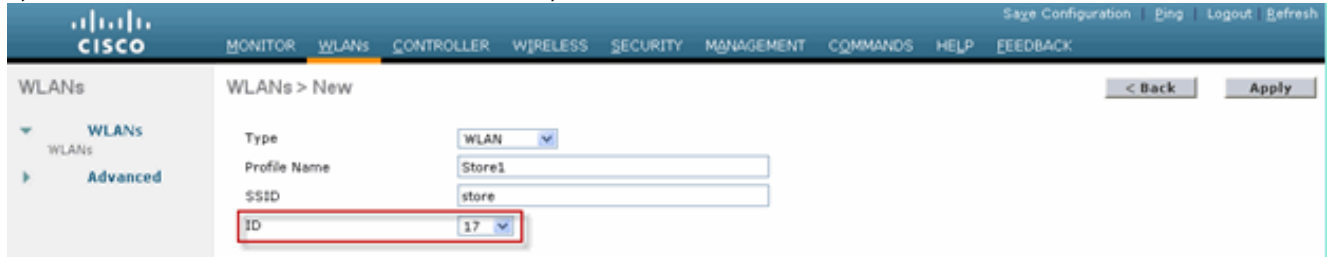
图 8：使用AP组的无线网络设计参考



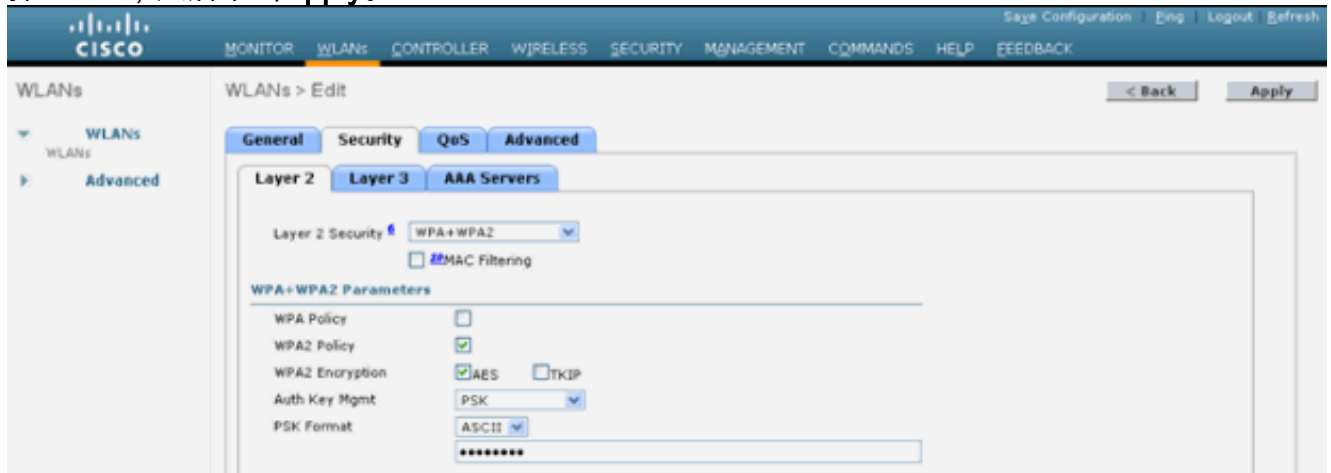
来自WLC的配置

请完成以下步骤：

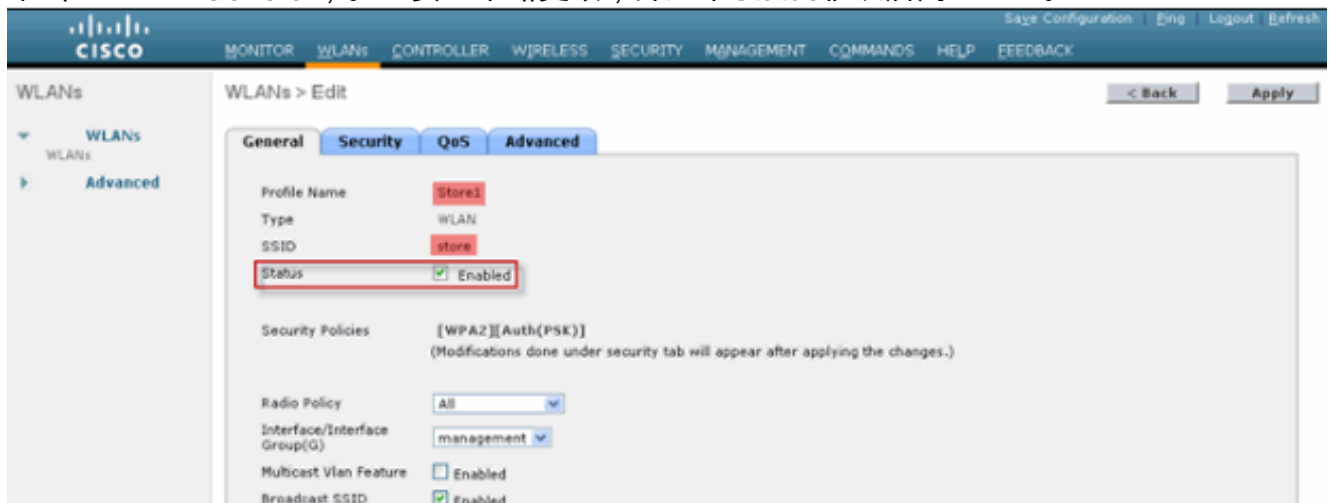
1. 在WLANs > New页面，在Profile Name字段中输入Store1，在SSID字段中输入store，然后从ID下拉列表中选择17。**注意：**WLAN ID 1-16是默认组的一部分，无法删除。为了满足我们对每个存储使用相同SSID存储和不同WPA2-PSK的要求，您需要使用WLAN ID 17及更高版本，因为这些WLAN ID 17不属于默认组，可以限制在每个存储。



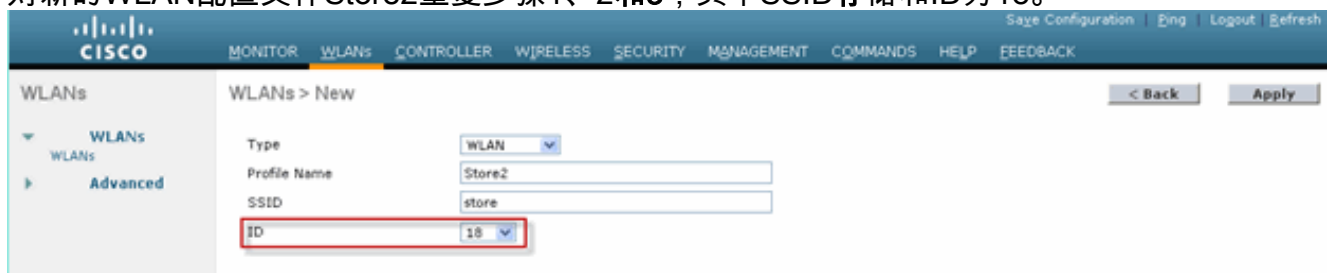
2. 在WLAN > Security下，从Auth Key Mgmt下拉列表中选择PSK，从PSK Format下拉列表中选择ASCII，然后单击Apply。

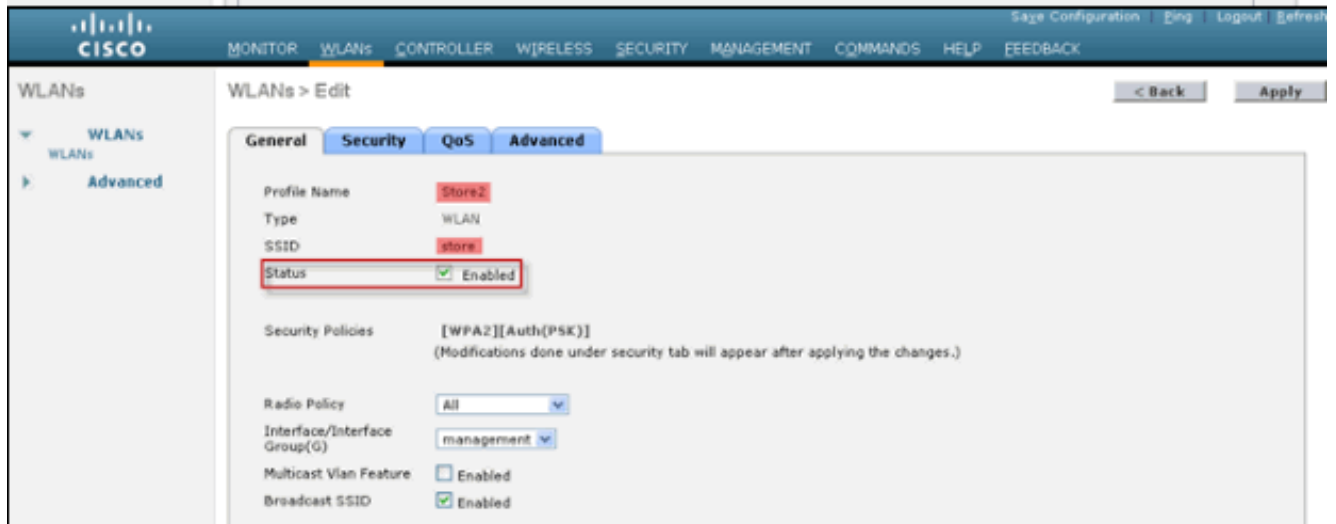
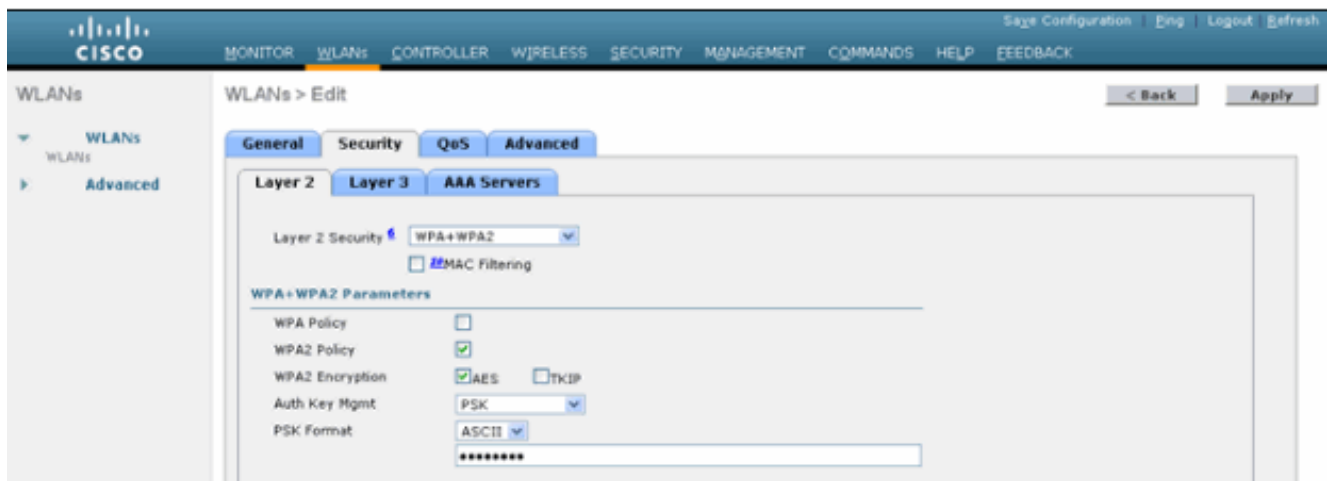


3. 单击WLAN > General，验证安全策略更改，并选中Status框以启用WLAN。



4. 对新的WLAN配置文件Store2重复步骤1、2和3，其中SSID存储和ID为18。

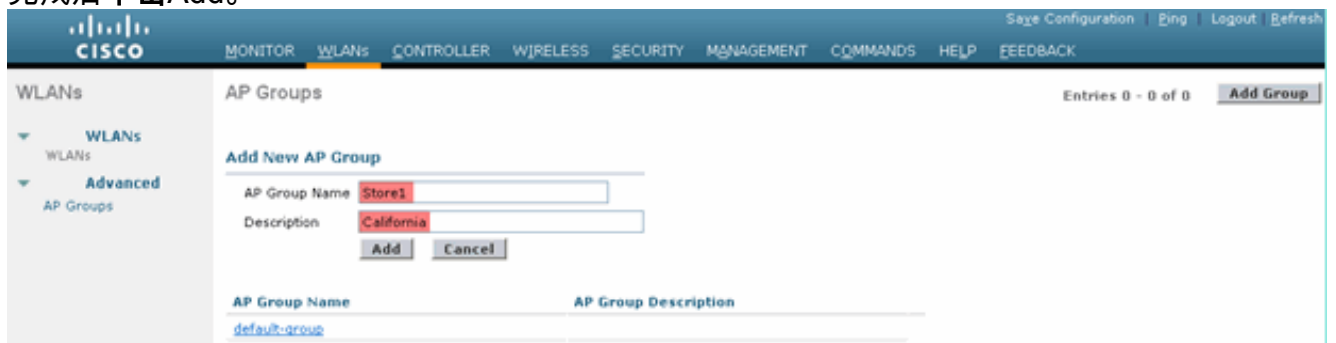




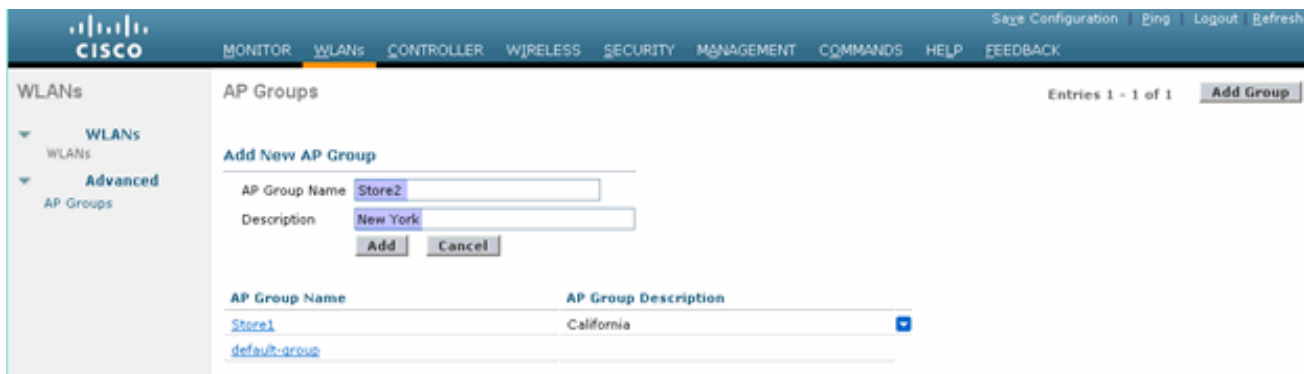
5. 使用配置文件名称数据中心、SSID数据中心和ID 1创建并启用WLAN配置文件。注意：在创建时，1-16的WLAN ID会自动成为default-ap-group的一部分。
6. 在WLAN下，验证WLAN ID的状态1、17和18。



7. 单击WLAN > Advanced > AP group > Add Group。
8. 添加AP组名称Store1，与WLAN配置文件Store1相同，并添加描述作为存储的位置。在本例中，California用作商店的位置。
9. 完成后单击Add。



10. 单击Add Group并创建AP Group Name Store2和Description New York。
11. 单击 Add。



12. 单击“WLAN”>“高级”>“AP组”以验证组的创建。



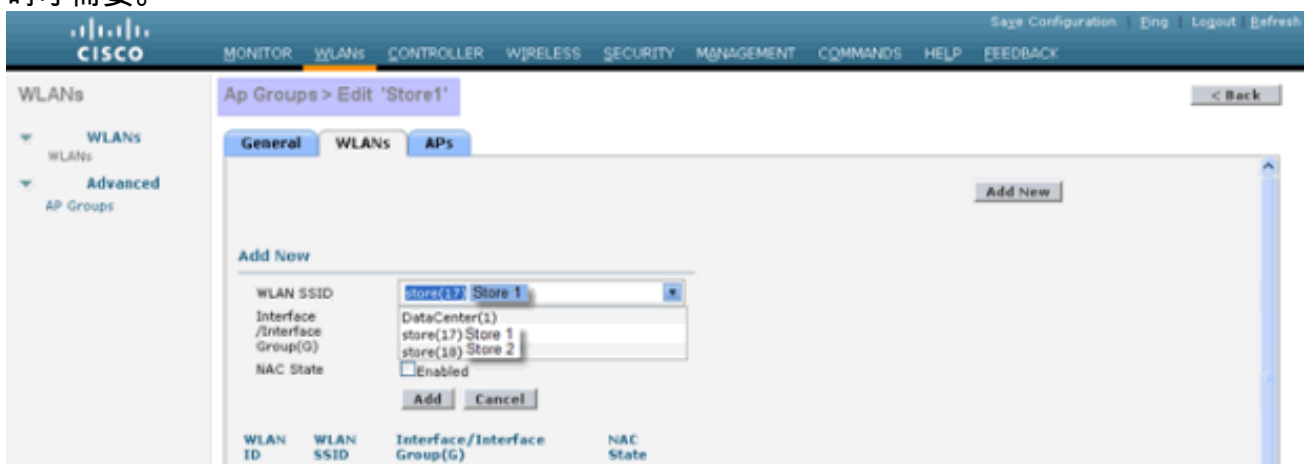
13. 单击AP Group Name Store1以添加或编辑WLAN。

14. 单击Add New以选择WLAN。

15. 在WLAN下，从WLAN SSID下拉列表中，选择WLAN ID 17 store(17)。

16. 选择WLAN ID 17后，单击Add。

17. 对WLAN ID 1数据中心(1)重复步骤14 -16。此步骤为可选步骤，仅在您要允许远程资源访问时才需要。



18. 返回WLAN > Advanced > AP Groups屏幕。

19. 单击AP Group Name Store2以添加或编辑WLAN。

20. 单击Add New以选择WLAN。

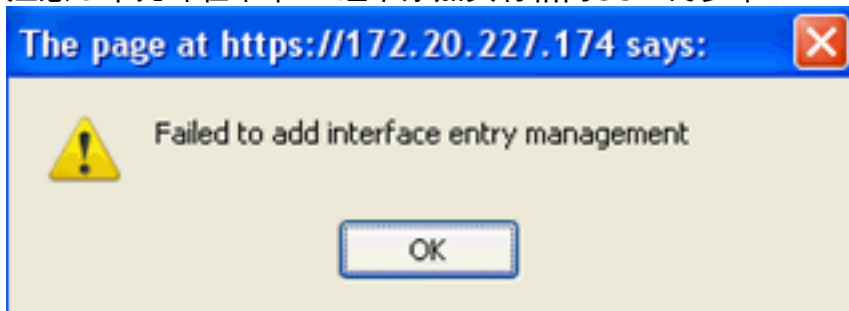
21. 在WLAN下，从WLAN SSID下拉列表中，选择WLAN ID 18 store(18)。

22. 选择WLAN ID 18后，单击Add。

23. 对WLAN ID 1数据中心(1)重复步骤14 -16。



注意：不允许在单个AP组下添加具有相同SSID的多个WLAN配置文件。



注意：本文档未捕获向AP组添

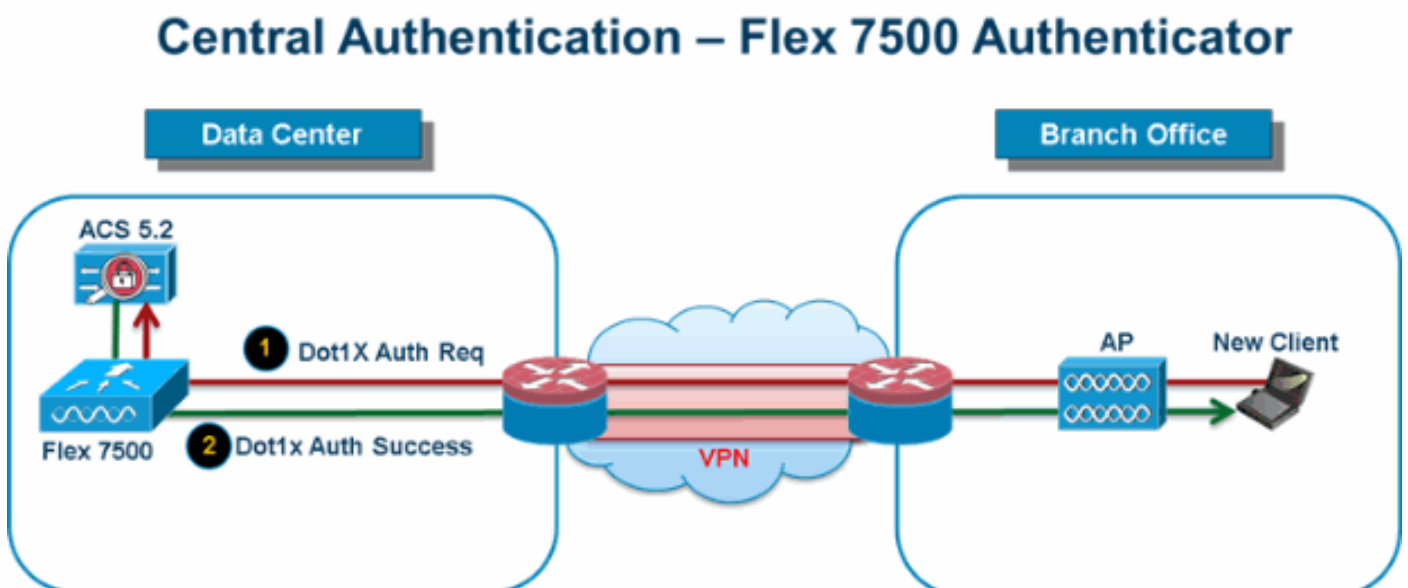
加AP，但客户端需要添加AP才能访问网络服务。

摘要

- AP组可简化网络管理。
- 故障排除易于按分支机构粒度进行
- 提高灵活性

FlexConnect组

图 9：中央Dot1X身份验证（Flex 7500充当身份验证器）



在大多数典型的分支机构部署中，很容易预见客户端802.1X身份验证在数据中心集中进行，如图9所示。由于上述方案完全有效，因此会引起以下问题：

- 如果Flex 7500发生故障，无线客户端如何执行802.1X身份验证并访问数据中心服务？
- 如果分支机构和数据中心之间的WAN链路发生故障，无线客户端如何执行802.1X身份验证？
- 在WAN故障期间，分支机构移动性是否受到影响？
- FlexConnect解决方案是否不提供分支机构运营中断？

FlexConnect组主要设计并应创建以应对这些挑战。此外，它还简化了每个分支站点的组织，因为每个分支站点的所有FlexConnect接入点都是单个FlexConnect组的一部分。

注意： FlexConnect组与AP组不类似。

FlexConnect组的主要目标

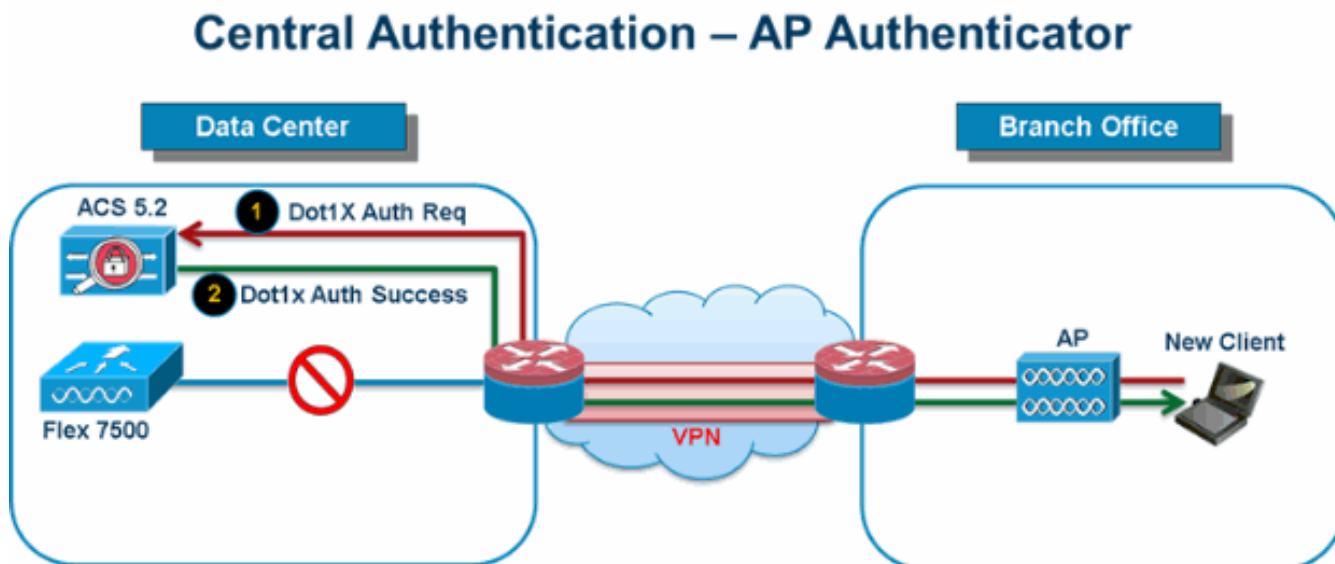
备份RADIUS服务器故障转移

- 您可以配置控制器，使其允许独立模式的FlexConnect接入点对备用RADIUS服务器执行完全802.1X身份验证。为了提高分支机构的恢复能力，管理员可以配置主备份RADIUS服务器或主备份RADIUS服务器和辅助备份RADIUS服务器。这些服务器仅在FlexConnect接入点未连接到控制器时使用。

注意： 不支持备份RADIUS记帐。

本地 认证

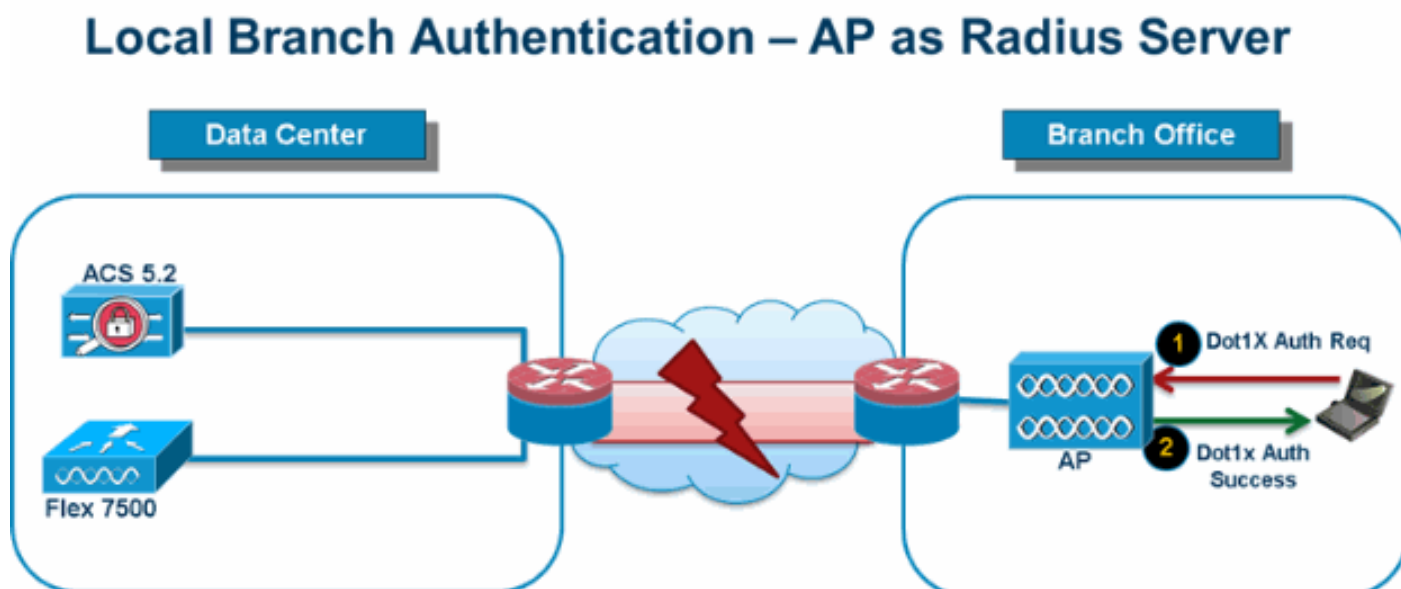
- 在7.0.98.0代码版本之前，仅当FlexConnect处于独立模式时，才支持本地身份验证，以确保在广域网链路故障期间不会影响客户端连接。7.0.116.0版本现在支持此功能，即使FlexConnect接入点处于连接模式。**图 10：中央Dot1X身份验证（充当身份验证器的FlexConnect AP）**



如图10所示，当FlexConnect分支AP与Flex 7500失去连接时，分支客户端可以继续执行802.1X身份验证。只要RADIUS/ACS服务器可以从分支站点访问，无线客户端就会继续验证和访问无线服务。换句话说，如果RADIUS/ACS位于分支机构内，则客户端将进行身份验证并访问无线服务，即使在广域网中断期间也是如此。**注意：**此功能可与FlexConnect备份RADIUS服务器功能结合使用。如果FlexConnect组配置了备份RADIUS服务器和本地身份验证，则FlexConnect接入点始终尝试先使用主备份RADIUS服务器对客户端进行身份验证，然后使用辅助备份RADIUS服务器（如果主服务器无法访问），最后使用FlexConnect接入点上的本地EAP服务器（如果主服务器和辅助服务器无法访问）。

本地EAP（本地身份验证继续）

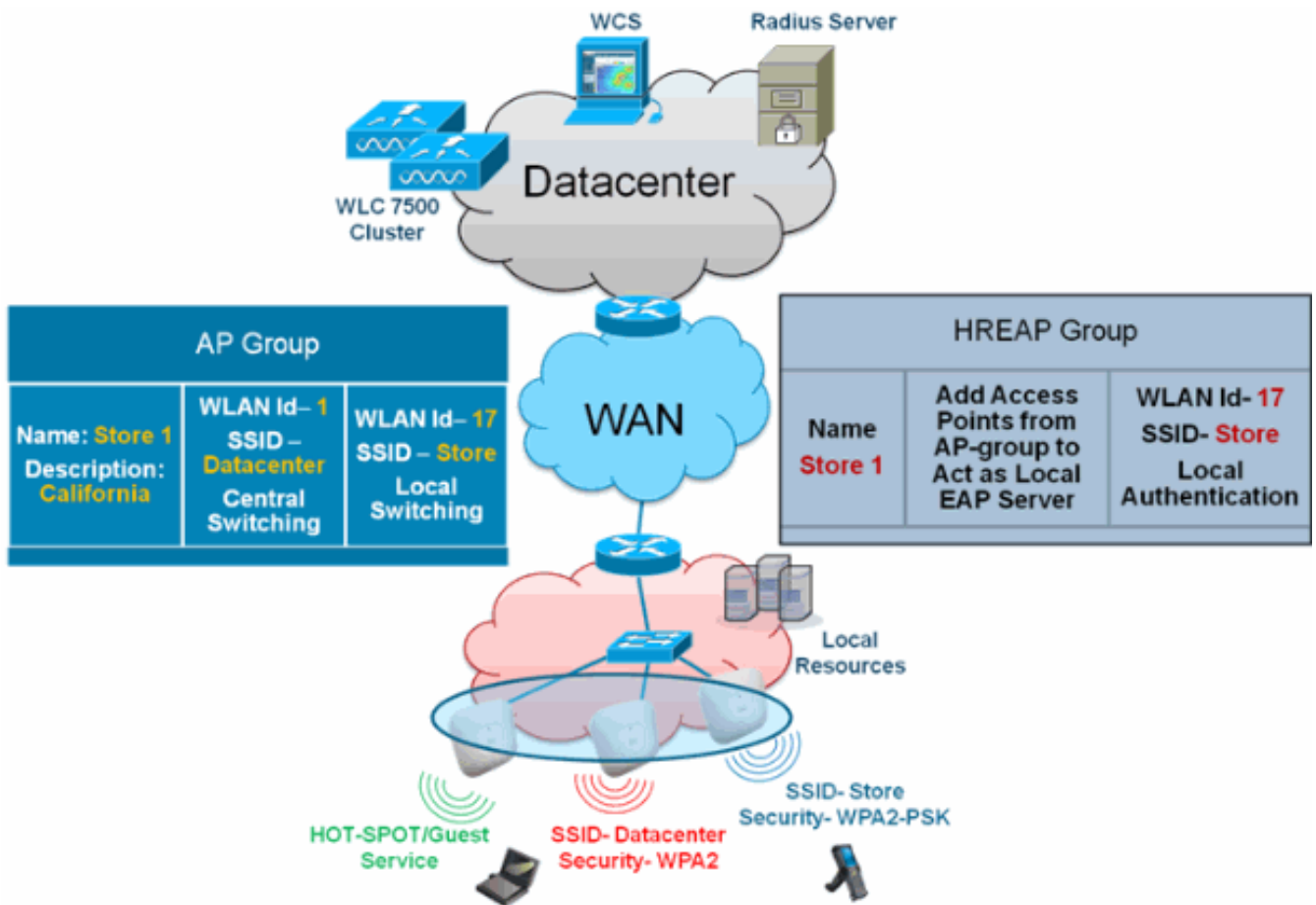
图 11 : Dot1X身份验证 (充当本地EAP服务器的FlexConnect AP)



- 您可以配置控制器，使FlexConnect AP在独立或连接模式下执行LEAP或EAP-FAST身份验证，最多支持100个静态配置用户。当控制器加入控制器时，控制器会将用户名和口令的静态列表发送到该特定FlexConnect组的每个FlexConnect接入点。组中的每个接入点仅对自己的关联客户端进行身份验证。
- 此功能非常适合从自主接入点网络迁移到轻量级FlexConnect接入点网络且对维护大型用户数据库或添加其他硬件设备以取代自主接入点中可用的RADIUS服务器功能不感兴趣的客户。
- 如图11所示，如果数据中心内的RADIUS/ACS服务器无法访问，则FlexConnect AP会自动充当本地EAP服务器，以对无线分支客户端执行Dot1X身份验证。

CCKM/OKC快速漫游

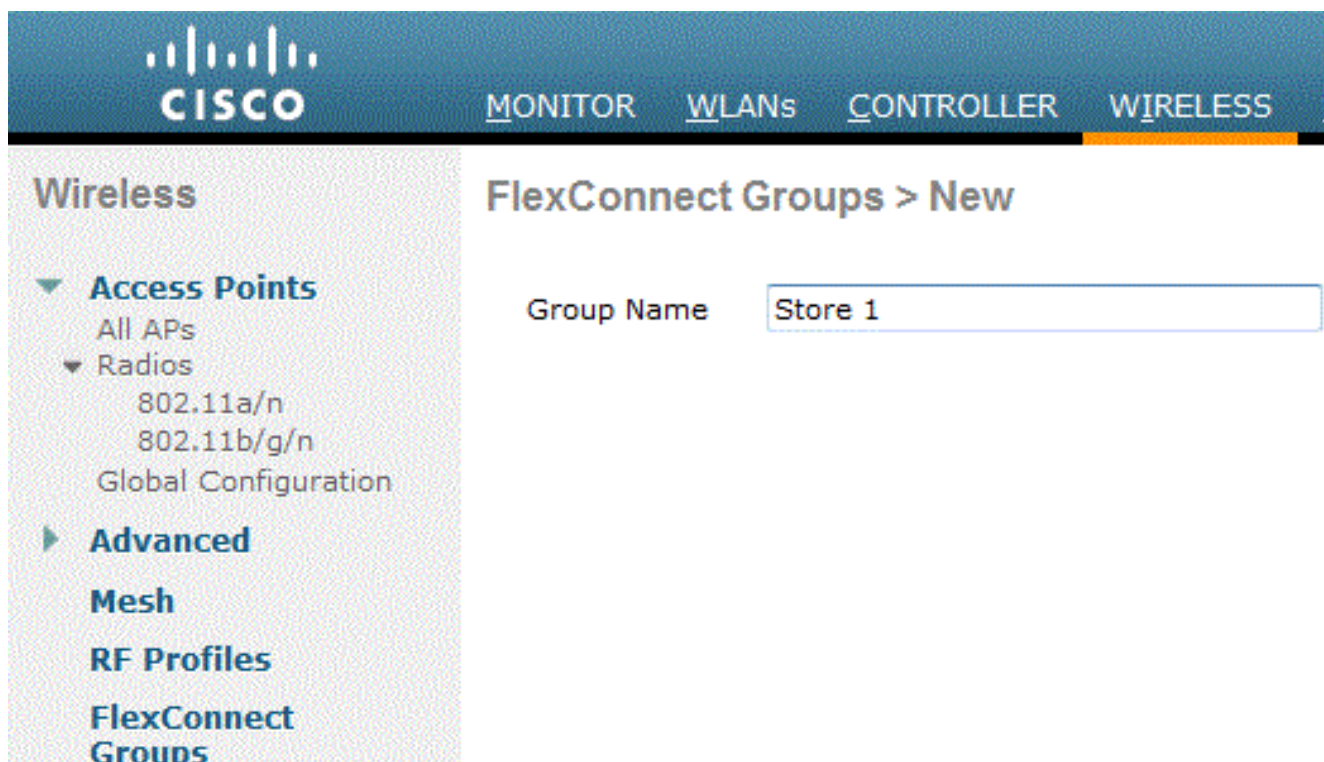
- CCKM/OKC快速漫游需要FlexConnect组才能与FlexConnect接入点配合使用。快速漫游是通过缓存来自完整EAP身份验证的主密钥的衍生项来实现的，以便当无线客户端漫游到不同的接入点时，可以进行简单且安全的密钥交换。当客户端从一个接入点漫游到另一个接入点时，此功能可防止执行完全RADIUS EAP身份验证。FlexConnect接入点需要获取所有可能关联的客户端的CCKM/OKC缓存信息，以便他们可以快速处理该信息，而不是将其发回控制器。例如，如果您有一个控制器，该控制器有300个接入点和100个可能关联的客户端，则向所有100个客户端发送CCKM/OKC缓存是不切实际的。如果创建包含有限数量接入点的FlexConnect组（例如，在远程办公室中为四个接入点创建组），客户端仅在这四个接入点之间漫游，CCKM/OKC缓存仅在客户端关联到其中一个接入点时分配在这四个接入点之间。
- 此功能与备份RADIUS和本地身份验证(Local-EAP)一起确保分支机构站点不会停机运行。**注意**：不支持在FlexConnect和非FlexConnect接入点之间进行CCKM/OKC快速漫游。图 12：使用FlexConnect组的无线网络设计参考



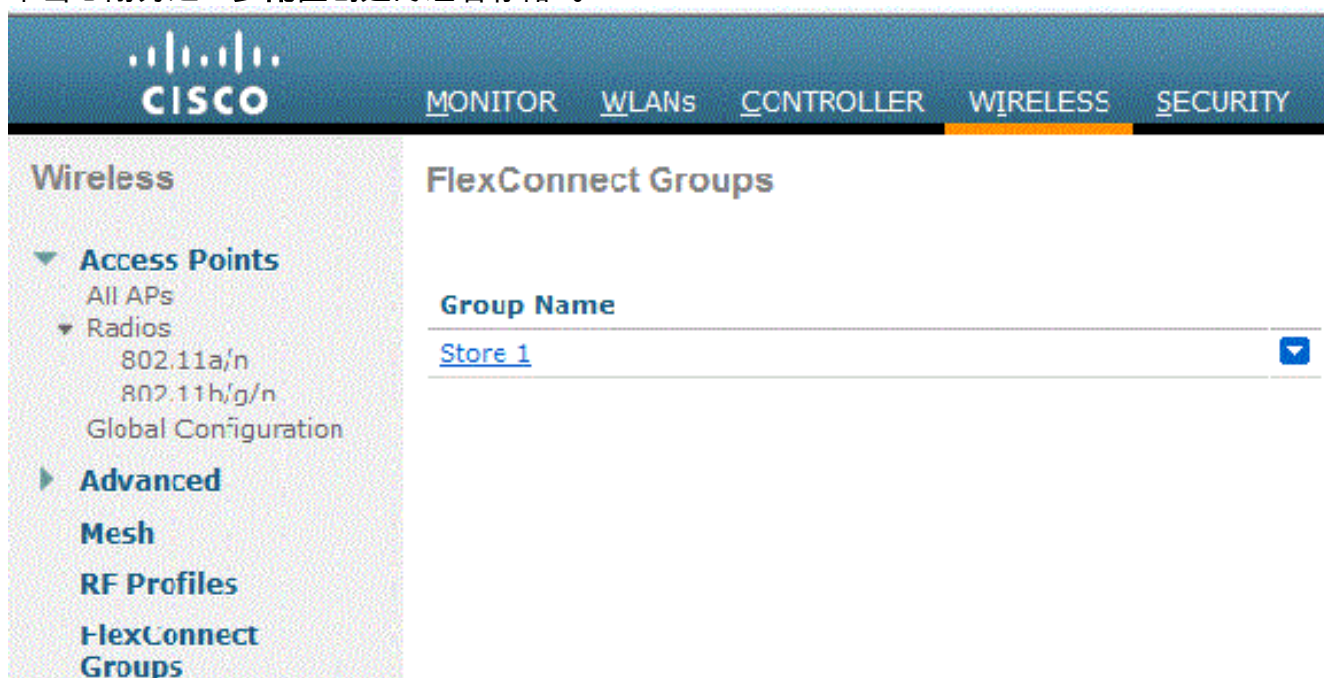
从WLC配置FlexConnect组

完成本节中的步骤，以便当FlexConnect处于连接或独立模式时，将FlexConnect组配置为支持使用LEAP的本地身份验证。图12中的配置示例说明了AP组和FlexConnect组之间的目标差异和1:1映射。

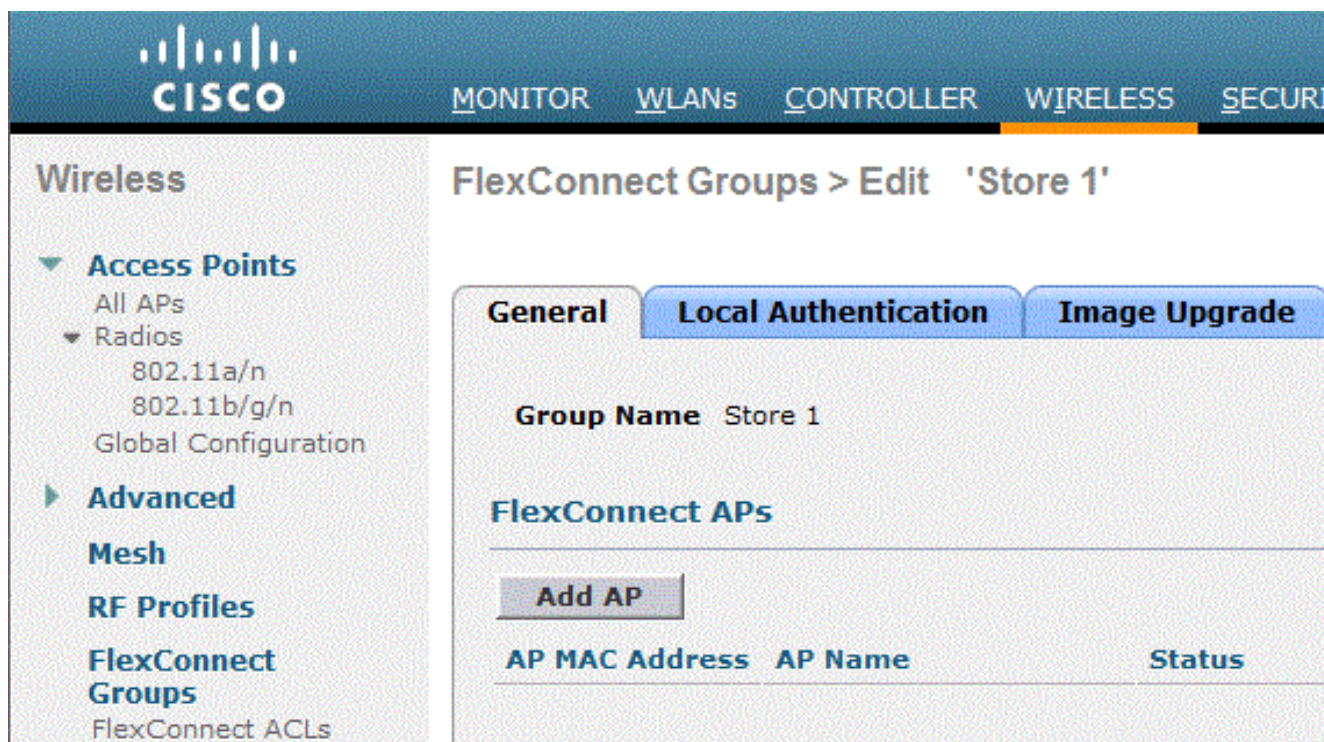
1. 单击“Wireless”>“FlexConnect Groups”下的“New”。
2. 分配组名存储1，类似于图12所示的配置。
3. 设置组名后，单击应用。



4. 单击您刚为进一步配置创建的组名存储1。



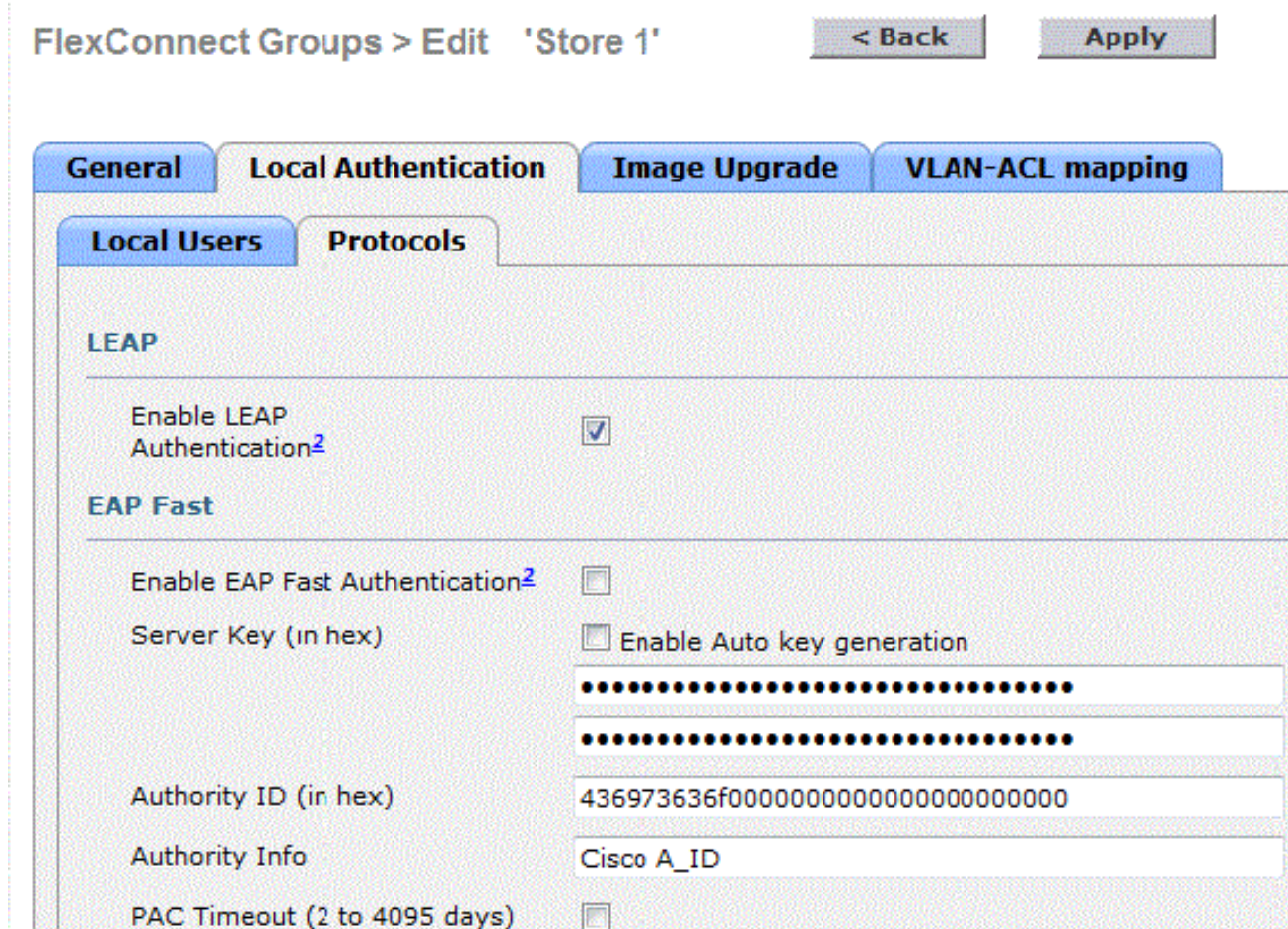
5. 单击Add AP。



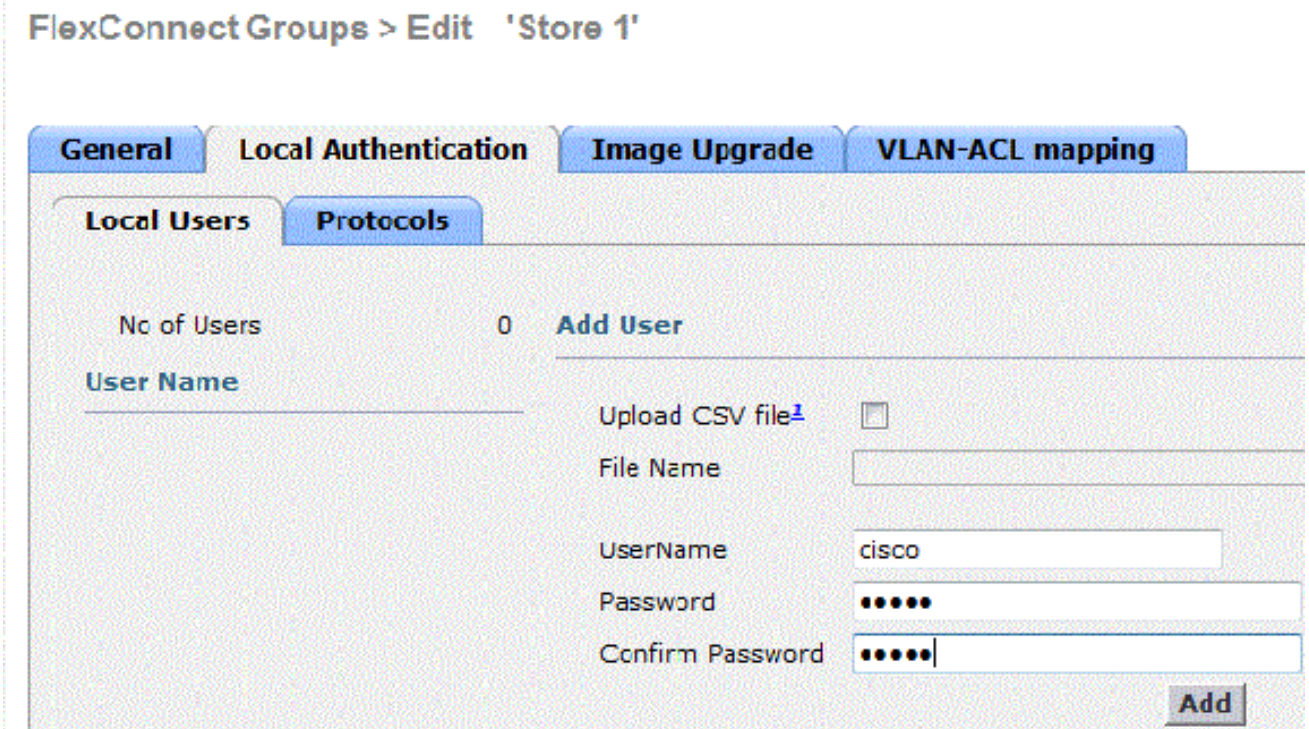
6. 选中**Enable AP Local Authentication**框，以在AP处于独立模式时启用Local Authentication。
注意：步骤20显示如何为连接模式AP启用本地身份验证。
7. 选中**从当前控制器**选择AP复选框以启用AP名称下拉菜单。
8. 从下拉菜单中选择需要成为此FlexConnect组一部分的AP。
9. 从下拉列表中选择AP后，单击**Add**。
10. 重复步骤7和8，将AP添加到此FlexConnect组，这些AP也是AP组存储1的一部分。请参阅[图12](#)，了解AP组和FlexConnect组之间的1:1映射。如果已为每个存储创建AP组([图8](#))，则理想情况下该AP组的所有AP都应是此FlexConnect组的一部分([图12](#))。AP组和FlexConnect组之间保持1:1的比率可简化网络管理。



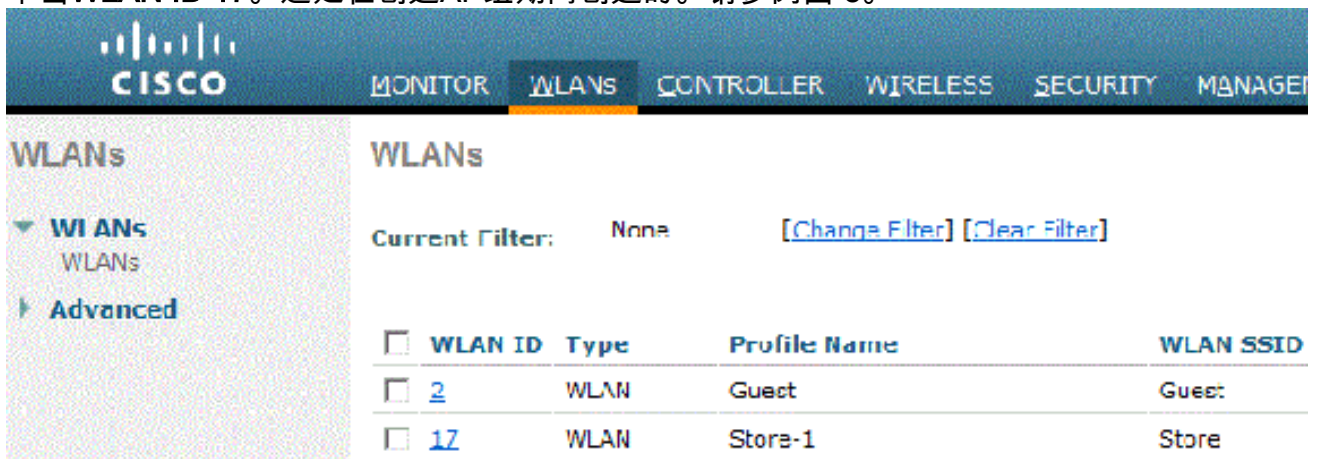
11. 单击Local Authentication > Protocols并选中Enable LEAP Authentication框。
12. 选中后单击“应用”。注意：如果您有备份控制器，请确保FlexConnect组相同，并且每个FlexConnect组都包含AP MAC地址条目。



13. 在Local Authentication下，单击**Local Users**。
14. 设置Username、Password和Confirm Password字段，然后单击**Add**以在驻留在AP上的本地EAP服务器中创建用户条目。
15. 重复步骤13，直到您的本地用户名列表用尽。不能配置或添加100个以上的用户。
16. 在步骤14完成后单击**Apply**，并验证“No of Users”计数。



17. 在顶部窗格中，单击**WLANs**。
18. 单击**WLAN ID 17**。这是在创建AP组期间创建的。请参阅图 8。



19. 在WLAN > Edit for WLAN ID 17下，单击**Advanced**。
20. 选中**FlexConnect Local Auth**框以在连接模式下启用本地身份验证。**注意**：仅对具有本地交换的FlexConnect支持本地身份验证。**注意**：在WLAN下启用本地身份验证之前，请务必创建FlexConnect组。

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还提

供FlexConnect Local Auth复选框，以便在连接模式下启用本地身份验证，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

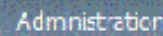
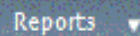
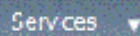
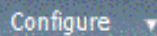
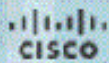
Configure > Controllers > [Controller] > WLANs > WLAN Configuration :

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还提供过滤和监控FlexConnect本地身份验证客户端的工具，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:01:b4		IPv4	Unknown		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	Unknown		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进行验证

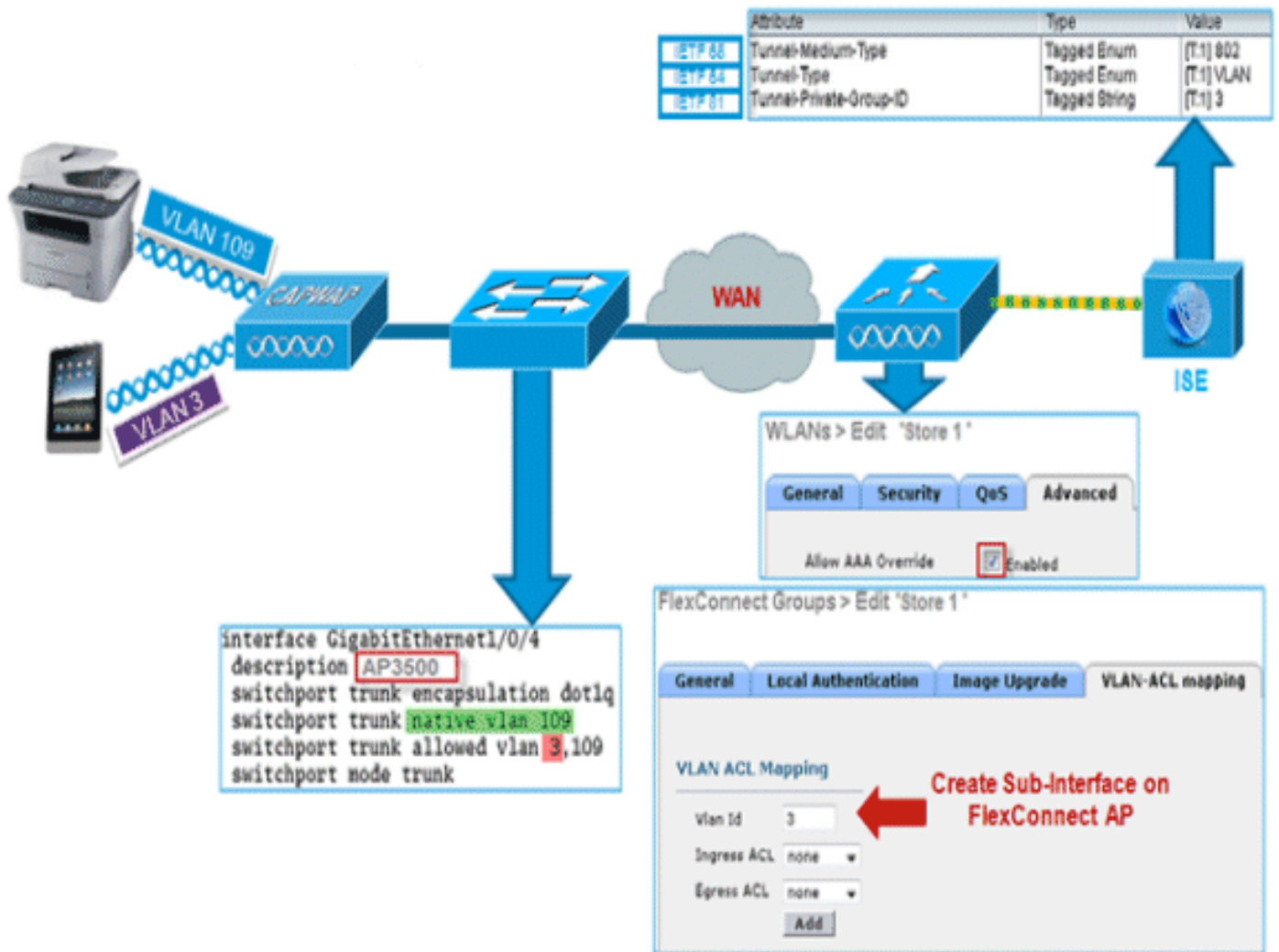
在WLC上使用以下CLI可快速验证客户端身份验证状态和交换模式：

```
(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覆盖

在当前FlexConnect架构中，WLAN与VLAN的严格映射，因此，在FlexConnect AP上与特定WLAN关联的客户端必须遵守映射到该VLAN的VLAN。此方法有局限性，因为它要求客户端与不同的SSID关联，以继承不同的基于VLAN的策略。

从7.2版开始，支持在为本地交换配置的单个WLAN上对VLAN进行AAA覆盖。为了进行动态VLAN分配，AP将根据为单个FlexConnect AP使用现有WLAN-VLAN映射或在FlexConnect组上使用ACL-VLAN映射的配置，为VLAN预先创建接口。WLC用于在AP上预创建子接口。



摘要

- 从版本7.2开始，AAA VLAN覆盖受支持，适用于在中央和本地身份验证模式下为本地交换配置的WLAN。
- 应在为本地交换配置的WLAN上启用AAA覆盖。
- FlexConnect AP应从WLC预先创建VLAN以分配动态VLAN。
- 如果AP客户端上不存在AAA覆盖返回的VLAN，它们将从AP的默认VLAN接口获取IP。

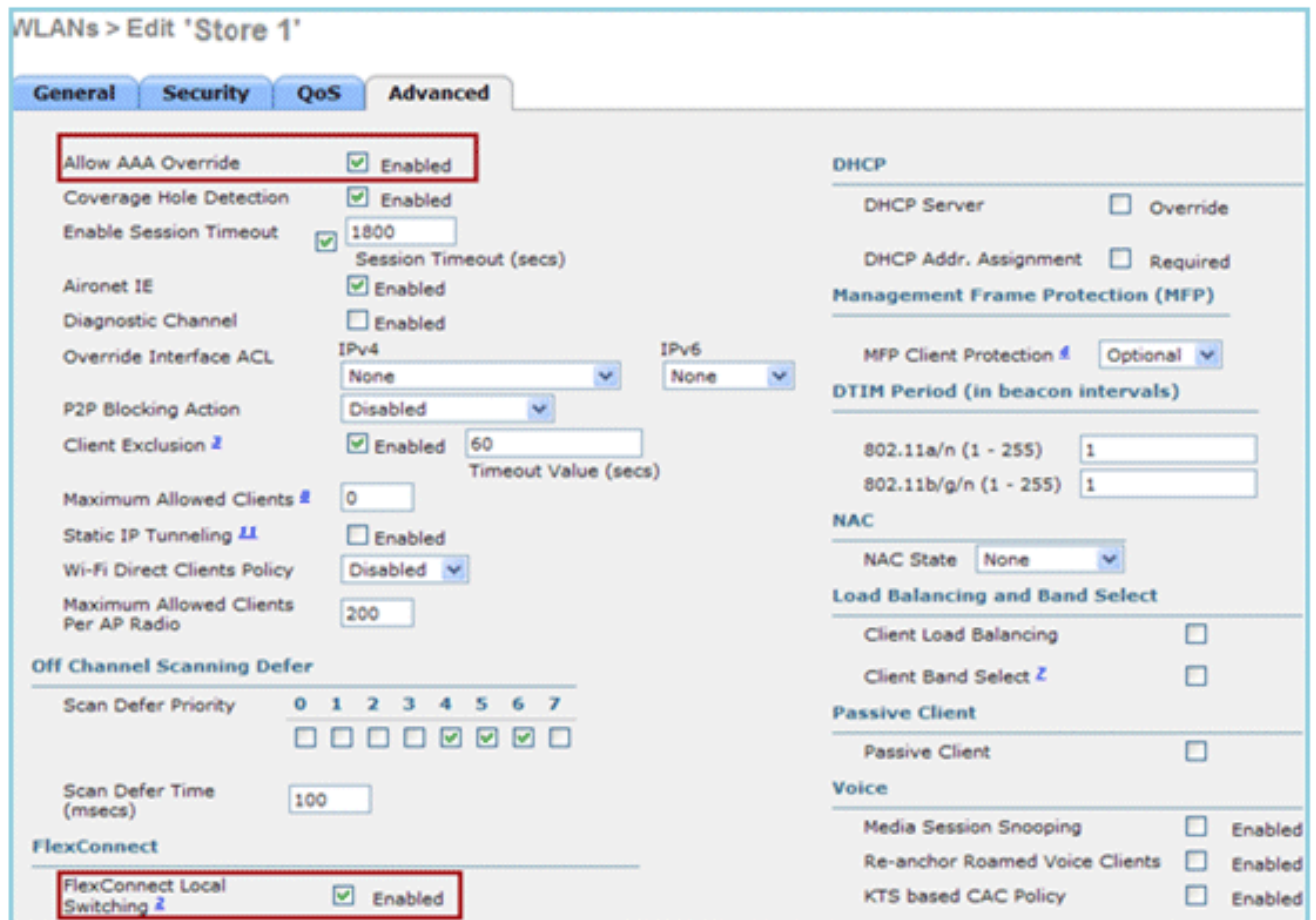
步骤

请完成以下步骤：

1. 创建用于802.1x身份验证的WLAN。



2. 在WLC上为本地交换WLAN启用AAA覆盖支持。导航至WLAN GUI > WLAN > > WLAN ID > Advance 选项卡。



3. 在控制器上添加AAA服务器详细信息，以进行802.1x身份验证。要添加AAA服务器，请导航至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. 默认情况下，AP处于本地模式，因此将模式转换为FlexConnect模式。通过转到“无线”>“所有AP”，然后单击“单个AP”，可将本地模式AP转换为FlexConnect模式。

All APs > Details for AP3500

General | Credentials | Interfaces | High Availability | Inventory | Advanced

General

AP Name: AP3500
 Location: default location
 AP MAC Address: cc:ef:48:c2:35:57
 Base Radio MAC: 2c:3f:38:f6:98:b0
 Admin Status: Enable
 AP Mode: FlexConnect
 AP Sub Mode: None
 Operational Status: REG
 Port Number: 1
 Venue Group: Unspecified
 Venue Type: Unspecified
 Venue Name: [Redacted]
 Language: [Redacted]
 Network Spectrum Interface Key: 0D45BA896226F4117D98BA920FBA8A16

Versions

Primary Software Version: 7.2.1.69
 Backup Software Version: 7.2.1.72
 Predownload Status: None
 Predownloaded Version: None
 Predownload Next Retry Time: NA
 Predownload Retry Count: NA
 Boot Version: 12.4.23.0
 IOS Version: 12.4(20111122:141426)\$
 Mini IOS Version: 7.0.112.74

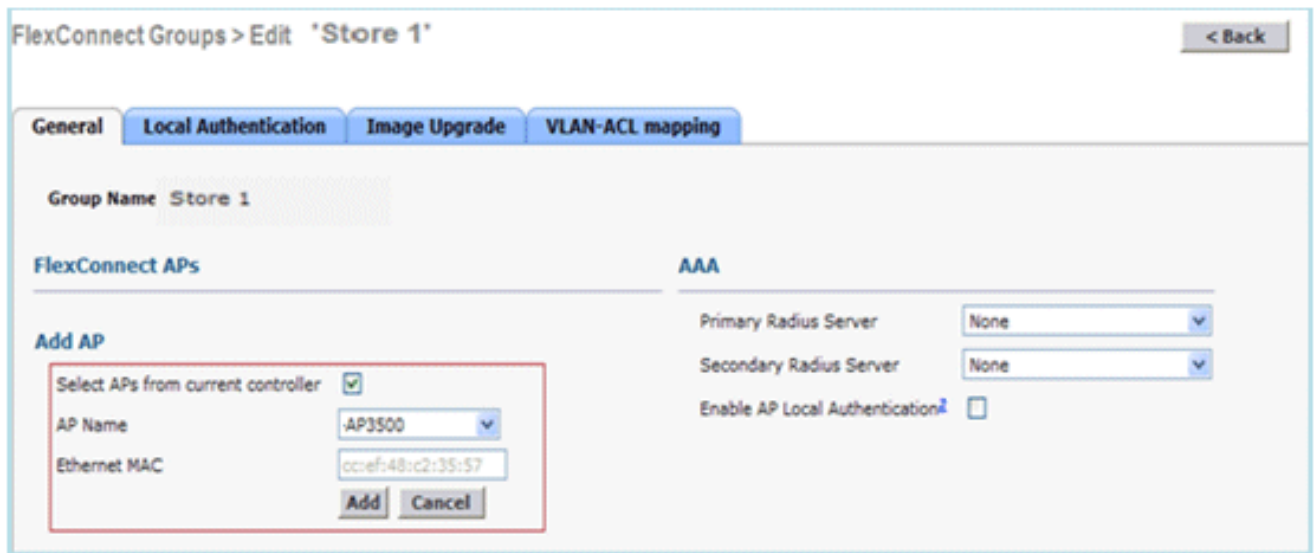
IP Config

IP Address: 10.10.10.132
 Static IP:

Time Statistics

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. 将FlexConnect AP添加到FlexConnect组。在WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General 选项卡 > Add AP下导航。



6. FlexConnect AP应连接在中继端口上，WLAN映射VLAN和AAA覆盖的VLAN应允许在中继端

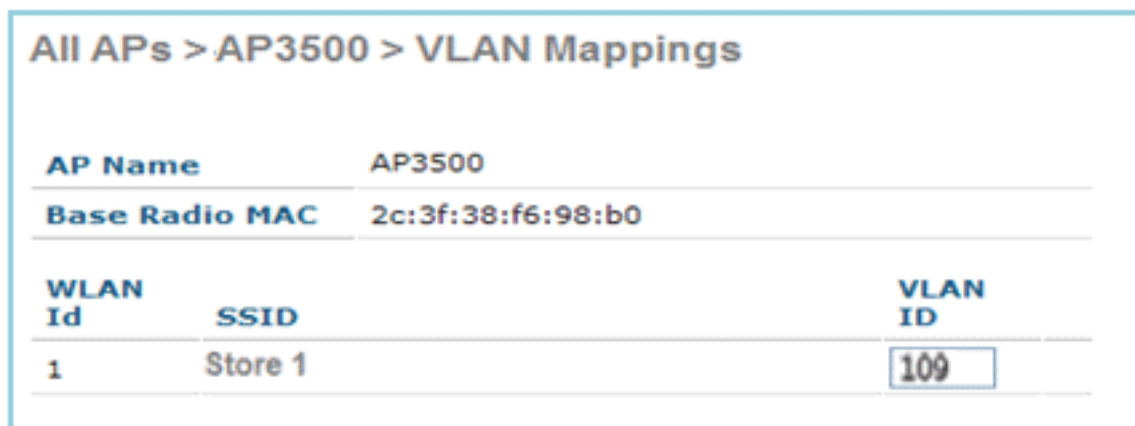
```
interface GigabitEthernet1/0/4
description AP3500
switchport trunk encapsulation dot1q
switchport trunk native vlan 109
switchport trunk allowed vlan 3,109
switchport mode trunk
```

口上。

注意：在此配置中，vlan 109用于WLAN

VLAN映射，vlan 3用于AAA覆盖。

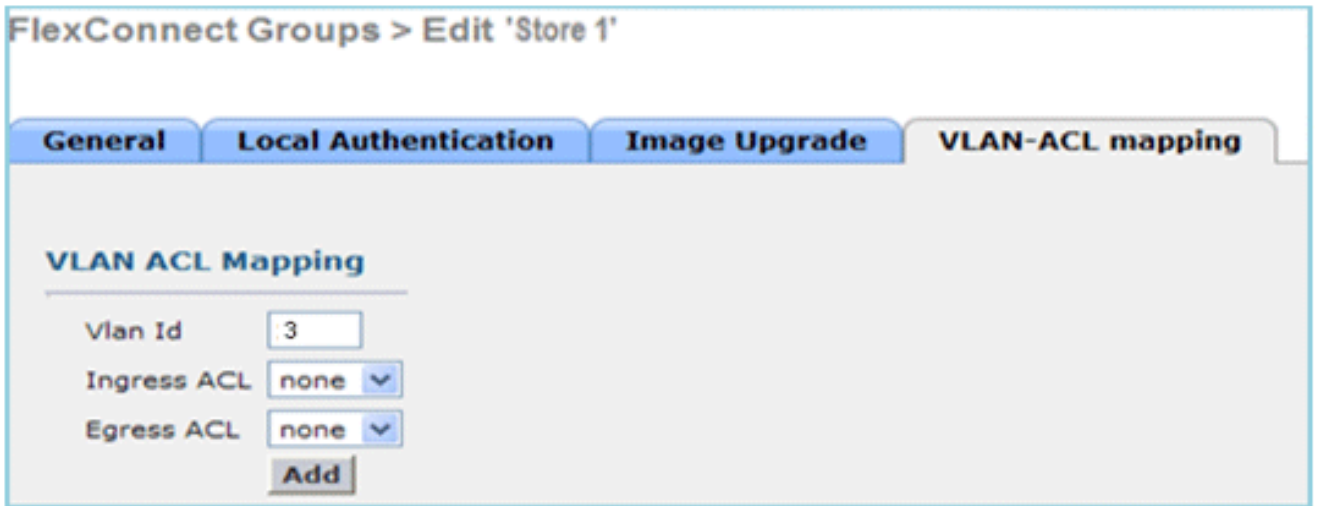
7. 为FlexConnect AP配置WLAN到VLAN的映射。根据此配置，AP将具有VLAN的接口。当AP收到VLAN配置时，将创建相应的dot11和以太网子接口并将其添加到网桥组。关联此WLAN上的客户端，当客户端关联时，会分配其VLAN（默认值，基于WLAN-VLAN映射）。导航至WLAN GUI > **Wireless** > All APs > 单击特定AP > **FlexConnect**选项卡，然后单击**VLAN映射**。



8. 在AAA服务器中创建用户，并将用户配置为在IETF Radius属性中返回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. 为了进行动态VLAN分配，AP将根据使用单个FlexConnect AP的现有WLAN-VLAN映射或在FlexConnect组上使用ACL-VLAN映射的配置，为动态VLAN预先创建接口。要在FlexConnect AP上配置AAA VLAN，请导航至WLC GUI > **Wireless** > **FlexConnect Group** > 单击特定FlexConnect组 > **VLAN-ACL映射**，然后在Vlan ID 字段中输入VLAN。



10. 关联此WLAN上的客户端，并使用AAA服务器中配置的用户名进行身份验证以返回AAA VLAN。
11. 客户端应从通过AAA服务器返回的动态VLAN接收IP地址。
12. 要进行验证，请单击WLC GUI > Monitor > Client >单击特定客户端MAC地址以检查客户端详细信息。

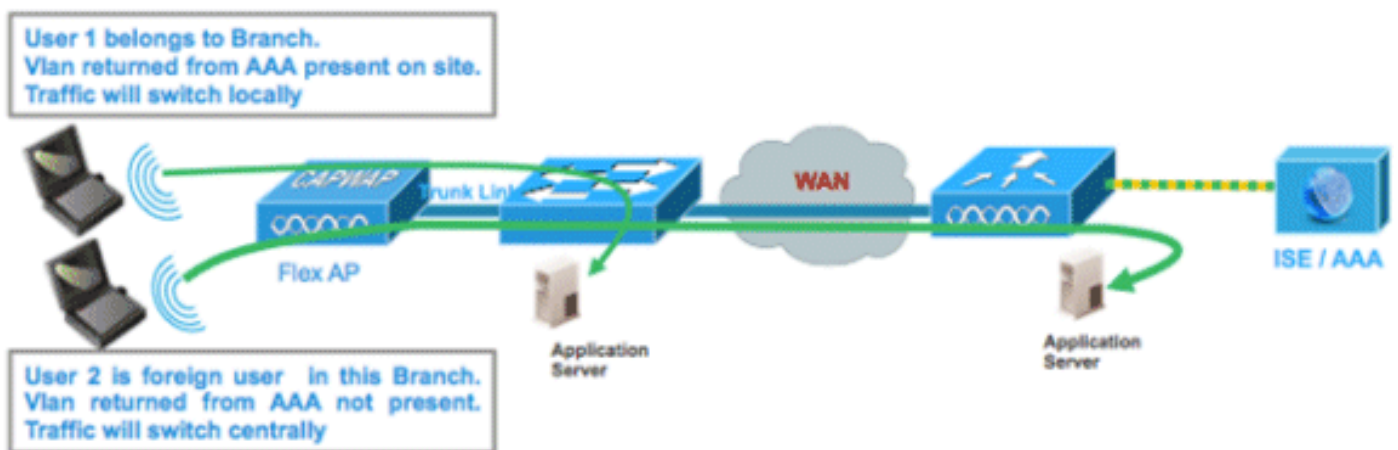
限制

- 不支持Cisco Airespace特定属性，并且仅支持IETF属性VLAN ID。
- 在每个AP配置中，最多可以通过WLAN-VLAN映射为单个FlexConnect AP配置，或在FlexConnect组上使用ACL-VLAN映射配置16个VLAN。

基于FlexConnect VLAN的中央交换

在控制器软件版本7.2中，本地交换WLAN的AAA覆盖VLAN（动态VLAN分配）会将无线客户端置于AAA服务器提供的VLAN中。如果AAA服务器提供的VLAN不存在于AP中，客户端将被置于该AP上的WLAN映射VLAN中，流量将在该VLAN上本地交换。此外，在版本7.3之前，根据WLAN配置，可以集中或本地交换来自FlexConnect AP的特定WLAN的流量。

从7.3版开始，来自FlexConnect AP的流量可以集中交换或本地交换，具体取决于FlexConnect AP上是否存在VLAN。



摘要

当Flex AP处于连接模式时，为本地交换配置的WLAN上的流量：

- 如果VLAN作为AAA属性之一返回，且Flex AP数据库中不存在VLAN，则流量将集中交换，并且如果WLC上存在VLAN，则会为客户端分配从AAA服务器返回的此VLAN/接口。
- 如果VLAN作为AAA属性之一返回，且Flex AP数据库中不存在该VLAN，流量将集中交换。如果WLC上也不存在该VLAN，将为客户端分配映射到WLC上WLAN的VLAN/接口。
- 如果VLAN作为AAA属性之一返回，且FlexConnect AP数据库中存在该VLAN，则流量将在本地交换。
- 如果AAA服务器未返回VLAN，客户端将在该FlexConnect AP上分配WLAN映射VLAN，流量将在本地交换。

当Flex AP处于独立模式时，为本地交换配置的WLAN上的流量：

- 如果AAA服务器返回的VLAN不存在于Flex AP数据库中，则客户端将被置于默认VLAN（即Flex AP上的WLAN映射VLAN）。当AP重新连接时，此客户端将取消身份验证并集中交换流量。
- 如果AAA服务器返回的VLAN存在于Flex AP数据库中，客户端将被放入返回的VLAN中，流量将在本地交换。
- 如果VLAN未从AAA服务器返回，客户端将在该FlexConnect AP上分配WLAN映射VLAN，流量将在本地交换。

步骤

请完成以下步骤：

1. 为本地交换配置WLAN并启用AAA覆盖。

WLANs > Edit 'Store 1'

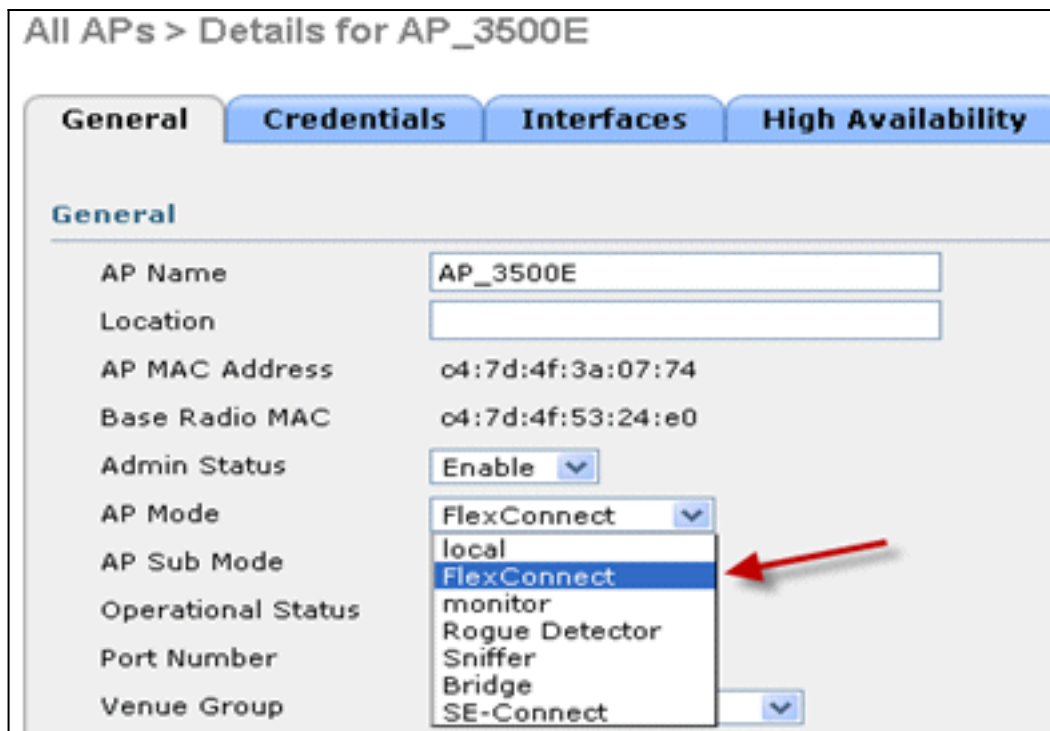
General	Security	QoS	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled	
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/>	Enabled	
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. 在新创建的WLAN上启用基于VLAN的中央交换。

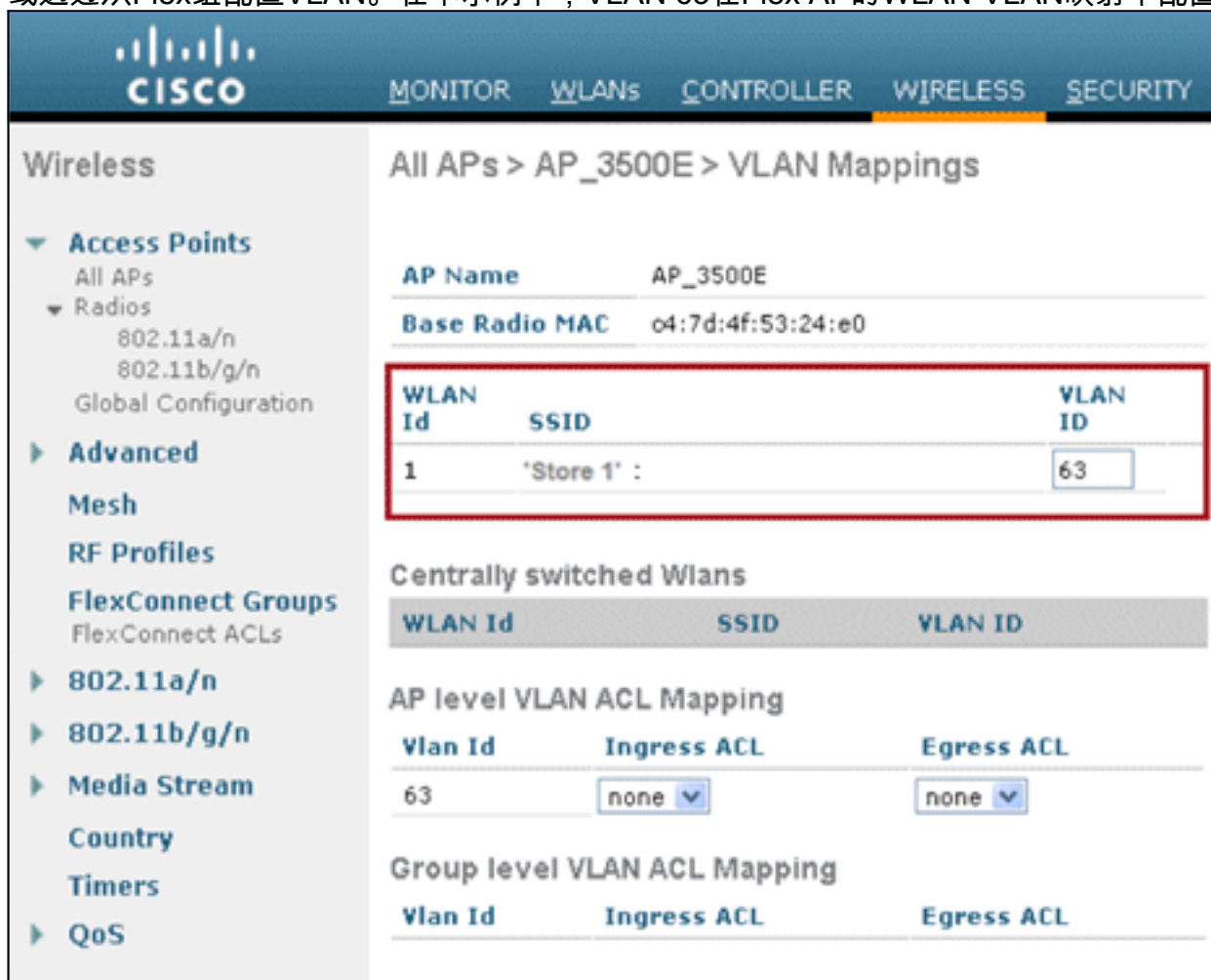
WLANs > Edit 'Store 1'

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	IPv6 None
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	
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. 将AP模式设置为FlexConnect。



4. 确保FlexConnect AP的数据库中存在某些子接口，可通过特定Flex AP上的WLAN-VLAN映射或通过从Flex组配置VLAN。在本示例中，VLAN 63在Flex AP的WLAN-VLAN映射中配置。



5. 在本例中，VLAN 62在WLC上配置为动态接口之一，且未映射到WLC上的WLAN。WLC上的WLAN映射到管理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. 将客户端关联到此Flex AP上步骤1中配置的WLAN，并从AAA服务器返回VLAN 62。此Flex AP上不存在VLAN 62，但它作为动态接口存在于WLC上，因此流量将集中交换，并且客户端将在WLC上分配VLAN 62。在此处捕获的输出中，客户端已分配VLAN 62，且“数据交换和身份验证”(Data Switching and Authentication)设置为**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	betauser		
Port Number	1		
Interface	dyn		
VLAN ID	62		

注意： 请注意，虽然WLAN已配置为本地交换，但此客户端的Data Switching字段是基于VLAN存在的Central（即，从AAA服务器返回的VLAN 62不存在于AP数据库中）。

7. 如果另一用户与此创建的WLAN上的同一AP关联，并且从AP和WLC上不存在的AAA服务器返回一些VLAN，则流量将集中交换，并且客户端将分配到WLC（即，本示例设置中的VLAN 61）上的WLAN映射接口，因为WLAN映射到管理接口为VLAN 61配置

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：请注意，虽然WLAN已配置为本地交换，但此客户端的“数据交换”字段是基于VLAN存在的中心字段。即，从AAA服务器返回的VLAN 61不存在于AP数据库中，但也不存在于WLC数据库中。因此，为客户端分配了默认接口VLAN/接口，该接口映射到WLAN。在本例中，WLAN映射到管理接口（即VLAN 61），因此客户端从VLAN 61收到IP地址。

8. 如果另一用户在此创建的WLAN上与其关联，并且VLAN 63从AAA服务器（此Flex AP上存在）返回，则将为客户端分配VLAN 63，并且流量将在本地交换。

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

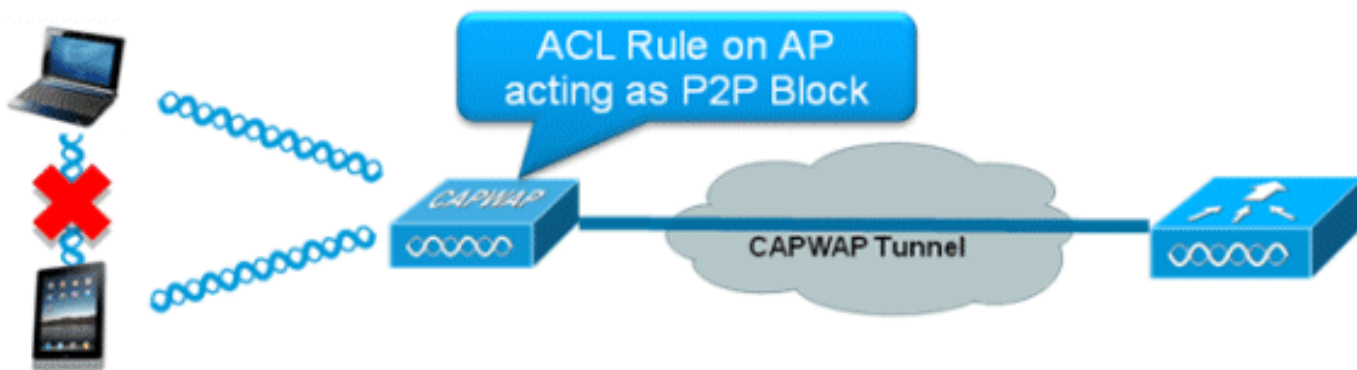
限制

- 仅为集中身份验证和本地交换配置的WLAN支持基于VLAN的集中交换。
- AP子接口（即VLAN映射）应在FlexConnect AP上配置。

FlexConnect ACL

在FlexConnect上引入ACL后，有一种机制可满足FlexConnect AP的访问控制需求，以保护和完整性来自AP的本地交换数据流量。FlexConnect ACL在WLC上创建，然后应使用VLAN-ACL映射为

AAA覆盖VLAN配置FlexConnect AP或FlexConnect组上存在的VLAN。然后，这些设备会被推送到AP。



摘要

- 在控制器上创建FlexConnect ACL。
- 在AP级别VLAN ACL映射下FlexConnect AP上存在的VLAN上应用相同的VLAN。
- 可应用于VLAN-ACL映射下FlexConnect组中的VLAN（通常针对AAA覆盖的VLAN完成）。
- 在VLAN上应用ACL时，选择要应用的方向，即“入口”、“出口”或“入口和出口”。

步骤

请完成以下步骤：

1. 在WLC上创建FlexConnect ACL。导航至WLC GUI > Security > Access Control List > FlexConnect ACLs。

2. 单击 **New**。
3. 配置ACL名称。

Access Control Lists > New

Access Control List Name

4. 单击 **Apply**。
5. 为每个ACL创建规则。要创建规则，请导航至WLC GUI > Security > Access Control List > FlexConnect ACLs，然后单击上面创建的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. 单击 **Add New Rule**。

Access Control Lists > Rules > New

Sequence

Source IP Address IP Address Netmask

Destination IP Address IP Address Netmask

Protocol

DSCP

Action

注意： 根据要求配置规则。如果允许任何规则在末尾未配置，则存在隐式拒绝，将阻止所有流量。

7. 创建FlexConnect ACL后，可以在单个FlexConnect AP下映射WLAN-VLAN映射，也可以应用于FlexConnect组上的VLAN-ACL映射。
8. 在AP级别上为各个VLAN映射上为各个FlexConnect AP在VLAN映射下配置的FlexConnect ACL。导航至WLC GUI > Wireless > All AP >单击特定AP > FlexConnect 选项卡> VLAN Mapping。

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也可应用于FlexConnect组中的VLAN-ACL映射。在FlexConnect组的VLAN-ACL映射下创建的VLAN主要用于动态VLAN覆盖。

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上最多可配置512个FlexConnect ACL。
- 每个ACL可以配置64条规则。
- 每个FlexConnect组或每个FlexConnect AP最多可映射32个ACL。
- 在任意给定时间点，FlexConnect AP上最多有16个VLAN和32个ACL。

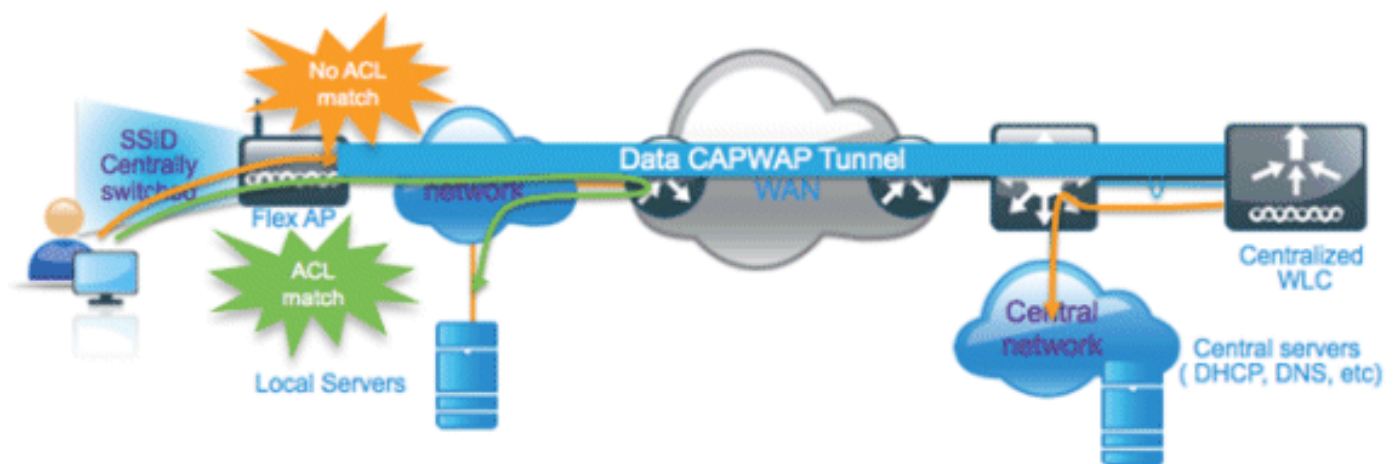
FlexConnect拆分隧道

在7.3之前的WLC版本中，如果与集中交换WLAN关联的FlexConnect AP上连接的客户端需要将一些流量发送到本地站点/网络中的设备，则他们需要通过CAPWAP将流量发送到WLC，然后通过CAPWAP或使用一些带外连接将相同流量返回本地站点。

从7.3版开始，**分割隧道**引入了一种机制，通过该机制，客户端发送的流量将使用Flex ACL根据数据包内容进行分类。匹配的数据包从Flex AP本地交换，其余数据包通过CAPWAP集中交换。

分割隧道功能是OEAP AP设置的额外优势，企业SSID上的客户端可以直接与本地网络上的设备（打印机、远程LAN端口上的有线计算机或个人SSID上的无线设备）通信，而不会通过CAPWAP发送数据包而消耗WAN带宽。OEAP 600 AP不支持分割隧道。可以使用规则创建Flex ACL，以允许本地站点/网络上的所有设备。当来自公司SSID上无线客户端的数据包与OEAP AP上配置的Flex ACL中的规则匹配时，该流量在本地交换，其余流量（即隐式拒绝流量）将通过CAPWAP集中交换。

分割隧道解决方案假设与中心站点中的客户端关联的子网/VLAN不存在于本地站点（即，从中心站点上存在的子网接收IP地址的客户端的流量将无法在本地交换）。分割隧道功能旨在为属于本地站点的子网本地交换流量，以避免广域网带宽消耗。匹配Flex ACL规则的流量在本地交换，并执行NAT操作，将客户端的源IP地址更改为可在本地站点/网络上路由的Flex AP的BVI接口IP地址。



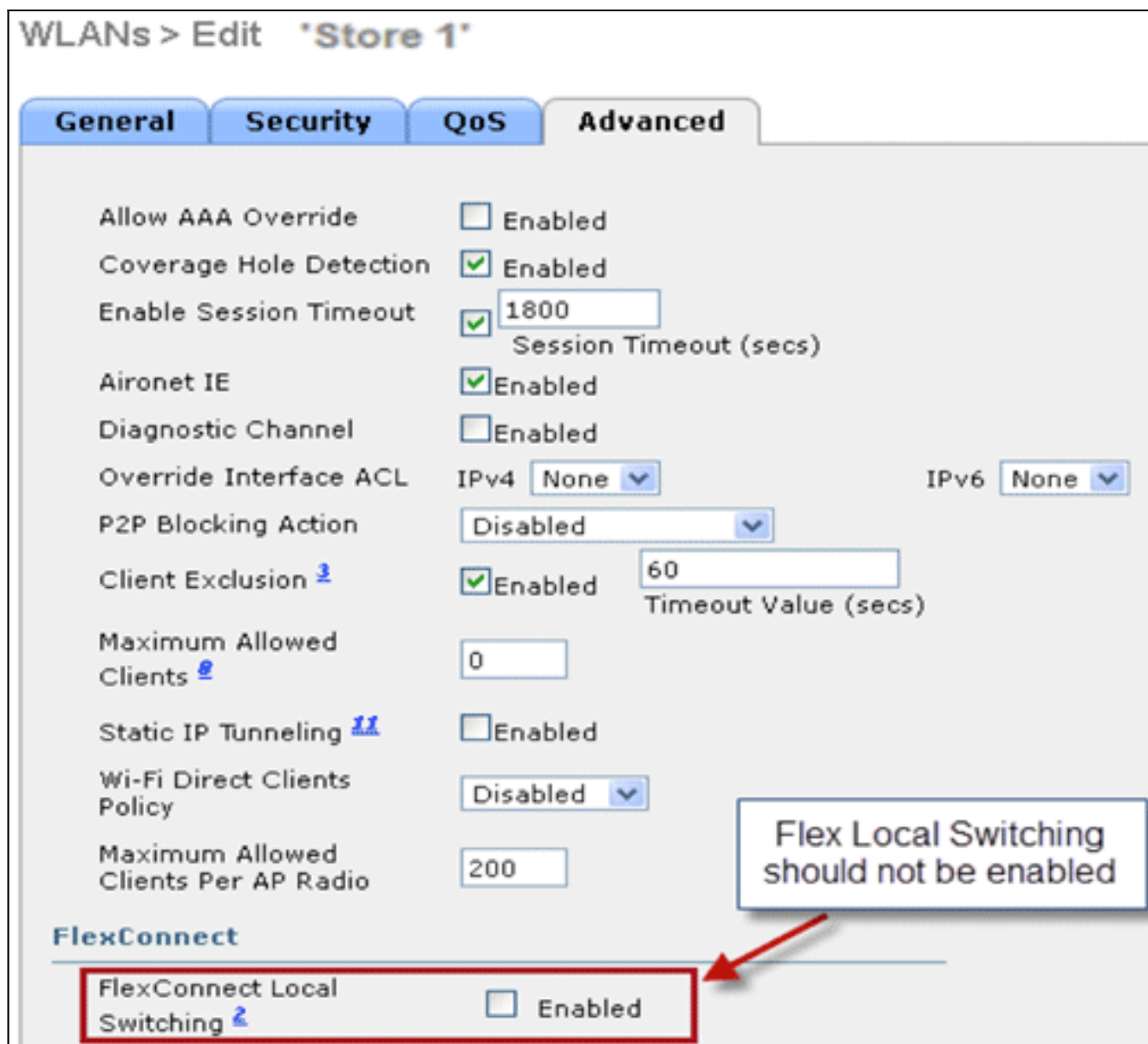
摘要

- 仅Flex AP通告的为中央交换配置的WLAN支持分割隧道功能。
- 在为分割隧道配置的WLAN上应启用所需的DHCP。
- 分割隧道配置应用于每个WLAN，这些WLAN配置用于每个Flex AP或FlexConnect组中的所有Flex AP的集中交换。

步骤

请完成以下步骤：

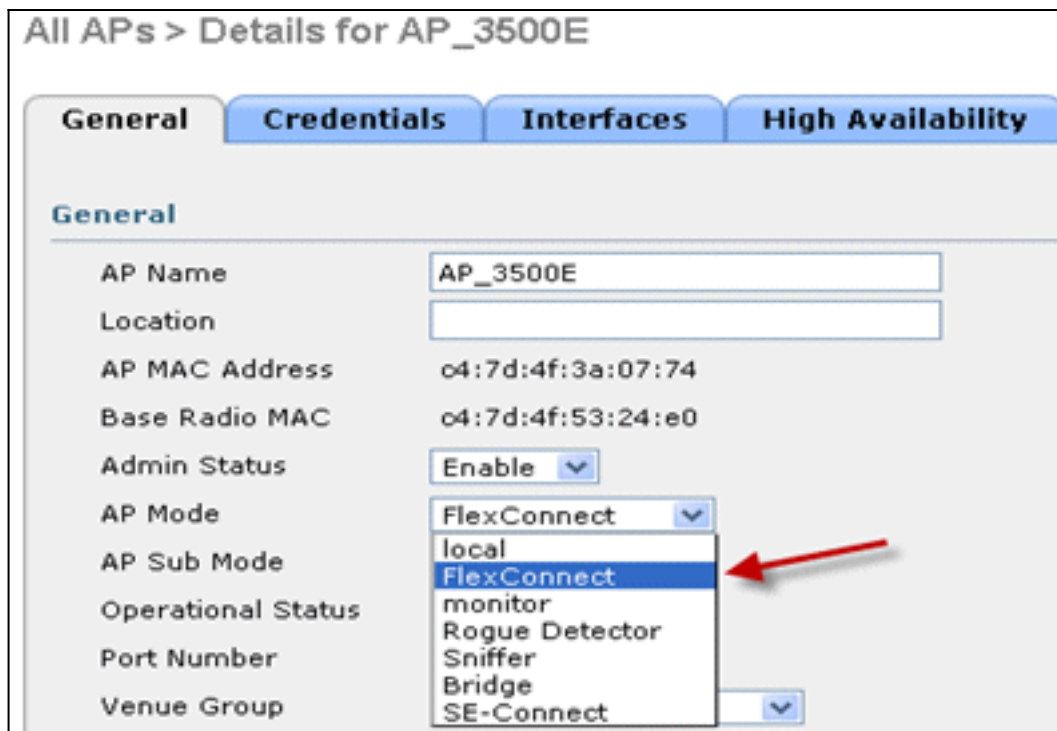
1. 为中央交换配置WLAN(即，不应启用Flex Local Switching)。



2. 将DHCP Address Assignment (DHCP地址分配) 设置为Required(必需)。



3. 将AP模式设置为FlexConnect。



4. 为应在中央交换机WLAN上本地交换的流量配置FlexConnect ACL的允许规则。在本例中，配置了FlexConnect ACL规则，以便在Flex AP上应用NAT操作后，它会将来自9.6.61.0子网（即中心站点上存在）的所有客户端的ICMP流量警报到9.1.0.150，以便在本地交换。其余流量将达到隐式拒绝规则，并通过CAPWAP进行集中交换。



5. 此创建的FlexConnect ACL可以作为分割隧道ACL推送到单个Flex AP，也可以推送到Flex Connect组中的所有Flex AP。要将Flex ACL作为本地拆分ACL推送到单个Flex AP，请完成以下步骤：单击Local Split ACLs。

The image shows the Cisco Wireless Controller configuration page for AP_3500E. The 'FlexConnect' tab is selected and highlighted with a red box. In the left-hand navigation menu, 'Local Split ACLs' is also highlighted with a red box and has a red arrow pointing to it. The main configuration area shows 'VLAN Support' checked, 'Native VLAN ID' set to 57, and 'FlexConnect Group Name' as 'Not Configured'. There are links for 'External WebAuthentication ACLs' and 'Local Split ACLs'.

选择应启用分割隧道功能的WLAN Id，选择Flex-ACL，然后单击Add。

The image shows the 'ACL Mappings' configuration page for AP_3500E. The 'WLAN ACL Mapping' section is highlighted with a red box. It contains a 'WLAN Id' field with the value '1', a 'Local-Split ACL' 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 header with columns for 'WLAN Id', 'WLAN Profile Name', and 'Local-Split ACL'.

Flex-ACL作为本地拆分ACL推送到Flex AP。

All APs > AP_3500E > ACL Mappings

AP Name AP_3500E

Base Radio MAC c4:7d: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

要将

Flex ACL作为本地拆分ACL推送到FlexConnect组，请完成以下步骤：选择应启用分割隧道功能的WLAN Id。在WLAN-ACL映射选项卡上，从添加特定Flex AP的FlexConnect组中选择FlexConnect ACL，然后单击添加。

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

Flex-ACL作为本地拆分ACL推送到该Flex组中的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

- 不应使用与源和目标子网相同的permit/deny语句配置Flex ACL规则。
- 仅当无线客户端为本地站点上的主机发起流量时，配置为分割隧道的集中交换WLAN上的流量才能在本地上交换。如果流量由本地站点上的客户端/主机为这些已配置的WLAN上的无线客户端发起，它将无法到达目的地。
- 组播/广播流量不支持分割隧道。组播/广播流量将集中交换，即使它与Flex ACL匹配。

容错

FlexConnect容错功能允许在以下情况下对分支机构客户端进行无线接入和服务：

- FlexConnect分支AP与主Flex 7500控制器失去连接。
- FlexConnect分支AP正在切换到辅助Flex 7500控制器。
- FlexConnect分支AP正在重新建立与主Flex 7500控制器的连接。

FlexConnect容错和上述的本地EAP一起，在网络中断期间提供零分支机构停机时间。此功能默认启用，无法禁用。无需在控制器或AP上进行配置。但是，为确保容错工作顺利且适用，应保持以下标准：

- WLAN订购和配置必须在主控制器和备用Flex 7500控制器之间相同。
- VLAN映射必须在主控制器和备用Flex 7500控制器之间相同。
- 移动域名必须在主控制器和备用Flex 7500控制器上相同。
- 建议使用Flex 7500作为主控制器和备用控制器。

摘要

- 当AP连接回同一控制器时，如果控制器上的配置没有更改，FlexConnect将不会断开客户端。
- 如果配置没有更改且备份控制器与主控制器相同，则FlexConnect在连接到备份控制器时不会断开客户端连接。
- 如果控制器上的配置没有更改，FlexConnect将不会在连接回主控制器时重置其无线电。

限制

- 仅支持带本地交换的中央/本地身份验证的FlexConnect。
- 如果客户端会话计时器在FlexConnect AP从独立模式切换到连接模式之前过期，则集中身份验证的客户端需要完全重新身份验证。
- Flex 7500主控制器和备用控制器必须位于同一移动域中。

每个WLAN的客户端限制

随着流量分段，对限制访问无线服务的客户端总数的需求也随之而来。

示例：限制从分支隧道返回数据中心的访客客户端总数。

为了应对这一挑战，思科引入了“每WLAN客户端限制”功能，该功能可以限制每个WLAN上允许的客户端总数。

主要目标

- 设置最大客户端数限制
- 操作简便性

注意：这不是QoS的形式。

默认情况下，该功能被禁用，不强制限制。

限制

当FlexConnect处于独立操作状态时，此功能不强制客户端限制。

WLC 配置

请完成以下步骤：

1. 选择Centrally Switched WLAN ID 1 with SSID Datacenter(带SSID数据中心的集中交换WLAN ID 1)。此WLAN是在AP组创建期间创建的。请参阅图 8。
2. 单击WLAN ID 1的“高级”选项卡。
3. 为Maximum Allowed Clients文本字段设置客户端限制值。
4. 在设置“Maximum Allowed Clients”（允许的最大客户端数）的文本字段后，单击Apply。

The screenshot shows the 'WLANs > Edit' configuration page for a WLAN. The 'Advanced' tab is selected, and the 'Maximum Allowed Clients' field is highlighted in red and set to 0. Other settings include 'Allow AAA Override' (Enabled), 'Coverage Hole Detection' (Enabled), 'Enable Session Timeout' (Enabled, 1800 secs), 'Aironet IE' (Enabled), 'Diagnostic Channel' (Enabled), 'IPv6 Enable' (Disabled), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (Enabled, 60 secs), 'DHCP' (Override, Required), 'Management Frame Protection (MFP)' (Optional), 'DTIM Period' (1 for 802.11a/n and 802.11b/g/n), 'NAC' (NAC OOB State and Posture State both Enabled), and 'Load Balancing and Band Select' (Client Load Balancing and Client Band Select both Disabled). The 'Scan Defer' section shows a priority of 0-7 and a time of 100 msec.

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

Maximum Allowed Clients的默认值设置为0，这表示没有限制，且功能已禁用。

NCS配置

要从NCS启用此功能，请转至Configure > Controllers > Controller IP > WLANs > WLAN Configuration > 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

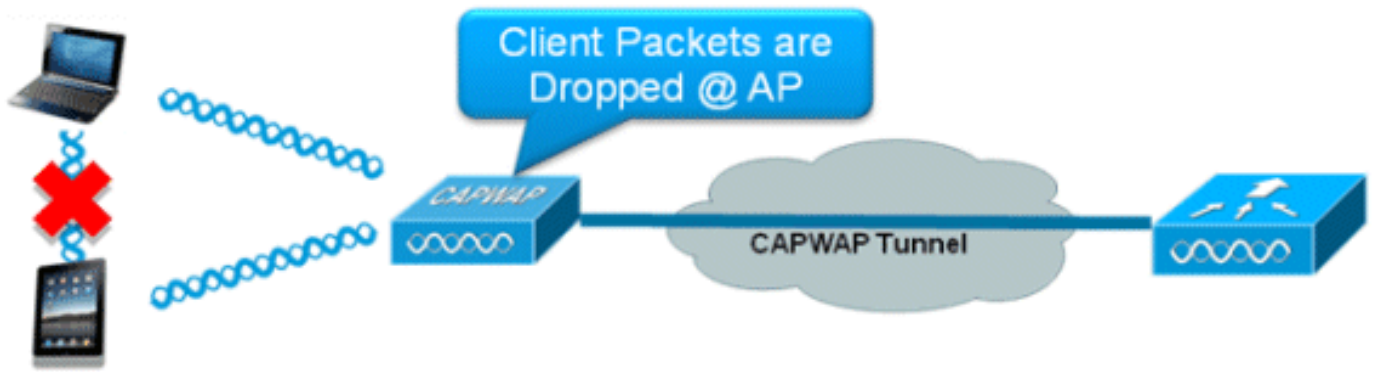
NAC

点对点阻塞

在7.2之前的控制器软件版本中，仅中心交换WLAN支持点对点(P2P)阻塞。在WLAN上，可以使用以下三种操作中的任意一种配置点对点阻塞：

- **禁用** — 在控制器内为同一子网中的客户端本地禁用点对点阻塞和桥接流量。这是默认值。
- **丢弃** — 使控制器丢弃同一子网中客户端的数据包。
- **Forward Up-Stream** — 使数据包在上游VLAN上转发。控制器上的设备决定对数据包采取什么操作。

从7.2版开始，本地交换WLAN上关联的客户端支持点对点阻塞。根据WLAN，控制器将点对点配置推送到FlexConnect AP。



摘要

- 每个WLAN配置对等阻止
- 根据WLAN，点对点阻止配置由WLC推送到FlexConnect AP。
- 在WLAN上配置为丢弃或上游转发的点对点阻止操作被视为在FlexConnect AP上启用的点对点阻止。

步骤

请完成以下步骤：

1. 在为FlexConnect本地交换配置的WLAN上，将“丢弃”(Drop)启用对等阻止操作。

2. 一旦P2P阻止操作在配置为本地交换的WLAN上配置为**丢弃或转发上游**，它就会从WLC推送到FlexConnect AP。FlexConnect AP将此信息存储在闪存的reap配置文件中。这样，即使FlexConnect AP处于独立模式，它也可以在相应子接口上应用P2P配置。

限制

- 在FlexConnect中，解决方案P2P阻止配置不能仅应用于特定FlexConnect AP或AP子集。它应用于广播SSID的所有FlexConnect AP。
- 中央交换客户端的统一解决方案支持P2P上行转发。但是，FlexConnect解决方案不支持此功能

- 。这被视为P2P丢弃，客户端数据包被丢弃而不是转发到下一个网络节点。
- 中央交换客户端的统一解决方案支持对与不同AP关联的客户端进行P2P阻止。但是，此解决方案仅针对连接到同一AP的客户端。FlexConnect ACL可用作此限制的解决方法。

AP预映像下载

此功能允许AP在运行时下载代码。AP映像前下载对于减少软件维护或升级期间的网络停机时间非常有用。

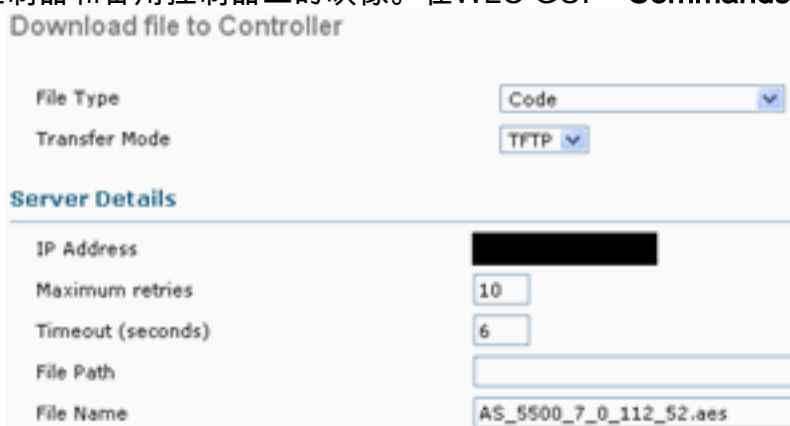
摘要

- 易于软件管理
- 按商店计划升级：需要NCS来完成此任务
- 减少停机时间

步骤

请完成以下步骤：

1. 升级主控制器和备用控制器上的映像。在WLC GUI > **Commands** > **Download File**下导航以开



Download file to Controller

File Type: Code

Transfer Mode: TFTP

Server Details

IP Address: [Redacted]

Maximum retries: 10

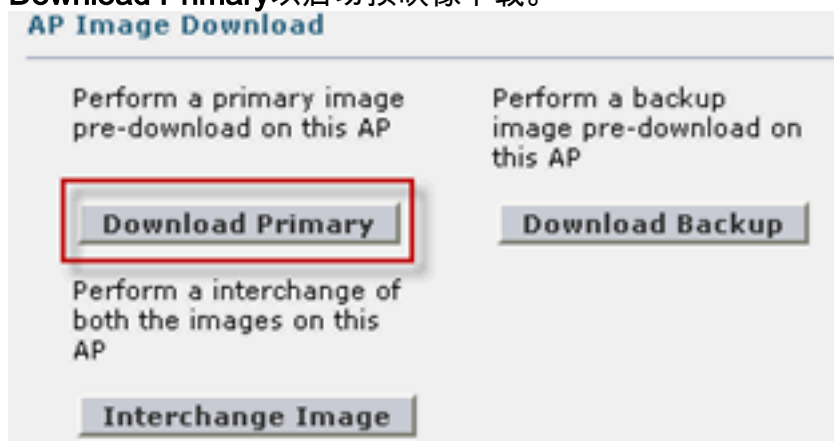
Timeout (seconds): 6

File Path: [Empty]

File Name: AS_5500_7_0_112_52.aes

始下载。

2. 保存控制器上的配置，但不要重新启动控制器。
3. 从主控制器发出AP pre-image download命令。导航至WLC GUI > **Wireless** > **Access Points** > **All APs**，然后选择接入点以开始预映像下载。选择接入点后，单击“高级”选项卡。单击 **Download Primary**以启动预映像下载。



AP Image Download

Perform a primary image pre-download on this AP

Download Primary

Perform a backup image pre-download on this AP

Download Backup

Perform a interchange of both the images on this AP

Interchange Image

```
*Sep 13 21:21:14 903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image ██████████ 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: ██████████
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 ██████████..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
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. 下载所有AP映像后，重新启动控制器。AP现在会回退到独立模式，直到控制器重新启动。注意：在独立模式下，容错功能将保持客户端关联。控制器恢复后，AP将自动重新启动，并使用预下载的映像。重新启动后，AP重新加入主控制器并恢复客户端服务。

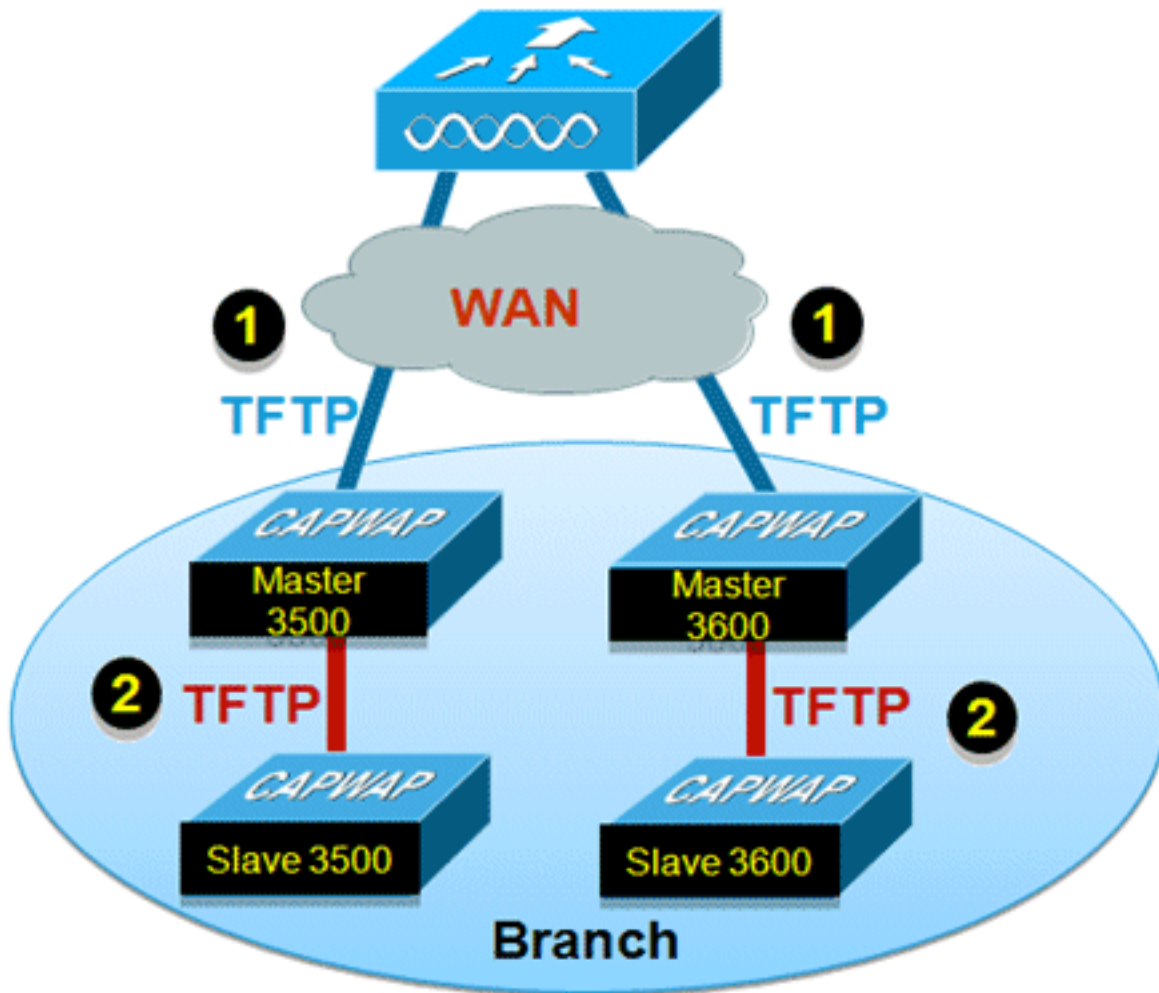
限制

- 仅与CAPWAP AP配合使用。

FlexConnect智能AP映像升级

预映像下载功能在一定程度上减少了停机时间，但所有FlexConnect AP仍必须通过WAN链路预下载各自的AP映像，延迟更高。

高效的AP映像升级将减少每个FlexConnect AP的停机时间。基本思想是每个AP型号中只有一个AP将从控制器下载映像并充当主/服务器，同一型号的其余AP将充当从/客户端，并将从主机预下载AP映像。从服务器到客户端的AP映像分布将在本地网络上，不会遇到WAN链路的延迟。因此，流程将更快。



摘要

- 每个FlexConnect组为每个AP型号选择主AP和从AP
- 主设备从WLC下载映像
- 从设备从主AP下载映像
- 减少停机时间并节省广域网带宽

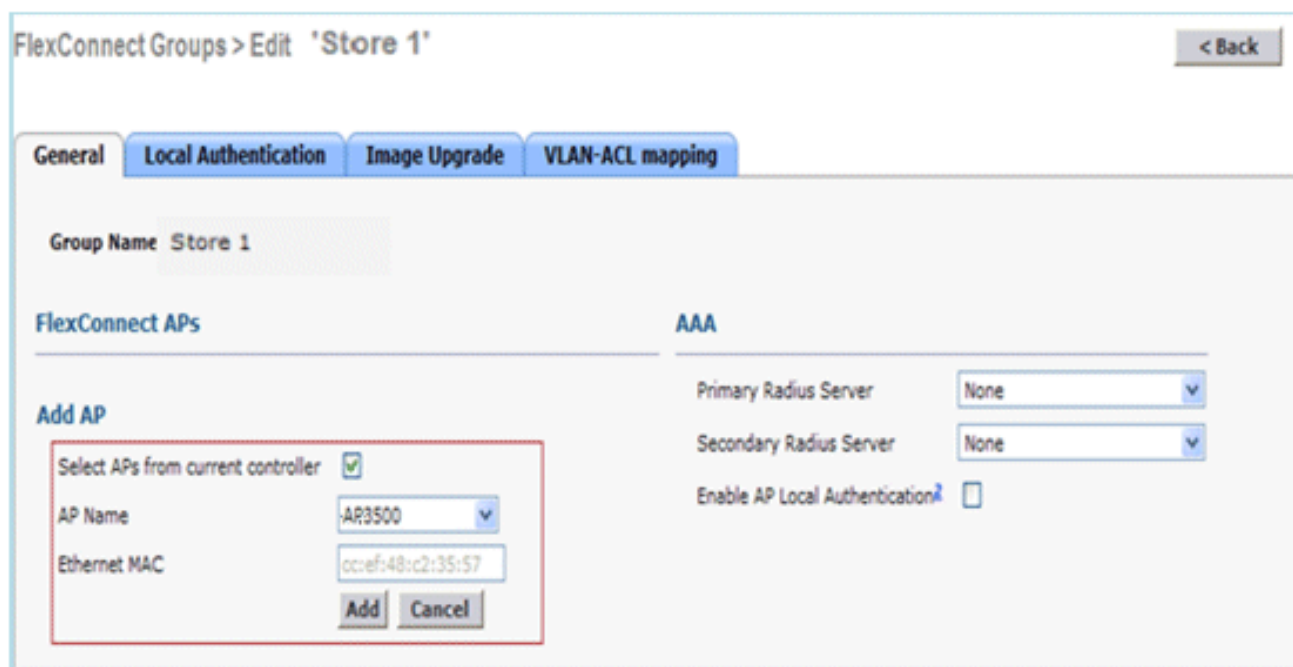
步骤

请完成以下步骤：

1. 升级控制器上的映像。导航至WLC GUI > Commands > Download File以开始下载。

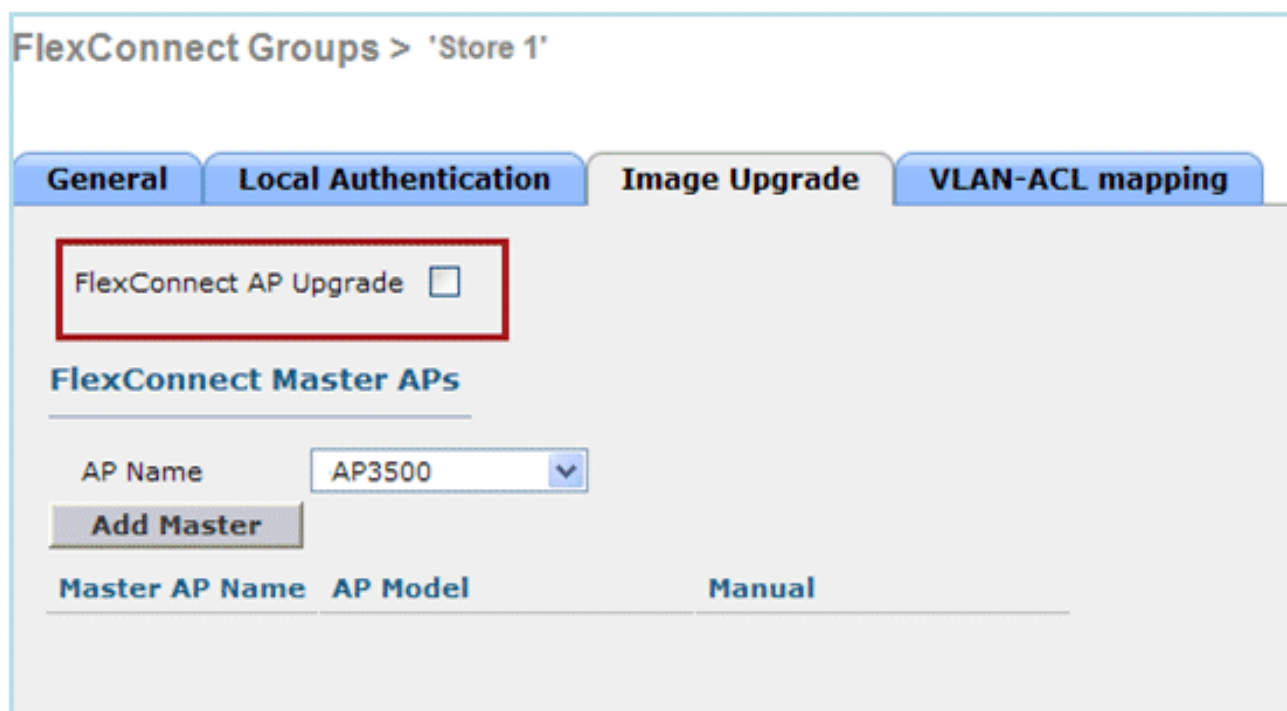
Download file to Controller	
File Type	Code
Transfer Mode	TFTP
Server Details	
IP Address	[REDACTED]
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_2_1_72.ess

2. 保存控制器上的配置，但不要重新启动控制器。
3. 将FlexConnect AP添加到FlexConnect组。导航至WLC GUI > Wireless > FlexConnect Groups >选择FlexConnect Group > General 选项卡> Add AP。



The screenshot shows the 'FlexConnect Groups > Edit 'Store 1'' configuration page. The 'General' tab is selected. The 'Add AP' dialog box is open, with the following fields: 'Select APs from current controller' (checked), 'AP Name' (AP3500), and 'Ethernet MAC' (0c:ef:48:c2:35:57). There are 'Add' and 'Cancel' buttons at the bottom of the dialog. In the background, the 'AAA' section shows 'Primary Radius Server' and 'Secondary Radius Server' both set to 'None', and 'Enable AP Local Authentication' is unchecked.

4. 单击“FlexConnect AP升级”复选框以实现高效的AP映像升级。导航至WLC GUI > Wireless > FlexConnect Groups >选择FlexConnect Group > Image Upgrade选项卡。



The screenshot shows the 'FlexConnect Groups > 'Store 1'' configuration page with the 'Image Upgrade' tab selected. The 'FlexConnect AP Upgrade' checkbox is highlighted with a red box and is currently unchecked. Below this, the 'FlexConnect Master APs' section has an 'AP Name' dropdown set to 'AP3500' and an 'Add Master' button. At the bottom, there is a table header with columns: 'Master AP Name', 'AP Model', and 'Manual'.

5. 主AP可以手动或自动选择：要手动选择主AP，请导航至WLC GUI > Wireless > FlexConnect Groups >选择FlexConnect Group > Image Upgrade 选项卡> FlexConnect Master AP，从下拉列表中选择AP，然后点击Add Master。

FlexConnect Groups > Edit 'Store 1'

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

FlexConnect AP Upgrade

Slave Maximum Retry Count: 44

Upgrade Image: Backup

FlexConnect Master APs

AP Name: AP3500

Master AP Name	AP Model	Manual
AP3500	c3500I	yes

注意：每个型号只能配置一个AP作为主AP。如果手动配置主AP，则“手动”字段将更新为是。要自动选择主AP，请导航至WLC GUI > Wireless > FlexConnect Groups > 选择FlexConnect Group > Image Upgrade选项卡，然后单击FlexConnect Upgrade。

FlexConnect Groups > Edit 'Store 1'

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

FlexConnect AP Upgrade

Slave Maximum Retry Count: 44

Upgrade Image: Backup

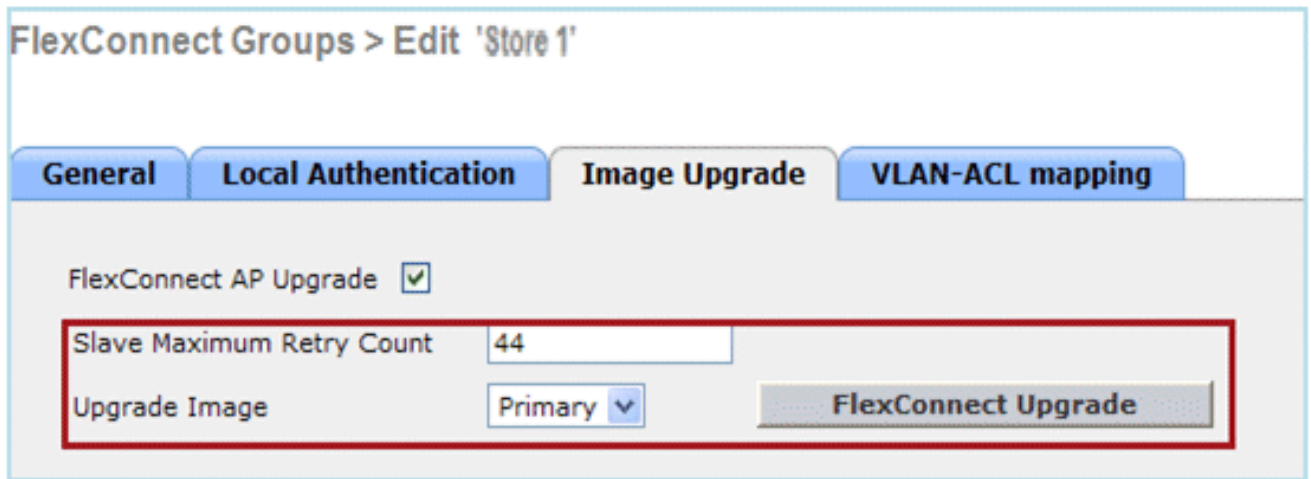
FlexConnect Master APs

AP Name: AP3500-1

Master AP Name	AP Model	Manual
AP3500-1	c3500I	no

注意：如果自动选择主AP，则“手动”字段将更新为否。

6. 要为特定FlexConnect组下的所有AP启动高效的AP映像升级，请单击FlexConnect升级。导航至WLC GUI > Wireless > FlexConnect Groups > 选择FlexConnect组 > Image Upgrade 选项卡，然后单击FlexConnect Upgrade。



注意： Slave Maximum Retry Count是从属AP从主AP下载映像时所尝试的次数（默认为44次），之后，从属AP将回退以从WLC下载映像。它将对WLC进行20次尝试以下载新映像，然后管理员必须重新启动下载过程。

7. 启动FlexConnect升级后，只有主AP将从WLC下载映像。在“所有AP”页面下，“升级角色”将更新为主/中心，这意味着主AP已从位于中心位置的WLC下载映像。从AP将从位于本地站点的主AP下载映像，这是“所有AP”页面“升级角色”下更新为“从/本地”的原因。要验证此情况，请导航至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

8. 下载所有AP映像后，重新启动控制器。AP现在会回退到独立模式，直到控制器重新启动。**注意：**在独立模式下，容错功能将保持客户端关联。控制器恢复后，AP将自动重新启动，并使用预下载的映像。重新启动后，AP重新加入主控制器并恢复客户端服务。

限制

- 主AP选择是按FlexConnect组和每个组中的AP型号进行的。
- 只有3个相同型号的从AP可以同时从其主AP升级，其余从AP将使用随机回退计时器为主AP重试以下载AP映像。
- 如果从AP由于某种原因无法从主AP下载映像，它将转到WLC以获取新映像。
- 这仅适用于CAPWAP AP。

在FlexConnect模式下自动转换AP

Flex 7500提供以下两个选项，以将AP模式转换为FlexConnect:

- 手动模式
- 自动转换模式

手动模式

此模式在所有平台上都可用，并且仅允许对每个AP进行更改。

1. 导航至WLC GUI > Wireless > All APs，然后选择AP。
2. 选择FlexConnect作为AP模式，然后单击Apply。
3. 更改AP模式会导致AP重新启动。

All APs > Details for AP3500

The screenshot shows the configuration page for AP3500 in the WLC GUI. The 'General' tab is selected. The 'AP Mode' dropdown menu is open, and 'FlexConnect' is highlighted. The 'Admin Status' is set to 'Disable'. The 'AP Sub Mode' is set to 'local'. The 'Operational Status' is currently blank. The 'Port Number' and 'Venue Group' fields are also blank.

有当前WLC平台上也可用。

此选项在所

自动转换模式

此模式仅适用于Flex 7500控制器，且仅使用CLI支持。此模式会触发所有已连接AP的更改。在启用此CLI之前，建议将Flex 7500部署在与现有WLC园区控制器不同的移动域中：

```
(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
```

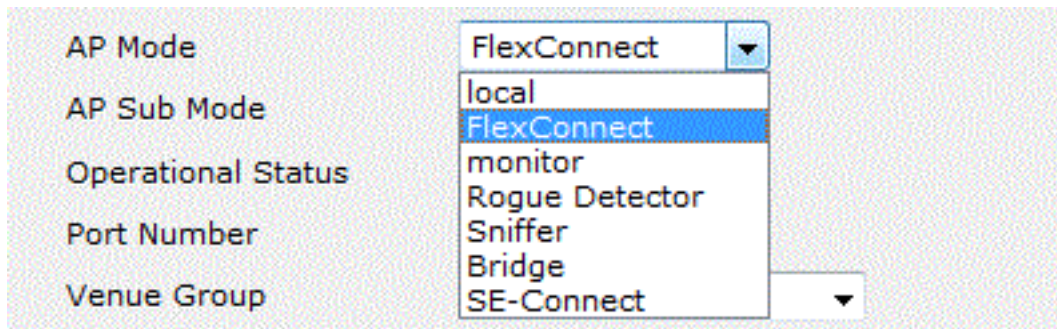
```
(Cisco Controller) >
```

1. 默认情况下，自动转换功能处于禁用状态，可以使用以下show命令验证：

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

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

不支持的AP模式=本地模式、嗅探器、欺诈检测器和网桥。



此选项当前仅通过

CLI可用。这些CLI仅在WLC 7500上可用。

2. 执行**config ap autoconvert flexconnect** CLI将网络中不支持AP模式的所有AP转换为FlexConnect模式。任何已处于FlexConnect或监控模式的AP均不受影响。

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

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

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

```
(Cisco Controller) >
```

3. 执行**config ap autoconvert monitor** CLI将网络中所有AP (不支持的AP模式) 转换为监控模式。任何已处于FlexConnect或监控模式的AP均不受影响。

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

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

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

没有选项可同时执行**config ap autoconvert flexconnect**和**config ap autoconvert monitor**。

[FlexConnect WGB/uWGB支持本地交换WLAN](#)

从7.3版开始，支持WGB/uWGB和WGB后的有线/无线客户端，并将作为配置用于本地交换的WLAN上的普通客户端工作。

关联后，WGB会为其每个有线/无线客户端发送IAPP消息，Flex AP的行为如下：

- 当Flex AP处于连接模式时，它会将所有IAPP消息转发到控制器，控制器将处理与本地模式AP相同的IAPP消息。有线/无线客户端的流量将从Flex AP本地交换。
- 当AP处于独立模式时，它会处理IAPP消息，WGB上的有线/无线客户端必须能够注册和取消注册。转换到连接模式后，Flex AP会将有线客户端的信息发回控制器。当Flex AP从独立模式转换到连接模式时，WGB将发送三次注册消息。

有线/无线客户端将继承WGB的配置，这意味着WGB后的客户端无需单独的配置，如AAA身份验证、AAA覆盖和FlexConnect ACL。



摘要

- WLC上无需特殊配置即可支持Flex AP上的WGB。
- WGB和WGB后面的客户端支持容错。
- IOS AP支持WGB:1240、1130、1140、1260 和 1250。

步骤

请完成以下步骤：

1. 无需特殊配置，即可在FlexConnect AP上为配置为WGB的本地交换配置的WLAN启用WGB/uWGB支持。此外，WGB后面的客户端被Flex AP视为本地交换配置的WLAN上的普通客户端。在WLAN上启用FlexConnect本地交换。

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

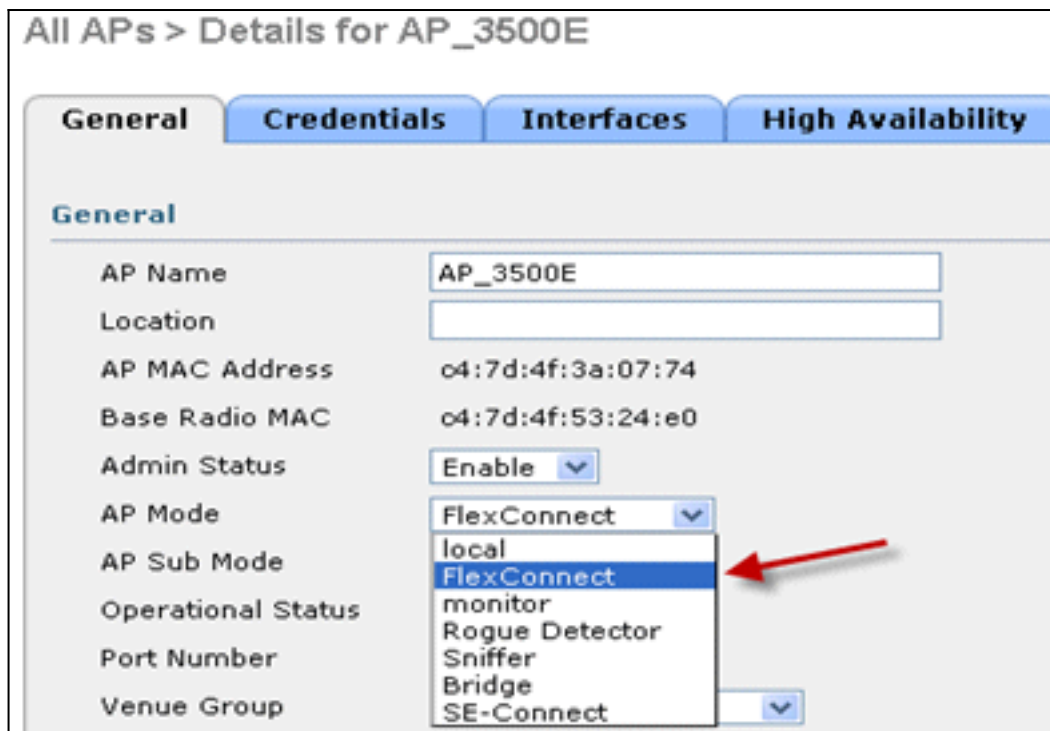
Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration Enabled

FlexConnect

FlexConnect Local Switching Enabled

2. 将AP模式设置为FlexConnect。



3. 将WGB与此配置的WLAN后面的有线客户端关联。

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. 要检查WGB的详细信息，请转至Monitor > Clients，然后从客户端列表中选择WGB。

Clients > Detail

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
		WLAN Profile	'Store 1'
		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

Client Type: WGB

Number of Wired Client(s): 2

5. 要检查WGB后的有线/无线客户端的详细信息，请转到Monitor > Clients，然后选择客户端。

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后面的有线客户端始终与WGN本身位于同一VLAN中。在为本地交换配置的WLAN的Flex AP上，不支持对WGB后面的客户端提供多个VLAN支持。
- 当与为本地交换配置的WLAN上的Flex AP关联时，WGB后最多支持20个客户端（有线/无线）。此数字与我们目前在本地模式AP上支持WGB的数字相同。
- 在为本地交换配置的WLAN上关联的WGB后面的客户端不支持网络身份验证。

支持更多的Radius服务器

在版本7.4之前，FlexConnect组中的RADIUS服务器配置是从控制器上的RADIUS服务器全局列表完成的。此全局列表中可配置的RADIUS服务器最大数量为17。随着分支机构数量的增加，每个分支机构必须能够配置RADIUS服务器。在版本7.4以后，可以按FlexConnect组配置主RADIUS服务器和备份RADIUS服务器，这些服务器可能或不是控制器上配置的17个RADIUS身份验证服务器的全局列表的一部分。

还支持RADIUS服务器的AP特定配置。AP特定配置的优先级将高于FlexConnect组配置。

FlexConnect组中的现有配置命令（需要控制器上全局RADIUS服务器列表中RADIUS服务器的索引）将被弃用并替换为配置命令，该配置命令使用服务器的IP地址和共享密钥在Flexconnect组中配置RADIUS服务器。

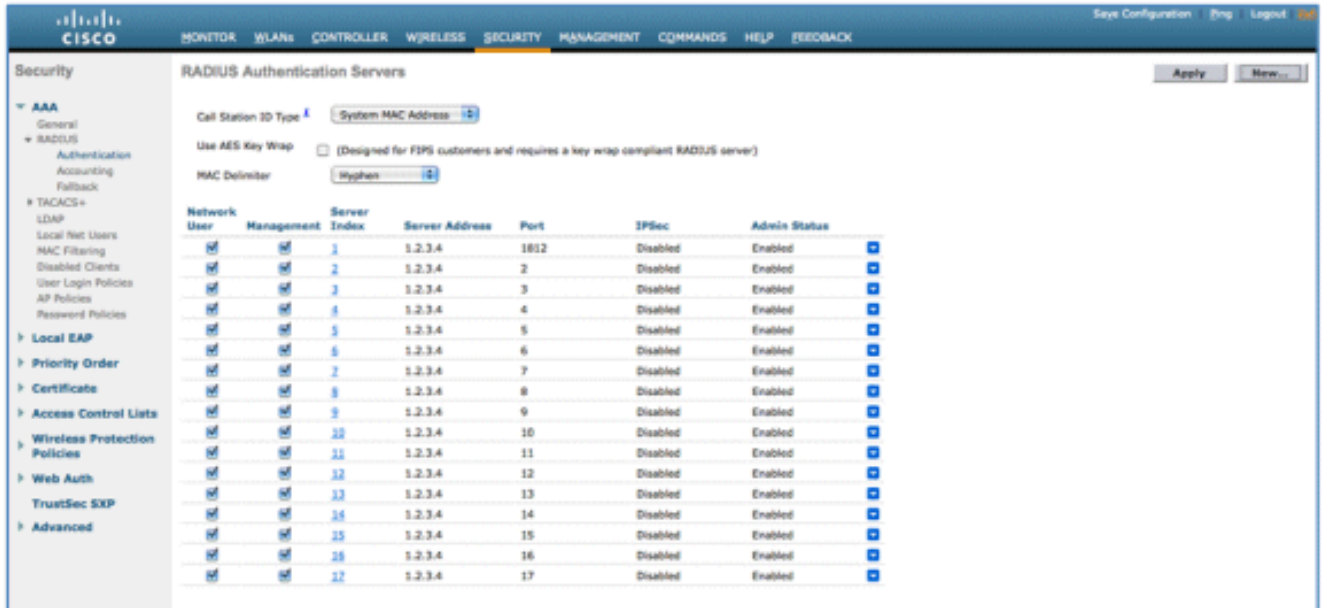
摘要

- 支持按FlexConnect组配置主RADIUS服务器和备份RADIUS服务器，该服务器可能存在或不存在于RADIUS身份验证服务器的全局列表中。
- 可添加到WLC上的唯一RADIUS服务器的最大数量是可在给定平台上配置的FlexConnect组数量乘以2。例如，每个FlexConnect组有一个主RADIUS服务器和一个辅助RADIUS服务器。
- 从以前版本到7.4版的软件升级不会导致任何RADIUS配置丢失。
- 允许删除主RADIUS服务器，而无需删除辅助RADIUS服务器。这与RADIUS服务器的当前

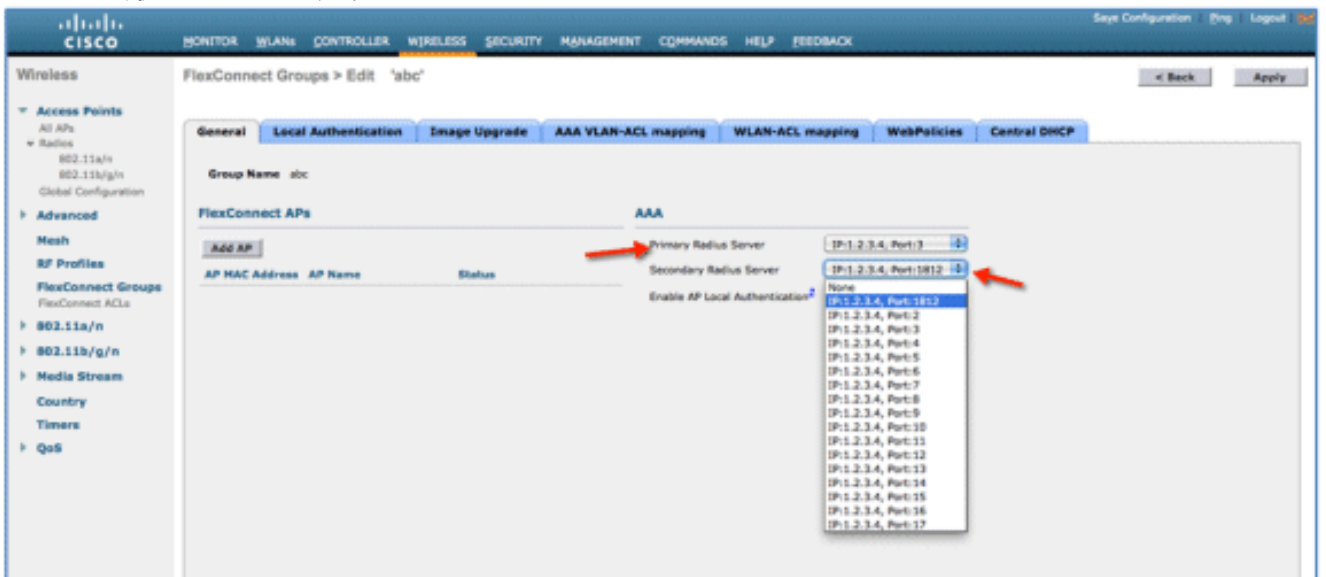
FlexConnect组配置一致。

步骤

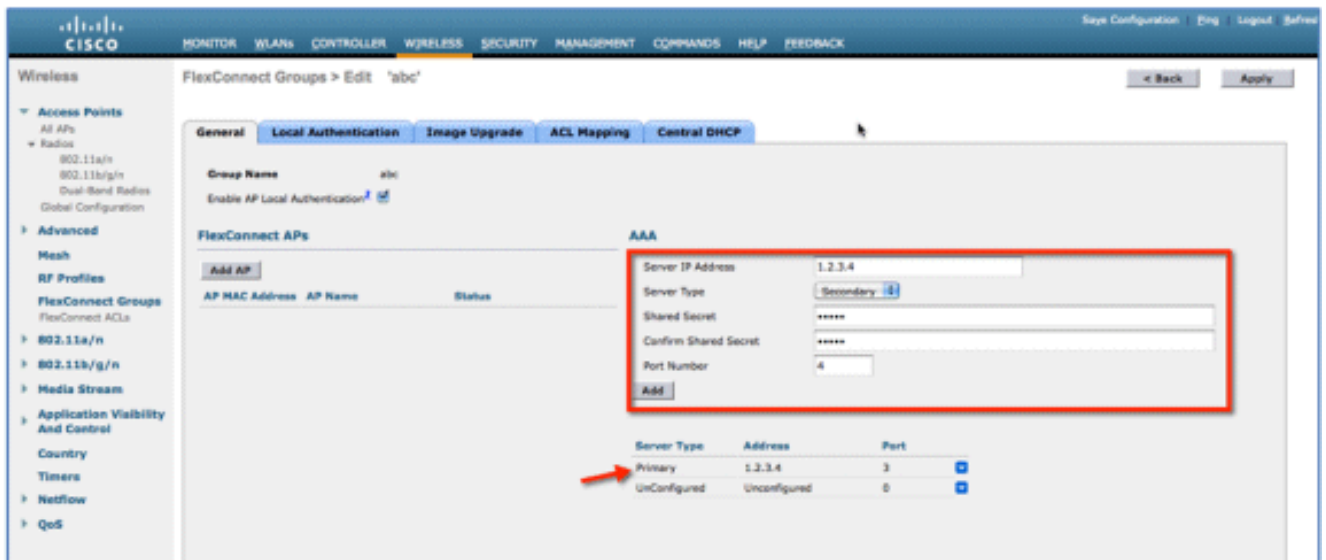
1. 版本7.4之前的配置模式。在AAA身份验证配置下最多可配置17个RADIUS服务器。



2. 主RADIUS服务器和辅助RADIUS服务器可以使用包含在AAA Authentication页面上配置的RADIUS服务器的下拉列表与FlexConnect组关联。



3. 版本7.4中FlexConnect组的配置模式。主RADIUS服务器和辅助RADIUS服务器可以使用IP地址、端口号和共享密钥在FlexConnect组下配置。



限制

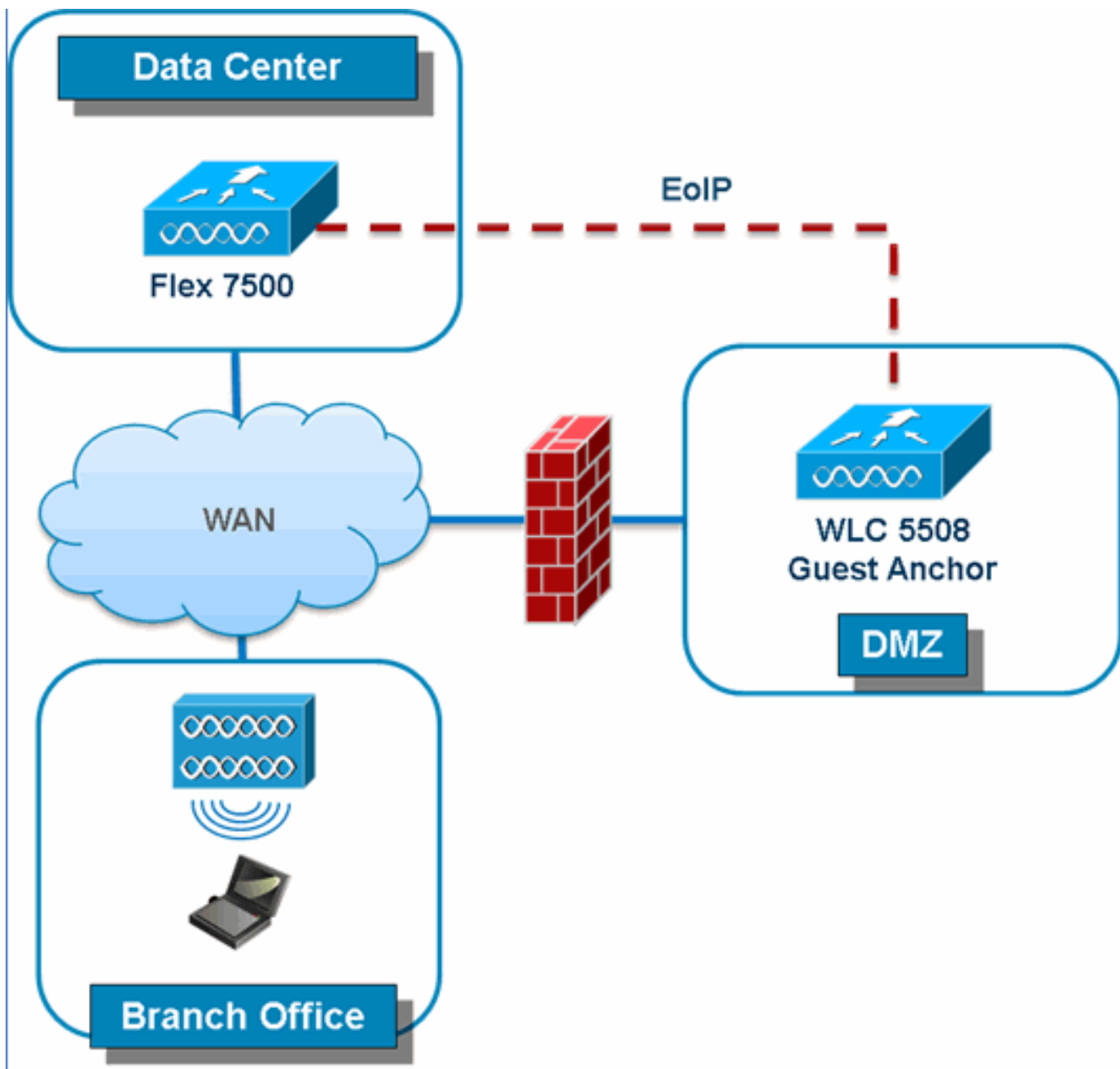
- 软件从7.4版降级到以前版本将保留配置，但有一些限制。
- 在配置上一个RADIUS服务器时配置主/辅助RADIUS服务器将导致旧条目被新条目替换。

增强的本地模式(ELM)

FlexConnect解决方案支持ELM。有关详细信息，请参阅ELM的最佳实践指南。

Flex 7500中的访客接入支持

图 13 : Flex 7500中的访客接入支持



Flex 7500将允许并继续支持创建到DMZ中的访客锚点控制器的EoIP隧道。有关无线访客接入解决方案的最佳实践，请参阅《访客部署指南》。

[从NCS管理WLC 7500](#)

从NCS管理WLC 7500与思科现有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
172.20.227.177	5508-Primary	5500		7.0.112.52	mobility	Reachable	Identical

有关管理WLC和发现模板的详细信息，请参阅[《思科无线控制系统配置指南7.0.172.0版》](#)。

常见问题

问： 如果我将远程位置的LAP配置为FlexConnect，我能否为这些LAP提供主控制器和辅助控制器？

示例： 站点A有主控制器，站点B有辅助控制器。如果站点A的控制器发生故障，LAP将故障切换到站点B的控制器。如果两个控制器都不可用，LAP是否会进入FlexConnect独立模式？

是的。 首先，LAP 可以故障切换到其辅助控制器。所有本地交换的 WLAN 没有变化，所有中央交换的 WLAN 的数据流将转到新控制器。如果辅助控制器发生故障，标记进行本地交换的所有 WLAN（和开放/预共享密钥身份验证/您正在执行 AP 身份验证程序）将保持运行。

问： 在本地模式下配置的接入点如何处理配置了FlexConnect本地交换的WLAN？

A.本地模式接入点将这些WLAN视为普通WLAN。身份验证和数据流通过隧道传回 WLC。在 WAN 链路故障期间，此 WLAN 将完全关闭，并且此 WLAN 上的所有客户端均处于非活动状态，直到与 WLC 的连接恢复。

问：我能否在本地交换模式下执行 Web 身份验证？

答：是，您可以启用Web身份验证的SSID，并在Web身份验证后在本地丢弃流量。本地交换模式下可以顺利进行 Web 身份验证。

问：能否在控制器上为SSID使用我的访客门户，该SSID由H REAP本地处理？如果可以，则与控制器的连接丢失时会发生什么情况？当前的客户端是否立即断开连接？

是的。由于此 WLAN 是在本地交换的，WLAN 可用，但由于网页不可用，新客户端无法进行身份验证。但现有客户端不会断开。

问：FlexConnect能否认证PCI合规性？

是的。FlexConnect解决方案支持欺诈检测以满足PCI合规性。

相关信息

- [HREAP设计和部署指南](#)
- [Cisco 4400 系列无线局域网控制器](#)
- [Cisco 2000 系列无线局域网控制器](#)
- [Cisco 无线控制系统](#)
- [思科3300系列移动服务引擎](#)
- [Cisco Aironet 3500 系列](#)
- [思科安全访问控制系统](#)
- [技术支持和文档 - Cisco Systems](#)